CNIPA
Centro Nazionale per l'Informatica
nella Pubblica Amministrazione
via Isonzo, 21/b - 00198 Roma
tel. 06 85264.1
www.cnipa.gov.it

23 i Quaderni Linee guida per la sicurezza ICT delle pubbliche amministrazioni – Piano Nazionale - Modello organizzativo

numero 23 - marzo 2006

CNIPA
Centro Nazionale per l'Informatica
nella Pubblica Amministrazione

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

23

marzo 2006

i Quaderni

sommario

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

Linee guida per la sicurezza ICT delle pubbliche amministrazioni

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 da 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	*Certification Authority*
CERT SPC	*Computer Emergency Response Team SPC*
CGSPC	Centro di Gestione SPC
CPS	*Certificate Practice Statement*
DoS	*Denial of Service*
IPSec	*Internet Protocol Security*
ISCOM	Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione
ISP	*Internet Service Provider*
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	*Public Key Infrastructure*
PNS	Piano Nazionale per la Sicurezza
Q-CN	*Community Network* qualificata SPC
Q-ISP	ISP qualificato SPC
QXN	*Qualified eXchange Network* dedicato alla PA
RA	*Registration Authority*
RUPA	Rete Unitaria della pubblica amministrazione
SCSPC	Struttura di Controllo SPC
SPC	Sistema Pubblico di Connettività
VPN	*Virtual Private Network*
TCL	*Trusted Certificate List*

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 sopraccitati 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 temini 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**)[1]. Inoltre, per evitare il proliferare dei sistemi proprietari di gestione dell'identità, si pro-

[1] 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 stimano 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. [2]
- il documento dal titolo "L'E-GOVERNMENT PER UN FEDERALISMO EFFICIENTE - UNA VISIONE CONDIVISA, UNA REALIZZAZIONE COOPERATIVA"[3], 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

[2] Il documento può essere trovato al seguante indirizzo :
http://www.innovazione.gov.it/ita/intervento/normativa/allegati/proposte_sicurezza_marzo04.pdf

[3] Il documento può essere trovato al seguante indirizzo :
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 efficiente 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[4]. 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[5].
Nel caso dei servizi di e-government la fiducia degli utenti è un elemento fondamentale che può favorirne o bloccarne lo sviluppo.

[4] Linee guida del Governo per lo sviluppo della Società dell'Informazione nella legislatura – Ministro per l'innovazione e le tecnologie

[5] 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[6], 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[7]. 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-

[6] 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.)

[7] Per calcolare tale valore si è considerato il PIL relativo al 2003 (dato ISTAT) e lo si è rapportato al periodo di disservizio ipotizzato.

titività, 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 [8] 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 le 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.

[8] 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[9], 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)[10] nonché ai problemi originati all'interno delle organizzazioni[11].
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 acquisendo 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-

9 Si cita, ad esempio, il Computer Crime and Security Survay del CSI/FBI

10 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

11 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 esplicare 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 favorirne 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 dì 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 fur Sicherheit in der Informationstechnik) tedesco, il "Secrétrariat 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 Direttrici 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[12].
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).

[12] 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[13], 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.

[13] 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 gia 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[14].
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).

[14] 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[15], 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

[15] 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[16].
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[17].
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

[16] 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)

[17] Ciò è vero soprattutto per i prodotti che usano il metodo quantitativo che considera, tra i fattoti 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 applicazione 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 oramai 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[18].
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.

[18] 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" [19].
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.

Analoga 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.

[19] 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 é 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.[20]

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.[21] 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[22] (servizi di trasporto, di comunicazione, di erogazione dell'energia elettrica,

[20] 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.

[21] 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.

[22] 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 adegua-

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[23] 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;

[23] 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[24], 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

[24] 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 attuale 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 rinviamo ai paragrafi successivi[25] 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

[25] 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..

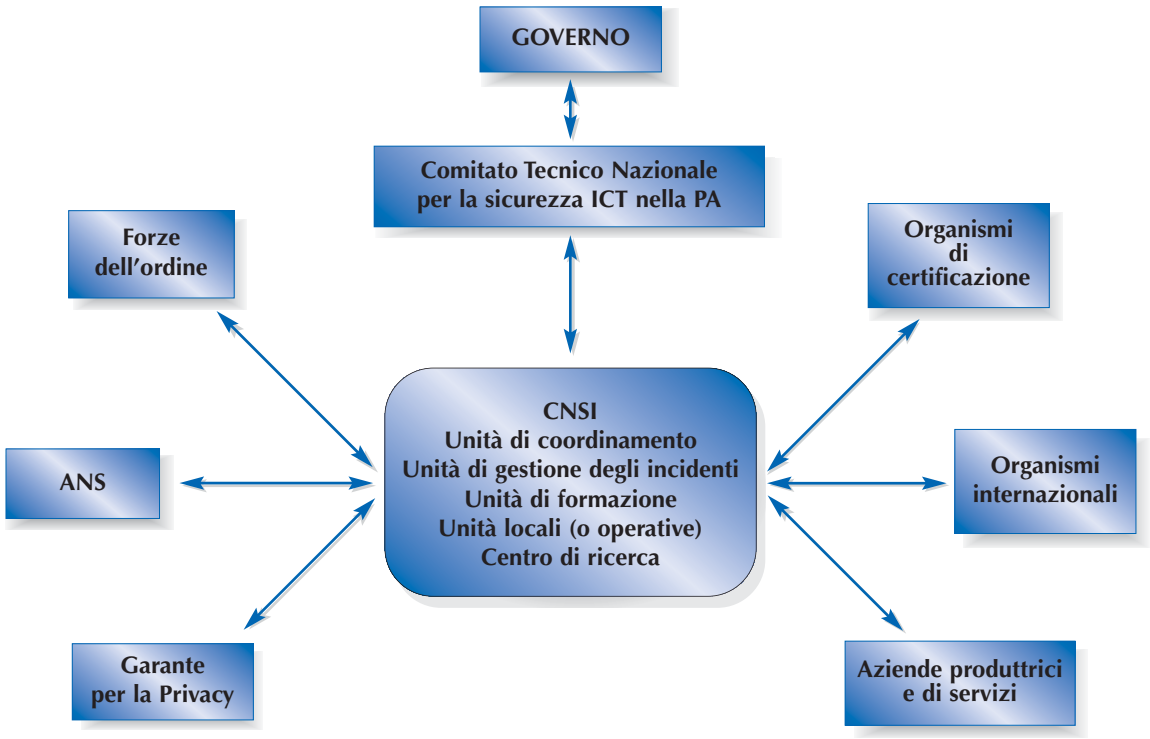

Figura 1 - Schema delle interrelazioni del CNSI

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 stimano 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 volta 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*)[26] 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[27].

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.

[26] La terminologia utilizzata per le attività di gestione della sicurezza è spesso disomogenea è 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

[27] 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[28].

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).

[28] 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[29] 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.

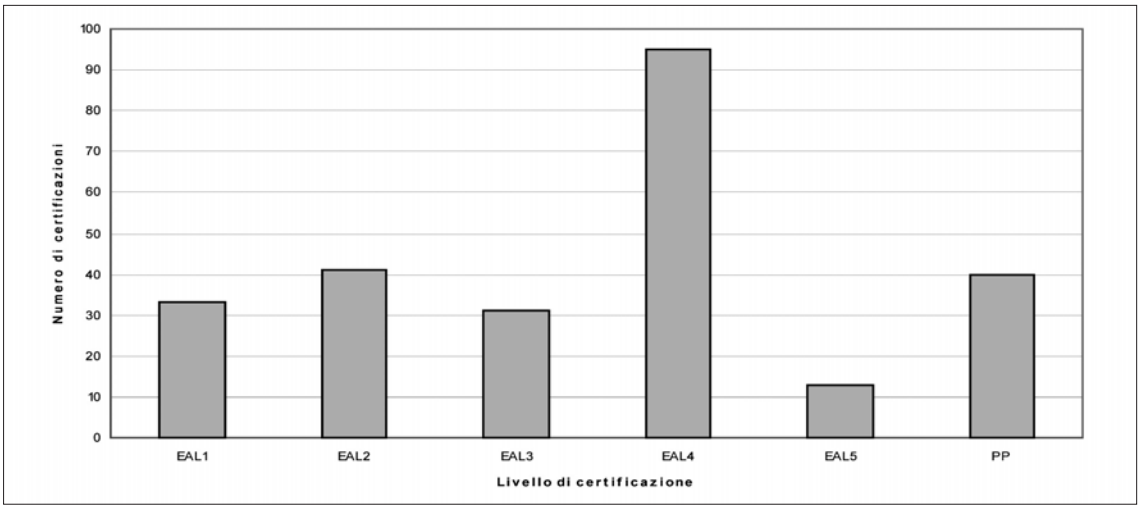

Figura 2 - Ripartizione per livelli di assurance delle certificazioni CC attualmente pubblicate sul sito www.commoncriteriaportal.org

[29] 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.

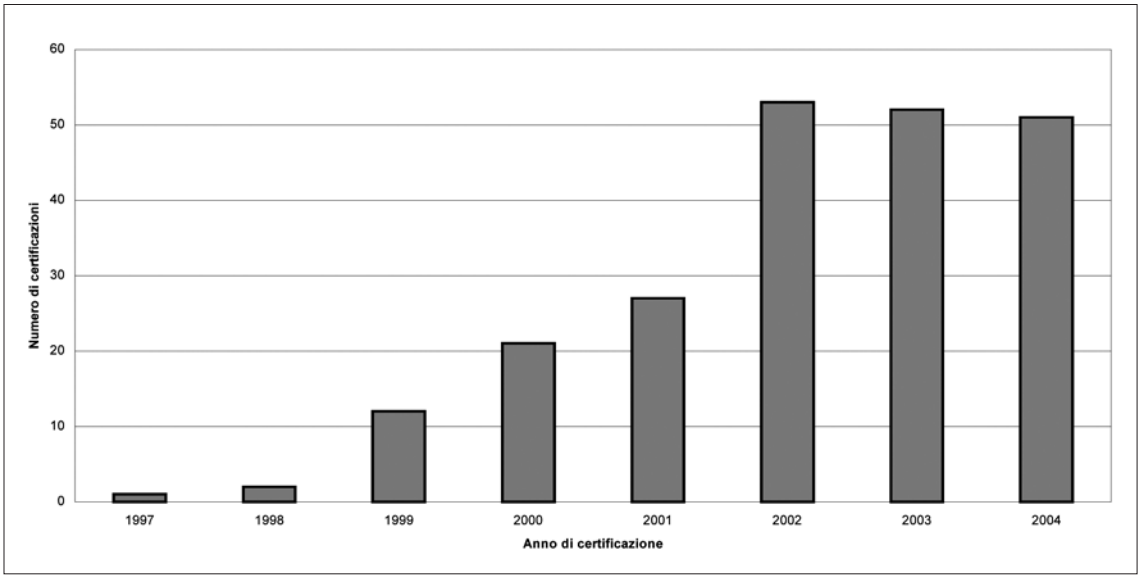

Figura 3 - Andamento del numero di certificazioni per anno (dati ricavati dal sito www.commoncriteriaportal.org)

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[30] 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-

[30] 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 Accreditamento – 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[31], 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 "deragliamento" 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[32].
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[33]. 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).

[31] I motivi possono essere errori, malversazioni, eventi accidentali, azioni dimostrative, eccetera...

[32] 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.

[33] 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 predeterminato 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[34]. 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.

[34] 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[35];
- 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[36].
Nel seguito vengono fornite alcune indicazioni su come sia opportuno indicare in un contratto gli eventuali requisiti di sicurezza.

[35] Eventualmente, come si vedrà in seguito, per ciascun evento è possibile indicare la 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.

[36] 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.)[37]. Il prodotto in ogni caso non dovrebbe presentare vulnerabilità diverse da quelle intrinseche o implicitamente ammesse nelle specifiche[38].
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[39]. 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.

[37] 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.

[38] 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.

[39] 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[40] 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[41].

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.

[40] 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.

[41] 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[42];
- il fornitore dovrà predisporre un sistema di recovery che dovrà consentire il recupero delle informazioni memorizzate anche nel caso di disastri o altri eventi imprevisti 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.

[42] 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[43].
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 back-up inoltre, al fine di garantire la leggibilità dei dati nel tempo, dovranno essere effettuati riversamenti su nuovi supporti perlomeno ogni cinque anni;

[43] 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[44].
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.

[44] 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[45].
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 cauteli 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.

[45] 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[46].
Si riporta di seguito un elenco non esaustivo di clausole che può essere opportuno inserire nei contratti di *ousourcing*:

- 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[47];
- 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

[46] 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.

[47] 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[48].
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[49].
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 sicurez-

[48] 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).

[49] 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[50]. 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.

[50] 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 imprevisti 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)[51], 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.

[51] 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*) [52].
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*

[52] 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 considerazioni 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, confluendo 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.

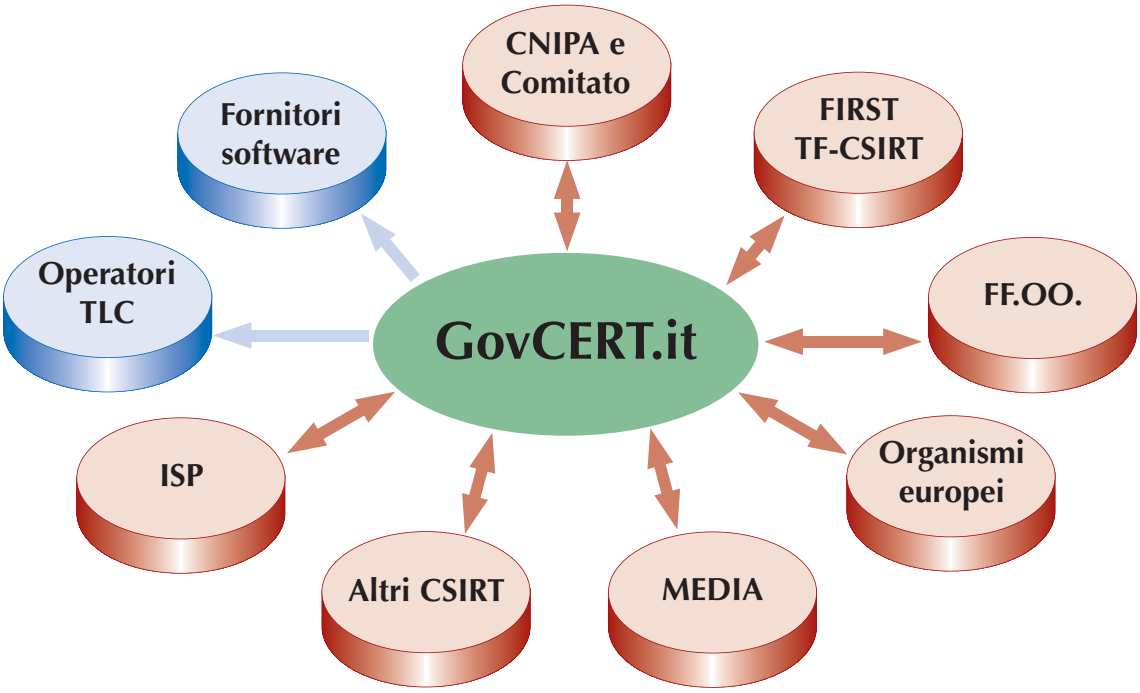

Figura 1 – Relazioni interne/esterne GovCERT.it

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[1] 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

[1] 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.

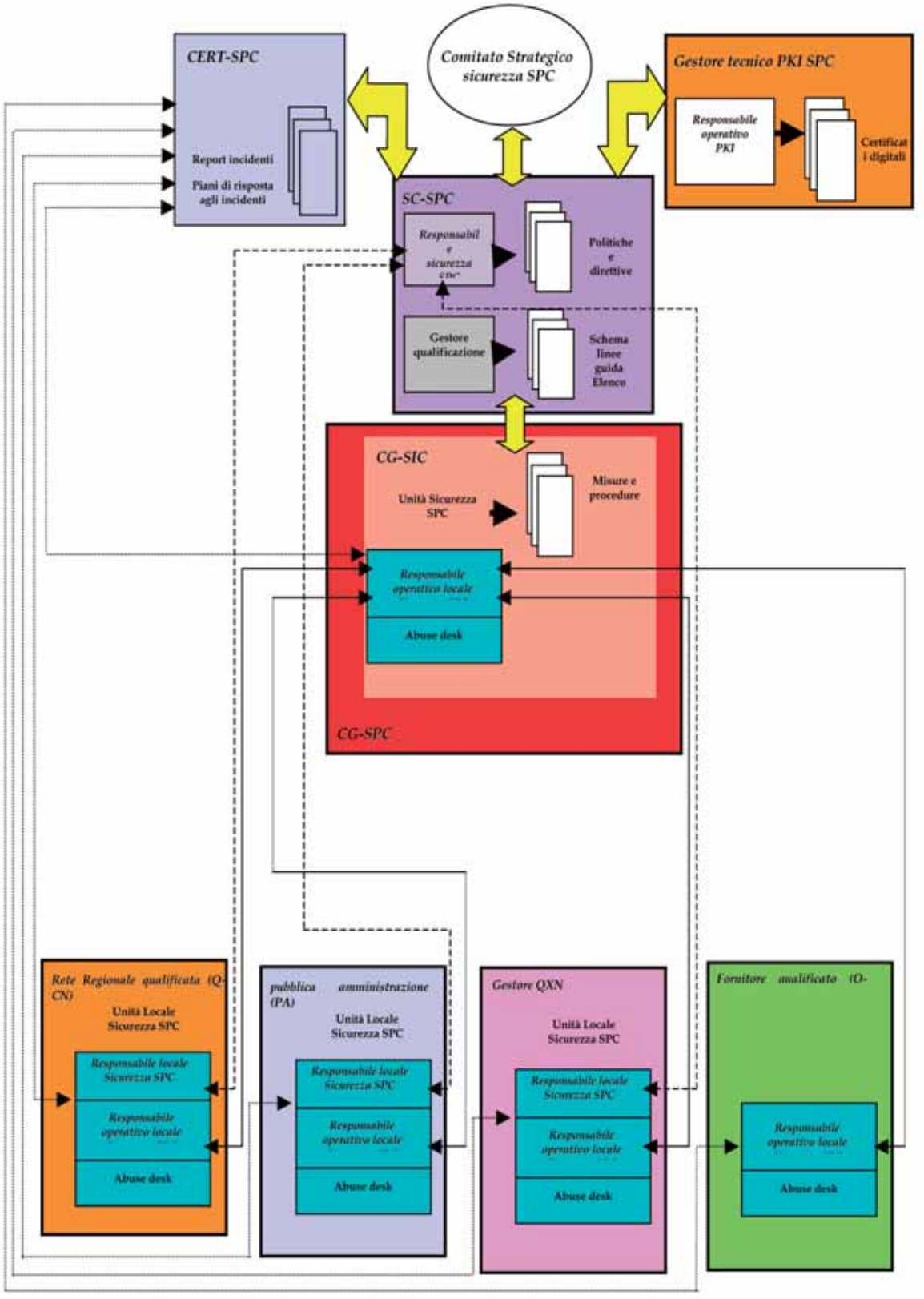

Figura 2 – Struttura dedicata alla sicurezza del SPC

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)[2] 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;

[2] 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)

- 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 Domino 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 sopraccitata 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 committenza 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 cauteli 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[3] 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-

[3] 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 userid 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.

Allorchè 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.

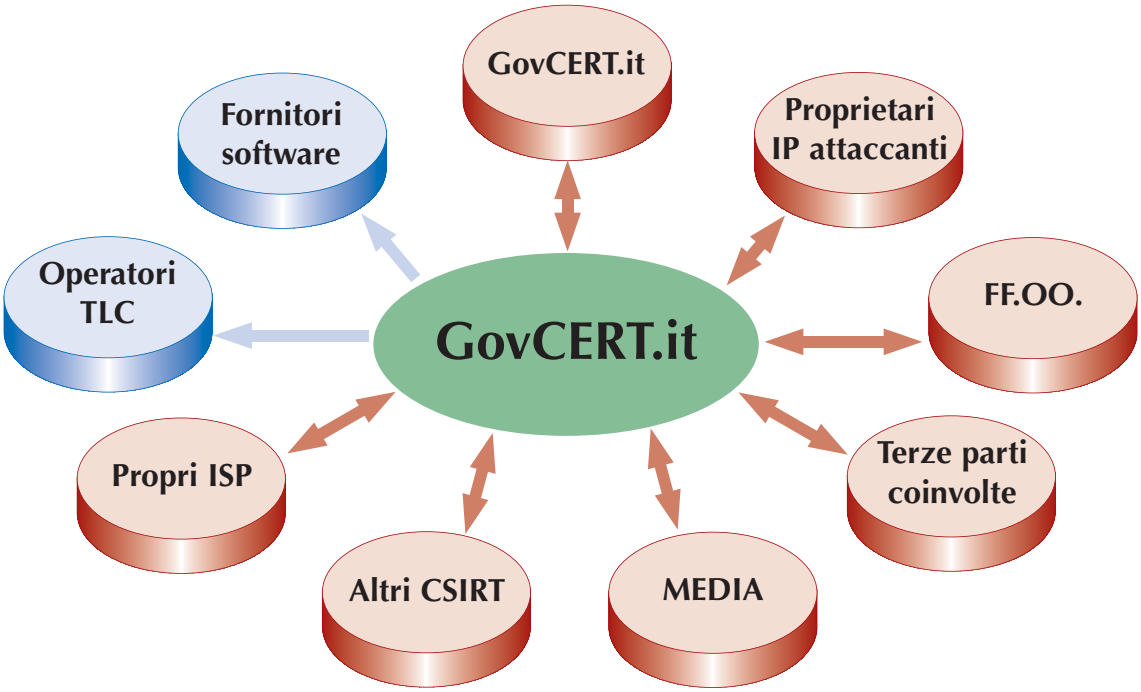

Figura 3 – Relazioni esterne CERT-AM

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[4].
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.

[4] 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'allocazione 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 princìpi 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.

L'Organismo di Certificazione riferisce semestralmente sull'attività al Dipartimento per l'Innovazione e le Tecnologie (DIT) della Presidenza del Consiglio dei Ministri.

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"[5].
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.

[5] Si riporta la definizione fornita da PriceWaterhouseeCooper: "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 funcion involved in this process include adding, updating, and deleting user information and permissions for a company's system, application, and data stores." (fonte PriceWaterhouseeCooper – 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[6].
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.

[6] 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.

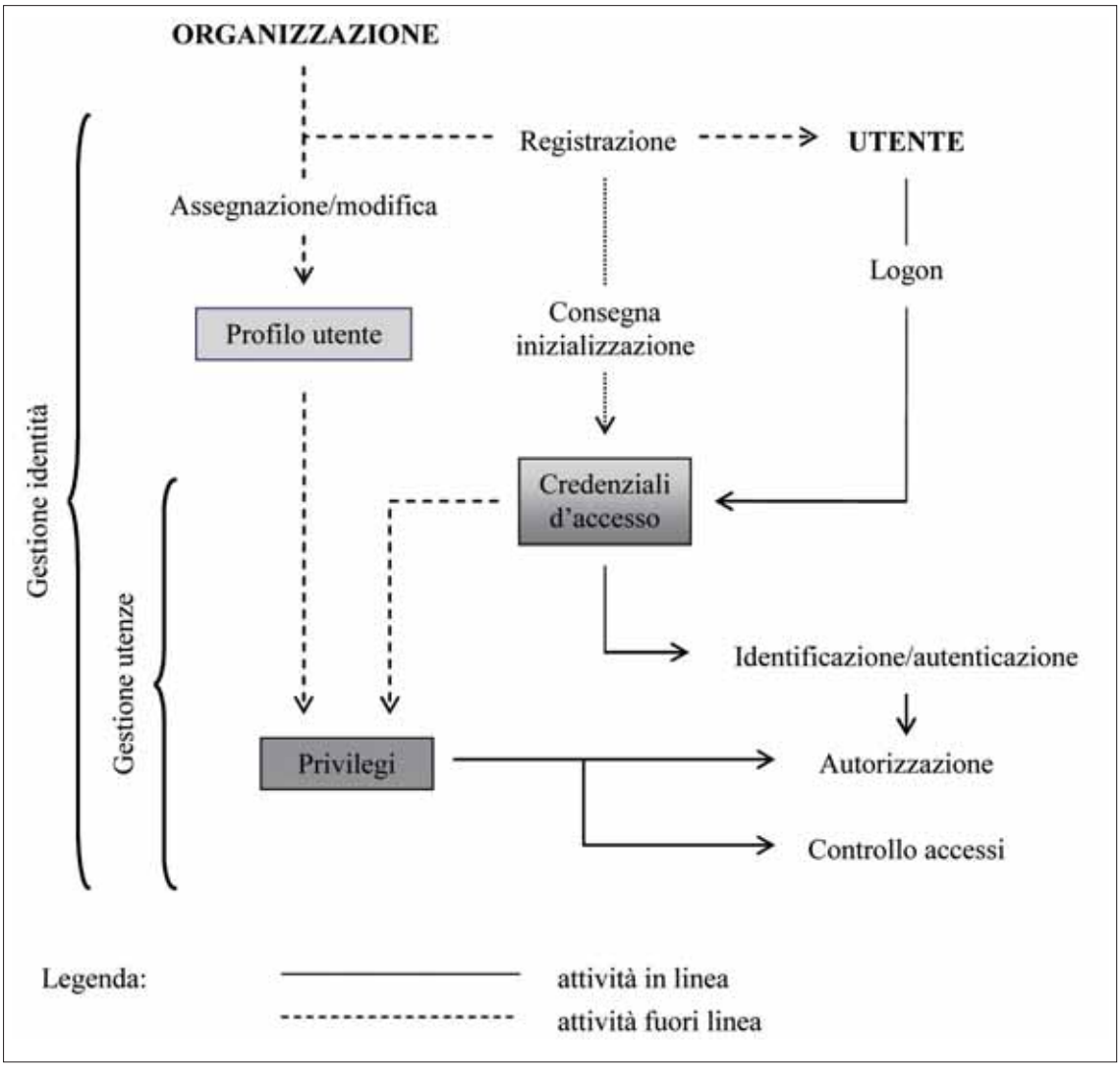

Figura 4 – Schema di riferimento per la gestione dell'identità

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*[7].
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 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.

[7] 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[8].
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.

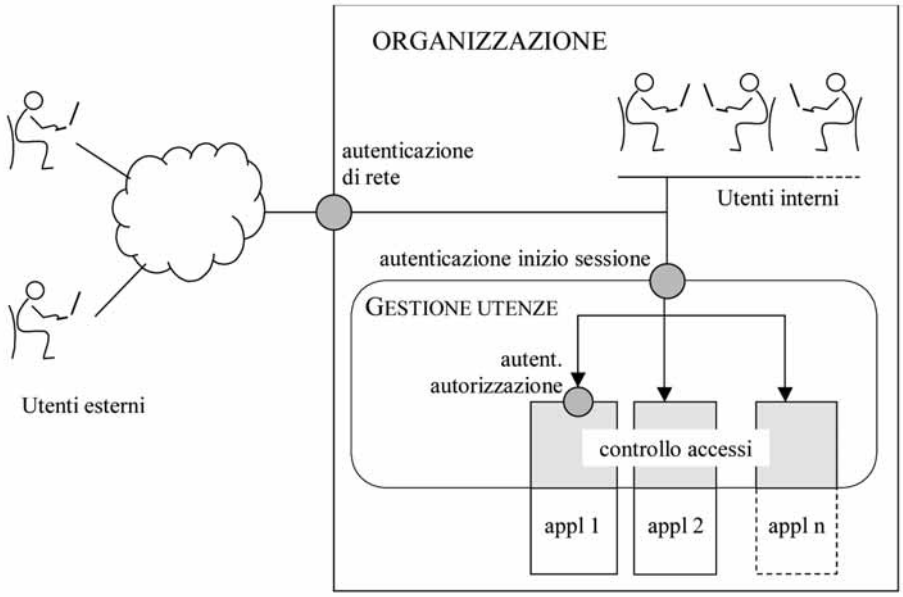

Figura 5 – Schema semplificato di gestione delle utenze in un'organizzazione

[8] 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[9].
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[10];
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[11].
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[12].
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

[9] 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.

[10] 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.

[11] Nel modello di funzionamento del Sistema Pubblico di Connettività, questa funzione è svolta dalla porta di rete e dalla porta applicativa.

[12] 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[13]. 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.

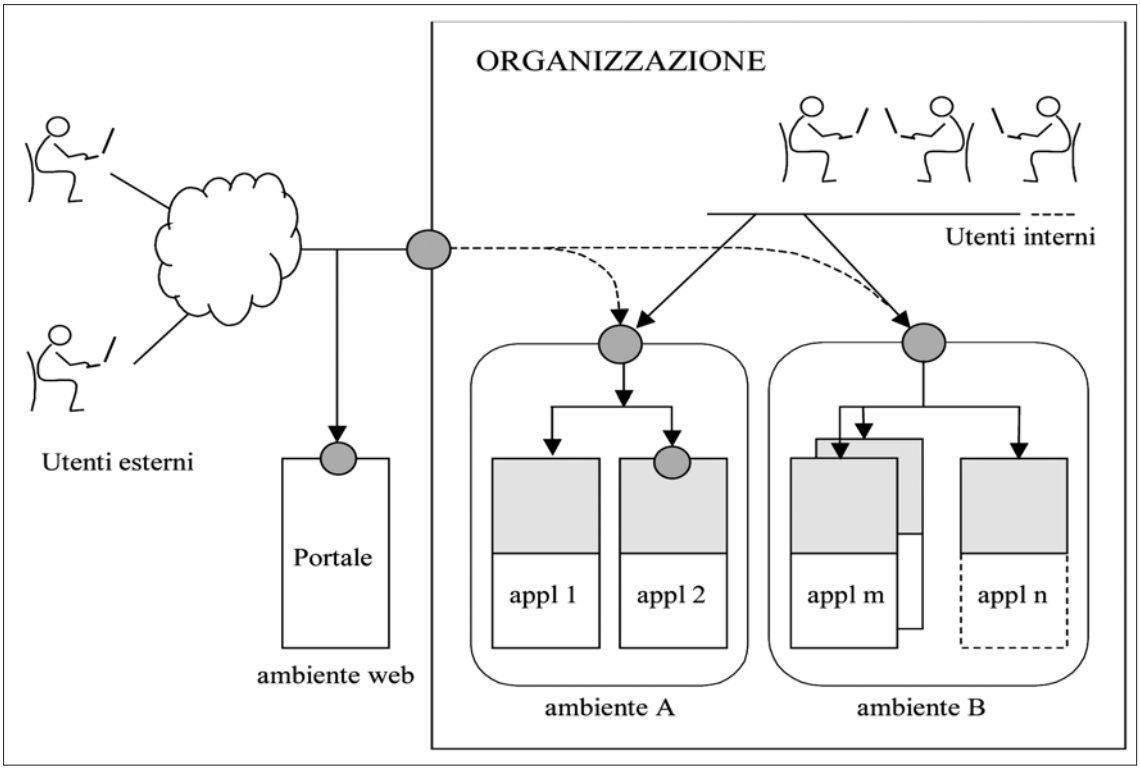

Figura 6 – Schema di gestione delle utenze in un'organizzazione con più ambienti elaborativi

[13] 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[14].
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[15].
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 de prevalere dell'una o dell'altra esigenza, l'identificativo può essere scelto con logiche diverse, come riportato in Figura 7.

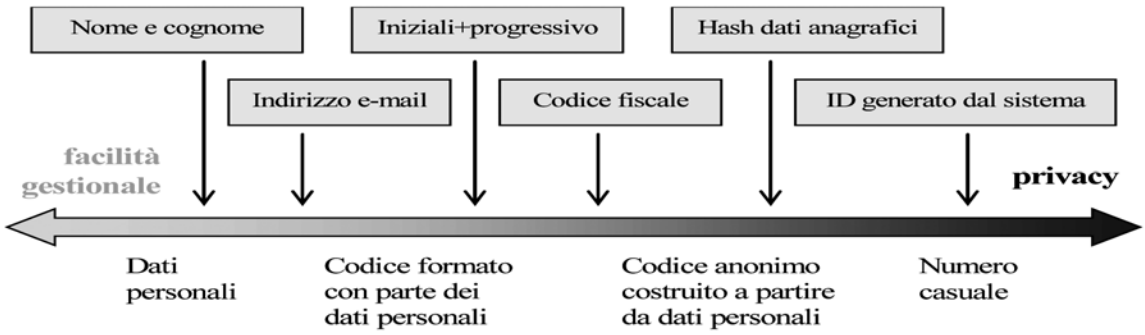

Figura 7 – Criteri per la formazione dell'identificativo utente (userid)

[14] 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.

[15] 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 stimolate 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 dì 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
SISTEMA DI GESTIONE DELLE MISURE	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).
UNITÀ DI MISURA	Frequenza
DATI ELEMENTARI DA RILEVARE	• data e ora di presa in carico dell'evento • data e ora di avvio dell'escalation
PERIODO DI RIFERIMENTO	XX mesi
FREQUENZA ESECUZIONE MISURE	YY volte l'anno
REGOLE DI CAMPIONAMENTO	Si considerano tutti gli eventi relativi al periodo di osservazione, all'interno della finestra temporale definita per l'erogazione del servizio.

(segue)

FORMULA DI CALCOLO	Dati necessari: • data e ora di presa in carico dell'evento (*Ti*), al minuto • data e ora di avvio dell'escalation (*Te*), al minuto Il ritardo di avvio dell'escalation viene così calcolato: $TES=Te-Ti$ Si calcola la frequenza dei ritardi inferiori al valore normale $FN_{TES} = \frac{N\text{ritardi(durata} \leq \text{valore normale)}}{N\text{eventi}} \times 100$ e la frequenza dei ritardi inferiori al valore limite $FL_{TES} = \frac{N\text{ritardi(durata} \leq \text{valore limite)}}{N\text{eventi}} \times 100$
REGOLE DI ARROTONDAMENTO	• la durata dei ritardi va arrotondata al minuto • la frequenza va arrotondata al punto percentuale sulla base del primo decimale • al punto % per difetto se la parte decimale è ≤ 0,5 • al punto % per eccesso se la parte decimale è > 0,5
OBIETTIVI (VALORI SOGLIA)	Obiettivi • TES ≤ valore normale con FN_{TES} ≥ frequenza normale • TES ≤ valore limite con FL_{TES} = frequenza limite Valori soglia • valore normale = 20 minuti per attività critiche • valore normale = 45 minuti per attività non critiche • valore limite = 4 ore per attività critiche • valore limite = 8 ore per attività non critiche • frequenza normale = 90% per attività di monitoraggio critiche • frequenza limite = 100% per attività di monitoraggio critiche
AZIONI CONTRATTUALI	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. 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.
ECCEZIONI	L'applicazione delle regole contrattuali inizia dopo un periodo di osservazione dall'avvio del servizio della durata di ZZ mesi.

Tabella 4 - TRE

INDICATORE/MISURA	**TEMPESTIVITÀ DI RISOLUZIONE DELL'EMERGENZA (TRE)**
SISTEMA DI GESTIONE DELLE MISURE	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. 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.
UNITÀ DI MISURA	Percentuale

(segue)

DATI ELEMENTARI DA RILEVARE	• data e ora di presa in carico dell'emergenza • data e ora di richiesta eventuale autorizzazione • data e ora di arrivo dell'eventuale autorizzazione • data e ora di chiusura intervento (risoluzione dell'emergenza)
PERIODO DI RIFERIMENTO	XX mesi
FREQUENZA ESECUZIONE MISURE	YY volte l'anno
REGOLE DI CAMPIONAMENTO	Si considerano tutti gli eventi relativi al periodo di osservazione, all'interno della finestra temporale definita per l'erogazione del servizio.
FORMULA DI CALCOLO	Dati necessari: • data e ora di presa in carico dell'emergenza (*Tie*) • data e ora di richiesta eventuale autorizzazione (*Tra*) • data e ora di arrivo dell'eventuale autorizzazione (*Taa*) • data e ora di chiusura intervento (risoluzione dell'emergenza) (*Tee*) Il tempo di risoluzione dell'emergenza viene così calcolato: $TRE = (Tee–Tie)–(Taa–Trs)$ Si calcola quindi la frequenza dei tempi inferiori al valore normale $FN_{TRE} = \frac{N\text{tempi(durata} \leq \text{valore normale)}}{N\text{eventi}} \times 100$ e la frequenza dei tempi inferiori al valore limite $FL_{TRE} = \frac{N\text{ritardi(durata} \leq \text{valore limite)}}{N\text{eventi}} \times 100$

REGOLE DI ARROTONDAMENTO	• la durata dei ritardi va arrotondata al minuto
	• la frequenza va arrotondata al punto percentuale sulla base del primo decimale
	  • al punto % per difetto se la parte decimale è ≤ 0, 5
	  • al punto % per eccesso se la parte decimale è > 0, 5

OBIETTIVI (VALORI SOGLIA)	Obiettivi • TRE ≤ valore normale con FN_{TRE} ≥ frequenza normale • TRE ≤ valore limite con FL_{TRE} = frequenza limite Valori soglia • valore normale = 8 ore • valore limite = 48 ore • frequenza normale = 90% • frequenza limite = 100%
AZIONI CONTRATTUALI	• 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. • 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.
ECCEZIONI	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'obbiettivo 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[16]) 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.

[16] 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[17].
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.

[17] 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 il 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[18] 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;

[18] 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[19]) 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[20] 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).

[19] Con tale termine si intende la "fotografia" dei dati che si ottiene con l'operazione di backup.

[20] 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 in formazioni 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 – Princìpi e modalità per la realizzazione della Rete Unitaria della PA.

Dir. P.C.M. 20 novembre 1997 – Princìpi 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 Analsysis.

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 istituto 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.

Decifratura
Tecnica usata per ricostruire i dati originali, precedentemente cifrati, in modo da renderli comprensibili. La decifratura 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
Potenziale 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.

OCSP (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 logon.

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'lEEE 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 (riconducendoli a un formato comune, anche se provenienti dai diversi strumenti) e correlarli 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 Worid 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 corrispondente 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 **Protocollo informatico e gestione dei flussi documentali nella PA**
Stato di attuazione
MARZO 2006

N. 21 **Manuale di gestione del protocollo informatico, dei documenti e dell'archivio delle PA** - ***modello di riferimento***
FEBBRAIO 2006

N. 20 **Rapporto 2005 –** ***Commissione interministeriale ICT disabili***
GENNAIO 2006

N. 19 **Voice over IP nella Pubblica Amministrazione italiana**
NOVEMBRE 2005

N. 18 **3rd workshop on legislative XML**
NOVEMBRE 2005

N. 17 **Linee guida per l'impiego delle tecnologie biometriche nelle PA**
Indicazioni operative
SETTEMBRE 2005

N. 16 **Digitale terrestre ed *e*-government**
LUGLIO 2005

N. 15 **La biometria entra nell'*e*-government**
MARZO 2005

N. 14 **Vademecum sull'impiego delle nuove tecnologie a banda larga nelle aree periferiche**
MARZO 2005

N. 13 **Linee guida sulla qualità dei beni e dei servizi ICT**
Esempi di applicazione
GENNAIO 2005

N. 12 **Linee guida sulla qualità dei beni e dei servizi ICT**
Appalto pubblico di forniture ICT
GENNAIO 2005

N. 11 **Linee guida sulla qualità dei beni e dei servizi ICT**
Strategie di acquisizione delle forniture ICT
GENNAIO 2005

N. 10 **Linee guida sulla qualità dei beni e dei servizi ICT**
Presentazione delle Linee guida
GENNAIO 2005

N. 9 **Linee guida per l'impiego delle tecnologie biometriche nelle pubbliche amministrazioni**
NOVEMBRE 2004

N. 8 **"Tante leggi: come orientarsi?"**
NOVEMBRE 2004