ALLEGATO B

OFFERTA TECNICA DEL FORNITORE

PROCEDURA RISTRETTA PER L'AFFIDAMENTO DEI SERVIZI DI CLOUD COMPUTING, DI SICUREZZA, DI REALIZZAZIONE DI PORTALI E SERVIZI ON-LINE E DI COOPERAZIONE APPLICATIVA PER LE PUBBLICHE AMMINISTRAZIONI
(ID SIGEF 1403)

Lotto 2

Offerta Tecnica

Selex ES
A Finmeccanica Company

IBM

FASTWEB
un passo avanti

e security

SISTEMI INFORMATIVI
An IBM Company

Si raccomanda la stampa a colori al fine di preservare la corretta leggibilità dei contenuti

Costituendo
Raggruppamento Temporaneo di Imprese
composto da:

Selex ES, E-Security
IBM, Sistemi Informativi,
Fastweb

22 Dicembre 2014

Pagina lasciata intenzionalmente vuota

Sommario

1 PREMESSA 1
2 PRESENTAZIONE E DESCRIZIONE OFFERENTE 1
3 ORGANIZZAZIONE 2
3.1 Distribuzione dei Servizi oggetto di fornitura 2
3.1.1 Razionali di distribuzione delle attività 3
3.2 Organizzazione a Supporto dell'erogazione dei Servizi 5
3.2.1 Adattabilità del modello organizzativo 6
3.2.2 Ruoli, responsabilità e referenti 9
3.2.3 Modalità operative dei processi gestionali 15
3.3 I Centri Servizi 16
3.3.1 Ubicazione dei Centri Servizi 17
3.3.2 Modello organizzativo e Caratteristiche tecnologiche dei Centri Servizi 18
3.4 Il Servizio di Help Desk 36
3.4.1 Modello Organizzativo 36
3.4.2 Metodologia di erogazione 38
3.4.3 Strumenti 39
3.4.4 Impiego delle risorse umane e formazione 39
4 SOLUZIONI 40
4.1 Soluzione per l'erogazione dei servizi di Identity Provider e I&AM 41
4.1.1 Soluzione organizzativa Identity Provider 42
4.1.2 Referenze 51
4.1.3 Soluzione organizzativa di Identity and Access Management (I&AM) 51
4.1.4 Soluzione tecnologica dei servizi Identity Provider e I&AM 57
4.2 Soluzione per l'erogazione di Servizi di Firma Digitale Remota e Timbro Elettronico 75
4.2.1 Soluzione Organizzativa 75
4.2.2 Soluzione tecnologica dei servizi di Firma e Timbro 79
4.2.3 Architettura tecnologica 80
4.3 Soluzione per l'erogazione di Servizi di Sicurezza 81
4.3.1 Referenze 82
4.3.2 Soluzione Organizzativa 82
4.3.3 Soluzione Tecnologica 90
4.3.4 Servizi Professionali 100
4.4 Servizi di Sicurezza - Miglioramento Requisiti Tecnici 101
4.5 Soluzione proposta per le modalità di affiancamento di fine fornitura (Phase Out) 101
4.5.1 La metodologia "SMOOTH TRANSITION" 102
4.5.2 Organizzazione a supporto del processo di Phase Out 103
4.5.3 Piano dei lavori proposto (GANTT) 103
4.5.4 Preparation 103
4.5.5 Planning 104
4.5.6 Operation 105
4.5.7 Validation 106
4.5.8 Extra Support 106
4.5.9 Project Control & Risk Management 106
4.6 Profili Professionali - Miglioramento Anzianità di Servizio 106
4.7 Profili Professionali – Certificazioni 107
4.8 Soluzione per la formazione e l'aggiornamento delle risorse 107
4.8.1 Formazione ed aggiornamento delle risorse 107
4.8.2 Il modello di gestione Organizzativa ed Operativa 108
4.8.3 Il funzionamento della Soluzione Organizzativa ed Operativa 108
4.8.4 Esempio del catalogo formativo 110
5 QUALITÀ 111

5.1 Miglioramento degli indicatori di qualità 111
5.2 Monitoraggio e governo della fornitura 111
5.2.1 Razionali della proposta 111
5.2.2 Soluzione organizzativa 112
5.2.3 Framework operativo 113
5.2.4 Strumenti a supporto del governo e monitoraggio 116
6 DOCUMENTAZIONE COPERTA DA RISERVATEZZA 118

Indice delle Figure

Figura 1: Modello organizzativo proposto 6
Figura 2: Referenti verso Consip/Agid/Amministrazioni 14
Figura 3: Referenti verso Consip/Agid/Amministrazioni 14
Figura 4: Flusso del Processo di proposizione e acquisizione dei servizi e adesione al CE 15
Figura 5: Flusso del Processo di attivazione e configurazione dei servizi 15
Figura 6: miglioramento continuo del servizio 15
Figura 7: Framework di standards e Best Practice del RTI 16
Figura 8: Modello concettuale ed Architettura della soluzione del RTI 17
Figura 9: Ubicazione Centri Servizi 17
Figura 10: Modello Organizzativo del Centro Servizi 18
Figura 11: Approccio adottato, vincoli, livelli di protezione conformi al SOA e output previsti 22
Figura 12: Organizzazione della sicurezza 23
Figura 13: Infrastruttura per la CO 29
Figura 14: Organizzazione per la CO 29
Figura 15: Infrastruttura ICT di ciascun Data Center 32
Figura 16: Architettura di Networking 34
Figura 17: Piattaforma IBM per l'ITSM ed OSS 35
Figura 18: Organizzazione Help Desk 37
Figura 19: Modello organizzativo IdP 43
Figura 20: Organizzazione I&AM 52
Figura 21: magic quadrant Identity as a service 58
Figura 22: innovatività di Lighthouse 59
Figura 23: Modularità della soluzione 60
Figura 24: Componenti Lighthouse 60
Figura 25: Architettura logica della soluzione 61
Figura 26: Architettura della Soluzione IdP 62
Figura 27: Soluzione pe il riconoscimento Audio/Video 63
Figura 28: Casi d'uso per il Portale dell'Identità Digitale 63
Figura 29: Mockup di portale del cittadino 64
Figura 30: Architettura fisica IdP 68
Figura 31: Architettura I&AM 71
Figura 32: Architettura Fiscia I&AM 73
Figura 33: Struttura Organizzativa per il Servizio di Firma/Timbro 76
Figura 34: Operazione di Login 78
Figura 35: Architettura Sistema di Firma e Timbro 80
Figura 36: modello organizzativo Servizi di Sicurezza 83
Figura 37: Ciclo di Vita dello Sviluppo Software 85
Figura 38: Modalità di Processo Operative per l'erogazione dei servizi di gestione delle Vulnerabilità 87
Figura 39: Flusso di gestione incidenti 89
Figura 40: Matrice di correlazione 90
Figura 41: Architettura del Centro Servizi 91
Figura 42: Magic Quadrant Gartner di Sicurezza Applicativa 92
Figura 43: Architettata della Soluzione IBM per la Sicurezza Applicativa 92
Figura 44: Architettura del servizio di Static Application Security Test 93

Figura 45: Utilizzo delle tecnologie Client-Side 93
Figura 46: Architettura del servizio di Dynamic Application Security Test....94
Figura 47: Architettura di Sistema del servizio di Mobile Application Security test 95
Figura 48: Architettura del servizio di Vulnerability Assessment....96
Figura 49: Gartner Magic Quadrant DLP 97
Figura 50: Architettura del servizio di Database Security 97
Figura 51: Architettura di Database Security 98
Figura 52: Gratner Magic Quadrant per Secure Web gateway 99
Figura 53:Architettura di Secure Web Gateway....99
Figura 54: Piano di Progetto di Phase Out....103
Figura 55: Incremento dell'effort nella fase di phase-out....103
Figura 56: Modello del processo di Resource management 108
Figura 57: Stakeholder monitoraggio e controllo....112
Figura 58: Framework Operativo per il governo e il monitoraggio. 113
Figura 59: Sistema Integrato di Governo e Gestione della Fornitura (SIGGF)....116
Figura 60: Mockup Portale di Governo della Fornitura....117
Figura 61: Cruscotto andamento dei servizi....117

Indice delle Tabelle

Tabella 1: Ripartizione Servizi per aziende del RTI (R=Responsabile – C=Collaboratore) 5
Tabella 2: Fasi del processo di supporto organizzativo 8
Tabella 3: Mappatura controlli ISO27001 con obiettivi di sicurezza 22
Tabella 4; Configurazione Data Center....27
Tabella 5: Configurazione Centri di Gestione 28
Tabella 6: Impatti in caso di eventi di indisponibilità 28
Tabella 7: Casi d'uso per impatti dovuti ad eventi disastrosi 28
Tabella 8: Team e Figure professionali previste per il servizio di Identity Provider....44
Tabella 9: Referenze I&AM....51
Tabella 10: Team e Figure professionali previste per il servizio di Identity & Access Management 52
Tabella 11: Riconosimenti analisti di mercato....59
Tabella 12: Tabella riepilogativa della fornitura HW/SW per IdP - simulazione per carico 2 mln utenti....69
Tabella 13: Tabella riepilogativa della fornitura HW/SW per I&AM - simulazione per carico 4 mln utenti 75
Tabella 14: Referenze Servizi id Sicurezza 82
Tabella 15: Confronto tra i requisiti tecnici richiesti, soddisfatti e migliorativi per i singoli servizi di sicurezza.101
Tabella 16: Razionali di sostenibilità del Phase Out. 102
Tabella 17: Descrizione delle attività relative alla fase di Preparation. 104
Tabella 18: Descrizione delle attività relative alla fase di Planning.....104
Tabella 19: Descrizione delle attività relative alla fase di Operation. 105
Tabella 20: Descrizione delle attività relative alla fase di Validation. 106
Tabella 21: Giorni minimi di formazione 110
Tabella 22: Razionali della proposta del RTI. 111
Tabella 23: Gli attori previsti nel modello organizzativo. 112
Tabella 24: Principali output del monitoraggio RTI nelle diverse fasi del ciclo di vita del Contratto Quadro....114
Tabella 25: Esempio di reportistica proposto per l'analisi del monitoraggio del Contratto Quadro. 117

Glossario

Acronimo	Descrizione
AAA	Authentication, Authorization, and Accounting
AD	Administrative Domain
AgID	Agenzia per l'Italia Digitale
Ajax	Asynchronous Javascript and XML
API	Application Programming Interface
APT	Advanced Persistent Threat
ARSS	ArubaPEC Remote Signing Server
ASIC	Application-Specific Integrated Circuit
ASP	Active Server Page
BaaS	Backup as a Service
BC	Business Continuity
BGP	Border Gateway Protocol
BI	Business Intelligence
BPM	Business Process Management
C&C	Command and Control
CAD	Codice dell'Amministrazione Digitale
CAdES-BES	CAdES Basic Electronic Signature
CAdES-T	CMS Advanced Electronic Signature (timestamp)
CCTA	Central Computer and Telecommunications Agency
CDC	Cyber Defence Capability
CD	Compact Disc
CDRL	Centro di Registrazione Locale
CE	Contratto Esecutivo
CED	Centro Elaborazione Dati
CEH	Certified Etical Hacker
CERT	Computer Emergency Response Team
CIFS	Common Internet File System
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
CLOSINT	Closed-Source Intelligence
CMDB	Configuration Management Data Base
CMMI	Capability Maturity Model Integration
CMS	Cryptographic Message Syntax
CNAIPIC	Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
CO	Continuità Operativa
COBIT	Control Objectives for Information and Related Technology
COBOL	Common Business-Oriented Language
CONSIP	Concessionaria Servizi Informativi Pubblici
CM	Change Management
CMS	Card Management System
CPU	Central Processing Unit
CQ	Contratto Quadro
CRAMM	CCTA Risk Analysis and Management Method
CS	Centro Servizi
CVS	Concurrent Versions System
CVSS	Common Vulnerability Scoring System
DAST	Dynamic Application Security Testing
DB	Database
DC	Data Center
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
DNS	Domain Name System
DoS	Denial Of Service
DPS	Documento Programmatico sulla Sicurezza
DR	Disaster Recovery
DSS	Decision Support System
DVD	Digital Versatile Disc
DWDM	Dense Wavelength Division Multiplexing
eIDAS	Electronic identification and trust services
EMODS	Energy Management Optimization and Decision Support
ENISA	European Network and Information Security Agency
EQF	European Qualifications Framework
ETL	Extract, Transform, Load
EUCIP	European Certification of Informatics Professionals
FAQ	Frequently Asked Question(s)
FCoE	Fiber Channel Over Ethernet
FIPS	Federal Information Processing Standard
FP	Focal Point
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
GBS	Global Business Services
GFID	Gestione Federata delle Identità Digitali
GLBA	Gramm-Leach-Bliley Act
GRC	Governance, risk management, and compliance
HA	High Availability
HD	Help Desk
HIPAA	Health Insurance Portability and Accountability Act
HPC	High Performance Computing
HSM	Hardware Security Module
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
HUMINT	Human Intelligence
HVAC	Heating, Ventilation and Air Conditioning
I&AM	Identity and Access Management
IaaS	Infrastructure as a Service
ICT	Information and Communication Technology
IDaaS	Identity as a Service
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IEC	International Electrotechnical Commission
IEM	IBM Endpoint Manager
INPS	Istituto Nazionale della Previdenza Sociale
IOC	Indicator of Compromise
IP	Internet Protocol
IPC	Interprocess Communications
IPMA	International Project Management Association
IPSec	Internet Protocol Security
iSCSI	Internet Small Computer Systems Interface
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
ITUP	IBM Tivoli Unified Process
IVR	Interactive Voice Response
L&D	Learning & Development
J2EE	Java 2 Platform, Enterprise Edition
JAX	Java API for XML
JSF	JavaServer Faces
JSP	Java Server Pages
K&LMS	Knowledge and eLearning Management System
KCS	Knowledge-Centered Support
KM	Knowledge Management
KPI	Key Performance Indicator
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LoA	Level of Assurance
LoB	Line Of Business
LPT	Line Printer
MARION	Méthodologie d'Analyse des Risques Informatiques et d'Optimisation par Niveau
MAST	Mobile Application Security Testing
MIGRA	Metodologia Integrata per la Gestione del Rischio Aziendale
MiX	Milan Internet eXchange
MPLS	Multiprotocol Label Switching
MTTR	Mean Time To Repair
MVC	Model-View-Controller
NaMeX	Nautilus Mediterranean eXchange point
NAT	Network Address Translation
NCIRC	NATO Computer Incident Response Capability
NFS	Network File System
NIST	National Institute of Science and Technology
NL-SAS	Near Line Serial-Attached SCSI

NOC	Network Operations Center
OBS	Organizational Breakdown Structure
OCSI	Organismo di Certificazione della Sicurezza Informatica
OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation
ODR	Operatore di Registrazione
OSI	Open Systems Interconnection
OSINT	Open-Source Intelligence
OSSTMM	Open Source Security Testing Methodology Manual
OTP	One Time Password
OWASP	Open Web Application Security Project
PA	Pubblica Amministrazione
PaaS	Platform as a Service
PAC	Pubblica Amministrazione Centrale
PAdES-T	PDF Advanced Electronic Signature (timestamp)
PAdES-BES	PAdES Basic Electronic Signatures
PA-DSS	Payment Application Data Security Standard
PAL	Pubblica Amministrazione Locale
PAT	Pubblica Amministrazione Territoriale
PC	Personal Computer
PCI	Payment Card Industry
PCI DSS	PCI Data Security Standard
PCO	Piano di continuità operativa
PCT	Processo Civile Telematico
PDF	Portable Document Format
PDL	Postazioni di Lavoro
PdS	Piano di Sicurezza
PEC	Posta Elettronica Certificata
PERL	Practical Extraction and Report Language
PDU	Power Distribution Unit
PGGF	Portale di Governo e Gestione della Fornitura
PHP	PHP: Hypertext Preprocessor
PL/SQL	Procedural Language/Structured Query Language
PMI	Project Management Institute
PMO	Project Management Office
PMP	Project Management Professional
PNG	Portable Network Graphics
PoD	Pool of Devices
PPM	Process & Performance Management collide con altro acronimo (Project Portfolio Management)
PRINCE	Projects IN Controlled Environments
PRM	Process Reference Model
PT	Penetration Testing

PUE	Power Usage Effectiveness
QA	Quality Assurance
Acronimo	Descrizione
QoS	Quality of Service
QVM	Qradar Vulnerability Manager
QXN	Qualified eXchange Network
RACI	Responsible, Accountable, Consulted, Informed
RAM	Rational Asset Manager
RDM	Release and Deployment Management
RIPA	Rete Internazionale delle PA
RPO	Recovery Point Objective
RTC	Rational Team Concert
RTI	Raggruppamento Temporaneo di Imprese
RTO	Recovery Time Objective
RTSS	Real Time Security Scanning
SaaS	Software as a Service
SACM	Service Asset and Configuration Management
SAL	Stato Avanzamento Lavori
SAML	Security Assertions Markup Language
SAN	Storage Area Network
SAST	Static Application Security Testing
SATA	Serial Advanced Technology Attachment
SCAPM	SmartCloud Application Performance Managenent
SCCD	SmartCloud Control Desk
SDE	Software Defined Environment
SDLC	Software Development Life Cycle
SFP	Small Form-factor Pluggable
SFTP	SSH File Transfer Protocol
SGAC	Servizio di Gestione Automatizzata dei Contratti
SGPW	Servizio di Gestione del Portale Web
SGQS	Servizio di Gestione dei Dati di Qualità e Sicurezza
SGSI	Sistema di Gestione della Sicurezza delle Informazioni
SICA	Servizi Infrastrutturali di Interoperabilità, Cooperazione ed Accesso
SICOTE	Sicurezza e Controllo del Territorio
SIEM	Security Information and Event Management
SIGGF	Sistema Integrato di Governo e Gestione della Fornitura
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SOA	Statement of Applicability
SOAP	Simple Object Access Protocol
SOC	Security Operation Center
SOX	Sarbanes-Oxley Act
SNMP	Simple Network Management

	Protocol
SPC	Sistema Pubblico di Connettività
SPConn	Sistema Pubblico di Connettività
SPID	Sistema Pubblico per la gestione dell'Identità Digitale
SPOC	Single Point of Contact – Punto di contatto univoco
SQL	Structured Query Language
S-RIPA	Servizi RIPA
SSD	Solid State Disk
SSH	Secure Shell
SSL	Secure Sockets Layer
SVN	Subversion
SW	Software
TBSM	Tivoli Business Service Manager
TCP	Transmission Control Protocol
TLC	Telecomunicazione
TDW	Tivoli DataWareHouse
TFVC	Team Foundation Version Control
TIFF	Tag Image File Format
T-SQL	Transact Structured Query Language
UCS	Unified Computing System
UDP	User Datagram Protocol
ULS	Unità Locale di Sicurezza
UNI	Ente nazionale italiano di unificazione
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTM	Unified Threat Management
VA	Vulnerability Assessment
VAS	Value Added Services
VB	Visual Basic
VCC	Video a Circuito Chiuso
VD	Virtual Desktop
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNIC	Virtual Network Interface Card
VOIP	Voice over Internet Protocol
VPN	Virtual Private Network
VVFF	Vigili del Fuoco
VTL	Virtual Tape Library
WAF	Web Application Firewall
WAN	Wide Area Network
WBS	Work Breakdown Structure
WS	Web Service
WSDL	Web Service Definition Language
XAdES-BES	XAdES Basic Electronic Signatures
XAdES-T	XML Advanced Electronic Signature (timestamp)
XML	Extensible Markup Language
XSS	Cross-Site Scripting

Di seguito sono presentati i Tag per marcare l'evidenza di corrispondenza ai criteri di valutazione utilizzati nel documento.

Adeguatezza	AD	Efficacia	EC	Facilità d'uso	FU	Innovatività	IN	Modularità	MO

1 PREMESSA

Selex ES S.p.A., Società con unico socio, soggetta ad attività di direzione e coordinamento della Finmeccanica Società per Azioni, con sede legale in Roma, in Piazza Monte Grappa 4 - CAP 00195, capitale sociale € 350.000.000,00, R.E.A. 1210448, iscrizione al Registro delle Imprese di Roma, codice fiscale e partita IVA n. 10111831003, rappresentata da Andrea Campora nato a Genova (GE) il 20 luglio del 1968 nella sua qualità di Procuratore Speciale (giusta procura autenticata nella firma in data 6 novembre 2014, dal Dottor Ignazio de Franchis Notaio in Roma repertorio n. 108140) domiciliato per la carica presso la sede societaria, quale Mandataria del costituendo Raggruppamento di Imprese

E-Security S.r.l. con sede Legale in Via Enrico Mattei n.21 66100 – Chieti (Ch) Fraz. Scalo - Italia, Iscritta al Registro Imprese di Chieti, codice fiscale e partita IVA n. 06432561006 Capitale Sociale Euro 128.000,00 interamente versato, rappresentata da Andrea Biraghi nato a Melzo (MI) il 31/01/1971 nella sua qualità di Amministratore Delegato e Legale Rappresentante domiciliato per la carica presso la sede societaria, quale Mandante del costituendo Raggruppamento di Imprese

IBM Italia S.p.A., Società con unico azionista, soggetta all'attività di direzione e coordinamento di "International Business Machines Corporation" (U.S.A.), capitale sociale di Euro 347.256.998,80 interamente versato con sede legale e domicilio fiscale in Segrate (Milano), C.A.P. 20090, Circonvallazione Idroscalo, tel. 06.59664442, iscritta alla C.C.I.A.A. di Milano al numero di iscrizione 01442240030 in data 19 febbraio 1996, Codice Fiscale numero 01442240030 e Partita IVA numero 10914660153, in persona del Procuratore Speciale con legale rappresentanza (giusta procura autenticata nella firma in data 25 luglio 2008, dal Notaio Dr.ssa Laura Cavallotti in Milano repertorio n. 5834/1845), Massimo De Lucia, quale Mandante del costituendo Raggruppamento di Imprese

Sistemi Informativi S.r.l.,Società con socio unico, Società soggetta a direzione e coordinamento di IBM Italia S.p.A., con sede in Roma, Via Sciangai 53 - 00144, tel. 0659666211, Capitale sociale € 2.697.375,00 interamente versato, codice fiscale 06310880585, partita IVA n. 01528071002, iscritta nel Registro delle Imprese di Roma al n. 06310880585, in persona dell'Amministratore Delegato, Direttore Generale e Consigliere, Carla Monguzzi, quale Mandante del costituendo Raggruppamento di Imprese

Fastweb S.p.A. con sede in Milano, Via Caracciolo 51, capitale sociale Euro 41.344.209,40 interamente versato, iscritta al Registro delle Imprese di Milano al n. 12878470157, codice fiscale e partita IVA n. 12878470157, rappresentata da Claudio Pellegrini, nato a Biella il 3/01/1965 C.F. PLLCLD65A03A859W ed Emidio Romano, nato a Benevento il 22/07/1966 C.F. RMNMDE66L22A783X, domiciliati per la carica presso la sede societaria, nella loro qualità di Procuratori Speciali (giusta procura autenticata nella firma in data 16 dicembre 2014, dal notaio D.ssa Elena Terrenghi in Milano repertorio n. 28656) aventi i poteri necessari in via tra loro congiunta per impegnare la società Fastweb S.p.A. nella presente procedura, quale Mandante del costituendo Raggruppamento di Imprese

di seguito "Raggruppamento" o "RTI"

- offre e, in caso di aggiudicazione in proprio favore, si impegna ad eseguire le attività relative alla prestazione dei servizi richiesti per il Lotto 2 della Procedura ristretta per l'affidamento dei servizi di cloud computing, di sicurezza, di realizzazione di portali e servizi on-line e di cooperazione applicativa per le pubbliche amministrazioni (ID SIGEF 1403) nel rispetto di tutti gli obblighi e gli adempimenti richiesti nel corpo del Capitolato Tecnico e delle altre parti della documentazione di gara;
- dichiara espressamente che tutti i prodotti/servizi offerti posseggono integralmente le caratteristiche, funzionalità ed i requisiti minimi stabiliti nella documentazione di gara e, pertanto, dichiara altresì che la proposta è da intendersi esclusivamente migliorativa degli stessi e pertanto eventuali discordanze sono da considerarsi come un mero refuso o errore di battitura ed il raggruppamento intende adempiere integralmente a tutte le obbligazioni, requisiti e adempimenti richiesta dalla lex specialis.

2 PRESENTAZIONE E DESCRIZIONE OFFERENTE

Il RTI è formato dalle aziende di seguito presentate.

Selex ES S.p.A., società di **Finmeccanica,** è un provider globale di sistemi, prodotti e soluzioni all'avanguardia in grado di rispondere alla crescente domanda di tecnologie avanzate nei settori della sicurezza, dell'informatica, della protezione di informazioni, infrastrutture e territorio, nonché nella gestione di infrastrutture strategiche. Con circa **10.300** dipendenti (a novembre 2014), e **ricavi per oltre 2 miliardi di euro**, Selex ES SpA ha una presenza capillare su tutto il territorio nazionale (le principali sedi sono a Genova, Roma, Pomezia, Milano, Torino, Firenze, L'Aquila, Gorizia, Napoli, Palermo). Il gruppo Selex ES ha oltre 6000 dipentenenti in paesi esteri quali Regno Unito, Stati Uniti, Germania, Turchia, Romania, Brasile, Arabia Saudita e India; e ricavi per oltre 3,5 Miliardi di euro, di cui più del 12% re-investiti in attività di Ricerca e Sviluppo. Selex ES è Leader nell'integrazione applicativa e dei sistemi ICT e service provider di infrastrutture in outsourcing per il settore pubblico ed il mercato Enterprise, Selex ES opera tramite le **Line of Business Cyber Security&Information Assurance** e **ICT & Networking** per realizzare piattaforme applicative per l'erogazione di servizi digitali, volti a supportare l'innovazione della Pubblica Amministrazione, in linea con gli obiettivi delle **Agende Digitali** nazionali ed europee. Selex ES dispone di circa 4.000 dipendenti con competenze specifiche in ambito ICT e Cyber Security, dislocati e/o allocabili su 46 sedi nazionali; vanta la

conoscenza/presenza su più di 10 grandi clienti della **Pubblica Amministrazione Centrale** e su più di 30 della **Pubblica Amministrazione Locale** tra cui: Ministero della Giustizia, Ministero dell'Economia e delle Finanza, Ministero dei Trasporti, Ministero dei Beni Culturali, Camera dei Deputati, Dipartimento della Protezione Civile, Comune di Roma e di Milano, DigitPA, INPS, INAIL, INPDAP. Selex ES ha realizzato il sistema di Incident Response della NATO applicato a tutti i paesi membri; nel mercato italiano ha realizzato il programma CDC (Cyber Defence Capabilities) per il Ministero della Difesa, gestisce il SOC della rete internazionale S-RIPA per la sicurezza delle ambasciate e consolati italiani ed importanti programmi di Cyber Security per molte altre Pubbliche Amministrazioni e Enti Italiani.

E-Security S.r.l. è un azienda controllata al 100% da Selex ES, interamente inclusa nella linea di servizio Cyber Security & Information Assurance. Possiede un Centro Servizi ed un Security Operation Center che annoverano tra i loro clienti pubbliche amministrazioni ed aziende private di rilevanza nazionale; eroga anche servizi per più di 3.000 piccole e medie imprese. E-Security gestisce anche l'infrastruttura di supercalcolo di Selex ES.

IBM Italia S.p.A. (IBM), è parte integrante della IBM Corporation leader globale del mercato dell'Information Technology. IBM si caratterizza per un'offerta end-to-end, in cui le tradizionali componenti hardware, software e servizi si armonizzano nel più ampio concetto di soluzioni atte ad indirizzare le esigenze di aziende e amministrazioni con elevati livelli di qualità. IBM Corporation ha chiuso il 2013 con un fatturato mondiale superiore a 99 miliardi di dollari con un profitto ante imposte di oltre 16.8 miliardi, realizzato nelle aree software, servizi ed hardware. La IBM è stata per il 21° anno consecutivo la società mondiale con il maggior numero di brevetti registrati nel campo della ricerca tecnologica. IBM è presente in Italia con un giro d'affari superiore ai **2 miliardi di euro** (operazioni nazionali) e circa **6000 dipendenti** con sedi a Milano, Roma, Bari, Bologna, Cagliari, Catania, Firenze, Genova, Napoli, Padova, Palermo, Torino. Il laboratorio di Ricerca e Sviluppo oggi presente in Italia impiega 300 tra sviluppatori, progettisti e architetti nella ricerca e sviluppo di aree quali il Cloud Computing, il System Management, Cyber Security , Web Development, Automation, Mobile. IBM Italia opera in tutte le aree dell'IT, e si propone come partner strategico per i clienti, accompagnandoli in iniziative di trasformazione delle piattaforme tecnologiche ed applicative, per un più efficace orientamento al business e al mandato istituzionale e un migliore sfruttamento delle opportunità tecnologiche (Cloud, Big Data, User Experience, Mobile), avvalendosi anche delle competenze presenti nei propri centri di eccellenza globali.

Sistemi Informativi S.r.l. è una società soggetta a direzione e coordinamento di IBM Italia S.p.A (di seguito nella presente relazione sarà citato come "**Gruppo IBM**" l'apporto congiunto IBM Italia S.p.A. e Sistemi Informativi S.r.l.), dispone di circa 1.100 dipendenti con oltre 600 certificazioni tecniche ed offre servizi e soluzioni per l'ottimizzazione dei processi dei propri clienti in termini di efficienza, competitività ed innovazione. La missione di Sistemi Informativi è di offrire soluzioni e servizi che contribuiscano a rendere i clienti più efficienti, competitivi e innovativi nei loro processi. Sistemi Informativi detiene una propria specificità determinata dall'esperienza maturata, dal 1979, nell'ambito della PA e del settore Bancario. Sistemi Informativi ha una presenza rilevante nel settore della Pubblica Amministrazione in virtù di significative esperienze in Consip, Sogei e Ministero dell'Economia e delle Finanze, Ministero della Difesa, Inail, Inps.

FASTWEB S.p.A. con circa 2 Milioni di clienti, 2.800 dipendenti (di cui 50% laureati), con specifiche competenze tecniche e manageriali in ambito TLC ed ICT, l'ingente estensione delle infrastrutture in fibra ottica, la ricca offerta di servizi avanzati, sedi a Milano, Genova, Torino, Bologna, Padova, Firenze, Pescara, Roma, Napoli, Bari, Palermo e Catania, è il principale operatore alternativo di telefonia fissa e connettività IP, nonché primario fornitore di servizi a valore aggiunto (VAS) per le Amministrazioni Pubbliche Centrali e Locali. Dalla sua fondazione a Milano nel 1999, Fastweb ha investito oltre 5 miliardi di euro per realizzare una rete in fibra ottica di nuova generazione che oggi supera i 32.000 chilometri di tracciato ed oltre 1.000.000 di Km di fibra (ad oggi la più estesa in Europa). Attualmente è presente in oltre 150 aree metropolitane.
Il mercato Enterprise rappresenta circa il 20% dei clienti di Fastweb e contribuisce per il 60% al fatturato. Nel segmento Enterprise Fastweb è riconosciuta come fornitore d'eccellenza per affidabilità e competitività dei servizi ed è il primo fornitore della Pubblica Amministrazione in Italia potendo vantare la presenza in una pluralità di enti della Pubblica Amministrazione Centrale e Locale tra cui INPS, MIUR, Regione Lombardia, oltre a numerosi clienti Enterprise.
La forte propensione agli investimenti nelle tecnologie d'avanguardia (Next Generation Network, IPTV, Cloud Services) ha reso possibile nel tempo: il lancio di servizi "Triple Play" (voce, dati/Internet e video) fruibili contemporaneamente con un solo collegamento, il dispiegamento diffuso delle reti NGN, la diffusione della banda larga mediante connettività in fibra con tecnologie FTTx, il rilascio di servizi di Cloud Computing erogati dai propri Data Center Tier IV e Tier III in Business Continuity. In quest'ambito Fastweb è l'unica azienda italiana a poter vantare un data center che ha ottenuto la certificazione TIER IV CONSTRUCTION (solo altri 4 in Europa e solo 16 nel mondo) e che implementa parametri di elevata qualità con la massima attenzione agli aspetti di riduzione dell'impatto ambientale.

3 ORGANIZZAZIONE

3.1 Distribuzione dei Servizi oggetto di fornitura

Il RTI esprime i seguenti **punti di forza**: **completa integrazione e complementarità** dei membri del RTI con competenze su servizi professionali e di sicurezza gestita (Selex ES, E-Security, Sistemi Informativi, Fastweb) tecnologiche (IBM), infrastrutturali (Fastweb), e di realizzazione di portali e servizi on line (Selex ES, IBM). Elevata sinergia delle aziende tramite le relazioni tra le varie unità operative Selex/E-Security (sviluppo ed integrazione di

sistemi informativi per le PA, Cyber Security e Managed Services) di IBM/Sistemi Informativi (tecnologie SW di base, servizi professionali, prodotti), e Fastweb (provider Telco Nazionale, Infrastrutture e capillarità).

3.1.1 Razionali di distribuzione delle attività

La digitalizzazione dei processi dell'Amministrazione e la contemporanea apertura degli stessi alla connessione con il mondo esterno, in unione alla costante evoluzione delle tecniche di attacco, accrescono fortemente l'esigenza di una maggiore protezione di quella particolare Infrastruttura Critica Nazionale che va sotto il nome di SPC, ovvero dei sistemi e servizi di connettività, di elaborazione ed applicativi della PA. Nel ventunesimo secolo l'infrastruttura ed i servizi della PA costituiscono infatti uno strumento strategico per il Paese, con impatto non solo sull'efficienza dell'attività amministrativa in senso stretto e della relazione con il cittadino (e-government, e-democracy), ma anche della crescita economica e della sicurezza dell'intero Sistema Paese.
In un contesto in cui la fiducia dei cittadini verso i nuovi servizi digitali è fondamentale per lo sviluppo dell'interazione online con le Amministrazioni, queste devono adottare le necessarie misure procedurali e tecnologiche atte a garantire adeguati livelli di riservatezza, disponibilità ed integrità dei propri dati a fronte di attacchi cibernetici di qualunque natura. I cittadini e le imprese devono infatti poter usufruire dei servizi senza il timore che i propri dati personali, inclusa la propria identità digitale, vengano violati o utilizzati fraudolentemente.
In questo contesto il RTI si propone come partner d'eccellenza, capace di offrire soluzioni innovative, sicure ed efficaci potendo contare sulle significative e provate competenze di ciascuna azienda del raggruppamento nella realizzazione di ogni singolo elemento architetturale individuato nella presente Gara. In quest'ottica, caratteristiche distintive del RTI sono:

- **integrazione** di grandi e solide Aziende di respiro internazionale, fortemente radicate sul territorio, che vantano precedenti collaborazioni e sinergie di successo in progetti complessi;
- **dimensioni** delle aziende coinvolte tali da garantire contemporaneamente agilità, specializzazione, capacità d'intervento con ridotti tempi di reazione, capacità d'investimento ed innovazione, elevato livello di qualità;
- **eccellenza** di alcuni membri del RTI nell'area della Cyber Security e della gestione delle Identità digitali;
- **conoscenza** approfondita del contesto generale della Pubblica Amministrazione;
- **esperienze** pluriennali nell'erogazione di servizi per la PA in contesti analoghi a quello della Gara con l'adozione di primari framework e best practice internazionali come ITIL, COBIT, CMMI e PMI;
- **capacità** di contribuire alla definizione di scenari evolutivi della PA.

Le aziende del RTI hanno deciso di raggrupparsi in quanto ritengono, anche sulla base delle precedenti esperienze di collaborazione, di poter erogare **sinergicamente** i servizi oggetto della Gara con livelli di **qualità, affidabilità, efficacia ed efficienza** massimizzati dalle loro caratteristiche di **complementarietà**, in termini di aree di esperienza ed eccellenza. Il RTI è organizzato come un'azienda di fatto, con responsabilità di governo dell'intera fornitura in capo alla Mandataria a garanzia di una razionalizzazione ed omogeneità dei servizi forniti verso la Committente e le singole Amministrazioni.

Punti di Forza delle singole aziende

Le aziende costituenti il RTI hanno competenze, sia tecniche sia commerciali, specifiche e complementari come illustrato nel seguito.
Selex ES, quale System Integrator, vanta esperienze sia nella personalizzazione sia nell'integrazione di sistemi complessi per una clientela di tipo Enterprise che richiede elevati livelli di qualità. Le unità operative coinvolte sui temi pertinenti a questa proposta sono in capo alle Linee Servizio/Business (di seguito LoB) Cyber Security & Information Assurance e ICT & Networking della Divisione Smart & Security System.
La **LoB Cyber Security & Information Assurance** di **Selex** ES lavora da decenni nel settore della sicurezza sia per il mondo della Difesa che per il mercato civile affiancando le istituzioni e le grandi aziende del settore industriale e dei servizi nella protezione delle infrastrutture critiche (energia, trasporti, telecomunicazioni), degli interessi pubblici, delle imprese e del singolo cittadino. L'azienda propone un'offerta di prodotti e servizi che va dall'analisi del rischio, alla progettazione e implementazione di architetture di sicurezza, al training per la prevenzione e la gestione di incidenti con circa 500 professionisti qualificati in grado di progettare e gestire programmi complessi.
Da giugno del 2014 Selex ES dispone di un nuovo centro realizzato con tecnologie allo stato dell'arte per la Cyber Security costituito da un Security Operation Center (SOC) e dall'Open Source Intelligence Center, dotato di una tra le principali architetture High Performance Computing per la fornitura di servizi di intelligence.
La **LoB ICT & Networking**, ha le competenze per fornire soluzioni ICT, realizzare infrastrutture digitali ed erogare servizi per sostenere le missioni istituzionali degli Enti Pubblici o migliorare i processi di business di Organizzazioni

Aziendali italiane ed internazionali. Leader nell'integrazione applicativa e dei sistemi ICT, Service Provider di infrastrutture in outsourcing per il settore pubblico ed il mercato Enterprise, Selex ES opera in linea con gli obiettivi delle Agende Digitali nazionali ed europee e come ICT Service Provider e Technology Partner del gruppo Finmeccanica. I centri di competenza Selex garantiscono il supporto necessario in termini di conoscenze e competenze per eventuali attività specialistiche.

E-Security, parte integrante della LoB Cyber Security & Information Assurance, gestisce dal 2007 il Security Operation Center italiano dedicato ai client esterni (tra i quali Telecom Italia, INPS, ENAV, Protezione Civile).

L'apporto di **Selex ES** e di **E-Security** all'interno del RTI (v. Tabella 1) è costituito dal contributo offerto dalle proprie figure professionali all'erogazione dei servizi di Identity Provider, Identity & Access Management ed ai servizi specifici di sicurezza previsti dalla Gara ed erogati con modalità sia "as a service" sia "on premise".

Selex ES mette anche a disposizione del RTI i propri asset per l'erogazione del servizio di Data Center di DR, come meglio specificato nel paragrafo 3.3 (Centro Servizi), asset e risorse per l'Help Desk relativo ai servizi di Sicurezza, capacità di sviluppo e system integration per la realizzazione del Portale di Governo e Gestione della Fornitura come richiesto dal Capitolato Tecnico - Parte Generale (rif. par. 6.2).

Svolgerà inoltre le attività di coordinamento previste dal ruolo di Mandataria a garanzia della razionalizzazione ed omogeneità dei servizi forniti verso la Committente e le singole Amministrazioni.

IBM porta nel RTI i vantaggi di un partner di livello mondiale con prodotti HW e SW di qualità riconosciuta dagli utenti e dagli analisti di settore. Oltre ad essere produttore di tecnologia Hardware, come server e Storage ha recentemente investito di nuovo nel settore della Sicurezza delle informazioni e Cloud, diventando player primario del settore, riorganizzando brand storici, come Tivoli e Rational, e realizzando nuove acquisizioni, LightHouse, Crossideas per la parte I&AM, Q1Labs per il monitoring e il security event management, Trusteer per il Fraud management, XGS come nuova frontiera dei network intrusion prevention system, Guardium per la sicurezza dei database, ridiventando in brevissimo tempo attore primario in questo campo, e ponendosi come indiscusso leader, con un catalogo prodotti tra i migliori sul mercato.

I servizi oggetto della fornitura saranno erogati dalla struttura di Security Services della IBM Global Technology Services (GTS), che costituisce una Business Unit di IBM Italia S.PA

L'Apporto di **IBM** e di **Sistemi Informativi** all'interno del RTI è costituito da tecnologie e competenze specifiche su metodologie e tematiche inerenti gli aspetti di sicurezza informatica per i servizi offerti.

I prodotti messi a disposizione includono: le suite ISIM (IBM Security Identity Manager) , ISAM (IBM Security Access Manager), IFIM (IBM Federated Identity Manager), per le componenti di Identity Provider e Identity & Access Management; Qradar per la raccolta ed analisi degli eventi di sicurezza, la suite IBM Security AppScan e Qradar QVM (IBM QRadar Vulnerability Manager) per i Servizi di Sicurezza "as a service" quali "static application security testing", "dynamic application security testing", "mobile application security testing" e "vulnerability assessment", nonché prodotti SW a supporto delle attività svolte presso il Centro Servizi.

Le attività saranno erogate da un centro di competenza in cui le professionalità e le esperienze sono poste a fattor comune e coordinate a favore di una continua efficienza nell'erogazione dei servizi da parte di tutto il team.

Fastweb è strutturata internamente in divisioni di Staff e di Business, alcune di queste direttamente coinvolte nelle attività previste nella Gara, in particolare: **Enterprise Division**, include le linee di business coinvolte nelle fasi di Service Operation, quali Vendite, Progettazione, Provisioning ed Assistenza Tecnica per i Clienti Enterprise (tra cui le Pubbliche Amministrazioni), nonché le strutture operative di Data Center e SOC coinvolte nei Centri Servizi del RTI; **Technology Division**, include le linee di business coinvolte nelle fasi di Service Design, Service Transition e Service Operation, tra cui le strutture di progettazione, delivery e gestione delle infrastrutture di Rete, Fibra Ottica, Data Center e Sistemi Informativi.

L'apporto **tecnologico** di **Fastweb** ai servizi erogati da RTI consiste nella disponibilità dell'unico Data Center Tier IV certificato Construction Facility in Italia e del secondo Data Center di Business Continuity dai quali saranno erogati i servizi previsti dalla Gara. I due Data Center sono già attivi per erogazione di servizi Cloud alla PA centrale e locale con elevata integrazione tra strutture virtuali e Data Center fisici dei clienti.

L'apporto in termini di **competenze** include l'esperienza nella realizzazione di servizi di comunicazione, l'accesso a larga banda alla rete SPC (di cui è uno dei service provider principali), l'esperienza nella realizzazione di architetture e servizi di Disaster Recovery e Business Continuity, asset e risorse per l'Help Desk relativo a Data Center e Centro Servizi, l'esperienza nell'erogazione di servizi di outsourcing ICT e la presenza nell'albo dei certificatori accreditati AgID come gestore di PEC (Posta Elettronica Certificata).

La **capillarità** delle strutture commerciali e operative di Fastweb presenti su tutto il territorio nazionale, garantisce la capacità di fornire pieno supporto tecnico e commerciale ai servizi oggetto di gara sia verso le Pubbliche Amministrazioni Centrali che verso le Territoriali anche di piccole dimensioni.

Come evidenziato ai capoversi precedenti, alla luce delle **complementarietà** delle aziende che costituiscono il RTI, ciascuna di esse ha adottato responsabilità specifiche (pur restando il RTI responsabile solidale per tutte le attività oggetto di erogazione del presente Lotto): il criterio di ripartizione ha privilegiato l'**efficacia**, l'**efficienza** e la **qualità** del servizio offerto. La matrice sotto riportata indica per ciascun servizio (o categoria di servizi) le aree di responsabilità primarie (R) e quelle in cui le varie aziende rivestono un ruolo di collaborazione significativa (C) che può esplicitarsi, ad esempio, in fornitura di prodotti/infrastrutture, attività di gestione sistemistica e messa a disposizione di spazi di Data Center, supporto specialistico di I e II livello, attività di consulenza e gestione di servizi "as a Service" e/o "on premise".

Tabella 1: Ripartizione Servizi per aziende del RTI (R=Responsabile – C=Collaboratore)

Servizi	Selex ES	e-Security	IBM	Sist. Infor.	Fastweb
Gestione ed erogazione servizi di Identity Provider e I&AM	R		C	C	C
Gestione ed erogazione servizi di Firma Digitale Remota e Timbro Elettronico	C		C		R
Gestione ed erogazione servizi di Application Security Testing (Static, Dynamic, Mobile, VA[1]	C	C	R		C
Gestione ed erogazione servizi di Protezione (DLP, DB Security, WAF/NGF, Web Gateway)[2]	R	C	C		C
Erogazione di Servizi Professionali a supporto del ULS	R		C		C
Data Center Primario e di Business Continuity (inclusa gestione operativa)					R
Data Center di DR	R				
Help Desk	R		C		C
Governo e gestione della fornitura e sistemi a supporto	R				

3.2 Organizzazione a Supporto dell'erogazione dei Servizi

L'organizzazione proposta dal RTI riflette le specificità della fornitura e le richieste della Committente, assicurando **efficacia e flessibilità** sia nella gestione complessiva del **Contratto Quadro (nel seguito CQ),** sia nell'erogazione dei singoli **Contratti Esecutivi (nel seguito CE).** Particolare attenzione è stata posta nella definizione dei ruoli del RTI che avranno un rapporto diretto con i Referenti Consip e AgID e delle Amministrazioni beneficiarie, al fine di individuare rapidamente responsabilità e competenze e rendere efficaci i processi di erogazione dei servizi oggetto dei Contratti. È opportuno sottolineare che tale organizzazione, nonché le metodologie e gli strumenti a supporto della fornitura, saranno oggetto di condivisione con Consip, AgID in fase di avvio delle attività, al fine di garantire il massimo allineamento con le esigenze dell'Amministrazione stessa.

Dato il perimetro e l'estensione temporale del CQ il RTI ha ritenuto opportuno impostare l'organizzazione a supporto della Fornitura secondo un modello di un'unica azienda strutturata in:

- un Comitato Direttivo di RTI a livello di **Governo** sia per il **CQ** sia per i **CE**;
- **unità/strutture operative,** deputate all'erogazione dei servizi, **flessibili** e **territorialmente distribuite**;

[1] Per la definizione si veda il Glossario

[2] Vedi nota precedente

- strutture e funzioni di supporto all'erogazione degli stessi.

La figura seguente riporta il modello organizzativo proposto.

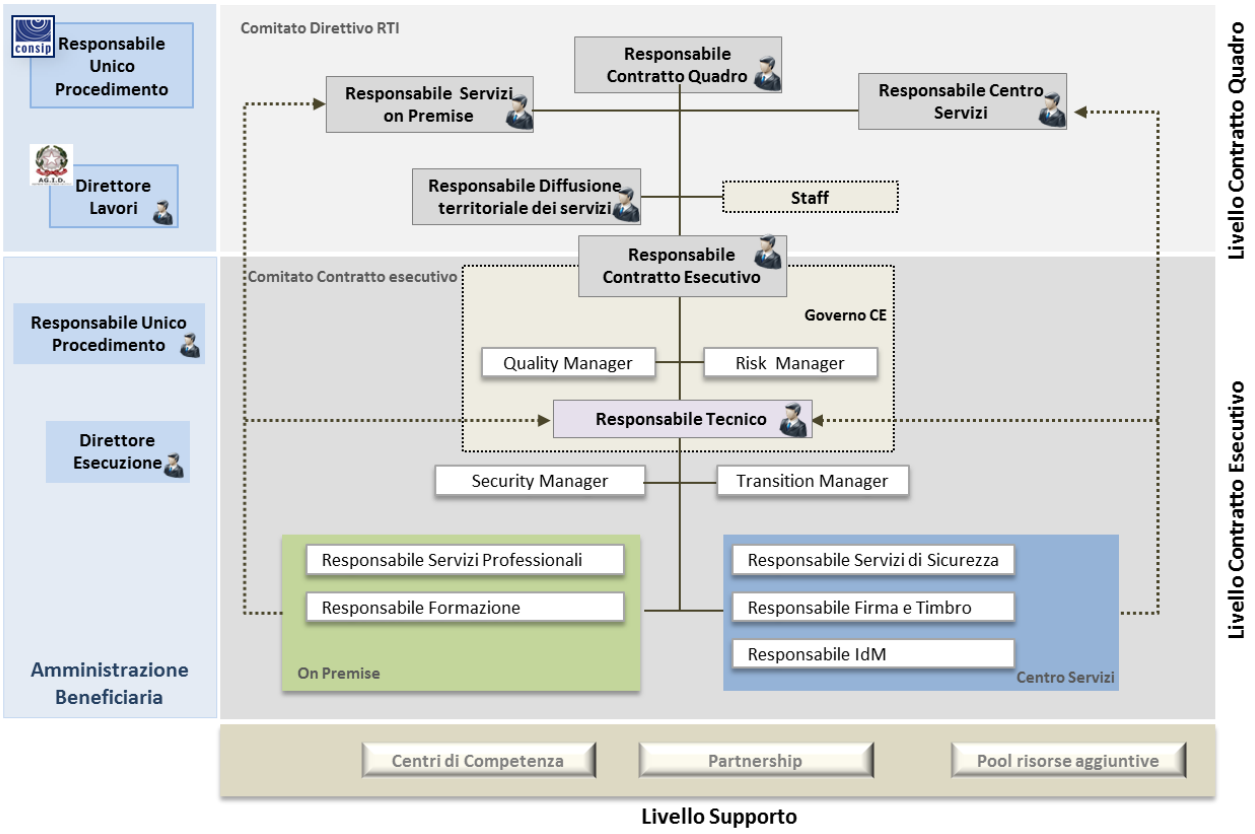


Figura 1: Modello organizzativo proposto

Il modello proposto per rispondere a tutti i requisiti previsti dalla Gara lungo l'intero ciclo di vita del CQ e per **adattarsi** efficacemente alle **diverse tipologie di Amministrazioni** ed ai vari CE.

Il modello si articola su tre livelli:

- Livello di governo del **Contratto Quadro**, che rappresenta il livello di organizzazione più elevato per la gestione e il coordinamento dell'intera Fornitura. È costituito dal **Comitato Direttivo** del RTI che rappresenta una struttura centralizzata affidata al **Responsabile del CQ** che svolge un'azione di indirizzo e controllo strategico in un'ottica di gestione unitaria dei CE stipulati con il RTI. Il Comitato Direttivo è responsabile sia della conduzione della fornitura nel suo complesso sia dell'intera struttura organizzativa; ha una visione unica ed integrata dell'andamento della Fornitura ed assicura la qualità complessiva dei CE erogati per conseguire la piena soddisfazione delle Amministrazioni;
- Livello del **Contratto Esecutivo**, che coordina ed eroga i servizi previsti per ogni CE attraverso il **Responsabile del CE**. Questa figura, le cui responsabilità sono dettagliate nel successivo paragrafo, svolge anche compiti di raccordo tra i due livelli. Il livello comprende tutte le risorse (Figure Apicali del RTI e risorse costituenti i team), le strutture operative e le strutture di supporto impiegate nell'esecuzione dei servizi. È progettato per **adattarsi** alle diverse tipologie di Amministrazioni che aderiranno, garantendo la qualità e fornendo la maggiore flessibilità possibile per l'erogazione dei servizi.
- Livello di **Supporto** all'erogazione dei Servizi: comprende, oltre ai Centri di Competenza delle aziende del RTI, Partnership aziendali, Community Practice, Collaborazioni con ambienti Universitari e scientifici di cui ciascuna azienda dispone su tematiche tecnologiche, funzionali e di processo. Tali relazioni consentono al RTI di supportare AgID, Consip e le Pubbliche Amministrazioni nelle attività di definizione e gestione di soluzioni particolarmente innovative, coadiuvando, ove opportuno, anche il RTI durante la fase di erogazione.

3.2.1 Adattabilità del modello organizzativo

Il modello, rappresentato in Figura 1, è stato progettato per introdurre e definire tutti i **ruoli di Governo** che il RTI ritiene **necessari per la corretta gestione ed esecuzione** dei servizi oggetto del CQ con i quali intende garantire **elementi di stabilità** per l' efficace governo della fornitura anche in termini di monitoraggio e rendicontazione (cfr. § 5.2) - sia a livello di CQ sia a livello di ciascun singolo CE - agevolando la relazione verso Consip, AgID e l'Amministrazione beneficiaria, il controllo di qualità e la massima condivisione delle conoscenze. Il modello

consente d'altro lato di introdurre anche **elementi di flessibilità e modularità** che permettono di adattarlo alle diverse esigenze degli specifici Enti della PA, tenendo conto di alcuni parametri individuati dal nostro RTI come significativi per rappresentare il **contesto tecnologico ed organizzativo** delle Amministrazioni ai fini di un efficace erogazione dei servizi.

Un **primo parametro** è la **dislocazione geografica del presidio del RTI** che è in grado di supportare Amministrazioni distribuite sull'intero territorio grazie alla numericamente significativa presenza e distribuzione delle sue sedi. Nel caso di PAC o PAL di dimensione significativa il presidio sarà generalmente effettuato dalle strutture di "Key Account" centrali e dedicate, sia commerciali sia tecniche; mentre nel caso delle PAL o degli altri enti locali il presidio è assicurato dalle molteplici e capillari strutture locali che il RTI coordinerà per garantire la migliore copertura. Il **numero** di Amministrazioni potenzialmente interessate ai servizi, **secondo parametro**, costituisce naturalmente un fattore rilevante che il RTI ha considerato per definire livello di adattabilità, flessibilità ed effort necessari per rispondere appropriatamente alle richieste che possono provenire da Amministrazioni eterogenee e variamente distribuite sul territorio. Il **terzo parametro** è la presenza all'interno delle diverse tipologie di Amministrazioni di una **Organizzazione IT strutturata**, sotto forma di una specifica funzione definita a livello di organizzazione con risorse dedicate. Il **quarto parametro** è la **Maturità digitale della PA**, ovvero la sua capacità di valutare l'impatto sui propri processi della digitalizzazione e dell'adozione di nuovi servizi ICT, che dipende dalla dimensione dell'organizzazione, dal grado di innovazione già presente, dalla natura del servizio erogato e dalla tipologia degli interlocutori tra cittadini ed imprese. Il **quinto parametro** è dato dal potenziale di aggregazione delle PAL in quanto Amministrazioni che intendono intraprendere un percorso di aggregazione rappresentano una significativa opportunità di allineamento dei servizi inizialmente in ottica di interoperabilità, poi allo scopo di favorire la standardizzazione ed in ultimo per effettuare il consolidamento di applicazioni, tecnologie ed infrastrutture. I servizi oggetto del Contratto sono disponibili da subito per favorire i primi due passi di questo percorso e possono notevolmente agevolare il consolidamento finale, a cui il RTI può significativamente contribuire in termini di supporto.

Il **sesto parametro** che il RTI ha ritenuto di dover considerare è dato dalla tipologia e dal mix di servizi richiesti che consente di poter disporre di un alto grado di efficienza organizzativa nell'erogazione degli stessi coprendo servizi multipli erogati per la stessa Amministrazione, che può così beneficiare di procedure unificate, strutture dedicate, punti di contatto unitari e di maggiore efficienza grazie alla sinergia tra le strutture che supportano l'Amministrazione.

Le diverse tipologie di contesti organizzativi e tecnologici con cui ci si potrà trovare ad interagire nell'ambito contrattuale sono, secondo il RTI, tutte fondamentalmente valutabili sulla base della composizione di questi parametri, identificando situazioni che vanno dalle più **complesse** alle più **semplici**; ad esempio: centralizzazione con massima delega al RTI, oppure centralizzazione con collaborazione operativa tra PA e RTI, oppure decentralizzazione con interazione solamente remota oppure progettazione congiunta di interventi evolutivi, ecc. ecc. L'analisi condotta ha quindi portato il Raggruppamento ad identificare un modello organizzativo costruito per interagire con le Amministrazioni potendo introdurre gli "adattamenti" opportuni per operare al meglio verso le diverse tipologie di interlocutori secondo tutte le dimensioni/parametri sopra introdotti.

Il modello realizzato individua quindi, sulla base delle dimensioni indicate, gli impatti sulle attività del RTI in termini **relazionali, operativi** e sui **processi di supporto** alle PA. In particolare traguarda, in termini **relazionali,** da un lato l'allineamento delle strutture dedicate del RTI che già gestiscono continuativamente relazioni commerciali e tecniche con gli enti centrali e dall'altro l'utilizzo complementare delle singole capacità e strutture periferiche delle Aziende costituenti a copertura capillare dell'intero territorio.

In termini **operativi** prevede un'erogazione flessibile e scalabile dei servizi, sia in termini tecnologici sia di organizzazione per l'erogazione (Centro Servizi). In termini di **supporto** alle Amministrazioni ciascun servizio verrà attivato ed erogato mediante un **processo strutturato** che comporta le fasi di "Proposizione e Acquisizione dei servizi", di " Attivazione Contratto Esecutivo e Configurazione" ed infine "Gestione/Utilizzo": queste devono essere opportunamente adattate per la classe di Amministrazione interessata.

La tabella seguente rappresenta in modo sintetico e completo la flessibilità e le variabilità inseribili nel modello per ciascuna tipologia di **contesto tecnologico ed organizzativo** identificato sulla base della **composizione delle dimensioni** precedenti in un **range** che va **da Complesso a Semplificato**. Tutte le indicazioni della tabella possono essere gestite nell'ambito delle strutture previste per il CE, permettendo di ottimizzare il modello di relazione ed ingaggio, la composizione dei team e l'efficacia operativa sulla base delle dimensione sopra analizzate.

Tabella 2: Fasi del processo di supporto organizzativo

<table>
<tr><th></th><th>Contesto tecnologico ed organizzativo</th><th colspan="4">Fase del processo di supporto organizzativo</th></tr>
<tr><th></th><th></th><th colspan="2">Proposizione e Acquisizione</th><th colspan="2">Attivazione e Configurazione</th><th>Erogazione del servizio</th></tr>
<tr><td rowspan="2">Principali interlocutori</td><td>Complesso</td><td rowspan="2">Responsabile Diffusione Territoriale dei Servizi</td><td>Responsabili Commerciali</td><td rowspan="2">Responsabile CE
Responsabile Tecnico</td><td>Responsabili Tecnici dedicati</td><td rowspan="2">Responsabile Centro Servizi
Responsabile Servizi on Premise
Responsabile Tecnico CE</td></tr>
<tr><td>Semplificato</td><td>Funzione Commerciale Strutture territoriali</td><td>Funzione Tecnica Strutture territoriali</td></tr>
<tr><td rowspan="2">Modello di interazione del RTI con la PA per Servizi “as a Service”</td><td>Complesso</td><td>Allineamento dei contenuti e dell'approccio dei Responsabili Commerciali del RTI verso i Referenti della PA, via canali e relazioni già consolidate</td><td rowspan="2">Supporto alla Definizione del Piano e collaborazione alla redazione del Progetto dei Fabbisogni da parte del RTI</td><td colspan="2" rowspan="2">Svolgimento delle attività di implementazione del Progetto dei Fabbisogni con attivazione delle componenti opportune del Centro Servizi</td><td rowspan="2">Servizio scalabile e flessibile in termini tecnologici e di delivery da Centro Servizi</td></tr>
<tr><td>Semplificato</td><td>Collaborazione tra le Funzioni commerciali delle strutture territoriali delle aziende del RTI</td></tr>
<tr><td rowspan="2">Modello di interazione del RTI con la PA per Servizi “On Premise”</td><td>Complesso</td><td>Allineamento dei contenuti e dell'approccio dei Responsabili Commerciali del RTI verso i Referenti della PA, via canali e relazioni già consolidate</td><td rowspan="2">Supporto alla Definizione del Piano e collaborazione alla redazione del Progetto dei Fabbisogni da parte del RTI</td><td colspan="2">Allineamento delle attività dei referenti tecnici del RTI già attivi nel contesto operativo delle strutture IT delle PA, al fine di efficientare l'erogazione e proporre l'innovazione dei servizi del RTI</td><td>Team stabili di esperti che collaborano con l’Amministrazione in continuità</td></tr>
<tr><td>Semplificato</td><td>Collaborazione tra le Funzioni commerciali delle strutture territoriali delle aziende del RTI</td><td colspan="2">Figure professionali multi-disciplinari distribuite sul territorio supportate da figure di eccellenza dei Centri di Competenza del RTI</td><td>Figure professionali multi-disciplinari distribuite sul territorio</td></tr>
<tr><td rowspan="2">Flessibilità della Governance</td><td>Complesso</td><td colspan="2" rowspan="2">In questa fase della Governance si applica sempre il processo standard definito dal RTI.
La personalizzazione della Governance è oggetto della fase di Configurazione dei servizi</td><td rowspan="2">Definizione modello per la governance del Contratto Esecutivo</td><td>Identificazione degli interlocutori PA e definizione dei canali di comunicazione</td><td>Interlocutori singoli con ruoli definiti secondo il modello organizzativo che si interfacciano con corrispettivi nella struttura della Amministrazione</td></tr>
<tr><td>Semplificato</td><td>Definizione dello SPOC e dei canali di comunicazione</td><td>SPOC di presidio per tutti i ruoli organizzativi con una singola interlocuzione che semplifica la relazione, garantisce efficienza e qualità della gestione operativa, favorendo comunicaz. ed evoluzione</td></tr>
</table>

L’obiettivo generale del RTI con l’applicazione di questo modello flessibile ed adattabile è di promuovere l’innovazione tecnologica introdotta dai servizi oggetto della Gara presso tutte le Amministrazioni, indipendentemente dal loro grado di maturità e di strutturazione. Questo obiettivo è congruente con le indicazioni del legislatore Comunitario (vedi Regolamento EIDAS) e Nazionale che sta introducendo progressivamente norme e strumenti (CAD, Agenda Digitale Italiana, Agenzia per l’Italia Digitale) per promuovere

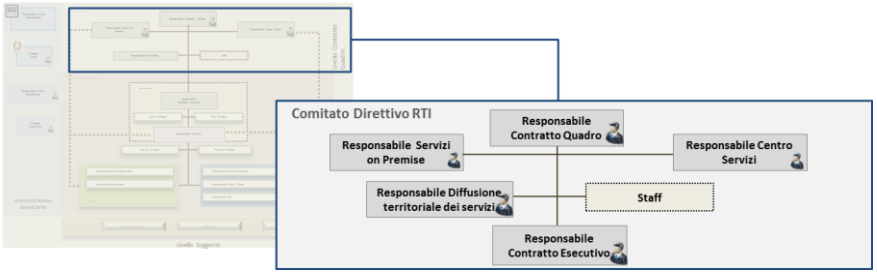
una riforma digitale della Pubblica Amministrazione, al fine di instaurare la fiducia da parte dei cittadini e delle imprese verso gli ambienti on line.
I paragrafi successivi dettagliano per ciascuno dei livelli rappresentati nel modello, ruoli, responsabilità e strutture che il RTI si impegna ad utilizzare per il Governo del CQ, dei singoli CE e del rapporto con AgID/Consip e le Amministrazioni.

3.2.2 Ruoli, responsabilità e referenti

Il RTI nella definizione della struttura organizzativa ha non solo recepito puntualmente le indicazioni e i requisiti presenti negli atti di gara ma, a migliore garanzia dell'efficacia e del monitoraggio delle operazioni, ha introdotto **ruoli** e **funzioni aggiuntive**, come nel seguito specificato. I ruoli sotto descritti saranno **continuativamente operativi** lungo tutto il ciclo di vita della fornitura a garanzia della continuità operativa e di governo del RTI.

3.2.2.1 Ruoli e Responsabilità Livello Contratto Quadro

Il **Comitato Direttivo** di **RTI** nasce con l'obiettivo di coniugare molteplici funzioni, ritenute necessarie e qualificanti dal RTI per gestire tutte le fasi del ciclo di vita del CQ e della successiva erogazione dei CE.
Il **Comitato Direttivo** di **RTI** è composto dal Responsabile del CQ, dal Responsabile del Centro Servizi, dal Responsabile dei Servizi on Premise, dal Responsabile Diffusione territoriale dei Servizi e dai Responsabili dei CE ed è coadiuvato da un insieme di figure di alto profilo organizzate in una struttura di **Staff**.



Il Comitato **è continuativamente attivo ed operativo** per tutta la durata del CQ e prevede incontri con cadenza almeno settimanale. Nel seguito ne sono descritte le figure e i ruoli.

Ruolo	Caratteristiche e Responsabilità
Responsabile CQ	Garantisce l'omogeneità e l'uniformità di interfaccia verso Consip/AgID/Amministrazione a livello di Governo del CQ vigilando sull'osservanza di tutte le indicazioni operative, di indirizzo e di controllo, che a tal scopo potranno essere predisposte da Consip e/o da AgID, per quanto di rispettiva competenza. Rappresenta, insieme al Responsabile del Centro Servizi, il RTI nel Comitato di Direzione Tecnica coinvolgendo, se necessario, figure presenti nella propria organizzazione. Per ricoprire questo ruolo il RTI ha individuato un professionista della Mandataria del Raggruppamento con più di 20 anni di anzianità lavorativa, autorevolezza ed esperienza pluriennale in progetti complessi e di grandi dimensioni, in contesti organizzativi complessi, sia a livello nazionale che internazionale, esperienza nella gestione di Accordi Quadro, **certificato PMI, COBIT e ITIL** con una notevole esperienza nel ruolo di Program Manager e di Direttore di Area Operativa.
Responsabile Centro Servizi	Coordina tutte le attività necessarie all'erogazione dei servizi previsti, ivi comprese quelle relative alla sicurezza. Nella fase di attivazione di un CE si coordina con il Responsabile tecnico dello specifico contratto nominando per ciascuna delle Amministrazioni Beneficiarie il Responsabile del Servizio richiesto dedicato all'Amministrazione stessa. Per questo ruolo il RTI ha scelto un professionista con più di 20 anni di anzianità lavorativa, esperienza nella gestione di Accordi Quadro, **certificato PMI e ITIL** e **ISO 27001**.
Responsabile Servizi on Premise	Ha il compito e la responsabilità di coordinare tutte le attività necessarie all'erogazione dei servizi previsti in modalità "on premise". Nella fase di attivazione di un CE si coordina con il Responsabile Tecnico, che costituisce il punto di riferimento per l'attivazione di nuovi servizi. Per questo ruolo il RTI ha scelto un professionista con più di **20 anni di anzianità lavorativa**, esperienza nella gestione di Accordi Quadro, **certificato PMI** e **ITIL.**
Responsabile Diffusione territoriale dei Servizi (aggiuntivo)	Per meglio soddisfare le specifiche esigenze che caratterizzano i contesti tecnologici e organizzativi delle Amministrazioni, il modello organizzativo prevede la **figura aggiuntiva** del **Responsabile Diffusione territoriale dei Servizi**, che fa parte del Comitato Direttivo RTI. Il Responsabile ha il compito di individuare ed organizzare, per la specifica fase di proposizione verso le Amministrazioni il team con competenze commerciali e tecniche che meglio indirizzano l'iniziativa specifica, all'interno delle strutture territoriali. Tali strutture sono articolate in Funzioni Commerciali e Funzioni Tecniche di Prevendita, che coprono efficacemente il territorio grazie alla presenza capillare delle Aziende del RTI. Il team supporta le Amministrazioni nella fase di redazione del piano di Fabbisogni e produce successivamente il Progetto dei Fabbisogni. In accordo con il Responsabile del CQ individua e coordina i **Procuratori** che hanno facoltà, se delegati dal Responsabile del CQ, di stipulare i CE con le Amministrazioni.

Responsabile Contratto Esecutivo	Partecipa, riporta e allinea il Comitato Direttivo rispetto alle attività, all'andamento e ai risultati del proprio Contratto Esecutivo.

Di seguito la descrizione delle **strutture organizzative** che sottendono all'organizzazione rappresentata.

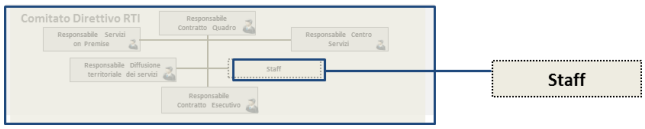
Strutture Territoriali (Responsabile Diffusione territoriale dei Servizi) : È una struttura centralizzata e condivisa a livello di RTI che si articola in Funzioni Commerciali e Funzioni Tecniche di Prevendita territorialmente distribuite grazie alla capillarità del presidio delle funzioni commerciali e delle sedi operative. In queste sono concentrate le competenze tecniche da ingaggiare nella fase di supporto alla redazione dei Piani di Fabbisogno e successivamente, attraverso l'attivazione delle unità operative e/o dei Centri di Competenza delle nostre Aziende per la stesura del Progetto dei Fabbisogni.

Direzione Commerciale *Nord, Centro, Sud*	È costituita dalle strutture commerciali capillarmente distribuite sul territorio nazionale presso le sedi delle aziende. Si compone di Responsabili commerciali dedicati alle Amministrazioni beneficiarie che dispongono di know how e conoscenze dei contesti presso i quali andare a posizionare i servizi oggetto del presente CQ.
Unità operative di Progettazione *Nord, Centro, Sud*	È costituita dalle strutture tecniche e di prevendita distribuite sul territorio nazionale presenti presso le sedi delle tre aziende. Si compone di Figure di alto profilo che dispongono di know how e competenze specifiche dei contesti del presente CQ maturate grazie alle attività svolte presso le specifiche Amministrazioni.

Centro Servizi (Responsabile Centro Servizi) : Per la descrizione puntuale del Centro servizi si faccia riferimento al §3.3

STAFF - Ruoli di supporto al Comitato Direttivo RTI

La struttura di Staff supporta il Comitato Direttivo RTI in controllo, indirizzamento e coordinamento delle varie componenti del CQ e dei CE, per tutte le problematiche e gli aspetti di carattere trasversale.

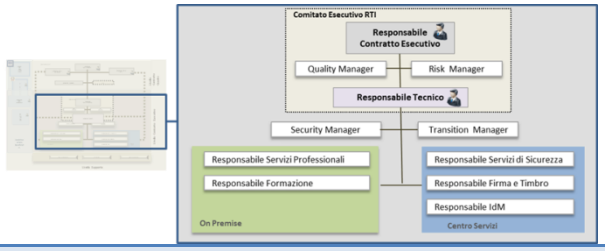


Struttura Staff	Caratteristiche e Responsabilità
Responsabile PMO (aggiuntivo)	È un Program Manager della Mandataria specializzato nella gestione di grandi progetti e di team di lavoro di dimensioni significative, attivo per tutti gli aspetti tecnici e operativi relativi alle attività dei CE. Si dedica, allineandosi con gli altri Responsabili della struttura di Staff, alla pianificazione e consuntivazione della Fornitura, alla predisposizione dei Piani di Lavoro e di Servizio, al controllo dei mix di risorse utilizzati nei servizi, analizzandone gli scostamenti rispetto alla pianificazione. Possiede le **certificazioni PMI e COBIT**.
Responsabile Resource Management (aggiuntivo)	È il Resource Manager del RTI dedicato alla ricerca, assegnazione e gestione qualitativa e quantitativa delle risorse impiegate nei team stabili per la fornitura dei servizi oggetto dei CE. Ha in gestione il Repository dei curricula che ogni Azienda mette a disposizione attraverso la soluzione di **Skill Inventory** per l'individuazione e l'allocazione di nuove risorse con competenze specifiche. Gestisce le risorse aggiuntive necessarie per azioni di rinforzo dei team per attività non pianificate o per rotazione. Pianifica e coordina le attività di formazione delle risorse del RTI impiegate nella fornitura.
Responsabile Gestione Contratti (aggiuntivo)	É la figura del RTI deputata a supportare il Responsabile del CQ per tutte le attività contrattuali. Si occupa della produzione e della gestione della documentazione contrattuale legata alla stipula dei CE e rappresenta inoltre il punto di riferimento per la gestione delle richieste di tipo contrattuale e/o amministrativo provenienti dall'Help Desk anche nella fase propedeutica alla stipula dei CE.
Responsabile Qualità (aggiuntivo)	Questa figura è stata inserita all'interno del modello organizzativo a livello di staff in quanto il RTI ha la convinzione che la garanzia della reale efficacia della Fornitura debba essere misurabile in maniera oggettiva, come pure debba essere riscontrabile il processo di continuo miglioramento. Pertanto il RTI ha inteso impiegare una figura centralizzata per il RTI che predispone e gestisce il Piano di Qualità generale richiesto entro 30 gg lavorativi dalla stipula del CQ e supporta il Responsabile del CQ nella gestione degli aspetti di qualità. Interagisce con i referenti indicati dalla Committenza per le attività di Audit. Riceve, controlla e coordina i Piani di Qualità relativi ai singoli Contratti recependoli dai Quality Manager di ogni CE. La figura di Responsabile Qualità proposta dal RTI ha un'esperienza ventennale nella gestione sia di contratti similari per la PA sia nella definizione, implementazione e audit di SGQ aziendali. Ha competenze in materia di pianificazione e gestione degli obiettivi di qualità e di controllo e verifica dei livelli di servizio contrattuali. La figura proposta ha una certificazione di **"Valutatore Sistemi di Gestione per la Qualità (corso qualificato CEPAS e AICQ-SICEV)"**, attestati di frequenza di corsi base **CMMI**, ed inoltre viene annualmente formata, internamente all'azienda, su metodologie per la gestione del monitoraggio e miglioramento dei contratti che sulla Gestione del rischio delle forniture.
Responsabile Sicurezza	É il riferimento unico del RTI per tutti gli aspetti legati alla sicurezza. Conduce assessment per supportare le Amministrazioni nelle modifiche ai Piani della Sicurezza ICT e successive modifiche; garantisce l'applicazione

	delle misure di sicurezza lungo tutta la filiera operativa, gestisce in prima persona gli incidenti di sicurezza. Attraverso questa funzione il RTI si impegna ad assicurare a Consip ed alle Amministrazioni Beneficiarie la sicurezza sia fisica che logica per tutti i servizi oggetto dei CE predisponendo, attuando ed aggiornando costantemente una politica della sicurezza, sia fisica che logica, conforme alle prescrizioni contenute nel Capitolato Tecnico, con particolare riferimento alla Parte Generale di detta documentazione. Al Responsabile spetta la responsabilità relativa alla produzione, emissione e formalizzazione, entro i termini previsti nei documenti di gara (Capitolato Generale par. 4.2.4 e par. 7.2.5), dei documenti richiesti per dettagliare le modalità di attuazione di tutti i requisiti di sicurezza. Possiede certificazioni specifiche di sicurezza quali **CISA, CISM, CISSP e CRISC**.
Responsabile Innovazione tecnologica (aggiuntivo)	Costituisce il riferimento unico per il RTI nei confronti di Consip, AgID e Amministrazioni per tutti gli aspetti legati agli standard tecnologici. La sua funzione è di promuovere e supportare l'innovazione tecnologica a livello strategico avendo approfondite competenze e conoscenze del CAD. Recepisce gli standard tecnologici di AgID, suggerisce integrazioni seguendo le tendenze tecnologiche del mercato. È stata inserita dal RTI nel modello organizzativo per proporre tecnologie e modelli di servizio innovativi, lanciati sul mercato dalle Aziende del RTI o identificati come trend emergenti, anche con workshop informativi; suggerisce iniziative di evoluzione utili per la fornitura, anche attraverso studi di fattibilità.
Responsabile Continuità Operativa (aggiuntivo)	Rappresenta il punto di contatto/riferimento per la segnalazione e la predisposizione di tutte le attività necessarie a ridurre l'impatto di un'emergenza ICT che possa compromettere l'erogazione dei servizi alla PA. Reagisce prontamente ed in maniera efficace in caso di interruzione delle funzioni ICT causati da disastri (dovuti ad attacchi o eventi naturali) o causati da errori/malfunzionamenti di processi, sistemi applicazioni, infrastrutture. È responsabile del mantenimento e degli aggiornamenti periodici del Piano di Continuità Operativa e del Piano di Disaster Recovery. È una risorsa certificata ITIL.
Responsabile Transition (aggiuntivo)	È il riferimento unico del RTI nei confronti di Consip e AgID del coordinamento delle fasi di Phase-in e Phase-Out di ciascun CE e delle attività necessarie a garantire alla Committente la migrazione di tutti i servizi al termine del CQ attraverso la condivisione del "Piano di Trasferimento Globale". A supporto della produzione dei "Piani di Trasferimento" della singola Amministrazione e del "Piano di Trasferimento Globale", predispone e mantiene il "Modello Generale per il Phase out" contenente approcci, metodi, soluzioni tecnologiche e il documento "Revisione Metodica degli Standard" che garantisce l'allineamento di standard di portabilità e interoperabilità. È una risorsa del RTI con certificazione PMI e ITIL con esperienza decennale nella pianificazione, gestione coordinamento di attività di presa in carico e trasferimento a fine fornitura per Contratti verso la PA.
Responsabile Gestione del Rischio (aggiuntivo)	È il responsabile unico e garante per il RTI della corretta applicazione delle metodologie di individuazione, mitigazione e monitoraggio del rischio. Collabora con il Responsabile Unico delle Attività contrattuali nella gestione proattiva dei rischi e dei relativi piani di mitigazione o azioni di miglioramento. Controlla l'andamento del CQ coordinandosi con i singoli Risk Manager con particolare attenzione alla rilevazione dei rischi e conseguente proposta di azioni di recovery, alla verifica dei risultati e al reporting.
Responsabile dei dati personali	Responsabile ai sensi dell'art. 4, comma 1, lett. g) del decreto legislativo 30 giugno 2003, n. 196, (Codice della privacy), ed individuato tra coloro che, per esperienza, capacità ed affidabilità, fornisce idonea garanzia per il rispetto delle disposizioni vigenti in materia dei dati personali, ivi compreso il profilo della sicurezza.

3.2.2.2 Ruoli e Responsabilità Livello Contratto Esecutivo

Il RTI applicherà per il governo del singolo CE e per l'erogazione operativa dei relativi servizi il modello organizzativo, rappresentato di lato, ottimizzandolo in funzione delle dimensioni, del contesto e del perimetro funzionale e tecnologico dell'Amministrazione. Nel seguito ne sono descritte le figure e i ruoli.



Ruolo	Caratteristiche e Responsabilità
Responsabile Contratto Esecutivo	Costituisce l'interfaccia unica verso il Responsabile del Procedimento dell'Amministrazione Beneficiaria. L'insieme dei Responsabili di ciascun CE, nel caso di più di un'aggiudicazione, si riunisce periodicamente nel Comitato Direttivo presente a livello di CQ per condividere informazioni e situazioni generali e per allinearsi con il Responsabile del CQ e le funzioni di staff. I Comitati Direttivi saranno convocati in funzione delle specifiche esigenze dei CE oppure per tipologia di servizi oggetto di allineamento o approfondimento.
Quality manager (aggiuntivo)	Supporta il Responsabile del CE nella gestione degli aspetti di qualità relativi agli specifici servizi oggetto del Contratto stesso. Interagisce e si allinea con il Responsabile della Qualità a livello di CQ per le attività afferenti il proprio contratto. Produce i Piani della Qualità e le successive revisioni. La figura proposta ha una certificazione di **"Valutatore Sistemi di Gestione per la Qualità (corso qualificato CEPAS e AICQ-SICEV)"**.
Risk Manager (aggiuntivo)	Costituisce la figura del RTI che supporta il Responsabile del CE nell'identificare e gestire i potenziali rischi associati alla fornitura dei servizi oggetto del proprio contratto per prevenirli e, nel caso non fosse possibile,

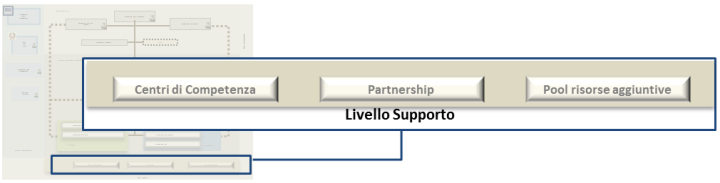
Ruolo	Caratteristiche e Responsabilità
	mitigarli e monitorarli. Interagisce e si allinea con il Responsabile Gestione del Rischio a livello di CQ per le attività afferenti il proprio contratto. Viene annualmente formata, internamente all'azienda, su metodologie sulla Gestione del rischio delle forniture.
Responsabile Tecnico	È il Responsabile unico delle attività tecniche e del raggiungimento degli obiettivi dei servizi oggetto del Contratto. Costituisce l'interfaccia unica verso il Direttore Esecuzione nominato dall'Amministrazione. Ha la visione complessiva e integrata di tutte le attività tecniche legate all'attivazione, all'erogazione e al rilascio dei servizi della fornitura e ne garantisce la qualità. Ottiene dalle aziende del RTI le risorse e i contributi necessari per conseguire gli obiettivi della fornitura. Si coordina in fase di attivazione di un CE con il Responsabile del Centro Servizi e con il Responsabile dei Servizi on Premise, attivando il Responsabile della linea di servizio oggetto di fornitura. A lui riportano tutti i Responsabili dei Servizi o gruppi di servizi. Possiede certificazione **PMI**.
Security Manager	È il riferimento unico del Responsabile Tecnico per tutti gli aspetti legati alla sicurezza del singolo CE. Riferisce e riporta a livello di CQ al Responsabile della Sicurezza. Possiede certificazioni specifiche di sicurezza quali CISA, CISM, CISSP.
Transition Manager (aggiuntivo)	Governa e controlla lo svolgimento delle singole attività in cui si articola il processo di Phase-in e di Phase-out del proprio CE. Coordina le attività di affiancamento monitorando il rispetto del piano di subentro. Verifica lo stato di avanzamento del processo e analizza i KPI col supporto del Quality Manager del proprio CE. In caso di scostamento dalla pianificazione propone ai Responsabili di Servizio, col supporto del Risk Manager, azioni preventive e/o correttive in grado di ripristinare la situazione (Risk Management). Riporta e allinea il Responsabile Transition a livello di CQ.
Responsabili Servizio: IdM, Firma / Timbro, Servizi di Sicurezza e Professionali	Il responsabile di ciascun servizio o gruppo di servizi coordina dal punto di vista operativo tutte le attività legate ai servizi di competenza e costituisce il punto di riferimento per l'attivazione di nuovi servizi. Produce i resoconti periodici, da presentare per discussione durante i SAL. Ciascun Responsabile di servizio riporta al Responsabile Tecnico. Avranno oltre 15 anni di anzianità lavorativa, esperienza pluriennale nella gestione e coordinamento di risorse umane, di progetti complessi e di gruppi di lavoro di grandi dimensioni, capacità relazionali, **certificazioni PMI e/o ITIL,** conoscenze consolidate nell'ambito del servizio in termini di processi, metodi e strumenti.

Di seguito la descrizione delle strutture organizzative che sottendono all'organizzazione rappresentata.

Team di lavoro (Responsabile Servizio) : Ciascun Team è a diretto riporto del Responsabile del Servizio. Sono costituiti sia dai Presidi tecnici permanenti che dai Team presenti nel Centro Servizi. Sono costituiti dai Responsabili dei Servizi dedicati alle Amministrazioni per ogni CE in accordo con il Responsabile Tecnico e con il coinvolgimento del Responsabile del Resource Management di RTI presente a livello di CQ. Tutti i team del nostro RTI operano in perfetta sinergia e condividono la stessa modalità di lavoro, un linguaggio operativo comune e obiettivi di successo orientati al raggiungimento dei risultati e alla soddisfazione della committenza.

3.2.2.3 Ruoli e Responsabilità Livello Supporto

Questo livello comprende le strutture e le risorse interne ed esterne rese disponibili dalle Aziende del RTI per l'erogazione dei servizi. Il riferimento per l'ingaggio di tali strutture è il **Responsabile del Servizio** specifico.



Centri di Competenza
Responsabile del servizio

I Centri di Competenza sono considerati come un supporto totalmente integrato nell'organizzazione nel quale sono presenti forti eccellenze che indirizzano nicchie molto innovative sulle quali il contributo fornito consiste prevalentemente in un know how molto caratterizzato e caratterizzante. Un Centro di Competenza può quindi fornire sia risorse che partecipano continuativamente ai progetti, sia on-site che off prendendosi in carico anche specifici task di sviluppo software, sia fornire risorse altamente specializzate e certificate per lo sviluppo di componenti ad alta specializzazione tecnologica. La dimensione globale delle aziende del RTI e la loro importanza nel panorama nazionale ed internazionale, garantisce la presenza di **molteplici Centri di Competenza funzionali, tecnici e tecnologici**. *Nella tabella si riportano i principali Centri di Competenza che ogni azienda potrà impiegare nell'ambito della presente fornitura, e di seguito* **si privilegia la descrizione di dettaglio di solo alcuni di questi**.	Selex ES & E-Security	. *Centro di competenca di Governance Laboratorio di Analisi* . *Security Operation Center* . *Information Assurance Labs* . *Laboratorio di Malware Analysis* . Open Source Intelligence Labs . *Cyber Security Labs* . *Network Protection Labs* . *Web Portals & Mobile Applications* . *Enterprise Architecture* . *Gestione Documentale (EDCM)*
	IBM & Sistemi Informativi	. *X-Force* . *e-Government Center* . *Tivoli Labs* . *Centro di Competenza IAM* . *Java Innovation Lab* . *Interactive Experience* . *CoC Portali ed Innovazione Mobile* . *Laboratorio di Application Testing* . *Systems & Software Center*
	FASTWEB	. *NOC - Network Operation Center* . *SOC - Security Operation Center* . *Fastweb Labs: Testing e certificazione apparati/tecnologie* . *Security labs: gruppi di lavoro internazionali su tematiche di sicurezza e frodi* . *NGN: Innovazione reti geografiche e di accesso* . *Cloud competence center: Tematiche di Iaas, Saas e PaaS*

Centro di competenza IAM	Nato dalla ventennale esperienza di IBM nella realizzazione di prodotti e progetti I&AM e federazione a livello nazionale ed internazionale, vanta la presenza di quasi 100 specialisti delle tecnologie e delle problematiche di solito rilevate nell'utilizzo di tali ambienti. Vanta persone che hanno già sviluppato progetti per le Amministrazioni italiane, come il SICA, GFID, partecipazioni a progetti italiani ed europei quali SPID, Stork, Eidas ed altri. Il Laboratorio è a Roma ed è oggi una realtà complessa e all'avanguardia in alcuni tra i settori più strategici del mondo IT, dove lavorano persone impegnate in attività di sviluppo, servizi, supporto alle vendite e ai clienti. Con l'acquisizione di CrossIdeas azienda italiana leader nei prodotti per l'identity governance, il laboratorio di IBM Italia sarà responsabile degli sviluppi sul prodotto di Identity Governance. Tale prodotto rappresenta uno dei punti di forza dell'offerta di IBM nell'area sicurezza. IBM è uno dei quattro membri fondatori del gruppo OASIS.
Centro di Competenza di Governance	Le aree di specificità del Centro di competenza vanno da attività di Risk Assessment, Audit, GAP Analysis, Guida alle certificazioni, Privacy, Disaster Recovery & Business Continuity, Training and Awareness e Security Design Review and Remediation Il personale del centro possiede una varietà di certificazioni specifiche di settore come Lead Auditor ISO 27001, Lead Auditor BS 25999, CISA - Certified Information Systems Auditor, CISM – Certified Information Security Manager, CRISC – Certified in Risk and Information System Control, CISSP – Certified Information System Security Professional, GIAC–CFA Global Information Assurance Certification - Certified Forensics Analyst (SANS Institute – USA). Il Centro ha una lunga esperienza nell'area del Risk Assessment e ha sviluppato una metodologia di Analisi del Rischio proprietaria (MIGRA - Metodologia Integrata per la Gestione del Rischio Aziendale).
Centro di competenza sicurezza gestita	Nato dall'esperienza Selex ES nella fornitura di questo tipo di servizi, vanta oltre 100 professionisti a livello internazionale, per indirizzare progetti, servizi e problematiche relative alla sicurezza perimetrale, degli end point e dei data center, tramite servizi di sicurezza gestiti. Il Security Operation Center, inaugurato nella sua nuova sede nel 2014 da funzioni Istituzionali.

Centro di competenza intelligence	Nato dall'esperienza di Selex ES nella realizzazione di sistemi di intelligence per fonti aperte/chiuse, vanta professionisti nelle attività di intelligence sia CLOSINT, OSINT e HUMINT e sistemi di raccolta delle informazioni, come ad esempio il centro di supercalcolo HPC di Selex ES. É orientate alla rilevazione e prevenzione delle minacce su fonti aperte. Il centro sviluppa capacità di Real-time reputation monitoring, Network analysis per attività di sorvrglianza e intelligence, Early Warning e valutazione rischi per infratrutture critiche CNI). Collabora attivamente con istituti universitari e di ricerca per la definizione di modelli matematici adattativi, eseguiti da lcentro di supercalcolo di Finmeccanica.
X-Force	il team di ricerca X-Force cataloga, analizza e conduce ricerche sulle divulgazioni delle vulnerabilità sin dal 1997. Con oltre 76.000 vulnerabilità della sicurezza catalogate, possiede il più grande database delle vulnerabilità del mondo. Questo database aiuta i ricercatori X-Force a comprendere le dinamiche che consentono la scoperta e la divulgazione delle vulnerabilità. IBM collabora con Enti Governativi, Società e Istituzioni a livello mondiale e favorisce l'adozione di open standard per rafforzare i protocolli aziendali e implementare un approccio olistico alla sicurezza. Inoltre congiunto al IBM Cyber Security Center of Excellence (CCoE), il laboratorio di R&D IBM di Beershava e dell'università Ben Gurion collabora nei temi di ricerca avanzata nell'ambito della cyber security e più in generale conduce studi sulla protezione di infrastrutture e asset critici dalle minacce cyber emergenti. La collaborazione tra IBM e l'università Ben Gurion sfrutta i punti di forza e la complementarità tra le due organizzazioni.

Partnership

Selex ES & E-Security	*Actian, Adobe Systems Italia, Checkpoint, Cisco, Entando, Ex Novell, Fortinet, IBM, Kodak Alaris, Mcafee, Microsoft, Oracle, Red Hat, RSA, Sap, Suse, Symantec, Vmware, Websense, F5*
IBM & Sistemi Informativi	*Apple, Oracle, SAP, SAS, F5, Check Point, Juniper Networks, Milestone, Workday, Salesforce, MobileIron, Brocade, Cisco, Infor, Lenovo, Microsoft, Red Hat, SUSE, Motorola Solutions, Citrix*
FASTWEB	*Cisco, Juniper, Huawei, HP, Adva, Alcatel Lucent, Brocade, Nokia Siemens, Oracle, Fortinet, Palo Alto, McAfee, Arbor networks, Dell, Stonesoft, IBM, NetApp, EMC², Fujitsu, VMWare, Microsoft, Dell, CTera*

Le aziende del RTI hanno attiva una rete di partnership, con aziende specializzate nell'erogazione di servizi ICT e con tutti i principali vendor di tecnologie in ambito data center, sicurezza e networking. Trasversalmente ad ogni struttura organizzativa, le aziende del RTI dispongono infatti di numerose partnership strategiche, tecnologiche e commerciali con i principali partner di mercato, dei quali segue costantemente di percorsi di Certificazione necessari a incrementare il livello di partnership e la qualificazione professionale del proprio organico. Tali accordi garantiscono quindi alle Amministrazioni la presenza di un'elevata disponibilità di competenze sulle rispettive tecnologie e di un livello continuo di aggiornamento. La dimensione globale delle aziende del RTI e la loro importanza nel panorama nazionale ed internazionale, garantisce la presenza di molteplici, diversificate ed importanti partnership. Fastweb, IBM e Selex ES partecipano alla associazione CLUSIT per promuovere e diffondere nel nostro paese la cultura e la consapevolezza della sicurezza informatica in tutti i suoi aspetti, in collaborazione alle consociate associazioni europee. La tabella sopra riporta le maggiori partnership applicabili al contesto del Lotto 2.

3.2.2.4 Referenti verso Consip/AgID/Amministrazioni

L'organizzazione proposta per l'interazione tra i Responsabili del RTI e Consip, AgID e le Amministrazioni deriva dall'esperienza delle aziende del RTI nell'erogazione di Contratti Quadro analoghi al presente e risponde puntualmente alle richieste avanzate nel Capitolato Tecnico – Parte Generale. Il modello intende rispondere a principi di chiarezza e semplificazione delle regole di comunicazione, oltre che alla tracciabilità delle interazioni tra i ruoli, per il monitoraggio ed il miglioramento continuo di tutti i processi di condivisione della conoscenza. Il RTI prevede che a livello di CQ i rappresentanti del Comitato di Direzione Tecnica siano il **Responsabile del CQ** e il **Responsabile del Centro Servizi** come indicato in Figura 2.

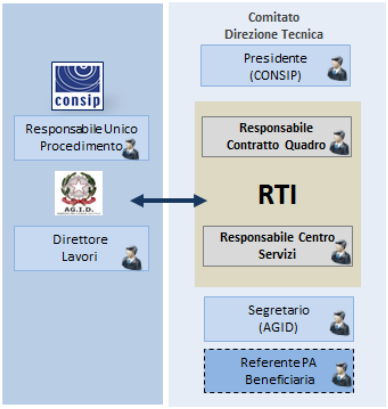


Figura 2: Referenti verso Consip/Agid/Amministrazioni

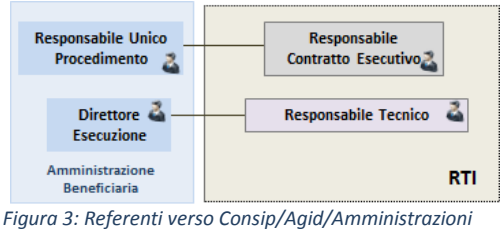


Figura 3: Referenti verso Consip/Agid/Amministrazioni

Essi potranno, laddove necessario o richiesto, convocare ulteriori figure del RTI, per supportare specifiche esigenze oppure per indirizzare problematiche specifiche. A livello di CE la Figura 3 rappresenta il modello di interazione tra i Referenti del RTI e le Amministrazioni.

3.2.3 Modalità operative dei processi gestionali

Il modello organizzativo individua univocamente i ruoli responsabili e le strutture coinvolte in ciascuna fase dei processi gestionali previsti, oltre che per l'erogazione dei servizi, anche per l'intero ciclo di vita di ciascun CE.

3.2.3.1 Processo di proposizione e acquisizione dei servizi e adesione al CE

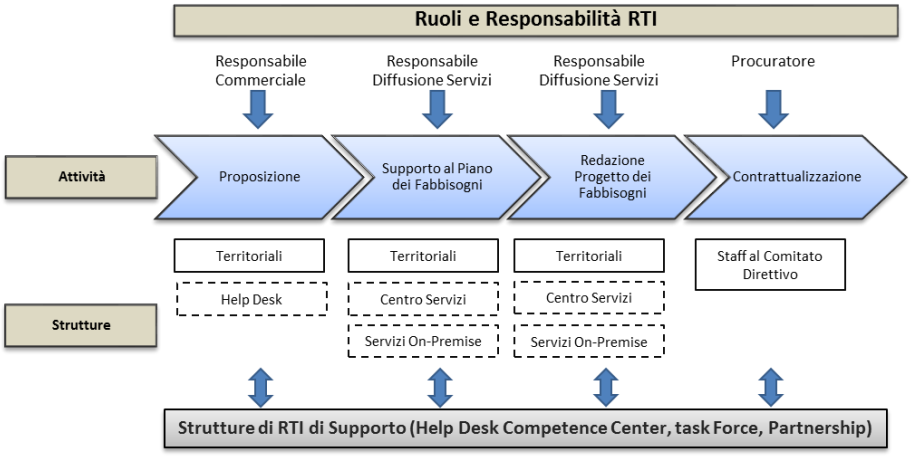


Figura 4: Flusso del Processo di proposizione e acquisizione dei servizi e adesione al CE

La responsabilità del processo di acquisizione dei servizi, che prevede l'esecuzione di ciascuna delle fasi/attività previste dal CQ per la stipula di ogni singolo CE, è assegnata, nel modello organizzativo proposto, al Responsabile Diffusione territoriale dei Servizi. che ingaggia le funzioni commerciali (Commerciale) e funzioni tecniche (Progettazione) territorialmente più appropriate. Il flusso del processo di acquisizione è descritto in tutte le sue fasi/attività nella Figura 4, con indicazione delle strutture coinvolte e dei ruoli responsabili dell'esecuzione di ciascuna attività.

3.2.3.2 Processo di attivazione e configurazione dei servizi

Il processo di attivazione dei servizi, prevede l'esecuzione di ciascuna delle fasi/attività richieste dal CE, propedeutiche alla erogazione di ciascuno dei servizi sottoscritti. Nel modello di processo proposto il Procuratore, una volta nominato il Responsabile del CE e il Responsabile Tecnico, attribuisce al primo la responsabilità dell'intero processo. Il flusso del processo di attivazione dei servizi è descritto in tutte le sue fasi/attività nella Figura 5, con indicazione delle strutture coinvolte e dei ruoli responsabili dell'esecuzione di ciascuna attività.

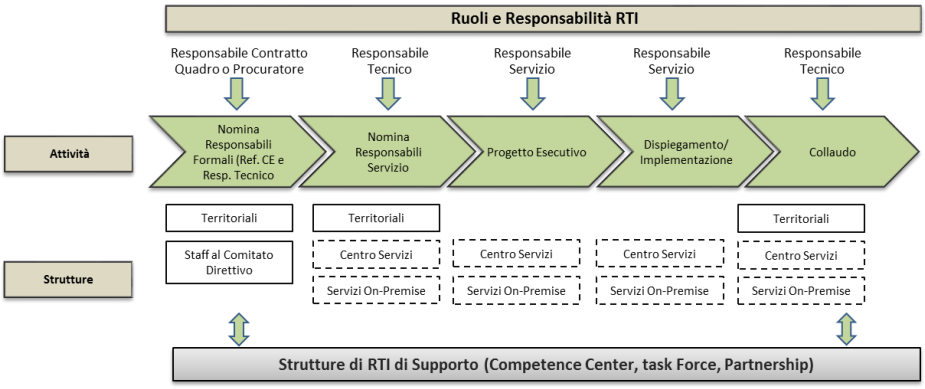


Figura 5: Flusso del Processo di attivazione e configurazione dei servizi

Mentre le prime due fasi/attività sono uniche per ciascun CE, le ultime tre si applicano a ciascun servizio sottoscritto dall'Amministrazione. È necessario sottolineare inoltre che il Responsabile del CE si occuperà degli aspetti Amministrativi. A valle del collaudo positivo da parte dell'Amministrazione (eseguito sulla piattaforma di Test Bed – cfr. § 3.3.2.2.3, nel caso di servizi che richiedano attività una tantum il servizio si ritiene terminato, mentre nel caso di servizi che richiedano attività continuative, il modello organizzativo prevede l'esecuzione del processo di Erogazione dei Servizi descritto nel paragrafo successivo.

3.2.3.3 Processo di erogazione dei servizi

Il processo prevede l'esecuzione delle attività cicliche necessarie per l'erogazione dei servizi di tipo continuativo. Tale processo, costruito sulla base del modello proprio della Best Practice ITILv3, garantisce il "Continual Service Improvement", ovvero il miglioramento continuo della qualità del servizio erogato non solo rispetto ai parametri di qualità previsti dal Capitolato Tecnico, ma anche relativamente agli indicatori tipici previsti da ITILv3.

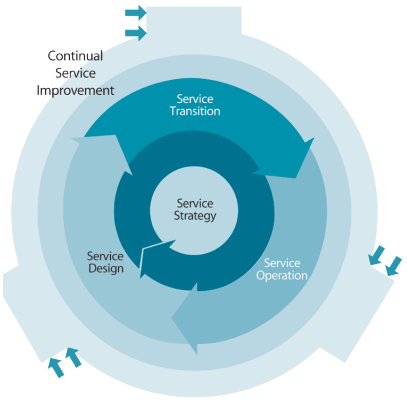


Figura 6: miglioramento continuo del servizio

3.2.3.4 Processo di Phase Out dei servizi

Il processo di Phase Out prevede l'esecuzione di ciascuna delle fasi/attività, richieste sia dal CQ che da ciascun CE, necessarie a garantire il trasferimento dei servizi e delle attività a fornitori terzi. Il dettaglio delle modalità operative e gestionali è descritto al § 4.5.

3.2.3.5 Metodologie

Il contesto metodologico nel quale saranno erogati tutti i servizi del CQ, e, in particolare i processi di governo, è un insieme collaudato ed utilizzato con successo dal RTI, di metodi e processi in grado di assicurare efficacia ed efficienza nell'esecuzione e governo delle attività, garantendo al contempo l'adattabilità al contesto e la massima flessibilità operativa.

Le aziende del RTI adottano da anni gli standard di riferimento, **ITIL** per la gestione e l'erogazione dei processi, **CObIT** per la gestione e il governo del IT interna e dei Centri Servizi, **CMMI** per la verifica del grado di maturità dei processi e servizi, oltreché le norme **ISO 27000 (ex BS-7799)** per la gestione della sicurezza delle informazioni, **ISO 22301 (ex BS-25999)** per la continuità operativa, **MIGRA** per l'analisi del Rischio.

Il RTI inoltre propone come modello di riferimento il **Knowledge Base IBM ITUP (IBM Tivoli Unified Process)** già integrato con gli strumenti adottati dalle aziende del RTI in supporto alla gestione delle infrastrutture tecnologiche ed erogazione dei servizi. In particolare, tale asset è continuamente allineato nei contenuti con i **knowledge base** delle aziende del RTI e garantisce le Amministrazioni nell'adozione delle migliori best practice di mercato e di settore.

La Figura 7 illustra la mappatura delle best practice all'interno del intero ciclo di gestione dei servizi IT.

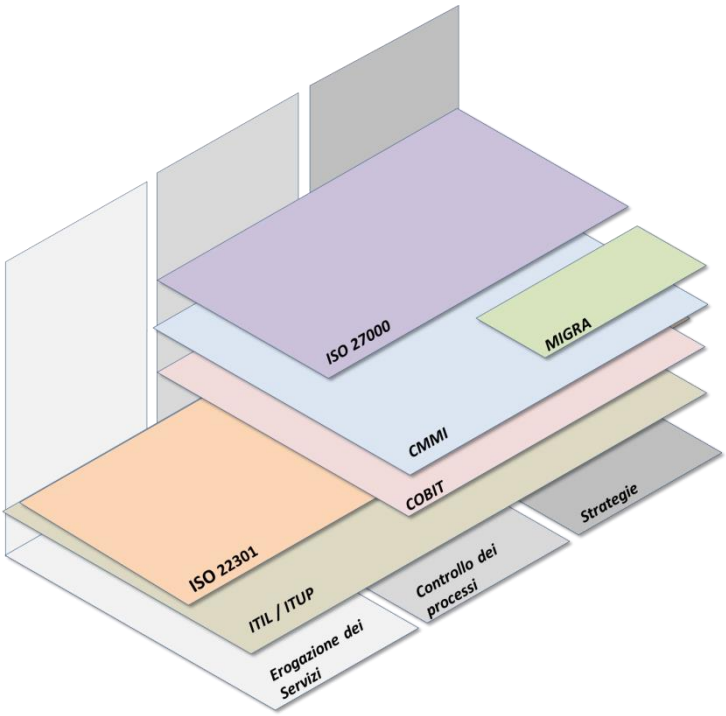


Figura 7: Framework di standards e Best Practice del RTI

L'utilizzo delle **best practice ITUP**, in aggiunta a quelle **ITIL, CObIT, CMMI e ISO 27000/22301** per la gestione del ciclo di vita dei servizi ICT consente di ► **fare leva** su consolidati standard e linee guida largamente utilizzati in tutte le fasi dei servizi, ► **accelerare** l'implementazione dei processi e ridurre i tempi di implementazione del servizio di gestione, ► **migliorare la maturità** dell'organizzazione ed il livello di automazione, fornendo al personale una guida dettagliata contestuale ai compiti che sono in esecuzione ► **indirizzare** il corretto utilizzo degli strumenti utilizzati, ► **chiudere** lacune di audit e/o conformità di processo, fornendo la verifica che i processi sono documentati con responsabilità chiare e definite, ► **facilitare**, anche con l'ausilio tecnologico di strumenti a supporto, quali GRC e DSS, le **decisioni**, basandosi su dati aggregati e indicatori di tendenza, con informazioni raccolte da tutte le fonti disponibili e ► **supportare** adeguatamente la formazione continua di tutti gli addetti al Centro Servizi. I processi di gestione e controllo della fornitura ed in particolare dei servizi/progetti integrano aspetti di Gestione della Qualità, Project Management e Gestione del Rischio, garantendo una visibilità sistematica ed organica di tutti i punti critici dei diversi CE.

3.3 I Centri Servizi

Il RTI ha sviluppato un modello di erogazione dei servizi in grado di adeguarsi in modo flessibile ed efficiente alle esigenze delle Amministrazioni. Caratteristiche fondamentali del modello sono:

- Focalizzazione **sull'erogazione dei servizi** secondo modalità che massimizzino i benefici per le Amministrazioni.
- **Integrazione dei processi**, delle risorse umane e delle infrastrutture IT in ottica di miglioramento continuo dei livelli di servizio.
- **Resilienza** per garantire la disponibilità e continuità dei servizi erogati.
- Adozione di **standard amministrativi, procedurali, organizzativi e gestionali** tali da assicurare all'Amministrazione un uso ottimale delle risorse professionali e finanziarie impiegate.

- Elevati livelli di **interoperabilità** per facilitare lo scambio di informazioni e servizi con i sistemi dell'Amministrazione, sia nella modalità di erogazione del servizio "*as a Service*" sia per le attività di supporto erogate dal Centro Servizi in modalità "*on Premise*".

Il modello concettuale proposto per il Centro Servizi è strutturato su quattro livelli (illustrati nella Figura 8). Il **livello 1** è rappresentato dai servizi erogati verso l'Amministrazione: servizi erogati "as a Service" e "on Premise" quali "**Servizi per la gestione delle Identità Digitali**", "**Servizi di Firma Digitale remota e Timbro Elettronico**" e "**Servizi di sicurezza**". L'efficace erogazione di tali servizi è assicurata dall'organizzazione proposta (**livello 2**) che include le migliori professionalità del RTI e dai processi di progettazione, erogazione e controllo dei servizi basata sulle migliori pratiche di mercato secondo i processi di gestione definiti dalla metodologia si mappa l'architettura definita dal RTI **ITUP – IBM Tivoli Unified Process** (cfr. § 3.3.2.1).

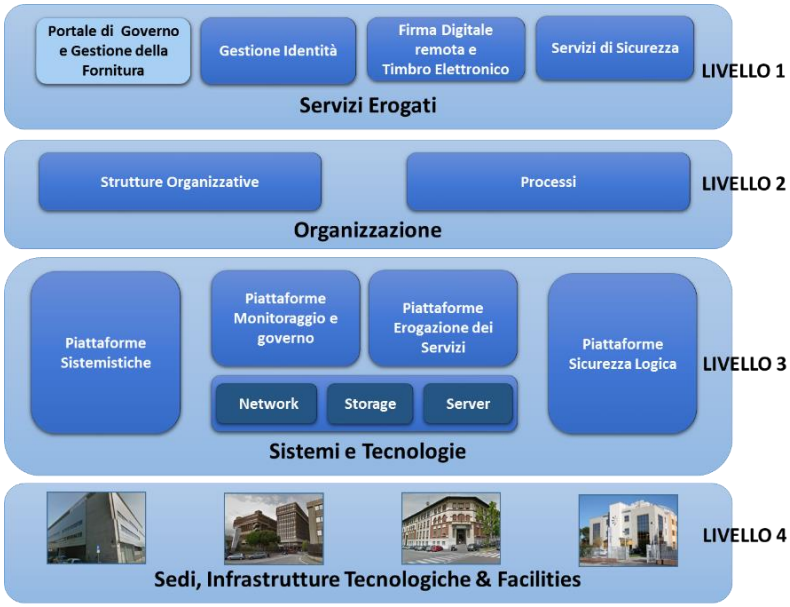


Figura 8: Modello concettuale ed Architettura della soluzione del RTI

Il **livello 3** rappresenta gli elementi tecnologici e le architetture ICT che rendono possibile l'attuazione dei processi per l'erogazione e controllo dei servizi. Appartengono a questo livello le piattaforme di **sicurezza** (cfr. § 3.3.2.1.2), **Sistemistiche** di **gestione del centro servizi** (cfr. § 3.3.2.2.4), di **monitoraggio e governo della fornitura** (cfr. § 5.2.4) e **di erogazione dei servizi operativi** (cfr. § 4). Il **Livello 4** concerne le infrastrutture logistiche e tecnologiche dei Data Center da cui vengono erogati i servizi, configurate in "continuità di servizio" e "disaster recovery" a garanzia della continuità operativa ed equipaggiati con tecnologie di ultima generazione ad elevata efficienza energetica.

La soluzione proposta si avvale delle **competenze gestionali e di sicurezza** di Selex ES ed E-Security ed è basata su: tecnologie avanzate di virtualizzazione; best practice ITUP e Piattaforme Sistemistiche **di IBM**; Data Center e Infrastrutture di rete Fastweb tecnologicamente **innovative**.

Le infrastrutture tecnologiche di ciascun sito, attraverso una rete dedicata, garantiscono alle unità operative distribuite su tutto il territorio nazionale di operare come un "**Centro Servizi Unico**", secondo il quale i siti di erogazione si comportano come un'unica entità logica in termini di organizzazione e tecnologie adottate. Pertanto nel resto del documento, a meno che sia diversamente indicato, qualsiasi riferimento a Centro Servizi è applicabile a tutti i siti (Centri Servizi).

3.3.1 Ubicazione dei Centri Servizi

Il modello di servizio adottato dal RTI è distribuito su più sedi nazionali come mostrato in Figura 9 dove per ciascuna sede è indicata la località in cui è ubicato il Centro Servizi (CS) e l'azienda del RTI responsabile delle infrastrutture e delle unità operativa in esso ospitate. L'ubicazione è scelta in particolare per garantire i massimi livelli di Continuità Operativa.

Figura 9: Ubicazione Centri Servizi

- Centro servizi **FASTWEB** di Via Caracciolo, 51 CAP 20155 Milano.
- Centro servizi **FASTWEB** di Via Bernina, 6 CAP 20158 Milano.
- Centro servizi **Selex ES** di Via Puccini, 2 – CAP 16151 Genova.
- Centro servizi **e-Security** di Via Enrico Mattei, 21 - CAP 66100 Chieti

L'erogazione dei servizi è basata su strutture organizzative, infrastrutture logistiche, tecnologiche (HW e SW) e di connettività di rete distribuite: (i) nel centro Fastweb Caracciolo come Data Center (DC) primario; (ii) nel centro di Fastweb Bernina come sito di **Business Continuity** (BC) in Campus Metropolitano; (iii) nel centro di Selex ES di Genova come sito di **Disaster Recovery (DR)**; (iv) nel centro di Selex ES di Chieti da cui vengono erogati i servizi del

Security Operation Center. L'operatività dei Data Center (**ICT Operation**) è assicurata da personale Fastweb della divisione Technology per i due CS di Milano e da personale Selex ES per il CS di DR. Le **piattaforme operative** (Sistema di governo e monitoraggio della fornitura, sicurezza ed erogazione) sono ospitate sul sito primario di Fastweb Caracciolo, configurate in BC sul sito di Fastweb Bernina e in DR sul sito di Selex ES Genova e sono gestite da personale selezionato del RTI. La configurazione architetturale e l'organizzazione proposte assicurano:

(i) la **Business Continuity** (BC) sia in termini tecnologici che di processi con la garanzia di valori di **RTO ed RPO prossimi allo zero,** in caso di indisponibilità del sito primario (cfr. § 3.3.2.1.3); (ii) valori di **RTO (≤ 4 ore)** ed **RPO (≤ 1 ora)** migliori di quelli richiesti dal presente bando di gara in caso di disastro su entrambi i siti in Campus. (iii) SOC con personale con altamente specializzato e piattaforme ridondate su due siti geografici (Chieti e Milano Caracciolo) per assicurare la continuità **operativa nella gestione della sicurezza**. (iv) Il servizio di **Help Desk** gestito da personale del RTI altamente specializzato ridondato su due siti (Genova e Milano) per assicurare la continuità del servizio di assistenza. (v) **La riduzione dell'impatto ambientale** e l'efficienza energetica come risultato delle scelte logistiche e delle soluzioni tecnologiche ed organizzative proposte (cfr. § 3.3.2.2.2).

3.3.2 Modello organizzativo e Caratteristiche tecnologiche dei Centri Servizi

3.3.2.1 Modello Organizzativo e di Funzionamento dei Centri Servizi

3.3.2.1.1 Strutture Ruoli e responsabilità

Il Centro Servizi Unico è composto da strutture organizzative ed ambiti operativi, definiti secondo la metodologia **ITUP (IBM Tivoli Unified Process)**, insieme di best practice sviluppate da IBM sulla base delle sue esperienze progettuali e realizzative a livello mondiale, riferite alla metodologie ITIL. Lo schema di funzionamento di ITUP partendo dalla modellizzazione di tutti i processi IT, secondo il Process Reference Model di IBM per l'IT (PRM-IT), si è successivamente arricchito mediante l'allineamento alle raccomandazioni e principi ITIL. Il framework, integrato con le knowledge base dei partner del RTI e l'adozione di strumenti di gestione (suite IBM – cfr. § 3.3.2.2.4), che nativamente adottano ed implementano le best practice ITUP, garantiscono le PA nell'adozione delle best practice a supporto dei processi di gestione. La linea gerarchica dei responsabili individuati dal RTI, permette un'efficace esecuzione delle attività dei diversi Centri ed una corretta direzione e controllo da parte del Comitato di Direzione Tecnica (cfr. § 3.2.2.1). Lo schema generale dell'Organizzazione del Centro Servizi Unico riportato in Figura 10, rappresenta ciascuno dei ruoli previsti, in funzione degli ambiti operativi. La tabella seguente descrive caratteristiche e responsabilità dei ruoli previsti negli ambiti più generali di **Governance del Centro Servizi Unico, di Continuità Operativa e di Sicurezza**. Le figure professionali previste in questi ambiti fanno parte del Comitato Direttivo RTI (cfr. § 3.2.2.1).

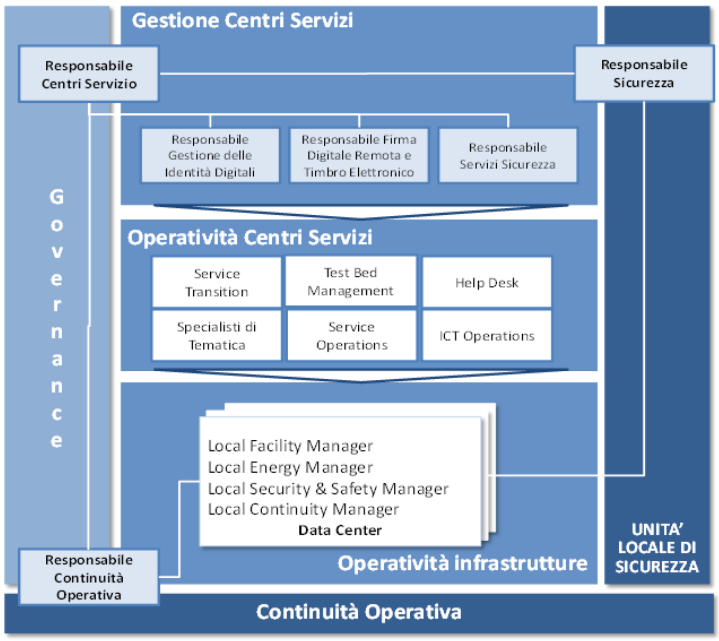


Figura 10: Modello Organizzativo del Centro Servizi

Ruolo	Caratteristiche e Responsabilità
Responsabile Centri Servizi	Ha il compito e la responsabilità di coordinare tutte le attività necessarie all'erogazione dei servizi da remoto previsti, ivi comprese quelle relative alla sicurezza. Tale ruolo ha la responsabilità di tutta l'organizzazione del Centro Servizi Unico.
Responsabile Continuità Operativa	E' responsabile di ogni attività tesa a ridurre l'impatto di un'emergenza che possa compromettere l'erogazione dei servizi alle PA. Reagisce prontamente in caso di disastri naturali, procurati, o causati da errori/malfunzionamenti di processi, sistemi, applicazioni o infrastrutture. Manutiene ed aggiorna il Piano di CO/DR. Tale ruolo coordina una struttura descritta nel paragrafo 3.3.2.1.3.
Responsabile della Sicurezza	E' responsabile della sicurezza logica dei Centri Servizi e rappresenta l'Unità Locale di Sicurezza secondo quanto richiesto dal Capitolato. Coordina le attività dei SOC al fine

	di garantire la sicurezza complessiva dei servizi erogati e le interazioni con il CERT della PA. Tale ruolo coordina la struttura descritta nel paragrafo 3.3.2.1.2.

La successiva tabella descrive i ruoli previsti nell'ambito di **Gestione del Centro Servizi Unico.** Questi, oltre ad essere previsti a Livello di Governo dei Contratti Esecutivi (cfr. § 3.2.2.2), rappresentano l'interfaccia tecnica per ogni singola Amministrazione e hanno la responsabilità della corretta erogazione dei servizi da remoto.

Ruolo	Caratteristiche e Responsabilità
Responsabile Gestione identità digitali (IDM) Responsabile Firma Digitale Remota e Timbro Elettronico Responsabile Servizi Sicurezza	Ciascuno, per la categoria dei servizi di propria competenza, è responsabile del coordinamento dal punto di vista operativo di tutte le attività legate alla erogazione del singolo servizio e alla gestione dei rapporti operativi di ciascuna Amministrazione. Coordina inoltre le attività di abilitazione ai servizi (eseguite dalla funzione di Service Transition) e ne verifica la qualità attraverso la valutazione dei livelli di servizio (monitorati dall'Operation Management).

I ruoli relativi all'ambito dell'**Operatività del Centro Servizi Unico** descritti nella successiva tabella hanno la responsabilità di tutte le attività tecnico operative necessarie alla erogazione dei servizi e dell'abilitazione alla fruizione delle Amministrazioni Beneficiarie.

Ruolo	Caratteristiche e Responsabilità
Help Desk Manager	**Coordina la struttura di Help Desk**. Responsabile della relazione diretta con le amministrazioni per la gestione delle richieste tecnico/amministrative e delle segnalazione di incident. Coordina i due livelli di Help Desk (cfr. § 3.4.1): • uno SPOC di 1° livello che raccoglie le richieste tecnico/amministrative e le segnalazioni di incident; ha la responsabilità dell'apertura dei problemi e della risoluzioni di tematiche semplici; • un Supporto di 2° livello per la gestione degli incidenti e dei problemi (analisi major incident, gestione problemi, supporto alla gestione del Knowledge base), apertura richieste di modifica (change) ed inoltro alle strutture di Operation Management e SOC per ulteriore risoluzione degli incident.
ICT Operation Manager	Coordina la struttura di Unità di ICT Operation, che si occupa della gestione di tutte le componenti tecnologiche necessarie all'erogazione dei servizi: Application e System Management, NOC, Monitoring, Backup, Asset & Configuration. E' attivato come Help Desk di secondo livello specialistico, per la risoluzione di malfunzionamenti e problemi legati ad una specifica tecnologia. Attraverso l'ausilio degli strumenti di monitoraggio controllo, garantisce il corretto funzionamento dei sistemi e delle applicazioni per una corretta erogazione dei servizi.
Service Operation Manager	Coordina la struttura di Unità di Service Operation, che si occupa della erogazione dei servizi E' responsabile della corretta abilitazione di una Amministrazione alla fruizione dei servizi sottoscritti. E' attivato come Help Desk di secondo livello specialistico, per la risoluzione di malfunzionamenti e problemi legati ad uno specifico servizio. E' responsabile della gestione tecnica dell'infrastruttura tecnologica dedicata alla erogazione dei servizi. Attraverso l'ausilio degli strumenti di monitoraggio controllo, garantisce la corretta erogazione dei servizi.
Specialista di tematica	Il team di Specialisti di Tematica è responsabile della progettazione dei servizi e della loro evoluzione. Valuta le necessità in termini di risorse e sviluppa le componenti architetturali, integrandole al fine di definire il servizio. Fornisce assistenza specializzate su tematiche inerenti la realizzazione dei servizi (es. processi, funzionalità, DB, sicurezza, prodotti e tecnologie, etc.).
Transition Manager	Coordina il team di Service Transition. E' responsabile della progettazione e dell'implementazione dei servizi proposti. Definisce le specifiche modalità implementative assicurandone la conformità ai requisiti previsti. Include l'unità di Capacity Management (responsabile dell'analisi dell'utilizzo delle infrastrutture e della redazione e mantenimento del Piano di Capacity).
Test Bed Manager	E' responsabile della funzione di Test Bed Management. Con il supporto della struttura di ICT & Service Operation e Transition Management gestirà le piattaforme di Test Bed relative alle infrastrutture dei centri servizi.

Nell'ambito della **Operatività delle Infrastrutture**, la successiva tabella individua caratteristiche e responsabilità delle figure professionali coinvolte per ciascuno dei Centri Servizi del RTI nella gestione locale di infrastrutture e facilities. Tali figure rappresentano l'elemento di raccordo tra il Centro Servizi Unico e le infrastrutture proprie di ciascuna azienda costituente l'RTI.

Ruolo	Caratteristiche e Responsabilità
Local Facility Manager	Ciascun Centro servizi prevede la presenza di un Local Facility Manager che ha la responsabilità della corretta configurazione e manutenzione degli impianti elettrici, energetici e di condizionamento.
Local Energy Manager	Ciascun Centro Servizi prevede la presenza di un Local Energy Manager che ha la responsabilità di monitorare i consumi energetici e di definire azioni volte a ridurre sia i consumi attuali che quelli previsti nei momenti di maggiore attività. Redige linee guida di intervento e conduzione rivolte alla complessiva riduzione dei consumi e quindi degli impatti ambientali.
Local Security & Safety Manager	Ciascun Centro Servizi preveda la presenza di un Responsabile locale che ha il compito di gestire le contromisure di sicurezza fisica, ambientale; effettua il monitoraggio degli eventi di sicurezza fisica; effettua il monitoraggio per la gestione delle frodi interne; gestisce le tematiche relative alla sicurezza dei lavoratori e degli ambienti utilizzati.
Local Continuity Manager	Ciascun Centro Servizi prevede la presenza di un Responsabile, della gestione operativa della "Crisi", del risk Assessment, del Testing e del Monitoring legato alla CO.

Unità Service Operation

L'unità è **coordinata dal Operation Manager.** E' la struttura specialistica per servizio preposta a garantire l'erogazione continuativa dei servizi, il controllo di qualità dei livelli di servizio secondo gli indicatori stabiliti. Tale struttura prevede l'introduzione degli ulteriori ruoli le cui caratteristiche sono descritte nella tabella successiva.

Ruolo	Caratteristiche e Responsabilità
Technical Service Manager	Responsabile tecnico dei servizi e delle risorse necessarie all'erogazione del servizio nel rispetto degli indicatori di qualità previsti
Data Analyst	Analisi dati, trend etc.
System Architect	Cura l'approccio tecnologico e la produzione dei risultati di progetto, garantendo i livelli di SLA previsti.
Specialista di processi	Specialista di processo in ambito Identity Management, IAM, Firma e Timbro digitale, Sicurezza
Specialista di prodotto /tecnologia	Possiede una profonda conoscenza delle tecnologie e delle problematiche di natura tecnica connesse con la realizzazione dei servizi di identità digitale, IAM, Firma e Timbro digitale, Sicurezza

Unità ICT Operation

L'unità di ICT Operation è la struttura **coordinata dal Operation Manager** e preposta a garantire l'operatività delle infrastrutture ICT dei Centri Servizi, attraverso la gestione e il monitoraggio di tutte le componenti tecnologiche HW/SW che li compongono. Tale struttura, sotto la responsabilità del ICT Operation Manager, prevede l'introduzione degli ulteriori ruoli le cui caratteristiche sono descritte nella tabella successiva.

Ruolo	Caratteristiche e Responsabilità
Application Manager	Responsabile dell'amministrazione, della gestione dei packages software, del middleware e del supporto tecnico, rispetto alle componenti software che realizzano i servizi.
System Manager	Responsabile dell'amministrazione e gestione (upgrade, sostituzione, etc.) delle infrastrutture server e storage e del relativo supporto tecnico.
Network Manager	Responsabile dell'amministrazione e gestione delle infrastrutture di networking sia geografica (WAN) che locale (LAN).
Monitoring Manager	Responsabile del monitoraggio e supervisione del corretto funzionamento delle infrastrutture ICT (hardware e software).
Backup Manager	Responsabile della configurazione ed esecuzione dei sistemi, delle policy e dei processi di backup & restore.
Asset & Configuration Manager	Responsabile della gestione degli asset infrastrutturali e tecnici necessari all'erogazione dei servizi. Identifica e controlla coerenza e consistenza delle configurazioni registrate nel CMDB attraverso audit periodici.

Come dettagliato nelle tabelle precedenti, i responsabili delle Unità Operative riportano al Responsabile del Centro Servizi, figura manageriale di alto profilo che avrà la responsabilità di gestire e coordinare gli aspetti organizzativi, procedurali, tecnologici e di performance del Centro Servizi. A tal fine è istituito un **Tavolo di Coordinamento Tecnico** presieduto dal Responsabile del Centro Servizi e costituito da: i Responsabili dei servizi di Gestione delle Identità Digitali, Firma Digitale Remota e Timbro Elettronico, Servizi Sicurezza nonché dall'Operation Manager, dall'Help Desk Manager, dal Responsabile della Sicurezza e dal Responsabile Continuità Operativa. Sono inoltre previste riunioni/sessioni specifiche su tematiche di efficientamento energetico finalizzato

alla riduzione dell'impatto ambientale, coinvolgendo anche i Referenti locali di Energy Management e KPI Monitoring & Analisys. Tale tavolo si riunisce di norma su base settimanale o straordinariamente in caso di problematiche che abbiano un impatto significativo sui servizi erogati. Analogamente i Responsabili delle Unità Operative attraverso riunioni periodiche provvedono all'allineamento del gruppo da loro coordinato. Inoltre il RTI utilizza strumenti di **Collaboration** e di **Knowledge Base** (vedi Piattaforme Sistemistiche, cfr. § 3.3.2.2.4) per una rapida ed efficace comunicazione e condivisione delle informazioni.

3.3.2.1.2 Sicurezza dei Centri Servizi

Il RTI garantisce la sicurezza dei Centri Servizi attraverso un approccio sistematico e collaudato maturato grazie a una lunga esperienza nel settore della "information assurance" ed "ICT security". In particolare Selex ES sta svolgendo il più grande contratto di cyber-security per la NATO (NCIRC – NATO Computer Incident Response Capability) ed ha una linea di business dedicata con oltre 200 professionisti del settore. I Centri Servizi che le aziende del RTI metteranno a disposizione, operano ciascuno sulla base del proprio Sistema di Gestione della Sicurezza delle Informazioni (SGSI) certificato ISO 27001. Gli SGSI saranno armonizzati ed estesi in modo da includere il perimetro tecnologico e di processi di interesse per la fornitura e costituire nel loro insieme il riferimento per la gestione della sicurezza del Centro Servizi Unico. In questo modo gli SGSI assicureranno che l'impianto di misure di sicurezza organizzativa, logica e fisica che sarà adottato soddisfi gli obiettivi di sicurezza definiti nel capitolato e mantenga nel tempo questa capacità seguendo l'evoluzione sia delle minacce sia dei servizi oggetto di fornitura.

Approccio Metodologico

Per lo svolgimento di queste attività il RTI ha deciso di adottare un processo collaudato da Selex ES che integra nelle sue fasi l'analisi del rischio condotta con la metodologia **MIGRA** e il corrispondente tool SW (approvato per l'inclusione nell'elenco ENISA delle metodologie e tool di gestione e assessment di sicurezza). L'approccio metodologico prevede lo svolgimento dei seguenti passi:

- **Analisi del contesto**: analisi di obiettivi, politiche, norme e best practice per la definizione del perimetro di indagine, degli asset (logistici, HW, SW, reti, dati e risorse umane) e l'identificazione delle minacce di tipo fisico, logico ed organizzativo.
- **Definizione del rischio e degli impatti:** fase tesa alla valutazione della probabilità di realizzazione delle minacce e del potenziale danno derivante (economico, violazioni di norme, immagine, all'operatività, al personale).
- **Piano di Gestione del Rischio:** Individuazione delle modalità di trattamento, eliminazione (soluzioni tecnico/organizzativo) o mitigazione (contromisure/procedure) dei rischi evidenziati. Eventuale trasferimento o accettazione del rischio residuo.
- **Governance e Gestione:** definizione dei punti di controllo ISO27001 applicabili, per la mitigazione del rischio, delle contromisure e dell'organizzazione di governo con l'assegnazione delle responsabilità di azione per l'inserimento nei SGSI. Condivisione formale dei rischi residui e dello stato degli indicatori di sicurezza.

La metodologia proposta è conforme alle norme ISO 27005 e ISO 27001. La compliance allo standard ISO27001 rispetto al quale sono certificati i centri servizi del RTI garantisce l'integrazione con le infrastrutture, ambienti fisici, processi organizzativi e logiche di gestione già ampiamente diffuse e consolidate nelle prassi ordinarie, ma anche con la cultura delle sicurezza parte integrante della cultura aziendale delle aziende del RTI. Durante la fase di preparazione della proposta il RTI ha svolto la prima esecuzione della metodologia sulla base della documentazione di gara e di esperienze dirette in servizi analoghi. I principali risultati di questa analisi sono riassunti nel seguito e costituiscono il progetto di SGSI.

Deliverable documentali

Ciascun sistema documentale SGSI sarà strutturato su tre livelli logici ► **Indirizzamento:** obiettivi di sicurezza, politica generale per la sicurezza, organizzazione generale e la normativa di riferimento applicabile ai servizi oggetto di fornitura ► **Metodologico**: linee guida e procedure ► **Operativo**: Piano di Sicurezza e Documento Programmatico sulla Sicurezza, istruzioni operative, manuali tecnici-operativi, etc.

Documentazione che sarà fornita nei tempi e nelle modalità richieste nel capitolato:

- **Piano di Sicurezza (PdS),** che descriverà approfonditamente le modalità logistiche ed organizzative, gli strumenti e i sistemi di cui sarà dotato il Centro Servizi per rendere sicuro e protetto l'ambiente che ospiterà le infrastrutture, il software e i dati dell'Amministrazione.
- **Piano di continuità operativa (PCO)** dei servizi erogati tramite i Centri Servizi, inclusivo del piano di disaster recovery, predisposto in conformità all'art. 50 bis del DPCM 1 Aprile 2008 ed in linea con le linee guida per il Disaster Recovery delle Pubbliche Amministrazioni redatte da AgID. (cfr. § 3.3.2.1.3).

- **Documentazione di attuazione del SGSI**, comprendente ► Procedura di Gestione dei documenti SGSI ► Gestione delle registrazioni ► Programma e procedura Audit ►Template dei campi del registro delle azioni ► Relazione annuale del riesame del SGSI ► Template per il Riesame del SGSI ► Processo di Incident Management e criteri di classificazione degli incidenti di sicurezza ► Modulo di reporting per le analisi periodiche di Incidenti, Criticità e Malfunzionamenti.
- **Documento Programmatico sulla Sicurezza** (DPS) che, in conformità alle direttive riportate nel D.Lgs 196/2003, dettaglia le procedure e gli strumenti adottati per garantire la sicurezza dei dati personali delle Amministrazioni trattati e scambiati nel Centro Servizi, in termini di Riservatezza, Integrità e Disponibilità.
- **Piano di Formazione del personale del Centro Servizi** per garantire la costante attività di informazione, formazione e addestramento sul rispetto dei principi e delle regole definite.

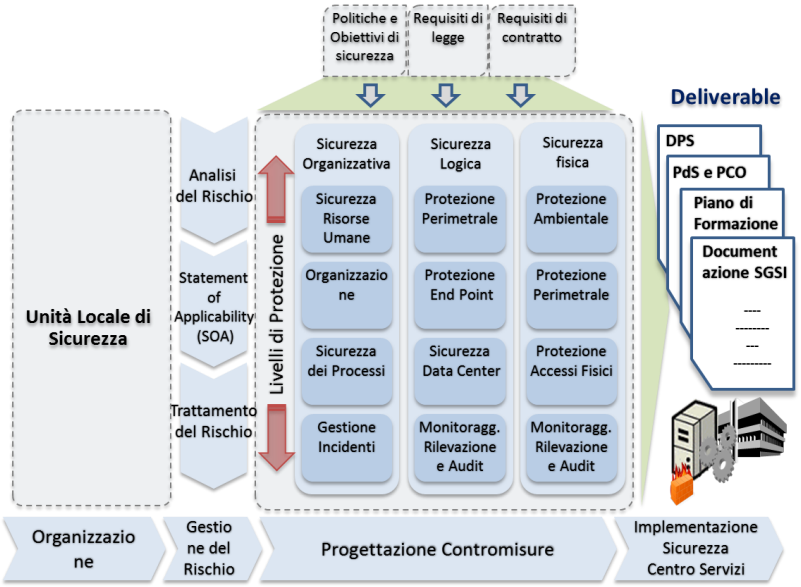


Figura 11: Approccio adottato, vincoli, livelli di protezione conformi al SOA e output previsti

Premesso che **verrà garantita la piena conformità a quanto indicato nel capitolato di gara**, nelle tabelle successive si riportano in sintesi i controlli ISO 27001:2013 applicabili per ciascun obiettivo di sicurezza indicato nel capitolato secondo la prima esecuzione dell'attività di analisi. Questi controlli, le cui modalità di applicazione all'interno dei Centri Servizi sono descritte nel seguito, entreranno a far parte della documentazione di attuazione del SGSI dei Centri Servizi.

Tabella 3: Mappatura controlli ISO27001 con obiettivi di sicurezza

Obiettivi di sicurezza da Capitolato	PUNTI CONTROLLO ISO/IEC 27001:2013 APPLICABILI
Assicurare la continuità dei servizi e delle applicazioni (Capitolato Tecnico – Parte Generale - Par. 4.2.1.1)	A.17 Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa – punti A.17.1; A.17.2
	A.12.3 Proteggere dalla perdita di dati.
Minimizzare i danni in caso di incidente e/o di avaria del Sistema Informativo (Capitolato Tecnico – Parte Generale - Par. 4.2.1.1)	A.16.1 Assicurare un approccio coerente ed efficace per la gestione degli incidenti relativi alla sicurezza delle informazioni, incluse le comunicazioni relative agli eventi di sicurezza e ai punti di debolezza.
Garantire la gestione della sicurezza in linea con la normativa nazionale e con gli standard internazionali (Capitolato Tecnico – Parte Generale - Par. 4.2.1.1)	A.18 Conformità – punti A.18.1 A.18.2
Normalizzare l'approccio alla gestione della sicurezza, ottimizzando e coordinando le risorse disponibili (Capitolato Tecnico – Parte Generale - Par. 4.2.1.1)	A.7 Sicurezza delle Risorse Umane – Punti A.7.1, A7.2, A.7.3
	A.6.1.5 sicurezza delle informazioni nell'ambito della gestione
Creare un'organizzazione della sicurezza condivisa, documentata, organica, efficiente e capillare (Capitolato Tecnico – Parte Generale - Par. 4.2.1.1)	A.6 Organizzazione della sicurezza delle informazioni - Punti A.6.1, A.6.2
Consentire un miglioramento continuo del sistema della sicurezza (Capitolato Tecnico – Parte Generale - Par. 4.2.1.1)	10.2 L'organizzazione deve migliorare in modo continuo l'idoneità, l'adeguatezza e l'efficacia del SGSI
	A.5 Fornire gli indirizzi ed il supporto della direzione per la sicurezza delle informazioni
	A.6 Organizzazione della sicurezza delle informazioni - Punti A.6.1, A.6.2 e par 6.1.2, 6.1.3
	A.12 Sicurezza delle attività operative - punti A.12.1, A.12.2, A.12.3, A.12.4, A.12.5, A.12.6, A.12.7
Politiche della sicurezza delle informazioni (Capitolato Tecnico – Parte Generale - Par. 4.2.2.1)	A.5 Fornire gli indirizzi ed il supporto della direzione per la sicurezza delle informazioni

Organizzazione del Fornitore (Capitolato Tecnico – Parte Generale - Par. 4.2.2.2)	A.6 Organizzazione della sicurezza delle informazioni - punti A.6.1 e A.6.2
Sicurezza dell'accesso di terze parti (Capitolato Tecnico – Parte Generale - Par. 4.2.2.3)	A.15 Relazioni con i fornitori – punti A.15.1, A.15.2 A.9 Controllo degli Accessi - punti A.9.1 , A.9.2, A.9.3, A.9.4
Gestione degli asset (Capitolato Tecnico – Parte Generale - Par. 4.2.2.4)	A.8 Gestione degli Asset – punti A.8.1, A.8.2, A.8.3
Classificazione delle informazioni (Capitolato Tecnico – Parte Generale - Par. 4.2.2.5)	A.8.2 Assicurare che le informazioni ricevano un adeguato livello di protezione in linea con la loro importanza per l'organizzazione.
Sicurezza delle risorse umane (Capitolato Tecnico – Parte Generale - Par. 4.2.2.6)	A.7 Sicurezza delle Risorse Umane – Punti A.7.1, A7.2, A.7.3
Sicurezza fisica e ambientale (Capitolato Tecnico – Parte Generale - Par. 4.2.2.7)	A.11 Sicurezza Fisica e Ambientale - punti A.11.1 A.11.2
Procedure operative (Capitolato Tecnico – Parte Generale - Par. 4.2.2.8)	A.12 Sicurezza delle attività operative - punti A.12.1, A.12.2, A.12.3, A.12.4, A.12.5, A.12.6, A.12.7
Controllo degli accessi logici (Capitolato Tecnico – Parte Generale - Par. 4.2.2.9)	A.9 Controllo degli accessi – punti A.9.1, A.9.2, A.9.3, A.9.4 A.13.1 Assicurare la protezione delle informazioni nelle reti e nelle strutture per l'elaborazione delle informazioni a loro supporto. A.13.2 Mantenere la sicurezza delle informazioni trasferite sia all'interno di un'organizzazione sia con qualsiasi entità esterna. A.13.1 Sicurezza delle Comunicazioni – punti A.13.1, A.13.2
Sviluppo e manutenzione dei sistemi informativi (Capitolato Tecnico – Parte Generale - Par. 4.2.2.10)	A.14 Acquisizione, Sviluppo e Manutenzione dei Sistemi - A.14.1, A.14.1, A.14.2, A.14.3
Gestione degli incidenti relativa alla sicurezza delle informazioni (Capitolato Tecnico – Parte Generale - Par. 4.2.2.11)	A.16.1 Assicurare un approccio coerente ed efficace per la gestione degli incidenti relativi alla sicurezza delle informazioni
Gestione della continuità operativa (Capitolato Tecnico – Parte Generale - Par. 4.2.2.12)	A.17 Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa – punti A.17.1; A.17.2

Sicurezza Organizzativa

Al fine di implementare i controlli sopra definiti il RTI istituirà una Unità Locale di Sicurezza (ULS) con i compiti di cui all'art. 21, commi 6 e 9 del DPCM 1 Aprile 2008. La struttura della ULS è rappresentata in Figura 12 con i ruoli identificati e le relative responsabilità di seguito descritte:

Figura 12: Organizzazione della sicurezza

Responsabile della Sicurezza – Oltre quanto specificato nel § 0), in qualità di Responsabile della ULS: (i) valuta, periodicamente, la conformità ed efficacia delle procedure e contromisure di sicurezza adottate e fornire i dati necessari per curare i rapporti con le Amministrazioni, Agid, CERT-PA e Consip e per le comunicazioni ufficiali; (ii) valuta con i Security manager (cfr. § 0), all'atto dell'attivazione dei contratti esecutivi, gli specifici requisiti di sicurezza ed attuare le necessarie contromisure; (iii) pianifica, organizza e dirige le attività di sicurezza coordinando i singoli responsabili e le strutture operative interne ai CS; (iv) pianifica e gestisce le attività interne di formazione e security awareness; ed infine (iv) partecipa a tavoli nazionali ed internazionali di confronto su tematiche di sicurezza.

SOC Manager: coordina il SOC primario riportando al Responsabile della Sicurezza ed ha il compito di: gestire i dispositivi di protezione perimetrale; di protezione degli end point; effettuare il monitoraggio degli eventi di sicurezza logica e la gestione incidenti; effettuare il monitoraggio periodico dei livelli di sicurezza. In caso di disastro sul sito primario coordina l'attivazione del SOC sul sito ove è replicato (in Continuità Operativa). Utilizza Piattaforme di gestione SIEM per il monitoraggio, controllo e attivazione delle contromisure degli eventi che possano minacciare la sicurezza logica.

Local Security & Safety: riporta al Responsabile della Sicurezza ed ha il compito di gestire le contromisure di sicurezza fisica e ambientale; effettuare il monitoraggio degli eventi di sicurezza fisica e ambientale e di rilevazione delle frodi interne; gestire le tematiche relative alla sicurezza dei lavoratori e degli ambienti utilizzati.

Risk Policy & Compliance, struttura coordinata dal Responsabile della Sicurezza, ha il compito di effettuare i cicli periodici di analisi del rischio in conformità ai requisiti del Capitolato di Gara; definire, emettere ed aggiornare politiche e linee guide di sicurezza; effettuare delle verifiche interne di conformità alle policy coordinandosi con il SOC Manager per le attività operative di Audit.
Fraud Management, risponde al Responsabile della Sicurezza ed ha il compito di gestire le frodi coordinandosi con il SOC Manager e con la struttura di Local Security & Safety per le attività di raccolta, analisi e gestione delle evidenze; interfacciarsi con le Autorità esterne (Garante per la Protezione dei Dati Personali, Magistratura in relazione a possibili richieste di accesso ai dati trattati per le finalità ammesse, Polizia Postale nell'azione di prevenzione e contrasto della criminalità informatica).
Il corretto flusso delle informazioni e delle problematiche all'interno dell'unità operativa è garantito dall'utilizzo della piattaforma di Collaboration e da periodiche riunioni di allineamento e condivisione.
Nelle tabelle successive si riportano in sintesi le principali azioni che saranno implementate dal RTI tramite la ULS per attuare i punti di controllo ISO27001:2013 pertinenti alla sicurezza organizzativa.

Modalità di applicazione dei controlli ISO 27001:2013 (A.7)
Sicurezza delle risorse umane. Mantenimento dei livelli di formazione ed informazione del personale mediante piani di formazione del personale del CS ►**Controlli alla selezione del personale** differenziati in funzione dei livelli di criticità delle informazioni trattate. ►**Certificazioni di sicurezza.** Il personale impiegato nei Centri Servizi è in possesso delle principali certificazioni di sicurezza, rilasciate da Vendor leader del mercato di sicurezza e dalle organizzazioni internazionali sulla sicurezza delle informazioni.
Modalità di applicazione dei controlli ISO 27001:2013 (A.6, A.18, A.16, A.9)
Organizzazione del fornitore: i ruoli sono disegnati prevedendo la separazione delle responsabilità per la gestione di attività focali per la sicurezza logica, quali gestione incidenti, fraud management e policy compliance.
Modalità di applicazione dei controlli ISO 27001:2013 (A.5, A.8.1, A8.2, A.12, A.9, A.14, A.17)
Politiche della sicurezza delle informazioni. Procedure e direttive per il supporto ed il mantenimento dei livelli di sicurezza delle informazioni trattate, in funzione dei requisiti di legge, requisiti di contratto e degli obiettivi di sicurezza prefissati. ► **Gestione degli asset.** Formalizzazione ed aggiornamento periodico dell'inventario di tutti i beni (utilizzando la piattaforma di Configuration Management) teso a valutare i livelli di rischio associati ai servizi e i conseguenti trattamenti. ► **Classificazione delle informazioni.** Formalizzazione di criteri, metriche valutative e modalità operative (valore, prescrizioni legali, e criticità) adottate la classificazione delle informazioni trattate dai servizi oggetto di fornitura. ► **Procedure operative.** Formalizzazione di attività, ruoli e responsabilità per tutte le attività di controllo previste dalla norma ISO/IEC 27001, ivi comprese le procedure e le istruzioni operative per il corretto utilizzo dei dispositivi di sicurezza logica e fisica. ► **Controllo degli accessi logici.** Definizione di procedure per la sicurezza degli accessi logici ai sistemi IT, ispirate al principio del least privilege, comprensive di procedure di provisioning, procedure di deprovisioning, procedure di verifica periodica dei profili di accesso e dei registri di accesso, procedure per il corretto utilizzo delle credenziali di accesso rilasciate. ►**Sviluppo e manutenzione dei sistemi informativi.** Processi e procedure per garantire la sicurezza in tutte le fasi del ciclo di vita dei sistemi software, comprensive di best-practice con principi di base quali data validation, error handling, execution privilege e linee guida avanzate per lo sviluppo sicuro in ambienti Web e la protezione del traffico di rete. ► **Gestione della continuità operativa**: processi e procedure per il mantenimento della continuità operativa, (cfr § 3.3.2.1.3)
Modalità di applicazione dei controlli ISO 27001:2013 (A.12.4, A.16)
Il processo di gestione degli eventi di sicurezza, allarmi ed incidenti, in carico al SOC, costituisce l'elemento primario per il mantenimento nel tempo dei livelli di sicurezza ► **Procedure e istruzioni operative** per il rilevamento, il tracciamento, la classificazione, la gestione e l'eventuale escalation degli eventi di sicurezza, rilevati attraverso l'infrastruttura tecnologica a protezione del perimetro e degli end-point. Fanno parte delle procedure: matrici diagnostiche di supporto per gli operatori del SOC, in modo da agevolare il riconoscimento degli indicatori di compromissione (IOC) e la classificazione degli eventi; procedure operative per la gestione di eventi codificati (infezioni virali, scansioni, ecc.) per i quali le azioni di trattamento / contrasto risultano formalmente preautorizzate.

Sicurezza Logica

Le contromisure tecnologiche, in combinazione con quelle fisiche ed organizzative, implementate nei centri servizi, garantiscono: **riservatezza** delle informazioni permettendo l'accesso solo a chi è autorizzato; **integrità** delle informazioni impedendo modifiche non autorizzate o manomissioni; **disponibilità** delle informazioni e dei servizi garantendo che l'accesso agli stessi da parte delle entità autorizzate possa avvenire nel rispetto dei requisiti di Capitolato. Le tecnologie utilizzate sono le più efficaci presenti sul mercato, o sviluppate internamente dai competence center del RTI, che tra l'altro dispone: un centro di eccellenza per lo studio avanzato di malware e di tecniche di attacco mediante analisi manuale degli artefatti non convenzionali e di attacchi zero-day, anche supportati dal gruppo X-Force di IBM, primo gruppo a livello mondiale; Security Operation Center per la fornitura di servizi di gestione della sicurezza a clienti commerciali e Difesa in Italia, UK e Germania realizzati e gestiti da

Selex ES; un Open Source Intelligence Center in cui è installato un High Performance Computer usato da Selex ES per l'erogazione di servizi Cyber Intelligence. La soluzione proposta prevede l'implementazione, per i centri servizi, di contromisure di sicurezza logica secondo il principio di "difesa in profondità" strutturato secondo livelli che comprendono più strati di protezione. A titolo esemplificativo e non esaustivo, nelle tabelle successive si riportano in sintesi le modalità di applicazione di alcuni i controlli ISO 27001 applicabili alla **sicurezza logica** dei Centri Servizi. Nelle tabelle successive si riportano in sintesi le principali azioni che saranno implementate dal RTI tramite la ULS per attuare i punti di controllo ISO27001:2013 pertinenti alla sicurezza logica.

Modalità di applicazione dei controlli ISO 27001:2013 (A.12, A.13, A.14)
Protezione Perimetrale. Utilizzo di dispositivi di sicurezza di ultima generazione in grado di rilevare e bloccare attacchi o attività anomale. Le infrastrutture di sicurezza logica sono gestite e monitorate dal SOC, operante presso i centri servizi . ► **Firewalling** (su piattaforme di Next Generation), **Intrusion Detection & Prevention System, Accesso remoto tramite VPN, Threat Emulation** (soluzioni di Anti malware dinamico ad es. per eseguire file dichiarati sospetti in ambienti operativi sicuri), **Web Content Management** (per l'accesso al web da parte degli operatori dei centri servizi), **Traffic monitoring e Network Behaviour Analysis** (sistemi di Deep Packet Inspection e Full-Packet Capture), **Web Application Firewall** (per la protezione da attacchi delle applicazioni web esposte), **Anti DDoS** (per la protezione dei servizi da tentativi di attacchi DDoS volumetrici, con protezione effettuata direttamente presso il provider internet.
Modalità di applicazione dei controlli ISO 27001:2013 (A.9, A.13, A.6)
Protezione degli End Point: protezione dei server e delle PdL (fisse/mobili) degli operatori e controllo degli accessi sulle PDL, server e database dei centri servizi, per la protezione in profondità e la capacità di fronteggiare eventuali minacce che potrebbero sfuggire ai controlli perimetrali. Tali infrastrutture implementano anche controlli basati sui principi di "Need to know" e "Segregation of Duties". ► **Malware protection e Data Loss Prevention** tramite SW antimalware, di tipo signature based e anomaly based. **Identity & Access Management e Privileged Identity Management.** L'accesso a tutti i sistemi e alle applicazioni degli operatori dei centri servizi è gestito centralmente. Il sistema è rispondente ai requisiti del D.lglvo del Garante 196/2003 e quello del 24/12/2008.
Modalità di applicazione dei controlli ISO 27001:2013 (A.9, A.17, A.13)
Oltre alle normali contromisure per la protezione degli end-point e perimetrali, applicabili anche in questo dominio, questi controlli assicurano la protezione del Data Center per garantire il massimo livello di resilienza delle infrastrutture e protezione dei dati. ► **Core Networking ridondato.** Infrastruttura di rete realizzata con elementi ridondati per la massima resilienza della rete interna. Utilizzo di protocolli di VRF e VRRP per il bilanciamento e l'affidabilità delle reti. ► **Network Segregation.** VLAN con riduzione dei domini di broadcasting, network firewall per filtraggio del traffico interVLAN. ► **Sicurezza degli ambienti virtuali.** switch e virtual firewall per la segregazione intra-hypervisor, e analisi malware agentless.
Modalità di applicazione dei controlli ISO 27001:2013 (A.12, A.6, A.9)
Log Management. Eventi e log vengono raccolti, collezionati e memorizzati in ottemperanza al d.lgvo 196/2003. ► **Monitoraggio e Correlazione.** Monitoring per la disponibilità delle risorse e degli eventi, compresi quelli di sicurezza. ► **Audit interni e del certificatore.** Audit Interni (freq. semestrale), in aggiunta agli audit degli enti di certificazione ISO 27001. ► **Threat Intelligence e AntiPhishing.** Attività di Early warning tramite il centro di supercalcolo HPC del RTI (Chieti) e feed open source e dei vendor, per la rilevazione proattiva di vulnerabilità e minacce e monitoraggio antifrode e antiphishing.

Al fine di veicolare in maniera opportuna i requisiti di protezione sopra identificati, il RTI ha previsto l'utilizzo dei seguenti strumenti enterprise.

Strumenti	Descrizione
AntiDDoS ► volumetrico ► applicativo su link internet ► su link Altro Operatore	Monitoraggio del traffico proveniente da Internet, analisi, attivazione delle contromisure, invio della sola porzione di traffico legittima. ► Accesso affidabile ai servizi di rete essenziali rilevando e bloccando le minacce alla disponibilità, come gli attacchi DDoS e altri tipi di cyber-attacchi. ► AntiDDoS hardware-based. Riconoscimento e prevenzione degli attacchi DDoS.
Firewall perim. IDS/IPS	Oltre alle tradizionali funzioni di firewall, IPS e IDS, eroga funzionalità di UTM.
Web Application Firewall	Protezione da attacchi applicativi come ad esempio SQL injection e Cross Site Scripting. Funzionalità di anti-defacement, funzioni di Content Delivery.
Virtual Firewall	Appliance virtuale di firewall, IDS, IPS, Antivirus & Antispyware, Web Filtering.
Application Delivery Controller	Load Balancing, SSL Offloading, IP Reputation
SIEM e Log Management	Gestione automatizzata analisi log, Windows Event, Database, Application e Syslog.
Identity & Access Management	Gestione degli accessi e delle identità, Identity governance e analytics
Report e analisi log	Report e analisi dei dati di capacità e utilizzo della rete

Sicurezza Fisica ed Ambientale

Nei Data Center del RTI sono state realizzate, in conformità alla norma ISO 27001 e ai requisiti di gara, contromisure organizzative e tecnologiche volte alla protezione nei confronti di: danni dovuti ad incendi, inondazioni, esplosioni, tumulti e altre forme di disastro naturale o causati dall'uomo; accessi non autorizzati e mirati a danneggiare sistemi e dati (manomissione e furto delle informazioni, manomissione e furto degli apparati IT, impedimento allo svolgimento dei servizi e dei processi IT, manomissioni ed interruzioni delle attività).

Al fine di ottenere una protezione globale, tali contromisure sono strutturate secondo diversi Livelli di protezione interagenti tra loro: Protezioni Ambientali a garanzia della sicurezza da minacce esterne ed eventi ambientali; Protezioni Perimetrali per rilevare, segnalare ed impedire violazioni del perimetro dell'intero sito e delle aree interne; Protezione degli Accessi fisici per regolamentare e controllare l'accesso alle aree sicure (con diversi criteri di sicurezza); attività di Monitoraggio e Audit per gestire l'insieme delle contromisure e il loro continuo miglioramento.

Nelle tabelle successive si riportano in sintesi le principali azioni che saranno implementate dal RTI e le caratteristiche comuni di tutti i siti del centro servizi pertinenti alla sicurezza fisica

Modalità di applicazione dei controlli ISO 27001:2013 (A.11.2)
Prevenzione, identificazione di eventi ambientali dannosi, segnalazione al presidio on-site ed alle autorità competenti, esecuzione di azioni di rimozione o contenimento. ►**Impianto antincendio** composto di sensori di temperatura ambientale, sensori di rilevamento del calore, di tipo lineare, installati in tutti i cablaggi, sensori di fumo, sistema di estinzione incendi a spruzzo basato su agenti neutri, estintori portatili. ►**Impianto antiallagamento** composto di sensori di rilevazione della presenza di acqua posti sotto il pavimento flottante, sistema di pompe per l'espulsione forzata dell'acqua. ► **Impianto di alimentazione elettrica di emergenza** a garanzia della continuità all'operatività e alle eventuali azioni di emergenza. ► **Impianto di protezione dalle scariche atmosferiche**. ►**Misure preventive**. Divieto di fumare e di usare fiamme libere; assenza nelle vicinanze di fabbricati a rischio incendio o esplosione; utilizzo di materiali da costruzione ignifughi ed autoestinguenti; utilizzo di armadietti, chiusi a chiave, per la conservazione di materiale cartaceo o comunque facilmente infiammabile; sistema di blocco del gasolio dei generatori elettrici in caso d'incendio.
Modalità di applicazione dei controlli ISO 27001:2013 (A.11.1)
Insieme delle risorse umane (guardiania, centrale operativa, reception); strumenti in grado di rilevare, segnalare ed inibire ingressi non autorizzati; infrastrutture gestite dal personale della Centrale Operativa a protezione del perimetro fisico esterno ed interno dei CS. ► **Centrale Operativa**, attiva H24 x 365 gg per tutti i CS, intensificato con ronde armate nelle ore notturne. ► **Recinzioni esterne** in maglia zincata ed elettrosaldata con protezione antiscavallamento. ►**Sbarra o cancello di protezione** azionato dalla postazione di guardiania per regolamentare l'accesso dei veicoli. ► **Videosorveglianza esterno ed interno** a circuito chiuso con tecnologia Motion Detection collegato alla Centrale operativa. ►**Sistema Antintrusione Perimetrale** esterno a doppia tecnologia (microonde ed infrarossi) per la rilevazione degli ingressi non autorizzati e funzionante sia nelle ore diurne sia in quelle notturne. ►**Sistema antintrusione** nelle zone interne del fabbricato composto di: sensori volumetrici a doppia tecnologia (microonde ed infrarossi), barriere perimetrali su finestre, rivelatori di rottura dei vetri, contatti magnetici su porte e finestre. ► **Protezione degli uffici critici (es. archivi cartacei sensibili)** protetti con badge/pwd/biometria. ► **Uscite di sicurezza** protette da sistema di allarme. ► **Segregazione delle aree di carico e scarico** non comunicanti con gli accessi alle aree sicure. ► **Protezione dell'area dedicata alle PA** tramite Cage con ingresso controllato tramite Badge o codice.
Postazione di guardiania presidiata H24 per 365 gg/anno. ► **Reception di accoglienza** per la registrazione di fornitori, visitatori e clienti. ► **Accessi alle zone interne** protetti tramite tornelli consentiti al solo personale abilitato tramite badge negli orari lavorativi e nelle sole aree di pertinenza. ► **Preventiva autorizzazione di Visitatori o Fornitori** con procedura di registrazione che prevede la compilazione di un modulo con: dati anagrafici (documento di riconoscimento valido), dati (numero seriale) di eventuali dispositivi elettronici (PC, fotocamere, registratori audio e/o video), riferimento della persona che autorizza l'accesso e che convalida l'uscita. ► **Ascensori e montacarichi** non a libero uso ma azionati dalla postazione di guardiania o tramite badge abilitati. ►**Postazioni di lavoro** degli operatori protette dall'accesso con password. **Ubicazione separata degli Impianti IT e facilities** (server, storage, network, UPS, Generatori elettrici, condizionamento, etc.) con accesso selettivo al solo personale autorizzato per la manutenzione**.**
Modalità di applicazione dei controlli ISO 27001:2013 (A.11.1, A.11.2)
Attività di Monitoraggio e Audit mediante strumenti e personale dedicato H24x365 gg/anno al fine di individuare tempestivamente situazioni di allarme al verificarsi delle quali verranno innescate procedure di gestione delle emergenze. Inoltre saranno effettuati periodici interventi di audit utili al miglioramento dei sistemi e alle procedure di protezione. ► **Centrale Allarmi** in cui confluiscono oltre a tutti gli allarmi degli impianti tecnologici (generatori elettrici, UPS, chiller, HVAC, etc) anche quelli relativi ai sistemi di rilevazione delle minacce fisiche ed ambientali. La centrale segnala l'evento, in funzione della tipologia, al personale reperibile e alle competenti autorità (VVFF, forze dell'ordine). ► **Centrale Operativa** presidiata H24x365 gg/anno dove vengono raccolti (Console degli allarmi) i segnali di allarme provenienti dalla Centrale Allarmi, i segnali video (Monitor di videosorveglianza VCC) e gli allarmi del sistema di Motion Detection. Il verificarsi di un evento di allarme innescherà la procedura di emergenza con l'attivazione dei gruppi e delle procedure del caso.

3.3.2.1.3 Continuità Operativa

Il RTI vanta una riconosciuta esperienza internazionale nello sviluppo di soluzioni di Continuità Operativa (CO) per grandi aziende, amministrazioni e organismi governativi di rilevanza mondiale avendo realizzato e curando la gestione di più di 150 Datacenter dedicati al DR e alla BC. Inoltre IBM ha partecipato e collaborato al tavolo per lo sviluppo delle Linee Guida della Continuità Operativa emesse da AgID in attuazione del DL 235, 30/12/2010 CAD. La sintesi di queste esperienze e conoscenze ha permesso di progettare e realizzare la **soluzione altamente ridondata e resiliente** qui proposta secondo la metodologia della **"Continuità Progettuale"** coerentemente alle Linee Guida emesse da AgID per le soluzioni e i sistemi di gestione della CO, in linea con le normative internazionali ISO 27001, ISO 22301, ISO 24762 e strutturata secondo l'impostazione convenzionale di ITIL v3. Sarà garantita la costante disponibilità dei Sistemi ICT e delle Funzioni Organizzative prevedendo una soluzione (BC) in "Campus Metropolitano" costituita dai due DC Fastweb di Milano che, in caso di disastro del sito primario, assicura **tempi di RTO ed RPO prossimi allo zero** e in caso di disastro di entrambi, una soluzione di **Disaster Recovery con i migliori parametri richiesti dal capitolato**. La robustezza della soluzione di BC è ampiamente collaudata, essendo in uso da anni sui due Data Center Fastweb per l'erogazione di servizi Cloud verso enti pubblici e grandi aziende private. La soluzione tecnologica di Business Continuity implementata dal RTI rappresenta una realizzazione del **Tier 6 descritto dalle "Linee Guida per il Disaster Recovery delle Pubbliche Amministrazioni"** pubblicate da **AgID,** applicate in un contesto di Continuità Operativa, garantendo RTO prossimo allo zero ed RPO pari a zero. Mentre la soluzione di DR, con sito posto a distanza geografica, rappresenta una realizzazione **del Tier 4 di tali Linee guida** ponendosi al di sotto del valore minimo del RTO e del valore massimo di RPO da queste specificati.

La soluzione proposta assicura questi risultati grazie a:

- **Data Center con elevati livelli Tier (Uptime Institute):** (i) Sito Primario Fastweb – Caracciolo **certificato Tier IV – Constructed Facility (unico in Italia)** dal Uptime Institute. (ii) Sito di Fastweb – Bernina in Business Continuity rispondente alle **caratteristiche Tier III**, (iii) sito di Disaster Recovery Selex ES – Genova rispondente alle **caratteristiche Tier III**. Tutti i DC garantiscono alti livelli di ridondanza (N+N o N+1) di tutte le componenti tecnologiche con collegamenti multipli contemporaneamente attivi.
- **Componenti ICT in alta affidabilità** nei singoli data center.
- **Monitoraggio continuo** dei KPI delle componenti architetturali ed organizzative atto a prevenire eventi dannosi o a contenerne gli effetti.
- **Simulazioni di Disaster Recovery** effettuate sulle componenti infrastrutturali ed organizzative, con ambienti di Test separati da quello di produzione, per verificare l'efficienza e la robustezza delle infrastrutture e dei processi di Recovery e gli eventuali miglioramenti tecnologici o organizzativi da apportare.

I risultati garantiti in termini di Continuità Operativa sono:

- **Elevati valori di Disponibilità dei singoli siti:** e pari rispettivamente a 99,997% e 99,98% per i DC in campus, e 99,98% per il Datacenter di Disaster Recovery.
- Valori di **RTO ed RPO prossimi allo zero su tutti i servizi configurati in BC nel Campus Metropolitano**.
- Valori di **RTO ≤ 4 ore e di RPO ≤ 1 ora** su tutti i servizi per il **Disaster Recovery**. Possibilità di svolgere attività di **manutenzione sul sito primario (anche non pianificata),** senza impatti negativi sulla funzionalità del Data Center e sui servizi erogati.
- **La Resilienza al singolo guasto** rispetto alla fruibilità dell'infrastruttura: ogni elemento in alta affidabilità opera funzionalmente in continuità e quindi il singolo guasto ha impatto nullo sui servizi erogati.

Modello di Funzionamento della Continuità Operativa

Nelle tabelle seguenti viene riportata come le infrastrutture di erogazione dei Servizi, i servizi di supporto e le Unità Operative vengono distribuiti nei Centri Servizi.

Tabella 4: Configurazione Data Center

INFRASTRUTTURE TECNOLOGICHE (Data Center)	FASTWEB MILANO Caracciolo	FASTWEB MILANO Bernina	Selex ES GENOVA
Piattaforme di erogazione dei Servizi S1 S2 S3	Primario	Business Continuity	Disaster Recovery
Piattaforme di gestione dei DC (HD, ICT, NOC e SOC)	Primario	Business Continuity	Disaster Recovery

Tabella 5: Configurazione Centri di Gestione

	Unità OPERATIVE (Personale)	FASTWEB MILANO Caracciolo	Selex ES GENOVA	E-Security CHIETI
Help Desk		Continuità Operativa	Attivo	
ICT Operation		Attivo	Continuità Operativa	
Servizio S1: Gestione Identità Digitali		Attivo	Attivo	
Servizio S2: Firma Digitale e Timbro elettronico		Continuità Operativa	Attivo	
Servizio S3: Servizi di Sicurezza		Attivo		Attivo
ULS / SOC Interno		Attivo		Attivo

Nella seguente tabella vengono elencati gli eventi che potrebbero compromettere la CO e, per ciascuno di essi, vengono descritti gli impatti sull'Amministrazione e i meccanismi e le azioni intraprese per il ripristino delle normali condizioni operative.

Tabella 6: Impatti in caso di eventi di indisponibilità

Evento	Attività, Impatti e Livelli di Servizio
Indisponibilità totale del sito primario	**L'amministrazione non avrà alcun impatto. (RTO ed RPO prossimi allo zero).** – La configurazione in campus metropolitano consente il failover (parziale o totale) sul sito alternativo in area metropolitana. Il Sito primario verrà fatto ripartire alla rimozione delle cause di blocco. Le strutture di ICT Operation e Service Operation verranno ricollocate presso il sito alternativo.
Indisponibilità totale di entrambi i siti conseguente ad evento disastroso.	**L'amministrazione avrà il ripristino dei servizi con i parametri minimi richiesti (RTO ≤ 4 ore RPO ≤ 1 ora).**I meccanismi di DR e le unità operative designate alla sua gestione permetteranno la ripartenza dei servizi sul sito di DR con i tempi dichiarati. Al momento della rimozione dell'evento disastroso verrà fatto ripartire, sempre da queste unità, il sito primario secondo quanto previsto dal piano di CO/DR. Le strutture di gestione dell'ICT e quelle di Service Operation del Sito di DR prenderanno il pieno controllo dei sistemi del Data Center dando continuità organizzativa ai servizi alla ripartenza dei sistemi.

Di seguito si descrive il caso d'uso per gli impatti che l'Amministrazione potrà avere in base alle modalità di gestionedei servizi (attivo/attivo, attivo/continuità operativa) (cfr. Tabella 4: Configurazione Data Center e Tabella 5: Configurazione Centri di Gestione).

Tabella 7: Casi d'uso per impatti dovuti ad eventi disastrosi

Evento	Attività, Impatti e Livelli di Servizio
Unità Operative Attive contemporaneamente su due siti distanti: Indisponibilità totale del personale di uno dei siti per evento disastroso che provochi indisponibilità dell'infrastruttura tecnologica del sito o eventi particolari (scioperi, pandemie, etc.)	**L'Amministrazione non avrà alcun impatto** La configurazione con doppio sito attivo consente l'automatica presa in carico delle operazioni da parte dell'altro sito attivo. Gli operatori del sito non colpito dall'evento continueranno ad operare per le attività cui sono assegnati assorbendo anche il carico di lavoro proveniente dalla caduta dell'altro sito, portando a termine eventuali attività non ancora completate.
Unità Operative attive sul sito primario ed in Continuità Operativa su un sito distante: Indisponibilità totale del personale presso il sito primario per evento disastroso che provochi indisponibilità dell'infrastruttura tecnologica del sito o eventi particolari (scioperi, pandemie, etc.)	**L'Amministrazione potrà avere una riduzione dei livelli di servizio** ma trattandosi di eventi di carattere disastroso le unità operative e quindi i servizi ad esse legati verranno fatti ripartire sul sito di Continuità operativa. Gli operatori del sito in continuità opereranno sulle attività cui sono assegnati assorbendo tutto il carico di lavoro e portando a termine eventuali attività che non fossero state ancora completate

Infrastruttura tecnologica per la Continuità Operativa

Le componenti tecnologiche realizzate per la Continuità Operativa prevedono:

- Link realizzati tra i Centri Servizi con collegamenti dedicati in alta affidabilità in **tecnologia DWDM.**
- a livello di Storage una **replica sincrona (RPO = 0)** tra i siti in Campus , ed una **replica asincrona (RPO ≤ 1 ora)** tra il sito primario ed il sito di DR.
- Un **meccanismo di ridondanza delle risorse virtualizzate** nel sito di BC **(RTO prossimo allo 0)** ed un meccanismo di avvio dei servizi sul sito di DR (**Site Recovery Manager con RTO ≤ 4 ore**).
- Una **rete geografica** che configura i siti con lo stesso indirizzamento e gestisce dinamicamente (protocollo BGP) gli istradamenti con preferenza del sito primario in caso di normale funzionamento e del sito di BC o DR in caso di "Crisi".

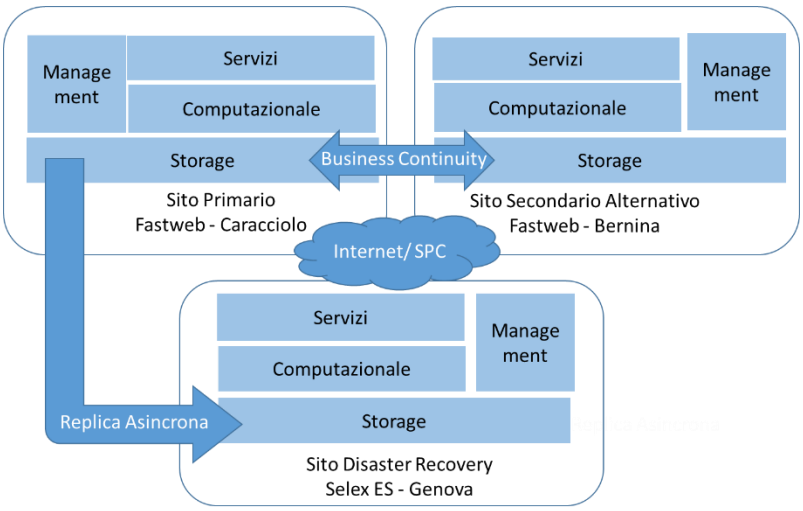


Figura 13: Infrastruttura per la CO

- **Ambienti di "Test isolati",** equivalenti agli ambienti di produzione, per effettuare **prove di Business Continuity** e **di simulazione di Disaster Recovery** per valutare l'efficienza infrastrutturale ed operativa senza impatti sugli ambienti di produzione. Inoltre tali test verranno pianificati ed eseguiti in giorni/orari con bassi carichi di lavoro al fine di contenere eventuali rischi. Incaricati dell'Amministrazione potranno accedere su richiesta ai Test e ai loro risultati, a scopo di verifica o audit.

Le soluzioni predisposte garantiranno anche la continuità operativa delle strutture organizzative di Help Desk, di ICT Operation, SOC e di Service Operation che saranno tutte replicate(con pari skill e pari conoscenze) in modalità **Attiva** o **Continuità Operativa** su un sito alternativo. Pertanto in caso di dichiarazione di disastro le Unità Operative ripartiranno entro i tempi massimi previsti nel sito scelto per la continuità operativa. L'infrastruttura di connettività utilizzata e i servizi di rete intelligente (Next Generation Network), configurati sulle numerazioni di accesso, consentiranno il re-routing di tutte le linee voce verso le strutture del sito di Continuità, prevedendo anche piani di "Emergency Link".

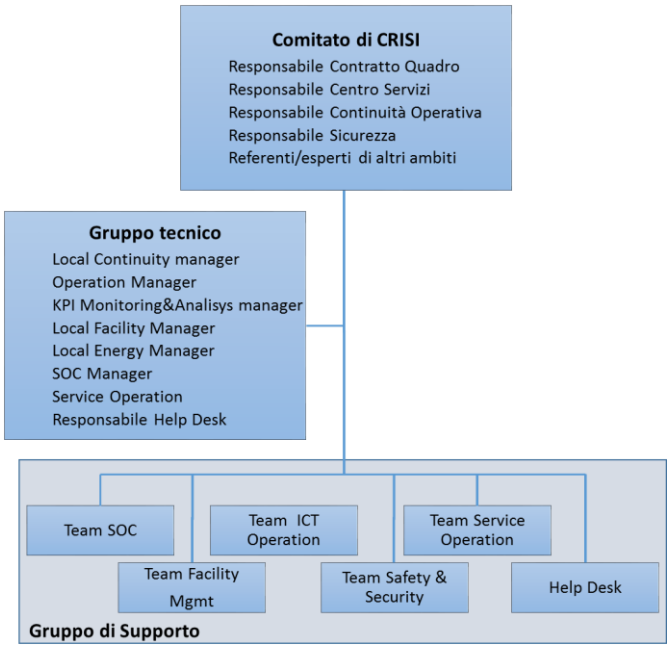


Figura 14: Organizzazione per la CO

Struttura organizzativa e processi della Continuità Operativa

Il RTI garantirà il governo della Continuità Operativa, mediante l'attivazione di una struttura efficace e flessibile sia per la fase di cosiddetto "normale funzionamento" (Redazione dei Piani di CO/DR, Testing e Miglioramento) che per la fase di "Disastro" durante la quale verranno garantiti **tempi decisionali eccezionalmente ristretti,** adeguati alle emergenze e che rispettino i Livelli di Servizio assicurati. L'efficacia, la flessibilità e i tempi saranno garantiti da

Funzioni dedicate alla Continuità Operativa:

- **Responsabile della Continuità Operativa:** punto di contatto delle attività tese a ridurre l'impatto di un'emergenza che possa compromettere l'erogazione dei servizi alle PA. Reagisce prontamente in caso di disastri naturali, procurati, o causati da errori/malfunzionamenti di processi, sistemi, applicazioni o infrastrutture. Manutiene ed aggiorna il Piano di CO/DR. E' Membro del Comitato di Crisi. Coordina i Referenti per la CO dei singoli Centri Servizi (cfr. § 3.2.2.2). Collabora con il responsabile della Qualità definendo e

gestendo le procedure e con il supporto dei referenti della CO ne effettua il monitoraggio. Sulla base dei risultati promuove: azioni di adeguamento del Piano/procedure; azioni specifiche sulle infrastrutture per migliorare la soluzione di CO; azioni di adeguamento del piano formativo.

- **Local Continuity manager**: Responsabile, per il singolo Centro Servizi, della gestione operativa della "Crisi", risk Assessment, Testing e Monitoring legate alla CO. Attiva il Comitato di Crisi in caso di evento disastroso. Interagisce con le funzioni Service Design e Transition per valutare i requisiti di CO, e con le funzioni ICT e Service Operation per le attività operative. Collabora alla produzione e gestione del Piano di CO/DR. E' membro del Gruppo tecnico.
- **KPI Monitoring & Analysis Manager**: collabora alla definizione dei KPI impattanti sulla CO, ne colleziona le misure rilevate dal Team di Monitoring e le analizza a fini di un'analisi: puntuale (utile a segnalare la necessità di azioni proattive/reattive); predittiva degli andamenti dei KPI (utile al livello strategico e alle azioni di miglioramento del Piano di CO/DR); di tipo "what-if" (utili alla valutazione della robustezza e di vulnerabilità nascoste).

Funzioni di supporto alla Continuità Operativa

- **Local Energy Management:** Responsabile diretto delle attività legate alla gestione efficiente dell'energia e alla diminuzione dell'impatto ambientale dei singoli CS. In relazione alla CO predispone e gestisce le attività per garantire l'attivazione degli UPS e dei generatori di emergenza in caso di fault all'alimentazione elettrica.
- **Local Facility Management:** Amministra e gestisce gli asset delle facilities del Centro Servizi. Collabora con il Team di Capacity management e con il responsabile della CO per le valutazioni di fabbisogni futuri, inoltre supporta il Referente della CO nel corso delle "Crisi" per la parte infrastrutturale e impianti.

Gruppi non permanenti composti da più funzioni che attingono le risorse dalle Unità Operative dei CS per svolgere le attività di Monitoring, Testing, Assessment e Gestione delle Crisi. Sono strutturati su tre livelli e consentono di accorciare la linea di comando e di avere la disponibilità di tutte le risorse necessarie soprattutto durante le "Crisi":

- **Comitato di Crisi:** responsabile delle azioni di **Livello Strategico** e delle interazioni con le Amministrazioni. Si occupa della scelta e della valutazione delle soluzioni e delle risorse, dell'approvazione del Piano di CO e delle strategie di Testing. In caso di "**Crisi**" esso viene immediatamente riunito e, se necessario, dichiara lo "**stato di Crisi**" a seguito del quale vengono avviate tutte le azioni tattiche ed operative a cui il Comitato conferisce l'autorità decisionale straordinaria. E' responsabilità del Comitato di Crisi controllare lo svolgimento di tali azioni fino alla valutazione e decisione di rientro nelle condizioni di normale attività.
- **Gruppo Tecnico**: gestito dal **Responsabile della Continuità Operativa** per la realizzazione delle azioni di **Livello Tattico.** Supporta la definizione, il disegno e la redazione e della Soluzione di CO e il suo aggiornamento con la fase di Risk Assessment. In particolare si occupa della sua realizzazione, in termini di infrastrutture, piani esecutivi, piano di formazione e procedure, valutandone la robustezza ed efficienza tramite l'analisi dei dati di Test pianificati e dei dati di monitoraggio proattivo. In caso di "**Crisi**" valuta l'impatto dell'emergenza, attiva il Comitato di Crisi e coordina il gruppo di Supporto fornendo le priorità di allocazione delle risorse fino al ritorno alla normalità operativa (anche per quanto riguarda **l'Help Desk)**. Aggiorna costantemente il Comitato con i dati di monitoraggio del corso della Crisi stessa e fornisce le "lesson learned" utili all'aggiornamento del piano di CO conseguenti agli eventi di Crisi accaduti.
- **Gruppo di Supporto**: Gestito dal Referente della Continuità Operativa con responsabilità delle azioni di **Livello Operativo.** Esegue le attività operative relative al Risk&Vulnerability Assessment, ai test di robustezza ed efficienza e al Monitoraggio proattivo, sintetizzando per il Gruppo Tecnico, dei report con i risultati e le eventuali evidenze di problematiche infrastrutturali. In caso di **Malfunzionamenti** di componenti ridondati interviene per la loro sostituzione, mentre in caso di incidenti gravi/disastri effettua l'escalation al Gruppo Tecnico. In caso di "**Crisi**" esegue le attività operative sulle infrastrutture di BC/DR in base al Piano e alle procedure e producendo report necessari al gruppo Tecnico. Cura le fasi di rientro nella normale attività.

Il corretto flusso delle informazioni e delle problematiche all'interno della struttura organizzativa è garantito dall'utilizzo della piattaforma di Collaboration e da periodiche riunioni di allineamento e condivisione.

I processi (Control IT Service Continuity) che compongono il Sistema di gestione generale della Continuità Operativa, conformemente a quanto richiesto da AGID (vedi par. precedente), sono presieduti, gestiti e supportati dalle strutture organizzative dell'RTI e coinvolgono le PA in funzione di end-user, controllo e governo per dare conto dell'efficacia delle soluzioni e di migliorare le soluzioni di continuità in relazione ai bisogni espressi dalle singole Amministrazioni. Tali processi sono stati suddivisi in:

- Redazione, manutenzione e adattamento del piano di Continuità Operativa e Disaster Recovery.

- Design e realizzazione delle soluzioni infrastrutturali ed organizzative e di adeguamento ai fabbisogni futuri.
- Valutazione ed approvazione delle necessità di Formazione del Personale.
- Monitoraggio dei KPI e dei parametri funzionali.
- Testing e Miglioramento Continuo.
- Gestione delle "Crisi" e del piano di Disaster Recovery.

Il **Piano** di **Disaster Recovery** sarà sviluppato sin dalle prime fasi in completa integrazione all'interno del RTI con un piano di test che ne controlli a scadenza stabilita: Chiarezza e comprensibilità della documentazione per le procedure e i piani; Efficacia e Fattibilità dei piani; Consistenza delle informazioni relative a backup e loro effettiva utilizzabilità in una procedura di ripristino; Effettivo funzionamento dell'infrastruttura residente nel sito di DR;
I Test condotti saranno di tipo cartaceo, con revisione strutturata e interviste con checklist, per la verifica della effettiva preparazione delle figure chiave e di simulazione su ambienti paralleli.

3.3.2.2 Caratteristiche tecnologiche dei Centri Servizi

I Data Center da cui il RTI eroga i servizi sono dotati delle più moderne tecnologie in grado di garantire gli elevati livelli di sicurezza, automazione e standardizzazione richiesti dal Capitolato. Allo scopo di evidenziare come l'innovatività, l'efficacia e la modularità della soluzione proposta sia adeguata all'erogazione di servizi di Cloud Computing alla PA, i prossimi paragrafi descrivono le caratteristiche tecnologiche dei Data Center con particolare attenzione alle tematiche indirizzate dal documento "*Linee Guida per la razionalizzazione della infrastruttura digitale della Pubblica Amministrazione",* evidenziando come la riduzione dell'impatto ambientale sia di particolare rilevanza per il RTI.

3.3.2.2.1 Logistica e infrastrutture

Logistica, spazi fisici e impianti, sono concepiti in un disegno omogeneo e modulare, che utilizza tecnologie integrate al fine di garantire le massime prestazioni, efficienza energetica e soprattutto la possibilità di scalare modularmente i servizi senza impatti sull'operatività. La robustezza delle metodologie e delle soluzioni è ulteriormente garantita, per i Data Center in Campus, dalla certificazione ISO 22301, standard internazionale per la continuità operativa. I Data Center proposti dal RTI, tutti di nuova costruzione o di recente ristrutturazione, vantano un grado di ridondanza proprio del livello Tier IV (sito primario) e Tier III (sito di BC e sito di DR). In particolare: le linee elettriche in Media Tensione hanno ridondanza N+N, con percorsi diversificati e attestazione a due diverse sottostazioni di trasformazione; gli UPS sono realizzati in maniera modulare (sezionabilità e scalabilità) e con ridondanza N+N (N+1 Tier III); i generatori di emergenza sono equipaggiati con motori Diesel, hanno ridondanza N+N (N+1 Tier III) e sono in grado di supportare tutto il carico elettrico del DC; Gli SLA per il rifornimento del gasolio sono garantiti da sistemi automatici di rilevazione dei livelli di riempimento dei serbatoi; gli impianti elettrici hanno ridondanza N+N (N+1 Tier III) ed alimentano sistemi di distribuzione di potenza (PDU) intelligenti; i sistemi di condizionamento delle sale dati hanno tutti caratteristiche di modularità (sezionabilità e scalabilità) con chiller ridondati N+N e HVAC ridondati N+N (N+1 Tier III). Le suddette principali caratteristiche garantiscono elevati valori di disponibilità, di seguito riportati:

Data Center	Fastweb – Caracciolo	Fastweb - Bernina	Selex ES - Genova	Selex ES - Chieti
Livello Tier	IV	III+	III+	III
Disponibilità garantita	99,997%	99,98%	99,98%	99,98%

Tali valori garantiscono ampiamente il rispetto degli SLA (ad es. indicatore IQ17) richiesti dal capitolato. L'estensione attuale complessiva delle sale dati supera i 3.500mq e lo spazio disponibile è più che sufficiente ad ospitare i rack che saranno ubicati in aree segregate e dedicate alle PA. Lo spazio complessivo ancora disponibile nei fabbricati per essere infrastrutturato come "sala dati" (oltre 30.000 mq), consente una elevatissima scalabilità e lo spazio fisico segregato (*Cage*) dedicato l'erogazione dei servizi alle PA, può essere ampliato fino alla saturazione. La scalabilità della soluzione è ulteriormente favorita dalla scelta di strutture modulari innovative (rack) ad **elevato grado di densità** ed **elevata potenza**.

3.3.2.2.2 Soluzioni per la riduzione dell'Impatto Ambientale

Una particolare attenzione è stata posta, nelle fasi di Design e di Costruzione dei Data Center, alle soluzioni tecnologiche che consentono una drastica **riduzione dell'impatto ambientale** attraverso l'abbattimento delle emissioni di CO^2 e la minimizzazione dei consumi energetici. I risultati sono riscontrabili dai valori eccezionalmente bassi dei **PUE (Power Usage Effectiveness)** di ciascun Data Center e che si compongono complessivamente in un **valor medio di 1,55** nettamente inferiore al valore di 1,6 previsto come obiettivo dalle "Linee Guida per il Consolidamento dei Datacenter della Pubblica Amministrazione" di AgID. In particolare, il Data Center **tier IV** in Campus Metropolitano di **Fastweb Caracciolo** per l'erogazione dei servizi, dispone di soluzioni tecnologiche tali da avere un **valore di PUE pari 1,25,** che rappresenta l'eccellenza nello scenario nazionale. Le

principali soluzioni tecnologiche implementate per garantire tali livelli di efficienza energetica agiscono sulla riduzione del fabbisogno energetico dei dispositivi in uso, sulla riduzione della dissipazione di calore e sull'efficienza del sistema di condizionamento e sulla scelta di componenti ICT ad alta efficienza:

- **impianti di Illuminazione** progettati e realizzati con tecnologie e materiali a basso consumo energetico e con dissipazione di calore prossima allo zero (lampade a led, fluorescenti o a basso consumo);
- **dispositivi di monitoraggio e attuatori** che consentono il controllo e lo spegnimento automatico dei dispositivi utilizzatori che non risultano necessari all'operatività (ad es. lampade con sensori di movimento);
- **PDU (Power Distribution Unit) intelligenti** ad alta efficienza che governano la distribuzione della potenza in funzione del carico e che quindi minimizzano gli overload e quindi la dissipazione di calore;
- **alimentatori degli apparati IT a singola fase** e dotati di regolatori di tensione a bassa dispersione;
- **sistemi di raffreddamento dei rack ad elevato rendimento**: 1) ad acqua con alta efficienza del rapporto tra potenza refrigerante e calore dissipato; 2) ad aria utilizzante un flusso front to back mai interrotto o deviato durante il suo percorso che minimizza la quantità di aria necessaria al raffreddamento;
- **sistemi di condizionamento free cooling** che sfruttando la differenza di temperatura tra l'ambiente interno ed esterno diminuendo il fabbisogno energetico dei chiller;

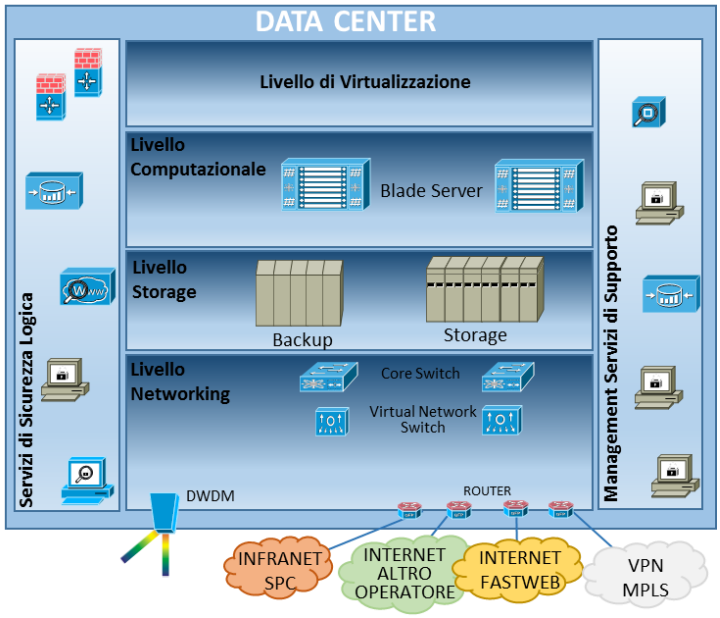


Figura 15: Infrastruttura ICT di ciascun Data Center

- **sistemi di condizionamento modulari** permettono di impostare in modo adattivo le potenze refrigeranti in funzione del calore che deve essere dissipato;
- **sistemi di compartimentazione** che segmentano le aree dati (Rack) in corridoi caldi e freddi che evitano la miscelazione tra aria calda e fredda;
- **sistemi UPS ad alto rendimento** con fattori di potenza estremamente elevati e con bassi contenuti di armoniche che massimizzano la potenza fornita agli apparati IT e minimizzano le perdite di potenza attiva;
- **sistemi UPS modulari** che favoriscono la scalabilità e l'adattamento alle variazioni di carico del Data Center (minimizzazione dei gruppi UPS attivi);
- **server ad elevata densità** (in termini di CPU, core e memoria) ad alte prestazioni ridurranno ancor più il numero di macchine fisiche necessarie a parità di capacità computazionale, minimizzando il consumo per processore;
- **meccanismi di CPU Scaling** disponibili nelle tecnologie prescelte, permetteranno la gestione della potenza elaborativa in funzione del carico applicativo delle singole macchine permettendo la modulazione del consumo energetico delle CPU;
- **cavi SFP+ CU** riducono i consumi energetici rispetto ai tradizionali 10GBASE-T (0,7 W/porta rispetto ai 2-5 W/porta);
- **Dynamic Power Capping** ovvero gestione di soglie dei consumi sui singoli server o su insiemi di server/enclosure.

Struttura organizzativa e processi per il controllo e l'abbattimento dell'impatto ambientale

Parallelamente alle soluzioni tecnologiche elencate, l'RTI si è dotata di strumenti e di **un'organizzazione dedicata** a rendere ancora più efficaci le misure adottate. Questa comprende unità operative, processi di gestione e di miglioramento con una precisa assegnazione delle responsabilità specifiche. La responsabilità dei processi di monitoraggio, analisi e miglioramento dell'efficienza energetica è assegnata, in ciascun centro servizi, al **Local Energy manager.** Questa figura coordina le Unità di Energy Management dedicate al controllo, monitoraggio e Assesment dei dati di impatto ambientale e alla gestione degli impianti tecnologici (cfr. § 3.3.2.2.3) interagendo con le strutture di Local Facility Management. L'Energy manager ha anche la responsabilità di individuare e promuovere azioni di miglioramento tecnologico/organizzativo per l'adattamento alle nuove tecnologie,

interagendo con il Responsabile dell'innovazione tecnologica ed con il supporto del Capacity Manager. Sarà sua cura, infine, redigere report ed analisi da sottoporre mensilmente al Responsabile tecnico e al Responsabile dell'Evoluzione Tecnologica con l'obbiettivo di verificare l'aderenza alle caratteristiche dichiarate e promuovere eventuali azioni di miglioramento. Per rendere ancora più efficace il processo di efficientamento energetico, i Local Energy manager sono supportati da **EMODS (Energy Management Optimization and Decision Support),** piattaforma specifica di gestione e monitoraggio energetico interamente progettata e sviluppata nei laboratori e nell'Energy Competence Center di Selex-ES. EMODS controlla tutti i dispositivi e le apparecchiature, offrendo una serie di funzionalità di analisi utili a definire azioni di efficienza immediate per ridurre sia i consumi attuali sia quelli previsti nei momenti di maggiore attività. EMODS permette l'aggregazione, in "clusters" virtuali (di sito o di edificio), dell'insieme dei sensori e degli attuatori garantendo all'Unità Energy Management una gestione dinamica e proattiva delle criticità che generalmente limitano le opportunità di risparmio energetico. EMODS inoltre consente l'integrazione dei dati di misura rilevati con i dati meteo e le quotazioni di costo dell'energia elettrica, permettendo analisi e benchmark. Tali informazioni offrono una visione completa ed evolutiva dei processi dal punto di vista dell'energia assorbita in tutte le sue forme: energia elettrica, termica, acqua calda, frigorie, etc. L'Energy Management, attraverso l'elaborazione delle informazioni precedentemente descritte, è in grado di redigere linee guida di intervento e conduzione rivolte alla complessiva riduzione dei consumi e quindi degli impatti ambientali.

3.3.2.2.3 Architettura ICT

Le componenti architetturali ICT dei Centri Servizi utilizzano soluzioni tecnologiche leader di mercato e allo stato dell'arte. L'infrastruttura, basata su ambiente completamente virtualizzato, è estremamente modulare e ampiamente scalabile, in grado di sostenere le eventuali richieste aggiuntive di risorse elaborative. L'architettura adottata è di tipo "Multilivello" (Multi-layer Architecture) in cui le componenti sono organizzate in livelli contraddistinti da diversi domini di responsabilità (in linea con il principio di *separation of concerns*) e che comunicano solo attraverso interfacce ben definite. In sostanza, **ogni layer *disaccoppia* quelli confinanti**, consentendo così l'intrinseca modularità dei sistemi. Il concetto di architettura multilivello è ampiamente utilizzato nei sistemi ICT. L'esempio più noto è il modello ISO-OSI per i protocolli di comunicazione, ovvero il più semplice modello del TCP/IP. I razionali per la diffusione di questo modello architetturale sono ampiamente documentati in letteratura, si vuole qui solo ricordare quanto questi modelli siano abilitanti per la modularità, la flessibilità e la scalabilità dei sistemi che li adottano, a garanzia della disponibilità dei servizi che le piattaforme dovranno erogare: Nello specifico sono descritti: 1) Livello di Networking, 2) Livello Computazionale, 3) Livello di Storage, 4) Livello di Virtualizzazione. A supporto trasversale dei quattro Layer sono previsti i Servizi di Sicurezza (cfr. § 3.3.2.1.2) e le piattaforme di Management dei Servizi di Supporto (cfr. § 3.3.2.2.4)

Livello di Networking

Il livello di Networking individua le caratteristiche tecnologiche relative alla rete esterna ai Data Center e alla rete interna. FASTWEB in qualità di fornitore di servizi di connettività sia in ambito residenziale sia in ambito Enterprise ed in particolare rivolto verso le Pubbliche Amministrazioni (attualmente primo fornitore nell'ambito del contratto SPCConn), dispone di un'estesa infrastruttura di backbone altamente scalabile. I collegamenti esterni ai Centri Servizi saranno pertanto dimensionati in modo da gestire l'effort derivante dall'erogazione dei servizi ed eventuali picchi di attività, effettuando adeguati upgrade di banda. Di seguito riportiamo le componenti di interconnessione al backbone per i collegamenti esterni ai Data Center:

Collegamento	Descrizione
Tra tutti i Data Center	Collegamenti dedicati in alta affidabilità in tecnologia DWDM, in fibra ottica, e banda garantita. Elevata velocita e scalabilità.
Tra tutti i Centri Servizi	Rete VPN MPLS in alta affidabilità e con banda garantita, che realizza l'intranet di Back-end (Intranet di Management).
Da tutti i Data Center verso la Internet Pubblica	Collegamento in alta affidabilità con 2 ISP: Fastweb e Altro Operatore entrambi con banda garantita.
Da tutti i Data Center verso la rete SPC	Collegamento in alta affidabilità con banda garantita.

L'interconnessione diretta con i principali carrier nazionali ed internazionali, tramite peering dedicati o attraverso l'interconnessione diretta con i principali Neutral Access Point italiani (MiX e NaMex) e l'interconnessione diretta con la rete QXN SPC, garantisce al backbone un'ampia scalabilità, anche per i collegamenti Internet e Infranet. Lo stesso backbone fa parte dell'Autonomous System di Fastweb (AS12874). Le caratteristiche tecnologiche della rete interna, comprendono l'utilizzo di Core Switch di classe Data Center ad elevata densità e bassissima latenza. Le particolari caratteristiche di performance, scalabilità e propensione alla gestione di ambienti virtuali, ne fanno

dei dispositivi idonei agli ambienti Cloud. Tali apparati rappresentano il nodo centrale di interconnessione in tecnologia 10GigaEthernet IPv4 e IPv6 di tutti i Data Center.

Livello Computazionale

Le risorse costituenti questa parte di infrastruttura, virtualizzate dal software di virtualizzazione (Hypervisor) del Layer sovrastante, includono:

- **Nodi computazionali** Tale sottosistema hardware è costituito dai seguenti sistemi e componenti: (i) **sistemi di enclosure** costituiti da chassis con componenti fisiche ridotte nella numerosità (ridotta complessità e scarsa necessità di gestione) ed efficienti sistemi di raffreddamento; (ii) **server fisici** per i quali vengono utilizzati Blade Server multisocket e multicore ad alta densità, elevata efficienza energetica e bassa dissipazione.
- **Virtual Switch**: abilitano le estensioni alla rete di livello 2 tra nodi computazionali fisici diversi. Questi estendono logicamente la rete fisica alle macchine virtuali e consentono una gestione avanzata del traffico da e verso le singole macchine virtuali all'interno degli host VMware ESX/ESXi.

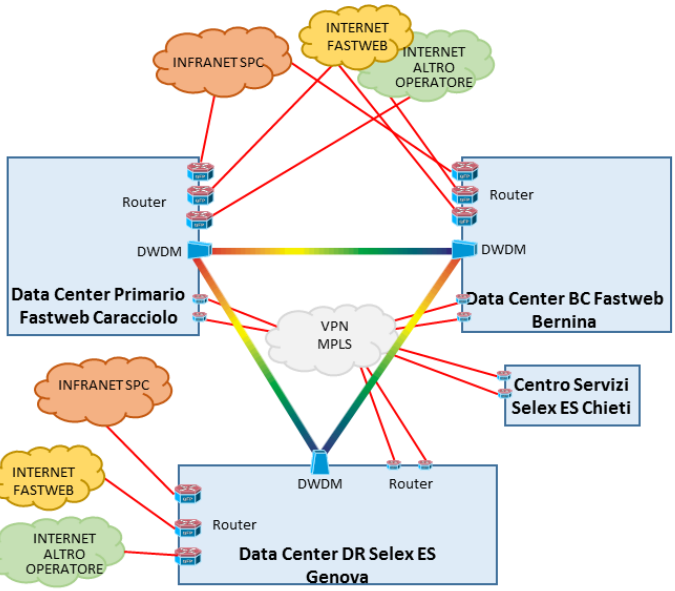


Figura 16: Architettura di Networking

- **Virtual appliance**: realizzano sistemi che implementano policy di sicurezza all'interno della virtual farm con le relative appliance di routing virtualizzate. Gli apparati virtual firewall permettono di gestire la sicurezza del traffico intra-server consentendo un'efficace interazione con i singoli server dell'ambiente ESX. Sulla base delle regole impostate è quindi possibile creare zone sicure con schemi di comunicazione fra macchine virtuali che prescindano dall'indirizzamento IP.

Livello di Storage

Il livello relativo alle risorse di memorizzazione massiva include i due sottosistemi:

- **Storage**: si occupa di offrire le risorse di memorizzazione dell'infrastruttura ed è configurato con dischi SSD, NL-SAS, SATA con funzionalità di autotiering e con protezione geografica del dato attraverso la replica sincrona verso il DC di BC ed asincrona verso il DC di DR garantendo un valore di RPO ≤ 1.
- **Backup**: viene utilizzata un'infrastruttura che garantisce sia la scelta del range temporale di salvataggio che i giorni di retention in conformità alle best practice e comunque ai requisiti di gara. Il sistema utilizza Server dedicati per il backup, proxy server su cui girano gli agent, una rete di backup dedicata (o VLAN) a questa attività al fine di non appesantire la rete di produzione.

Livello di Virtualizzazione

Si occupa della corretta configurazione e funzionamento delle risorse e delle soluzioni di "back-end" sia HW che SW, necessarie alla gestione **dell'infrastruttura multi-tenant**. L'Hypervisor impiegato è **vSphere di VMware** nella versione 5.5. I prodotti VMware, presenti sul mercato dal 1998, hanno ricevuto negli anni enormi riconoscimenti ed anche per il 2014 sono risultati posizionati nel Magic Quadrant di Gartner, ben al di sopra dei loro competitor. **È quindi il prodotto di eccellenza allo stato dell'arte**. Gli elementi principali con i quali si effettuerà la gestione dell'ambiente virtuale sono:

ESX server, software con architettura bare-metal che realizza la virtualizzazione con elevate prestazioni e che consente l'allocazione dinamica delle risorse di calcolo favorendo la scalabilità dei sistemi mettendo a disposizione un'infrastruttura ad alta affidabilità ed elevati requisiti di sicurezza. L'architettura bare-metal ha le seguenti caratteristiche: (i) consente l'accesso diretto ed efficiente alle risorse di I/O per la comunicazione lato rete e lato dischi; (ii) garantisce sicurezza intrinseca dello strato di virtualizzazione anche in virtù della limitata quantità di codice di cui è composto il kernel. Lo strato di virtualizzazione è installato in modalità più simile ad un sistema operativo piuttosto che ad una applicazione.

VirtualCenter è l'elemento attraverso il quale vengono forniti servizi di controllo degli accessi, monitoring delle performance, configurazione e gestione delle VM (virtual machine) che possono essere unificate a formare un singolo computing server. Il servizio **VMotion** di VCenter è la tecnologia con la quale si opera il trasferimento della configurazione software complessiva da un sistema fisico origine ad un sistema fisico destinazione. E' inoltre in

grado di trasferire lo stato della memoria di una VM attiva, da un server ESX ad un altro (i dati, il software e la partizione di boot sono collocati su infrastruttura Storage).

SRM-Site Recovery Manager è l'elemento attraverso il quale verranno implementate le soluzioni di Disaster Recovery e che quindi si occuperà di replicare gli ambienti vSphere automatizzando le procedure di partenza del sito di DR e la successiva ripartenza del sito primario al momento del ripristino delle funzionalità (garantendo in tal modo il requisito di RTO ≤ 4 ore).

Test Bed

Il fornitore metterà a disposizione di Consip/AgID una piattaforma tecnica (Test Bed), per tutta la durata del Contratto Quadro, che consentirà l'esecuzione di prove di collaudo atte a verificare la conformità dei servizi erogati a quanto richiesto dal Capitolato Tecnico e ad eventuali modifiche concordate in corso d'opera dal Comitato di Direzione Tecnica.

La piattaforma sarà ospitata presso uno dei centri servizi dell'RTI e consentirà l'esecuzione delle verifiche funzionali per i servizi richiesti. Il fornitore, oltre all'infrastruttura fornirà anche il personale necessario per l'esecuzione dei test. Il Test Bed sarà utilizzato per il collaudo di tutti i servizi del Lotto, ad esclusione dei servizi professionali. Oltre ai servizi relativi al lotto, il Test bed sarà utilizzato per i test ed il collaudo di:

- il portale di governo e gestione della fornitura.
- il portale di richiesta/configurazione dei servizi.
- gli strumenti di monitoraggio dei servizi, compresa l'interazione con i servizi di governance.

L'infrastruttura di Test Bed sarà allestita su una piattaforma di virtualizzazione che permetterà di riprodurre l'ambiente di produzione che permetterà di testare ogni singola funzionalità richiesta.

In particolare saranno presenti tutte le componenti SW, i moduli funzionali e le configurazioni richieste per l'erogazione del servizio oggetto di collaudo, ivi compresa l'alta affidabilità. Per la natura modulare dell'ambiente virtualizzato a supporto del Test Bed, tali configurazioni potranno essere salvate in un template e riutilizzate in tempi successivi per qualsiasi verifica, modifica o rilevazione si rendesse necessaria.

La gestione di tale infrastruttura sarà sotto la responsabilità della funzione di ICT Operation e del suo responsabile, che ne risponderà della corretta gestione e manutenzione, nonché di renderla disponibile per i test.

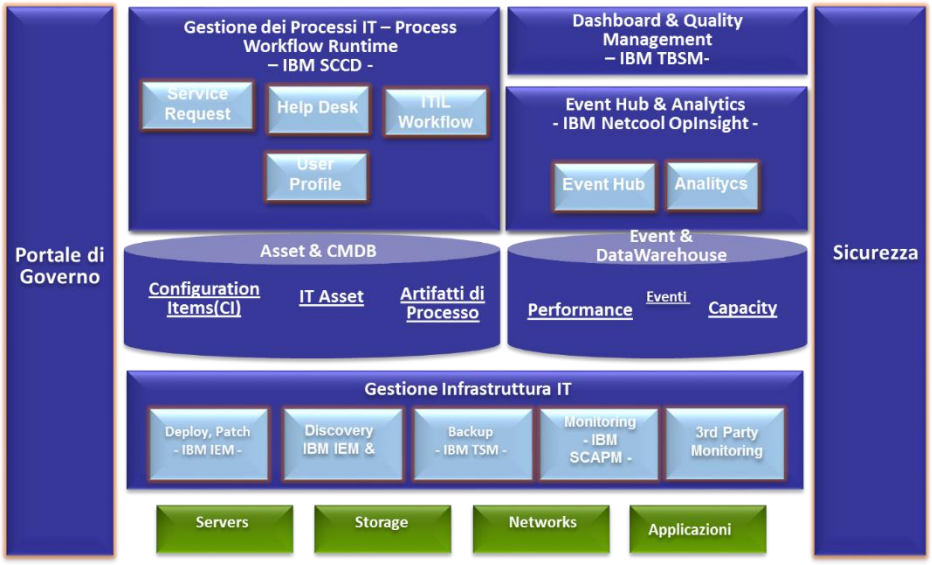


Figura 17: Piattaforma IBM per l'ITSM ed OSS

3.3.2.2.4 Piattaforme Sistemistiche

La soluzione tecnologica adottata per la gestione dei servizi IT è **IBM ITSM** che aderisce ad una architettura di riferimento di IT Service Management per le Service Operation in **conformità con le linee guida dello standard ITIL®v3 e con le linee metodologiche del Knowledge Base IBM ITUP** (IBM Tivoli Unified Process) descritto in precedenza. La piattaforma IBM proposta si posiziona da diversi anni consecutivi ai vertici delle soluzioni di mercato del settore cosiddetto Operations Support Systems (OSS). Gartner ha rilasciato di recente (Ottobre 2014) la nuova valutazione sui principali sistemi OSS di mercato confermando IBM nel quadrante Leaders per i vendor di queste tecnologie. L'architettura della soluzione adottata è imperniata sul CMDB (Configuration Management Database) e la gestione dei processi IT si basa sulle informazioni in esso contenute. Partendo dal basso, nella Figura 17, si rappresentano tutti gli elementi dell'infrastruttura IT ed i relativi gestori (Element Manager). Essi fungono anche da sorgenti informative del **CMDB** per il suo popolamento iniziale e per il suo continuo aggiornamento. La sicurezza all'interno della piattaforma viene gestita la profilazione degli utenti. Viene fornito con la piattaforma SCCD un vasto corredo di workflow allineati ad ITIL®v3. Attraverso di essi è possibile veicolare l'attribuzione delle responsabilità degli interventi a uno o più attori durante le automazioni.

Piattaforme componenti	Descrizione
IBM Smart Cloud Control Desk (SCCD)	Automazione e ottimizzazione dei processi IT: gestione delle richieste di servizio, gestione degli incident, dei problemi, dei livelli di servizio, change e configuration management, asset management, apertura dei trouble-ticket, richiesta di deployment di un server virtuale, installazione di un pacchetto applicativo, verifica di compliance ed installazione delle patch per un server, backup di un server o di una applicazione.
IBM Tivoli Storage Manager (TSM)	Backup e ripristino per una vasta gamma di sistemi operativi. TSM ha una struttura architetturale in grado di garantire un alto livello di prestazioni, è totalmente automatizzabile, estremamente scalabile e multipiattaforma sia in termini di server di salvataggio che di client da salvare.
IBM Connections	Strumento di social collaboration che abilita la comunicazione con le reti di esperti dei processi di business, facilitando una più efficiente condivisione di informazioni e documenti, la generazione di nuove idee, la valorizzazioni di skill e competenze, la gestione dei progetti. Ha come funzionalità principali: Dashboard; messaggistica Istantanea; file sharing; wiki; forum; bookmark; blog; ideation blog; attività.
IBM Netcool Operation Insight –Netcool	Raccolta e consolidamento di dati ed eventi di monitoraggio provenienti da tutta l'infrastruttura. Netcool/OI si basa sulle capacità di analisi in tempo reale degli eventi di IBM Tivoli Netcool/OMNIbus, leader di mercato degli strumenti di Event Management. Gli eventi sono raccolti all'interno di un database relazionale ad alta prestazioni (milioni di eventi al giorno) e presentati agli utenti tramite viste personalizzabili tramite appositi filtri. Interfaccia grafica accessibile via web anche da dispositivi mobile. Funzionalità di reportistica avanzata.
IBM Tivoli Business Service Manager (TBSM)	Gestione della Qualità del Servizio. Permette di visualizzare i servizi di business IT e assicurarsi che siano sempre disponibili all'interno delle finestre di servizio concordate. Analisi real-time dell'impatto di eventi sul servizio e gestione della procedura di assegnazione di eventi agli appositi utenti; tracking real-time delle metriche di SLA (downtime, best case availability, MTTR); viste di business personalizzabili, provviste di grafici e indicatori numerici di qualità dei servizi; visualizzazione dinamica degli indicatori di qualità rilevanti per il servizio; grafici relativi agli indicatori di qualità per i servizi. Visualizzazione dei livelli di servizio su dashboard customizzate.
IBM Rational Asset Manager (RAM)	Gestione degli asset. Implementa una Definitive Media Library che possa contenere e governare il ciclo di vita degli asset software in un ambiente collaborativo. Tale libreria consente di: catalogare, usare e riusare, gestire e creare report degli asset in essa contenuta siano essi software o più orientati al business.

3.4 Il Servizio di Help Desk

Il RTI erogherà il servizio di Help Desk attraverso un unico punto di contatto per i Referenti dell'Amministrazione; tale servizio, mediante più livelli di assistenza, svolgerà attività di accoglienza, interpretazione delle richieste, diffusione di informazioni, troubleshooting, Incident & Problem Solving, Change Management, Knowledge management e tutto quanto altro richiesto dal capitolato tecnico.

3.4.1 Modello Organizzativo

Per garantire l'efficacia del servizio è stata studiata una soluzione fondata sui seguenti principi ► Help Desk basato su: **1° Livello,** che, tramite la funzione di **Service Desk**, rispondendo al 90% delle domande con il Supporto Informativo, coadiuvato da figure di **"personal assistant"** esperti del contesto specifico di una determinata tipologia di amministrazione e con il Supporto Tecnico tenta una prima risoluzione degli incident di minor complessità, mirando a chiuderne fino al 60%; **2° Livello** altamente specializzato in funzione delle tematiche tecnico/applicative o contrattuali ► stretta interazione con la struttura organizzativa di gestione CQ e CE con processi agili di escalation ed efficaci modalità di formazione iniziale e continua del personale ► utilizzo di strumenti che permettono la condivisione di un'ampia **knowledge base** ed il pieno accesso di tutti gli operatori ai sistemi di monitoraggio della fornitura, anche in modalità collaborativa con il Referente dell'Amministrazione.

Le figure di responsabilità rappresentate nel disegno organizzativo sono: **Help Desk Manager**, che governa tutte le strutture di erogazione comprese nel 1°e 2° livello di HD e si interfaccia con il **Responsabile Formazione**, allo scopo di selezionare le risorse e programmare gli interventi formativi specifici per ogni livello di assistenza; **Responsabile della Knowledge Base** per supervisionare la raccolta dei contenuti e sistematizzare il processo di popolamento della base dati; Coordinatore Operatori e Coordinatore Tecnico, che hanno invece il compito di orchestrare il lavoro delle risorse che operano rispettivamente nel Service Desk e nel Supporto di 2° livello .

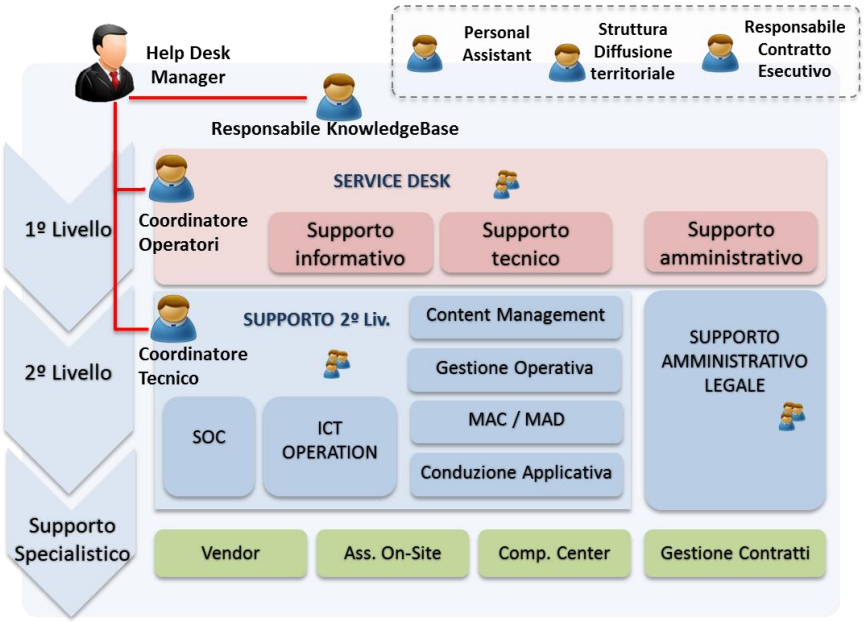


Figura 18: Organizzazione Help Desk

Il RTI, **quale elemento migliorativo** ha deciso di introdurre la figura di **Personal Assistant**, un ruolo che assume una particolare rilevanza quando l'Amministrazione contraente abbia in essere più rapporti contrattuali con le stesse aziende del RTI; questa funzione, rivestita dai Team Leader operativi di maggior seniority, consente una interazione diretta con le altre strutture interne, semplificando enormemente il processo di gestione e sgravando al Referente dell'Amministrazione il passaggio attraverso più strutture.

Team	Principali Responsabilità	Interazioni e Processi
Service Desk 1° Livello	accoglienza e primo punto di contatto coi Referenti PA; creazione Ticket e gestione del suo ciclo di vita; presa in carico delle richieste di tipo informativo, fino alla chiusura delle stesse; escalation delle richieste alle strutture di competenza; popolamento della Knowledge base; gestione proattiva dei ticket; richiesta feedback periodici all'Amministrazione; gestione reportistica dei livelli di servizio.	interagisce con l'Amministrazione per tutte le richieste di informazione e incident sui servizi; governa il processo di Request Fulfillment, Incident Mngt. collabora coi Personal Assistant che hanno completa visibilità sullo stato di avanzamento delle richieste/ segnalazioni. (Questa figura, dedicata al singolo CE, potrà essere contattata telefonicamente, attraverso la selezione dell'opportuna scelta IVR oppure tramite il canale web.) attiva la Struttura di Diffusione Territoriale in fase di Comprensione ed attivazione del CQ tramite interagisce con il Team di Supporto Amm./Legale per attivare la struttura di Gestione Contratti in fase di Contratto Esecutivo
Supporto Tecnico 1° Livello	Presa in carico degli Incident tecnici e primo tentativo di risoluzione con ausilio della knowledge base; popolamento della Knowledge base Tecnica; escalation degli incident verso il Supporto 2° Livello;	effettua l'analisi e la risoluzione degli Incident di tipo tecnico a bassa complessità; interagisce con il Supporto 2° Livello per l'analisi dei problemi e la valutazione dei change;
Supporto 2° Livello	gestione dei Ticket non risolti dal Supporto Tecnico; supporto tecnico per problematiche inerenti il servizio di Firma/Timbro; supporto tecnico per problematiche inerenti il servizio di Sicurezza; supporto per problematiche inerenti l'Identità Digitale apertura task di assistenza verso	interagisce con il Supporto Tecnico del 1° Livello per arrivare alla risoluzione degli Incident; coordina e gestisce i processi di Problem e di Change Management; interviene su specifiche tematiche tecnologiche/funzionali interagisce con strutture interne di Help Desk dell'Amministrazione; interagisce con le funzioni di Supporto Specialistico

	strutture di supporto specialistico interne ed esterne.	(Vendor, Assistenza on-site, Competence Center).
Supporto Amministrativo/Legale	supporto alla gestione degli aspetti amministrativi e legali relativi alla predisposizione di un nuovo CE diffusione di informazioni di dettaglio su dati amministrativi inerenti un CE in corso; guida all'utilizzo degli strumenti di collaboration, billing, document management, etc.	interagisce con i team di 1° Livello o con il Referente dell'Amministrazione per approfondire e comprendere le esigenze amministrative richieste; collabora direttamente con i Responsabili Diffusione Territoriale e Contratto Esecutivo per dirimere le questioni legali e amministrative più complesse; interagisce con le strutture di governo per segnalare problematiche nella gestione degli aspetti amministrativi.
Supporto Specialistico	Vendor; Centri di Competenza Assistenza on-site	interagisce con HD 2° Livello per supportare analisi e risoluzione degli Incident, Problem o risoluzione di bugs; partecipa al processo di Change Management

3.4.2 Metodologia di erogazione

Secondo l'impostazione del RTI l'Help Desk evolve da semplice punto di assistenza ad un punto di accesso ad informazioni e dati relativi al Contratto Quadro, in completa interazione con la struttura organizzativa di CQ e di CE e con gli strumenti di monitoraggio e governo della fornitura.

Fase	Assistenza Tecnica	Assistenza Amministrativa
Comprensione Contratto Quadro e Attivazione	Esposizione dei **benefici tecnici dei servizi** e inquadramento nella visione integrata dell'Agid. **materiale informativo** sui **contenuti tecnici** dei servizi **Fornitura di manualistica** e procedure di accesso a sistemi dimostrativi	**Informazioni sul valore economico** e simulazioni. Diffusione di **materiale informativo**, listini e documentazione contrattuale, modelli di piano dei fabbisogni etc. Accesso al contatto diretto con **Struttura Commerciale**
Contratto Esecutivo	Documentazione sull'**impianto metodologico** di erogazione dei servizi Richieste di documentazione dei **livelli di servizio** Apertura di **Incident/change ed attivazione del processo di risoluzione**	**Aggiornamenti** sullo stato avanzamento delle procedure contrattuali **e dell'attivazione dei servizi** secondo il piano dei fabbisogni Accesso alla **documentazione contrattuale** **Reportistica di dettaglio** sull'utilizzo dei servizi (per dipartimento/utente/periodo) **Supporto all'utilizzo** degli **strumenti** di gestione e monitoraggio anche mediante **accesso collaborativo**

L'Help Desk **multicanale**, erogato secondo gli orari ed i livelli di servizio previsti nella documentazione di gara, garantisce accessibilità e fruibilità con molteplici modalità quali: ► utilizzo del **numero verde unico**, appoggiato su di una infrastruttura VOIP ad alta affidabilità che connette i siti di erogazione in continuità operativa ►**fax** integrato con l'infrastruttura di HD ► modulo self service su **interfaccia web** e **posta elettronica**. Quale caratteristica migliorativa il RTI propone l'accesso anche tramite **app dedicate** per Android, iOs e Windows Phone. La condivisione della conoscenza e l'accesso al **PGGF** (cfr § 5.2.4.1), tramite cui poter sfruttare indistintamente moduli di collaboration, knowledge management, e-learning, base documentale, reportistica e altro ancora, sono la chiave del successo per un Help Desk totalmente integrato con strutture interne ed esterne al singolo Centro Servizi. I flussi di comunicazione sono infatti facilitati dall'utilizzo di un Portale trasversale a tutti i servizi e a tutti i livelli di organizzazione, sfruttato da tutte le strutture del RTI coinvolte e accessibile anche all'Amministrazione.
Nella fase di Comprensione Contenuto CQ e Attivazione, l'HD si configura come un vero e proprio sportello di **front office**, per accogliere qualsiasi tipo di richiesta, sia Tecnico, sia Amministrativo/Legale, per facilitare la comprensione dei contenuti e degli argomenti oggetto di una eventuale attivazione del CE, per attivare un contatto diretto con il personale di riferimento o soddisfare la richiesta tramite informazioni, chiarimenti, esempi e dimostrazioni pratiche su utilizzo e beneficio dei servizi offerti. Nella fase di Contratto Esecutivo, il principio che guida le procedure ed il funzionamento dei flussi di HD per l' **Assistenza Tecnica** si ispira al **Knowledge-Centered**

Support (KCS), una metodologia che racchiude processi ed azioni focalizzate sulla **condivisione della conoscenza** come la chiave per un'efficiente ed efficace organizzazione del customer & technical support. Secondo questa logica gli operatori, agevolati dagli **strumenti di collaboration** creano e raccolgono contenuti utili e riutilizzabili nel processo di Incident Management, adoperandosi per migliorarli e/o correggerli in tempo reale, in base alla domanda e alla loro utilità, specialmente allo scopo di coadiuvare i processi di Problem e Change Management. I dati raccolti nei ticket vanno ad incrementare il patrimonio di conoscenza ed esperienza proveniente dal bagaglio di competenze di tutti gli attori del Contratto Quadro. La KnowledgeBase nasce infatti già alimentata con tutto lo scibile pregresso, raccolto dalle aziende del RTI in anni di conduzione di servizi simili verso le PA e viene messa a disposizione di tutte le strutture operanti nell'erogazione dei servizi del CE, favorendo lo scambio e la condivisione di informazioni utili ad ogni livello di gestione della fornitura. L' **Assistenza Amministrativa** in fase di CE, grazie agli strumenti condivisi implementati nel PGGF (cfr § 5.2.4), attinge a piene mani ai contenuti della documentazione contrattuale, ai dati di monitoraggio e andamento dei servizi (KPI, fatturazione, etc…), al piano dei fabbisogni e ad ogni altra informazione che possa essere utile a soddisfare la richiesta. Il **Personal Assistant** in virtù della sua conoscenza dell'amministrazione e preparazione, può guidare l'operatore nella corretta risposta ed arricchire la KB con le informazioni utili alla risoluzione di problemi che trasversalmente impattano su servizi acquisiti da più contratti.

3.4.3 Strumenti

IBM SmartCloud Control Desk (SCCD) è la soluzione completa ed integrata di ITSM proposta dal RTI e che consente l'automazione e l'ottimizzazione dei processi IT, dal Trouble Ticketing, alla gestione delle richieste di servizio, alla gestione di incidenti, problemi, livelli di servizio, al Change e Configuration Management, all'Asset management. La suite è certificata per 12 processi ITIL® tramite Pink Elephant PinkVerify™. IBM SCCD fornisce in un unico prodotto la gestione dei processi che lavorano ed interagiscono tra di loro in maniera integrata, condividendo la stessa piattaforma tecnologica, la stessa base dati e lo stesso motore dei processi. Si possono aprire ticket tramite:

- **Modulo Self-service**: accedendo direttamente al menù dove utilizzare il service catalog o il ticket template; si può anche verificare lo stato delle richieste aperte e visualizzare la knowledge base.
- **E-mail**: scrivendo alla casella di posta predefinita per uso esclusivo di SCCD, che analizza tutte le mail non lette e apre automaticamente un nuovo ticket, riportando i dati della mail o aggiornando una richiesta già presente nel sistema, qualora nel subject sia stato indicato l'identificativo di un ticket preesistente.
- **Richiesta Telefonica con operatore** parlando direttamente con l'operatore che, dall'interfaccia apre una richiesta con i dati indicati dall'utente; **con sistema di Computer Telephony Integration**, con risponditore IVR e subentro successivo degli operatori che prendono il controllo delle chiamate dalla barra telefonica dell'interfaccia di SCCD.
- **Automatica** attraverso gli strumenti di monitoraggio, che inviano tramite il modulo di integrazione o email, segnalazioni di malfunzionamento o richieste di aggiornamento su segnalazioni aperte in precedenza.
- **Automatica tramite modulo di integrazione bidirezionale** con eventuali sistemi di HD delle Amministrazioni.

Il sistema dispone di funzioni di **knowledge management** per la raccolta delle soluzioni adottate o la registrazione di FAQ e procedure per l'esecuzione di attività ricorrenti. L'Interfaccia utente è unica, completamente configurabile e consente di definire e presentare pagine iniziali differenti (Start Center) sia per i diversi ruoli dei processi IT (Service Desk Manager, End-User, Change Manager, SLA Manager,...) sia per i ruoli organizzativi. SSCD consente un approccio pro-attivo al controllo degli SLA e degli indicatori di qualità con l'ausilio di specifici KPI, copre le esigenze di reportistica sia istituzionale (a posteriori) che real-time, visualizzata sull'interfaccia utente da un cruscotto sul quale si può vedere in tempo reale lo stato delle attività e l'esito di elementi di controllo predefiniti, come l'andamento di KPI, i risultati di query specifiche (in formato lista o grafico), lo stato delle attività assegnate. La reportistica basata sul motore IBM Cognos, viene pubblicata tramite web browser o come invio periodico dei report, nelle caselle di posta degli utenti, utilizzando la componente **IBM Tivoli Common Reporting**.

3.4.4 Impiego delle risorse umane e formazione

Una tra le caratteristiche organizzative di maggior pregio della presente offerta è rappresentata dall'elemento di **complementarietà tra le diverse aziende del RTI**, non soltanto in termini infrastrutturali e di continuità del servizio, ma anche in relazione all'ampia disponibilità di risorse, grazie alla quale lo staffing iniziale potrà essere impostato a livello di **numerosità** e di **qualità di skill** in maniera decisamente ampia. **L'interscambio dinamico delle risorse** tra le aziende del RTI, anche dislocate in siti differenti, rappresenta l'elemento abilitante allo sviluppo, alla condivisione ed al bilanciamento delle competenze, a garanzia della continuità e qualità del servizio

offerto, specialmente in caso di incremento massivo di lavoro. L'organizzazione dei turni per le attività di HD è frutto di un processo continuo di analisi e pianificazione, che tiene conto delle statistiche acquisite quotidianamente sulle chiamate del Centro Servizi per tipologia e durata. Il **dimensionamento è quindi flessibile e adattativo**, in conseguenza dei volumi di traffico in possesso del RTI e del numero di ticket stimato o fornito dall'Amministrazione per singolo CE e sarà studiato sulla base di pregresse esperienze consolidate e utilizzando strumenti di analisi affidabili e diffusi sul mercato, come la formula **Erlang B/C**, tramite cui, in base a tutte le variabili di servizio a disposizione (volumi, tempi di risposta/intervento, incremento di attività su base oraria, SLA etc.) si calcola con precisione il numero di risorse necessarie. Sono oggetto di analisi anche le tempistiche di attivazione e l'andamento dei servizi nelle diverse fasi contrattuali, dallo start-up all'erogazione a regime, nel corso della quale al verificarsi di situazioni che determinano **picchi di lavoro** o in caso di **attività in emergenza** il RTI potrà fare riferimento al bacino di disponibilità costituito da risorse aggiuntive già opportunamente formate e costantemente aggiornate mediante l'uso dello strumento di knowledge sharing, quindi immediatamente integrabili nei team di lavoro. Il RTI pone particolare attenzione alla copertura funzionale e tecnologica degli skill degli operatori e alla loro preparazione professionale, creando da subito un insieme di **precondizioni ottimali** tramite processi di **slezione** (dettagliati in tabella) e di **preparazione delle risorse a 360°**, su tecnologie, metodologie e norme amministrativo/legali in merito a procedure contrattuali, per ogni area tematica della PA. Per catalogare gli skill e le competenze, il RTI ha adottato un framework specifico, secondo il quale i dati dei CV sono memorizzati su un sistema di gestione delle competenze professionali, **Skill Management**, che contiene in forma strutturata le informazioni per ogni singolo tipo di profilo, non solo di Help Desk, e sono mantenuti aggiornati tramite verifiche periodiche.

Criteri di selezione risorse	Processo di Valutazione dell'adeguatezza delle risorse
alto posizionamento in merito a capacità e competenze tecniche	assertività e propensione ad una comunicazione efficace
possesso di nozioni di diritto e preparazione in ambito amministrativo	livello generale delle competenze e conoscenze richieste
maturità professionale ed esperienza pregressa nel ruolo	attitudine al problem solving, capacità di individuare soluzioni tecniche, di anticipare le criticità e di fronteggiare situazioni di stress
atteggiamento professionale e grado di motivazione verso la crescita	capacità di condividere e trasmettere la conoscenza
	propensione all' approccio analitico, a comprendere le variabili chiave di un problema, spirito collaborativo e adattabilità alla mutevolezza del contesto

Dalla consapevolezza che le esigenze di formazione e aggiornamento delle risorse su Contratti quali SPC, assumono una particolare importanza per via della loro durata e ampiezza, il RTI sceglie un approccio metodologico all'addestramento ispirato alle linee guida AGiD, in cui sono definite le norme generali ed i livelli essenziali delle prestazioni per la formazione e l'addestramento del personale. L'attività di formazione, caratterizzata da contenuti, metodologie didattiche e modalità di erogazione, che prevede le diverse tipologie: **tradizionale** in aula, **corso CBT**, fruibile su PC; **corso WBT**, con moduli e materiali didattici via WEB; **corso "blended"** in modalità di erogazione mista; **servizi di community** (Web-mail, Forum, News, Sondaggi e Suggerimenti, Chat e FAQ) sulla piattaforma didattica di **e-learning** PGGF (cfr 5.2), viene costantemente **rimodulata e adeguata**, sia in termini di contenuti sia di numero di risorse partecipanti per seguire l'andamento e l'evoluzione dei servizi. La formazione avverrà anche mediante meccanismi di "formazione ai formatori" e a cascata su gruppi omogenei di operatori (ad esempio "Skill Group"), ogni qualvolta si rilevi la necessità di interventi mirati in un'ottica di miglioramento continuo (ITIL). Per tali interventi formativi sarà predisposto opportuno materiale didattico, a cura dalla **Segreteria Didattica** (cfr. § 4.8) anche fruibili tramite piattaforma di Knowledge Management (cfr. § 5.2.4.5).

L'interazione diretta con le strutture organizzative garantisce un **costante aggiornamento trasversale** su tutte le competenze tecniche, tecnologiche, tematico/funzionali ed amministrative. La documentazione messa a disposizione e tutte le nozioni relative ai corsi di formazione rimangono sempre disponibili all'interno della **KnowledgeBase** per consultazioni successive, fornendo così a tutti gli utilizzatori l'opportunità di refresh formativi e la possibilità di consultazione a supporto del processo di risoluzione delle richieste.

4 SOLUZIONI

La seguente tabella riassume i razionali di sostenibilità delle soluzioni descritte nella presente proposta tecnica e delle caratteristiche che ne avvalorano la loro sostenibilità.

Ambito	Valore della proposizione del RTI	Vantaggio atteso per PA

Rispetto dei requisiti	I requisiti della Gara sono già stati oggetto di implementazioni da parte del RTI per altri progetti della PA	Approccio consolidato del RTI al tema Migliore soddisfazione degli impegni contrattuali Rispondenza alle normative e best practice nazionali e internazionali
Approccio al cambiamento	Approccio specifico alla gestione del cambiamento, dal quadro normativo, all'organizzazione, ai processi fino alle tecnologie - Organizational Resilient Model (ORM)	Migliore rispondenza ai requisiti Alta qualità ed affidabilità
Soluzione organizzativa	L'organizzazione risponde alle richieste della PA in modo rigoroso, avvalendosi di strumenti e modalità operative chiaramente definiti che supportano le fasi di acquisizione, configurazione e gestione, consentendo di introdurre le necessarie flessibilità	Maggiore rispondenza alle richieste di autonomia operativa, facilità d'uso, efficienza e flessibilità
Soluzione tecnologica	L'organizzazione risponde alle richieste della PA avvalendosi di soluzioni allo stato dell'arte e di eccellenze metodologiche e tecniche del RTI e dei suoi Competence Center, che favoriscono l'introduzione di proposizioni innovative, efficaci e modulari	Maggiore rispondenza ai requisiti di Gara in termini di efficienza operativa e di innovazione tecnologica
Strategie e piani di test, utilizzo di test automatici	Le strategie, l'organizzazione e gli strumenti di test adottati, in particolare quelli automatici, garantiscono qualità, affidabilità e performance del servizio	Rispondenza ai requisiti Alte qualità e affidabilità del software Aderenza agli standard
Utilizzo di strumenti e soluzioni tecnologicamente avanzate	L'adozione della strumentazione proposta facilita il rispetto dei requisiti di accessibilità, usabilità ed aderenza al sistema per la gestione delle Identità	Maggiore adozione dei Servizi di gestione delle identità e di sicurezza e promozione della cooperazione tra Amministrazioni
Multicanalità / usabilità	Possibilità ed opportunità di fruire del servizio mediante una pluralità di canali di contatto, quali ad es. device Smartphone, tablet, mobile via browser http/https.	Estrema usabilità, completezza ed affidabilità della soluzione offerta
Ulteriori elementi qualificanti della proposta	Introduzione di soluzioni evolute sotto il profilo funzionale, tecnologico e contenutistico, quali ad esempio il **Portale dell'Identità e di Firma/timbro,** gestione avanzata delle vulnerabilità applicative di ultima generazione, tecnologie di sicurezza innovative.	Proposta di soluzioni evolute, facilmente accessibili e evolutive rispetto ai requisiti

4.1 Soluzione per l'erogazione dei servizi di Identity Provider e I&AM

Nel presente paragrafo si descrivono i servizi per la **gestione delle Identità digitali** proposti dal RTI.

Lo scopo dei servizi di gestione delle Identità Digitali è, come indicato dal dall'art. 17-ter del decreto-legge 21 giugno 2013, n. 69 "favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità". E' infatti ormai riconosciuto in senso ampio e generale - si vedano, a puro titolo di esempio, il regolamento eIDAS, il Regolamento 910/2014 della Comunità Europea e svariati obiettivi della DG Connect - che la disponibilità di un mezzo di identificazione certo costituisce uno dei principali abilitatori della digitalizzazione dei processi dei settori pubblico e privato. L'identificazione digitale costituisce quindi condizione fondamentale per lo sviluppo dell'Agenda Digitale Europea e, pertanto, di uno dei 7 pilastri di quella Strategia Europa 2020 che intende rilanciare lo sviluppo, la crescita ed il ruolo dell'Europa e dei suoi Stati Membri nel contesto mondiale.

Riconoscendo la particolare criticità della corretta e sicura gestione delle identità digitali in rete, il governo italiano ha istituito con il predetto decreto, ed a cura dell'Agenzia per l'Italia Digitale, il sistema per la gestione delle Identità Digitali denominato SPID, con validità per l'ambito pubblico e privato, e con il successivo DPCM 24 ottobre 2014, pubblicato sulla G.U. 285 del 9-12-2014, ne ha definito le caratteristiche e le modalità di adozione. Tali caratteristiche e modalità non possono prescindere dalla disponibilità di una soluzione tecnologica ed operativa che implementi le funzionalità necessarie allo SPID: l'attuale gara individua questa soluzione nell'implementazione delle specifiche SAML 2.0, riferite ad un complesso contesto normativo, tecnologico ed organizzativo di seguito descritte. Il RTI propone anche funzionalità innovative e migliorative sulla base sia delle

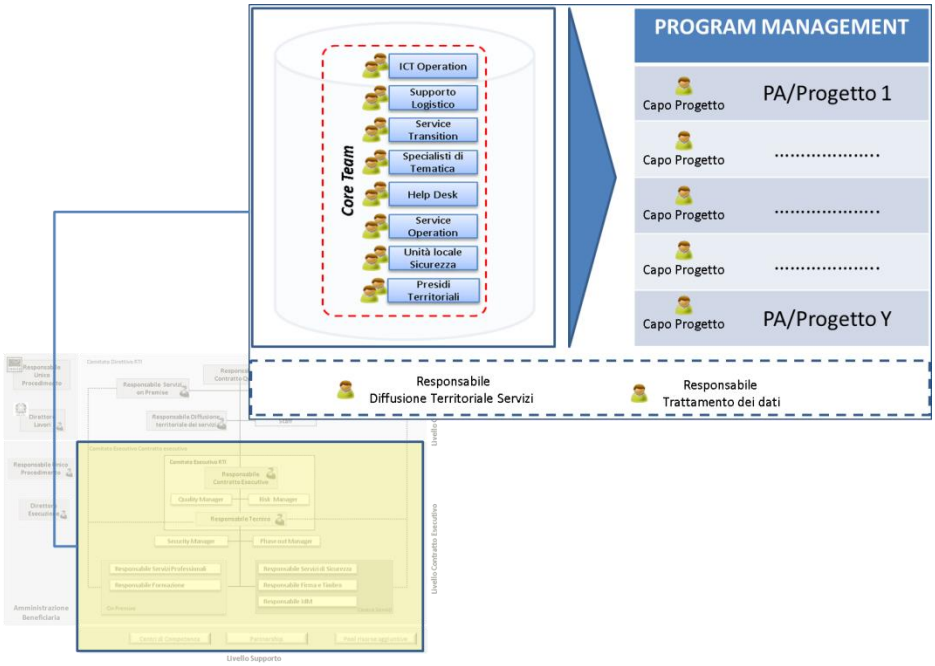
proprie esperienze operative sia della partecipazione delle aziende costituenti a comitati consultivi pubblici e di categoria (es. Confindustria Digitale, Assinform, Assintel) ed a gruppi di lavoro internazionali su temi specifici.
Di seguito l'esposizione si divide in descrizione delle soluzioni organizzative e tecnologiche. La soluzione organizzativa è di seguito divisa in due paragrafi, "Soluzione organizzativa Identity Provider" (cfr § 4.1.1) e "Soluzione organizzativa di Identity and Access management (I&AM)" (cfr. § 4.1.3). La soluzione tecnologica sarà invece introdotta in modalità congiunta (cfr. § 4.1.4) e poi specificata per i due servizi (IdP cfr. § 4.1.4.1, I&AM cfr. § 4.1.4.3)

4.1.1 Soluzione organizzativa Identity Provider

Il modello organizzativo per l'erogazione del servizio è ispirato ad alcuni concetti fondamentali particolarmente preziosi per massimizzare l'effort delle strutture operative impegnate a fronte di obiettivi chiari e ruoli ben definiti. I principi di resilienza, adattività e flessibilità sono dunque alla base di una gestione integrata dell'insieme di strutture, processi operativi e flussi informativi sottesi che saranno posti in essere dal RTI, al fine di soddisfare le mutevoli esigenze dell'Amministrazione e nel rispetto di livelli prestazionali condivisi. Nello specifico il RTI prevede:

- La disponibilità di una rete di **punti di servizio** (Presidi Territoriali) sul territorio nazionale, attivabile in modo flessibile, fino ad una dimensione di 15.000 punti, che coprono capillarmente il terriorio nazionale, con presenza diffusa a livello regionale, provinciale e comunale.
- **la costituzione di un gruppo di lavoro** ispirato ai principi del modello organizzativo ORM - Organizational Resilient Model, secondo cui un insieme eterogeneo di **Core Team**, specifici per tipologia di attività, saranno tra loro coordinati per gestire una pluralità di realizzazioni in parallelo e adeguarsi, in modo flessibile, alle necessità derivanti da picchi di lavoro, cambiamenti organizzativi, normativi e più in generale dello specifico scenario attuativo. I Core Team saranno supportati dal **Competence Center I&AM** (Rif. § 3.2.2.3), costituito da team multidisciplinari che attingono dalle reti la migliore competenza ed eccellenza metodologica e tecnica. La sua struttura è costituita da una **rete di specialisti nelle metodologie/tecnologie** di Sicurezza e gestione dell'Identità Digitale, a diretto contatto con i principali software/hardware vendor. Al suo interno sarà attivo un **Laboratorio Tecnologico** (dotato di **Certificazione ISO 27001:13** del **Sistema di Gestione della Sicurezza delle Informazioni, IMQ, CSQ**), che opera sia come osservatorio avanzato sul mercato delle tecnologie innovative, sia per approfondimenti tematici relativi a specifici ambiti progettuali.

> Le reti di competenza del RTI sono rappresentate da: il **SOC** (Security Operation Center) di **Selex-ES,** in grado di supportare PAC e PAL sia dal punto di vista metodologico che tecnologico in tutti gli stadi del processo di gestione dell'Identità Digitale nei suoi aspetti di sicurezza; **la Digital Agency** di **IBM** composta da 1.500 risorse nel mondo.



- Di volta in volta, per ogni Amministrazione, verrà costituito uno specifico Gruppo di Progetto, coordinato dal **Capo Progetto**, che opera in collaborazione con un **Responsabile Diffusione Territoriale Servizi** (per tutti gli aspetti legati all'analisi dei fabbisogni della PA), con il **Responsabile del Trattamento dei dati** ed i Responsabili di Team (per lo svolgimento di tutte le attività operative). Inoltre, all'avvio del primo servizio per ogni singola Amministrazione, il Capo Progetto potrà corrispondere al Responsabile del servizio stesso e quindi al Responsabile IdM (Rif. § 3.2.2.2). I diversi Gruppi di Progetto attingono dai Core Team le risorse necessarie alla composizione dei team tecnico/specialistici.

- Il **Gruppo di Progetto**:
- seguirà la realizzazione dei servizi di IdP curandone tutti gli aspetti (di processo, architetturali e tecnologici) nel rispetto dei tempi, delle normative e metodologie adottate e coerentemente con i processi dell'Amministrazione;
- è dotato di competenze e certificazioni specifiche rispetto alle principali tecnologie di mercato e proprietarie;
- ha conoscenza ed esperienza sugli aspetti implementativi e di processo, in relazione al ciclo di vita dell'Identità Digitale e già applicati in contesti internazionali;
- aggiorna le proprie competenze e/o risorse in linea con l'evoluzione del contesto (normativa, organizzativa, tecnologica) relativa al servizio erogato o all'Amministrazione di riferimento.

la definizione di un insieme di processi (corredati di procedure di dettaglio e flussi informativi), a supporto dell'erogazione del servizio sia nei confronti del Cittadino sia della Amministrazione, che saranno disegnati coerentemente con i principali modelli di gestione del ciclo di vita delle identità, ispirandosi a contesti internazionali similari e/o sviluppati nell'ambito di gruppi di interesse specifici a cui le aziende del RTI partecipano attivamente (es. WG 5 Identity Management and Privacy Technologies, ISO/IEC JTC 1). L'insieme dei processi sarà sviluppato nel rispetto delle regole tecniche e delle modalità attuative per la realizzazione dello SPID. La Figura 19 seguente illustra il modello organizzativo nelle varie fasi di servizio.

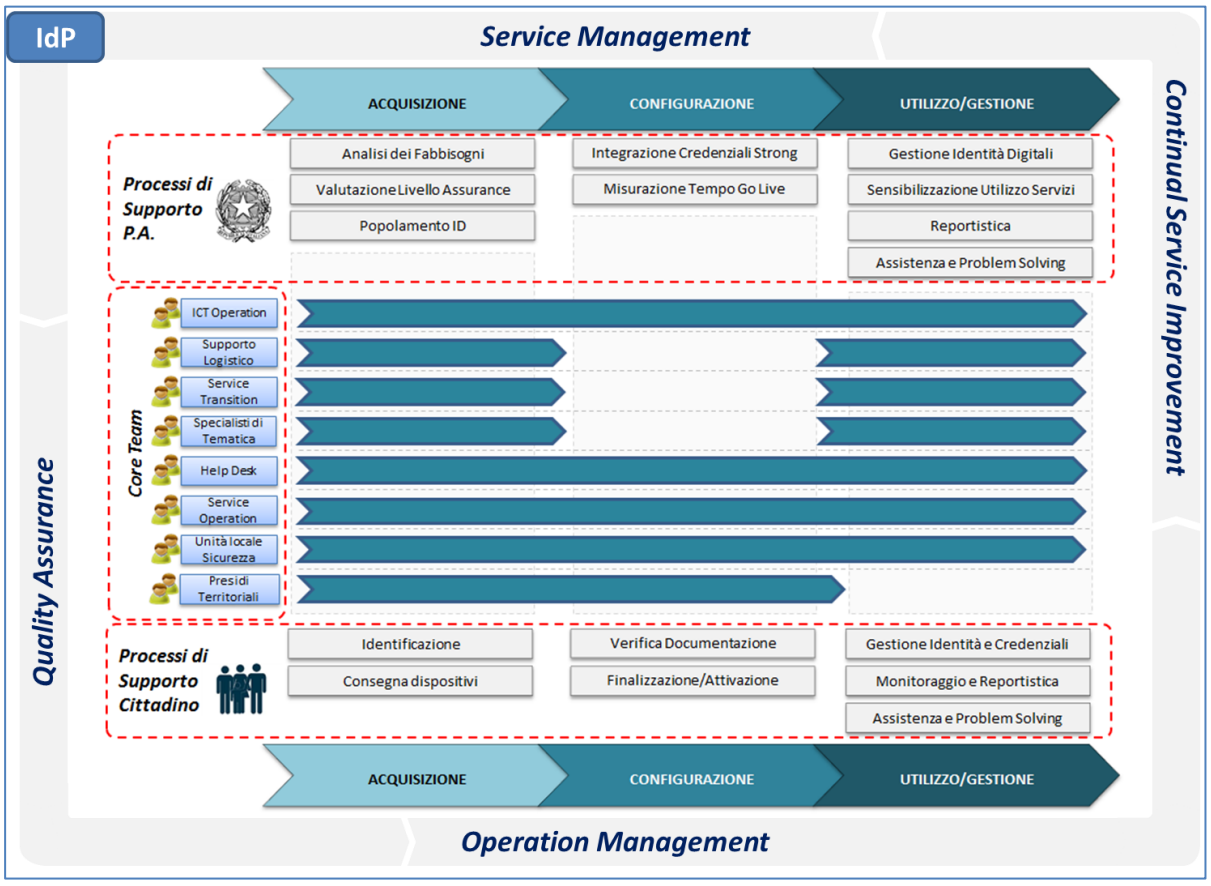


Figura 19: Modello organizzativo IdP

Nel dettaglio, la struttura organizzativa del **Team di Progetto** viene attivata prima della firma del Contratto Esecutivo e coordinata dal Capo Progetto, per avviare la fase di Acquisizione. I diversi **Team di Progetto** attingono dai Core Team le risorse necessarie alla composizione dei team tecnico/specialistici, così come mostrato in Figura 19.

Tale organizzazione, presentata alla PA tramite il "Piano di Attuazione" all'interno del Progetto dei Fabbisogni, permette di modulare dinamicamente la composizione dei vari team lungo le fasi che compongono il **ciclo di vita del servizio** di gestione dell'Identità Digitale (Acquisizione, Configurazione e Utilizzo/Gestione), in relazione alla specifica **fase** ed ai relativi **processi di supporto** (sia riferito alla PA che al Cittadino), bilanciando opportunamente l'impiego delle figure professionali coinvolte. L'intero flusso operativo è inserito all'interno di un contesto metodologico, basato su standard e best practice internazionali, prevede attività di

Service/Operation Management e Quality Assurance in un'ottica di miglioramento continuo del servizio (Continual Service Improvement).

4.1.1.1 Team e Figure Professionali

Di seguito le principali figure professionali coinvolte.

Figura professionale	Figura profess. RTI	Principali compiti/responsabilità
CAPO PROGETTO	**Responsabile IdP**	Supervisiona lo svolgimento del servizio e si coordina con i referenti della P.A. e del RTI (es. Resp. Contratto Esecutivo, Resp Diffusione Territoriale, ecc.). E' responsabile della consistenza e dell'adeguatezza sia quantitativa che qualitativa del team di cui dispone, coinvolgendo il Resource Manager qualora necessario.
RESP. Trattamento Dati Personali	**RESP. Trattamento Dati Personali**	Responsabile delle attività secondo quanto stabilito dal Garante per i Dati Personali di cui al d.lgs. 30.06.2003 n° 196
Responsabile delle attività di verifica dell'identità personale	**RESP. delle attività di verifica dell'identità personale**	Responsabile delle attività di verifica personale nel rispetto di quanto indicato nel Capitolato Tecnico al punto 2.1.

Nella tabella seguente i Core Team e le relative figure professionali coinvolte

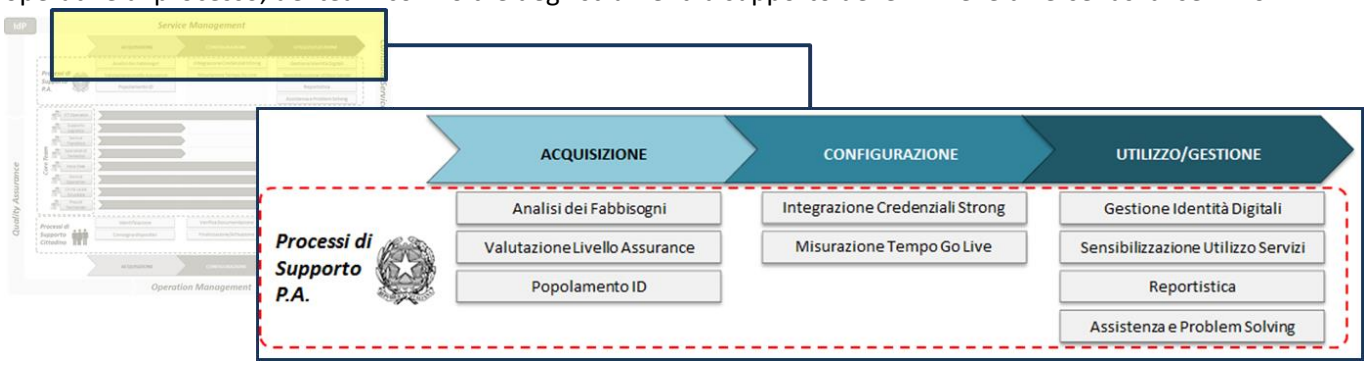
Tabella 8: Team e Figure professionali previste per il servizio di Identity Provider

Team	Figura profess. del Team RTI	Principali compiti/responsabilità
ICT OPERATION (Conduzione tecnologica infrastruttura)	**Rif. Centro Servizi**	Conduzione dell'infrastruttura tecnologica
SUPPORTO LOGISTICO (Logistica, trasporti, capacity planning, gestione scorte e materiali)	**Responsabile Logistica**	Responsabile attività di approvvigionamento e movimentazione materiali
	Addetto	Personale di supporto alle attività logistiche
SERVICE TRANSITION (Governo e controllo attività di transizione Servizi)	**Spec. di Change Management**	Esperto di metodologie e soluzioni tecnologiche per quanto concerne le tematiche legate alla portabilità ed interoperabilità
	Analista Funzionale	Responsabile analisi delle funzionalità che il sistema dovrà erogare
	Capacity Manager	Responsabile della produzione e dell'aggiornamento del capacity plan, che include la domanda di servizi attuale e la previsione dei bisogni futuri in relazione alla quantità di ID da gestire, della tipologia di credenziali e delle relative infrastrutture abilitanti, tenendo aggiornati ed allineati i tre Data Center da cui sono erogati i servizi.
SPECIALISTI DI TEMATICA (Figure specializzate su tematiche inerenti la realizzazione di servizi di IdP)	**Specialista di processo**	Specialista di processo (inclusi i temi di Privacy)
	Analista Funzionale	Responsabile analisi delle funzionalità che il sistema dovrà erogare
	Analista di Sicurezza	Identifica, verifica e garantisce l'efficacia delle misure di sicurezza adottate
	Data Base Architect	Progettazione delle basi dati e sviluppo strategie per l'acquisizione ed il caricamento
	Specialista di prodotto /tecnologia	Possiede una profonda conoscenza delle architetture e delle tecnologie specifiche in tema identità digitale
HELP DESK (SPOC per support PA e Cittadino)	**Responsabile HD**	Coordina il team di Help Desk
	Team Leader	Coordina gruppi di operatori organizzati per skill group
	Operatore	Operatore multicanale
SERVICE OPERATION (Conduzione tecnologica	**Technical Service Manager**	Responsabile tecnico dei servizi e delle risorse necessarie all'erogazione del servizio nel rispetto degli indicatori di qualità previsti

infrastruttura specialistica di IdP)	**Data Analyst**	Analisi dei dati sull'utilizzo dei servizi, trend e contenuti
	System Architect	Cura l'approccio tecnologico e la produzione dei risultati di progetto, garantendo livelli elevati di capacità analitica e di risultato in fase di analisi delle informazioni.
	Specialista di processi di ID	Specialista di processo in ambito ID
	Specialista di prodotto /tecnologia	Possiede una profonda conoscenza delle tecnologie e delle problematiche di natura tecnica connesse con la realizzazione dei servizi di identità digitale
UNITA' LOCALE SICUREZZA	**Resp. ULS**	Responsabile dell'Unità (rif. § 3.3.2.1.2)
	Resp. attività di verifica Identità Personali	Responsabile attività secondo quanto richiesto nel Capitolato Tecnico rif. 2.1.1 e 2.1.2
	Addetto	Personale di supporto alle attività
PRESIDI TERRITORIALI (Rete di punti di contatto per il Cittadino)	**Resp. di Presidio**	Opera in coordinamento con il Resp. delle attività di verifica delle Identità Personali e coordina gli addetti alle attività.
	Addetto	Personale di supporto alle attività

4.1.1.2 Modalità Operative di Processo e Strumenti a supporto della PA

Nel presente paragrafo verrà dettagliato il servizio di Identity Provider descrivendo nello specifico le macro fasi del servizio (Acquisizione, Configurazione e Gestione) ed i relativi processi, fornendo evidenza delle modalità operative di processo, dei team coinvolti e degli strumenti a supporto delle PA nelle diverse fasi di servizio.



Il RTI, sulla base del contenuto del Capitolato Tecnico e degli scopi finali del servizio di Identity Provider, illustrerà nel seguito del paragrafo gli elementi principali della soluzione che sarà in grado di garantire autonomia operativa, facilità d'uso, efficienza e flessibilità alle PA che aderiranno al servizio di Identity Provider (IdP). La soluzione proposta trova completezza di gestione in termini di modalità operativa all'interno delle fasi sopra elencate. L'attività di"chiusura" del servizio verrà descritta e dettagliata nel paragrafo § 4.5.

Nel seguito del documento le fasi di acquisizione, configurazione ed utilizzo/gestione del servizio, saranno declinate negli specifici processi, dettagliando per ognuno gli elementi salienti (descrizione, deliverable e team del RTI coinvolti). In ogni processo è previsto il coinvolgimento sia del RTI, sia della PA.

FASE	ACQUISIZIONE
PROCESSO DI SUPPORTO ALLA PUBBLICA AMMINISTRAZIONE	**Analisi dei fabbisogni** Deliverable: Piano/Progetto dei fabbisogni Team RTI coinvolti: Service Transition, Specialisti di Tematica, Help Desk Descrizione: a. Il RTI condivide con l'Amministrazione le caratteristiche operative del servizio ed il quadro normativo vigente al momento dell'acquisizione del servizio relativo alla gestione delle identità (ivi compresi gli aspetti legati alla privacy) per consentire una decisione autonoma e consapevole in merito a tipologia e numerosità di utenti da coinvolgere. Tale attività agevolerà i processi operativi anche nella successiva fase di configurazione; b. a supporto della definizione del piano dei fabbisogni, il RTI fornisce anche una strumentazione (es. cruscotto decisionale) con la quale è possibile analizzare le evidenze individuate a valle dell'analisi (es. dimensionamento).
	Supporto alla valutazione del Livello di Assurance (LoA2, LoA3 e LoA4) Deliverable: documento di analisi del rischio LoA2/3/4, modello di consegna in modalità sicura

FASE	ACQUISIZIONE

Team RTI coinvolti: Specialisti di tematica, Help Desk

Descrizione:

a. documento di analisi del rischio LoA2/3/4 - la corretta attribuzione del Livello di Assurance (LoA) da assegnare ai cittadini passa attraverso una valutazione del rischio cui sono soggette le applicazioni che faranno riferimento al servizio di Identity Provider. Al fine di rendere il processo di acquisizione delle identità quanto più efficiente possibile, garantendo la capacità di protezione necessaria, il RTI propone la propria elevata esperienza in questo tipo di analisi, supportando la PA nell'identificazione in totale autonomia del livello di assurance maggiormente opportuno da rilasciare al cittadino (associato ad un livello LoA2, LoA3 o LoA4). Ciò favorirà l'accesso ai servizi ed applicazioni da parte dei Cittadini e degli utenti delle aziende e PA interessate. Si ricorda che nel caso in cui i fornitori di servizi per i quali viene richiesta l'autenticazione siano Pubbliche Amministrazioni dovranno essere consentite solo i livelli di sicurezza LoA3 e LoA4 (rif. Capitolato tecnico 2.2.2.4), salvo differente indicazione come emerge dai chiarimenti alla Gara (*Rif. I tranche-199 - "Il livello di assurance (LoA) viene stabilito dall'amministrazione erogatrice di servizi (o applicazioni) web e può essere diverso da servizio a servizio (ad es. servizi orientati alle consultazioni possono avere associati dei LoA bassi, altri servizi potranno avere dei LoA di tipo 2 o superiore*).

b. i modelli di processo di generazione, rilascio e distribuzione delle credenziali LoA2/LoA3/LoA4 definiti dal RTI e presentati alla PA sono conformi agli standard di sicurezza previsti in questi casi (modalità sicura, rif. Cap. Tec. 2.2.2). I processi sottesi garantiscono altresì il necessario grado di autonomia di cui deve disporre la PA al fine di poter soddisfare i propri bisogni specifici (rapidità di esecuzione, "categorizzazione" degli utenti finali, ad es. solo persone giuridiche ecc.).

Popolamento identità digitali

Deliverable: report esito caricamento

Team RTI coinvolti: Service Transition, Specialisti di Tematica, Service Operation, Help Desk

Descrizione:

a. "migrazione", ricadono sotto questa modalità di popolamento, la presa in carico e la migrazione delle identità gestite dall'amministrazione, direttamente o tramite un fornitore terzo (rif. 2.7 Cap. Tec.). In considerazione del fatto che il servizio di IdP è sostanzialmente concepito per agevolare la migrazione delle identità digitali attualmente già detenute da un'amministrazione verso un identity provider esterno con il quale si è stabilita una relazione di fiducia (trust) (Rif. pag. 7 Capitolato Tecnico Lotto 2) ed al fine di agevolare un'analisi in completa autonomia della consistenza totale o parziale del contenuto informativo relativo al parco utenti già in possesso della PA, il RTI predispone specifici "manuali di istruzione" e relative "check list". Ciò permetterà anche di identificare le attività eventualmente necessarie per rendere il dato maggiormente consistente;

A supporto di un test efficace di valutazione dei volumi di utenti potenzialmente migrabili, il RTI predispone opportuna strumentazione, basata su una soluzione web based, che garantisce flessibilità e facilità d'uso, rendendo agevole la simulazione ed il caricamento massivo; la strumentazione supporta le operazioni di caricamento, con massima flessibilità grazie alla compatibilità con i principali standard del settore (LDAP, DB RDBMS, flat file, ecc.).

In ogni caso, la migrazione non può prescindere dall'attività di riconoscimento del richiedente l'identità digitale; in tale contesto, le modalità operative da seguire sono esplicitate nel paragrafo *seguente "ex-novo"*

b. "ex-novo"

- condivisione con la PA del modello attuativo relativo alle procedure di registrazione previste dal Capitolato Tecnico e dei relativi processi e strumenti a supporto (Portale dell'Identità Digitale, Presidi Territoriali, ecc.).;
- nel caso in cui la PA voglia effettuare per proprio conto le attività di verifica dell'identità personale, il RTI mette a disposizione il "Portale dell'Identità Digitale" attraverso cui l'Amministrazione potrà operare in completa autonomia. Tale Portale, che rappresenta un elemento aggiuntivo della presente offerta, è nativamente integrato con la piattaforma di attivazione dell'Identità e sarà realizzato nel rispetto dei criteri di usabilità ed accessibilità secondo la normativa vigente (cfr. Linee guida per i siti web della PA, 2011). L'attività di rilascio dell'identità verrà completata da parte del RTI, senza soluzione di continuità;
- tenendo conto del precedente deliverable "Documento di analisi del rischio LoA2/3/4", verrà richiesto all'Amministrazione di indicare la massima numerosità di utenti da registrare e gestire ed indicare il relativo LoA da assegnare. Il processo è reso particolarmente flessibile grazie alla pluralità di strumenti disponibili per l'autenticazione;
- le identità non immediatamente migrabili per insufficienza di attributi, pur detenendo l'Amministrazione alcuni dati, nonché il caso in cui il Cittadino si presenta presso un Presidio Territoriale per la registrazione, sono entrambi contemplati nel presente caso d'uso;

c. su base "incrementale"

Per ogni nuova Amministrazione che intenda usufruire sottoscrivere per la prima volta il servizio di Identity

FASE	ACQUISIZIONE
	Provider, sarà possibile attivare delle "economie di scopo" sfruttando identità digitali già censite per altre PA, valutando in completa autonomia la possibilità di associare anche la propria "titolarità" su ogni specifica identità.

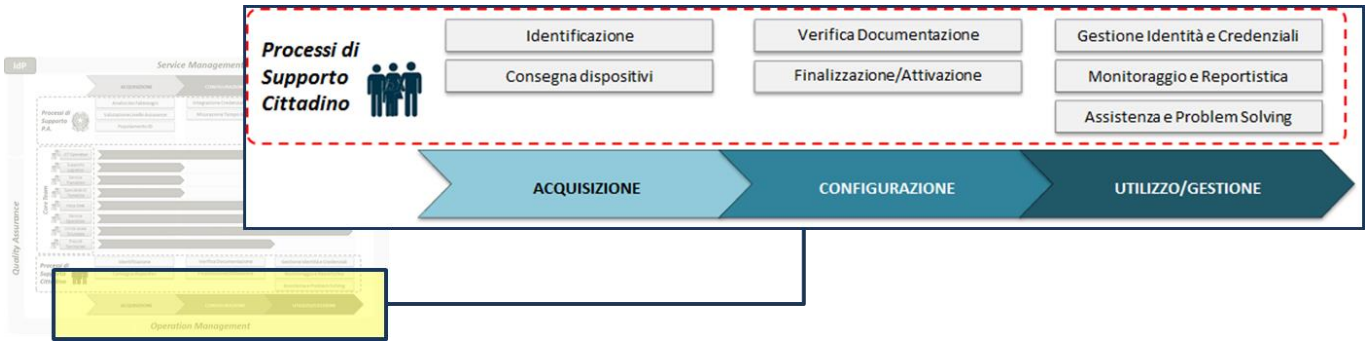
FASE	CONFIGURAZIONE
PROCESSO DI SUPPORTO ALLA PUBBLICA AMMINISTRAZIONE	**Integrazione credenziali strong per le identità digitali** Deliverable: Report sulla distribuzione Team RTI coinvolti: Service operation, Help Desk
	Descrizione: A tutti gli utenti che verranno dotati di identità digitale sarà necessario consegnare le nuove credenziali LoA2 ed i nuovi strumenti di autenticazione LoA3 o LoA4. Sarà compito del RTI rendere autonoma l'Amministrazione nella verifica dello stato di avanzamento della consegna. A tale scopo, mediante gli strumenti resi disponibili, verrà mostrato lo stato del processo di distribuzione, sino alla verifica della singola unità, e l'avanzamento nella rigenerazione delle credenziali LoA2. Nel caso di "migrazione" saranno implementati opportuni processi e meccanismi per rendere semplice, efficace e sicura la rigenerazione della password sul nuovo IdP.
	Misurazione del tempo di go-live Deliverable: Report di sintesi Team RTI coinvolti: Service Operation, Presidi Territoriali, Help Desk
	Descrizione: Il tempo di go-live rappresenta uno degli indicatori fondamentali per l'aggiornamento dell'Amministrazione sullo stato di avanzamento delle attività. Gli strumenti messi a disposizione dal RTI permettono di misurare e verificare accuratamente gli indicatori ed i tempi condivisi con l'Amministrazione nella fase di Acquisizione. Tale indicatore potrà giungere ad un approfondito livello di dettaglio (misurazione su singola identità), includendo anche il tempo di consegna del supporto di autenticazione LoA3 o LoA4.

FASE	GESTIONE/UTILIZZO
PROCESSO DI SUPPORTO ALLA PUBBLICA AMMINISTRAZIONE	**Reportistica** Deliverable: Report Team RTI coinvolti: Service Operation, Help Desk
	Descrizione: Alla PA è garantitala possibilità di verificare in autonomia quale sia lo stato di utilizzo del servizio. A tale scopo è resa disponibile ulteriore reportistica specifica, aggiuntiva a quella prevista, anche in forma aggregata accessibile mediante il "Portale dell'Identità Digitale" e il "Portale di Governo della Fornitura".
	Sensibilizzazione all'utilizzo dei servizi di Identity Provider Deliverable: Report del trend di utilizzo dei servizi digitali Team RTI coinvolti: Service Operation, Help Desk
	Descrizione: Il Portale dell'Identità Digitale rappresenta uno degli elementi abilitanti e di supporto per agevolare la PA nell'obiettivo di sensibilizzare l'utenza all'utilizzo dei servizi digitali. Esso costituisce un elemento catalizzatore di contatti e di divulgazione delle tematiche di Identity Provider e dei servizi messi a disposizione da ogni singola PA. Concepito secondo le metodologie di Responsive Design (garanzia di flessibilità e facilità d'uso) e Adaptive Design (simbolo di efficienza), ovvero con metodologie di sviluppo atte ad un miglioramento della strategia comunicativa e della fruibilità dei contenuti su tutti i dispositivi, opererà anche quale volano di ulteriori richieste di contatto/registrazione. A complemento dei contatti via Portale, per fornire informazioni sull'utilizzo dei servizi digitali e relative tendenze , verrà anche utilizzata la soluzione OSINT (http:// www.selex-es.com/it/-/cyber-security), nativamente dedicata alla sicurezza ed erogata mediante l'infrastruttura di supercalcolo di Selex ES, con esecuzione di servizi di sentiment analysis e brand reputation.
	Gestione Identità Digitale (Governo del ciclo di vita dell'identità digitale) Deliverable: processi e procedure tecnico/amministrative Team RTI coinvolti: Service Operation, Specialisti di Tematica, Unità Locale di Sicurezza, Help Desk
	Descrizione: Il Portale dell'Identità Digitale, mediante le sue molteplici funzionalità, permetterà una verifica puntuale dello stato delle identità digitali e delle credenziali associate nonché la gestione di tutte le attività tecnico/amministrative necessarie. Le operazioni saranno eseguite normalmente da personale del RTI ma la flessibilità e semplicità nell'utilizzo della soluzione consente che le stesse possano essere eseguite direttamente dall'Amministrazione, a fronte di espresse esigenze di sicurezza o organizzative.
	Assistenza e Problem Solving Deliverable: reportistica di riscontro Team RTI coinvolti: Help Desk, Service Operation, Specialisti di Tematica, Unità Locale di Sicurezza, ICT Operation
	Il Servizio di Help Desk Telematico costituisce il punto unico di contatto (SPOC) per le Amministrazioni in merito alle tematiche in ambito Identity Provider. L'Help Desk, attivato tramite una pluralità di canali di contatto dai referenti dell'Amministrazione, dialogherà con gli altri

FASE	GESTIONE/UTILIZZO
	Core Team operativi, provvedendo al loro ingaggio funzionale, al coordinamento ed al monitoraggio delle service request, gestendo le tematiche relative. In tale ambito il Portale di Governo della Fornitura costituirà l'interfaccia di comunicazione in uso all'Amministrazione per le attività di gestione, monitoraggio e reportistica. Per una descrizione di dettaglio si faccia riferimento al capitolo ad esso espressamente dedicato (cfr. § 3.4).

4.1.1.3 Modalità Operative di processo e strumenti a supporto del Cittadino

Nel presente paragrafo verrà dettagliato il servizio di Identity Provider descrivendo nello specifico le macro fasi del servizio (Acquisizione, Configurazione e Gestione) ed i relativi processi, fornendo evidenza delle modalità operative di processo, dei team coinvolti e degli strumenti a supporto del Cittadino.



Ogni attività è codificata all'interno di un workflow operativo, gestito mediante opportuni strumenti e soluzioni di tracking, in uso a tutti i team coinvolti, al fine di una gestione completa e facilitata dei processi, un monitoraggio continuo dei livelli di servizio, con relativa reportistica. Oltre quanto già evidenziato precedentemente per la Pubblica Amministrazione, l'interazione tra i diversi team di lavoro viene di seguito dettagliata.

FASE	ACQUISIZIONE
PROCESSO DI SUPPORTO AL CITTADINO	**Identificazione** Il rilascio di un'identità digitale passa attraverso due momenti fondamentali: il riconoscimento del soggetto richiedente e la registrazione dei relativi attributi identificativi, non identificativi e qualificati. Il riconoscimento rappresenta il momento più importante e delicato del rilascio, in quanto è in questa fase che deve essere verificata l'identità personale del soggetto richiedente. Il riconoscimento può avvenire secondo le diverse modalità previste nel Capitolato Tecnico. Il RTI ritiene incluse tutte le ulteriori modalità introdotte nel DPCM. Per alcune è prevista la presenza di personale del RTI opportunamente formato ed abilitato, mentre per altre sarà possibile far sì che il Cittadino agisca autonomamente, mediante apposita procedura guidata tramite il Portale dell'identità Digitale, che mette a disposizione la funzionalità di registrazione degli attributi. Il personale abilitato che svolgerà le attività in presenza, farà capo al Team di Presidio Territoriale, coadiuvato dal Team di Supporto Logistico per assicurare la disponibilità dei dispositivi, nonché le successive attività di distribuzione. **Consegna dispositivi** Solo dopo aver effettuato la verifica dell'identità del richiedente sarà possibile procedere con la registrazione degli attributi e con il rilascio delle relative credenziali da parte dell'Autorità di Registrazione. Il soggetto potrà essere dotato di uno dei livelli di sicurezza previsti dallo standard ISO/IEC DIS 29115: LoA2, LoA3 e LoA4 e la modalità di consegna del dispositivo sarà coerente con il livello di assurance (LoA) individuato. L'attività di consegna (credenziali/dispositivo) potrà avvenire in modo telematico, "in presenza", o tramite spedizione postale, a seconda del LoA definito, o delle opportunità legate al servizio ed alla dislocazione sul territorio dell'intestatario dell'identità, in ottemperanza con le politiche di sicurezza garantite dal Responsabile della Sicurezza, preventivamente concordate con la PA per il tramite dell'ULS. Nel caso di utilizzo del canale telematico l'utente sarà autonomo nel reperire quanto necessario mediante il Portale dell'Identità Digitale. Nel caso di consegna "in presenza" il Team di Presidio Territoriale, coordinandosi con il Team di Supporto Logistico, provvederà all'espletamento dell'attività di consegna del dispositivo. Infine, nel caso della spedizione, il RTI per il tramite del Team di Presidio Territoriale, provvederà alla consegna direttamente al domicilio dichiarato in fase di registrazione dall'utente. In ogni caso, il Team di Supporto Logistico ha il compito di mantenere sempre aggiornato il magazzino ed i Presidi Territoriali, garantendo la disponibilità dei dispositivi e gestendo il livello di riordino.

FASE	CONFIGURAZIONE

FASE	CONFIGURAZIONE
PROCESSO DI SUPPORTO AL CITTADINO	**Verifica Documentazione** L'attività di verifica della documentazione prodotta in fase di identificazione, verrà condotta in modalità automatizzata e con il supporto delle strutture di back office, al fine di verificare la correttezza di tutti gli attributi del richiedente sulla base di documenti, dati o informazioni ottenibili da fonti affidabili e indipendenti, secondo i criteri e le modalità stabilite dall'Agenzia per l'Italia Digitale. Il team di Presidio Territoriale avvia il processo di verifica, effettuata preferibilmente in modalità automatica mediante i sistemi e le soluzioni erogate presso il Centro Servizi ed in uso al Team di Service Operation, secondo le policy di sicurezza garantite dal Responsabile della Sicurezza. L'operatività, nei suoi aspetti di continuità e performance è garantita dal Team di ICT Operation. Eventuale verifica non telematica, sarà svolta con l'ausilio dei Presidi Territoriali. **Finalizzazione/Attivazione** Terminata la fase di identificazione e verifica del richiedente, il Team di Service Operation, nel rispetto delle procedure operative di sicurezza concordate dal Responsabile della Sicurezza con la PA, potrà finalizzare le attività tecniche volte a rendere operativa l'identità e le credenziali rilasciate. In generale, l'attivazione potrà avvenire in maniera non assistita o in modo interattivo su iniziativa dell'utente, utilizzando apposite funzionalità web, gestite anch'esse dal Team di Service Operation; il Presidio Territoriale interverrà soltanto nei casi in cui dovesse essere indicata come modalità maggiormente opportuna in merito ai vincoli di sicurezza, l'interazione con l'utente finale.

FASE	GESTIONE/UTILIZZO
PROCESSO DI SUPPORTO AL CITTADINO	**Gestione Identità e Credenziali** Nel corso del ciclo di vita dell'identità digitale, il cittadino può modificare degli attributi, nonché chiedere la revoca della propria identità e operare sulle proprie credenziali (rigenerazione per smarrimento). Le funzionalità, fruibili mediante il Portale dell'Identità Digitale e con le modalità eventualmente concordate con AgID, sono automatizzate sui sistemi gestiti dal Team di Service Operation e supportate dal Team di Help Desk. Il team di Presidio Territoriale interviene puntualmente in caso di riconsegna di dispositivi fisici. **Monitoraggio & Reportistica** In conformità con quanto richiesto e descritto nel Capitolato Tecnico ed a quanto specificato nelle regole tecniche definite con i regolamenti di cui all'art. 4 (req. 2.6 Cap. Tec.), il Cittadino avrà la possibilità di conoscere i propri dati personali raccolti durante la fase di acquisizione, nonché di ricevere segnalazione sull'utilizzo delle credenziali di accesso. Il RTI implementa questi requisiti tramite apposite soluzioni di auditing e reporting, in modalità self service, continuativa H24, tramite Portale dell'Identità Digitale. Anche le seguenti attività saranno gestite dal Team di Service Operation e supportate dal Team di Help Desk. **Assistenza e Problem Solving** Il Cittadino, durante la fase di utilizzo dei Servizi di Identità Digitale, sarà supportato in tutte le operazioni. Il Servizio di Help Desk Telematico costituirà il punto unico di contatto (SPOC), mediante il Team relativo che dialogherà a sua volta con tutti gli altri Core Team operativi, provvedendo al loro ingaggio funzionale ed al coordinamento e monitoraggio delle richieste di assistenza. Il servizio, integrato con il Portale dell'Identità Digitale, sarà erogato mediante i canali di contatto web ed email.

4.1.1.4 Modalità con cui vengono soddisfatti gli obblighi del gestore di Identità digitale.

Gli obblighi del gestore dell'Identità digitale saranno assolti tramite una specifica attività di Security Assurance, con lo scopo di garantire nel tempo la robustezza, l'efficacia e l'efficienza dei controlli e dei sistemi di sicurezza implementati, nonché l'aderenza puntuale alle norme vigenti.

Tale corpus documentale sarà prodotto con cadenza regolare e conterrà esplicitamente l'indicazione di quanto messo in campo rispetto a tutti gli obblighi espressi sul Capitolato Tecnico. Di seguito la descrizione delle modalità per ogni obbligo richiesto.

Definizione di Procedure e Metodi di Gestione A garanzia della PA, saranno identificate ed applicate procedure e metodi di gestione, definendo ruoli, responsabilità e modalità operative per ogni singolo obbligo del gestore. In particolare, la documentazione operativa del SGSI e del Centro Servizi sarà dettagliata al fine di definire ruoli, responsabilità e modalità operative proprie dei servizi di Identity Provider previsti in fornitura, come del resto già previsto dalle normative utilizzate dal RTI nella gestione dei servizi e del centro servizi (in particolare SGSI e ITIL). Il RTI individuerà, nell'ambito della propria struttura organizzativa, il responsabile delle attività di verifica dell'identità personale come previsto al punto 2.1.2 del Cap. Tec. Le modalità operative previste includono la possibilità, per l'Amministrazione, di effettuare per proprio conto le suddette verifiche o, in alternativa, di affidarle al fornitore.

Gestione misure anticontraffazione. Saranno predisposte tutte le misure idonee per la trasmissione/consegna delle credenziali di accesso (livello LoA2-3-4) all'utente utilizzando come standard di riferimento il ISO/IEC DIS 29115. Nella seguente tabella sono riportate alcune ipotesi di modalità di consegna delle credenziali.

LoA2: la credenziale è una stringa alfanumerica sarà consegnata in due fasi, una contestuale al rilascio e alla registrazione, in formato cartaceo, ed una per via telematica all'unico punto di contatto ufficiale dell'utente (indirizzo e-mail). L'invio della seconda componente è soggetta a conferma da parte dell'utente, perché l'identità diventi attiva. È richiesto il cambio password al primo accesso.
LoA3: la credenziale (es. codice di attivazione per App Mobile) viene rilasciata sotto forma di codice alfanumerico inviata via SMS all'utente (non visibile all'operatore). L'utente scarica l'App dallo Store e può attivare l'App solo inserendo tale codice.
LoA4: la credenziale (es. Smart Card) viene consegnata vuota, il codice di attivazione viene rilasciato via SMS all'utente (non visibile all'operatore). L'utente scarica il certificato sulla Smart Card solo dopo aver collegato la Card al PC via Lettore e inserimento sul portale del codice. Tali codici non sono memorizzati all'interno del sistema e la validità degli stessi viene fatta tramite confronto fra gli hash code.

Monitoraggio Continuo della Sicurezza: La struttura SOC dell'Unità Locale di Sicurezza effettuerà attività continua di monitoraggio della sicurezza tramite rilevamento degli allarmi e dei security incident, in conformità con la procedura di gestione incidenti, inclusa nel Sistema Documentale del SGSI (cfr. § 3.3.2.1.2). Le attività di monitoraggio saranno condotte secondo istruzioni operative specifiche per il rilevamento e la gestione incidenti all'interno del perimetro logico individuato dal servizio di Identity Provider. A titolo esemplificativo tali procedure declineranno le fasi di:

- rilevamento di eventi critici e/o comunque sospetti per la sicurezza dei sistemi e dei servizi di Identity Provider, quali tentativi di accesso multipli, login errati, login multipli, brute force attack, password guessing, accessi da indirizzi IP differenti, analisi del traffico spam tramite strutture di intelligence (es. X-force di IBM), e relativa classificazione degli eventi rilevati, attraverso matrici decisionali di supporto che guidino gli operatori responsabili del monitoraggio nell'analisi, favorendo la completezza, l'efficacia e l'omogeneità delle attività di classificazione;
- gestione degli allarmi e/o degli incidenti rilevati, definendo flussi di lavoro pre-codificati per il contrasto di attacchi noti e modalità operative che comunque favoriscano la rapidità e l'efficacia di intervento di tutte le strutture coinvolte, sino alla chiusura dell'allarme o incidente.

Sono inoltre utilizzati quale ulteriore fonte alimentante per le attività di monitoraggio anche elementi di Early Warning provenienti dall'infrastruttura HPC del RTI per la individuazione di minacce di phishing o evidenze provenienti dai servizi di Brand Reputation (Identità Digitale) e Sentiment Analysis per la valutazione dell'atteggiamento del cittadino nei confronti di tale servizio.

Rapporti con Autorità esterne alla PA. Al fine di assicurare comunicazione con l'Autorità Giudiziaria ed il Garante per il trattamento dei dati personali, saranno predisposti dal RTI degli appositi team di Authority Operation – coordinati dal Referente Fraud Management - all'interno della Unità Locale di Sicurezza. Essi, adeguatamente abilitati, gestiranno i rapporti con l'Autorità e provvederanno all'evasione di specifiche richieste, tra cui la possibilità di conoscere, per il tramite del gestore del servizio, l'identità personale dell'utente. Qualora ritenuto necessario dall'Amministrazione, saranno definite, all'interno del processo di gestione dell'incidente, delle procedure di escalation verso il CERT-PA o altre Autorità, in funzione di livelli di escalation predefiniti dettati dalla severità dell'incidente.

Analisi dei Rischi: Come previsto all'interno del piano di sicurezza sarà eseguita con cadenza almeno annuale l'analisi volta alla rilevazione dei rischi specifici per il servizio. I risultati saranno contenuti in un documento di Valutazione dei Rischi, che sarà consegnato ad AgID/Consip entro 30 gg dalla richiesta. In particolare sarà analizzata l'adeguatezza delle contromisure rispetto alle minacce tipiche del servizio come, ad esempio: Furto di Identità, Accesso Abusivo ai servizi Online, Interruzione di servizio (DoS, DDoS), Perdita dell'integrità/riservatezza dei dati privati e sensibili, Perdita dell'integrità/disponibilità dei log, Intercettazione dei dati in transito, Cancellazione insicura dei Dati personali/sensibili, Perdita delle chiavi di cifratura (dati su Storage e certificati LoA4), Attacchi di Ingegneria Sociale, Accesso abusivo ai siti e ai locali tecnici.

Piano della sicurezza: Il Piano di Sicurezza sarà consegnato ad AgID entro 30 gg dalla richiesta e regolarmente aggiornato. Il Piano di Sicurezza descriverà nel dettaglio tutte le misure progettate e realizzate in base ai risultati della valutazione dei rischi eseguita sul Servizio, a copertura di tutte le specifiche aree di esposizione alle minacce selezionate in fase di analisi.

In particolare, saranno declinate, oltre alle contromisure di sicurezza organizzativa e fisica, i meccanismi di sicurezza logica implementati ed eventuali controlli compensativi, per il contenimento dei livelli di rischio al di sotto di una soglia accettata e condivisa.

Allineamento delle procedure di sicurezza agli standard internazionali: I processi di sicurezza a supporto del servizio saranno allineati, oltre che allo standard ISO 27001, ad altri standard specifici la cui conformità sarà

certificata da un terzo abilitato. Il RTI dispone già di certificazioni internazionali delle caratteristiche richieste, tra cui ad es. l'ISO/IEC 22301:2012 - A Specification for Business Continuity Management, la PCI DSS v2.0, ecc.

Penetration Test: Il RTI verificherà stato di sicurezza e possibili rischi/minacce a cui l'infrastruttura per l'erogazione del servizio è sottoposta, commissionando almeno ogni sei mesi Penetration Test a terze parti qualificate ed indipendenti, i cui risultati verranno forniti all'Amministrazione. I penetration test saranno effettuati su tutte le componenti del servizio utilizzando come riferimento le metodologie OSSTMM e OWASP. Il perimetro di tali test includerà sia la parte tecnologica del servizio, sia quella organizzativa, utilizzando anche tecniche di social engineering per il personale coinvolto nell'erogazione del servizio.

Sicurezza tecnica e crittografica dei procedimenti e gestione sicura delle componenti riservate delle identità digitali: La protezione delle componenti riservate delle identità digitali si realizza intervenendo mediante misure di sicurezza fisica, tecniche e soluzioni di crittografia riconosciute a livello internazionale, recepite dal RTI nei processi e nei sistemi informativi a supporto e periodicamente verificate da terzi qualificati e controlli organizzativi, come descritto nel § 3.3.2.1.2. A titolo esemplificativo, gli storage e i Database su cui sono memorizzati i dati e i log di accesso sono cifrati mediante algoritmi conformi allo standard FIPS 140-2 ed i flussi applicativi interni sono tutti cifrati per impedire l'accesso ai dati in transito.

4.1.2 Referenze

Le referenze di seguito riportate sono quelle maggiormente significative rispetto alle specificità delle attività per il servizio in oggetto.

Tabella 9: Referenze I&AM

Cliente	Progetto e Descrizione
Arma dei Carabinieri	Digital Identity & Centralized HR Administrative Records Management) per 110,000 organici in forze, con valenza legale di documenti elettronici.
Ministero della Difesa	Sistema di Identiy & Access Management per il controllo degli accessi alle applicazioni del Ministero 100.000 utenti
INPS	Fornitura dei servizi di adeguamento del software applicativo dell'Istituto al sistema unico di Identity ed Access Management ed alla lotta all'evasione contributiva (38.000 utenti)
Finmeccanica	Progetto I&AM per il Gruppo Finmeccanica (80.000 utenti)

4.1.3 Soluzione organizzativa di Identity and Access Management (I&AM)

Analogamente a quanto descritto in merito alla soluzione organizzativa del servizio di Identity Provider, il RTI propone anche per l'Identity & Access Management una struttura allineata a quella descritta precedentemente, in termini di team coinvolti, strutture di supporto, ruoli e figure professionali.

Saranno trattati in dettaglio gli aspetti legati ai processi relativi alla Pubblica Amministrazione ed al Cittadino, cogliendone gli aspetti precipui secondo due differenti viste.

La metodologia inerente i flussi comunicativi, razionali di ingaggio, competenze e team, è analoga a quanto descritto precedentemente (organizzazione Identity Provider).

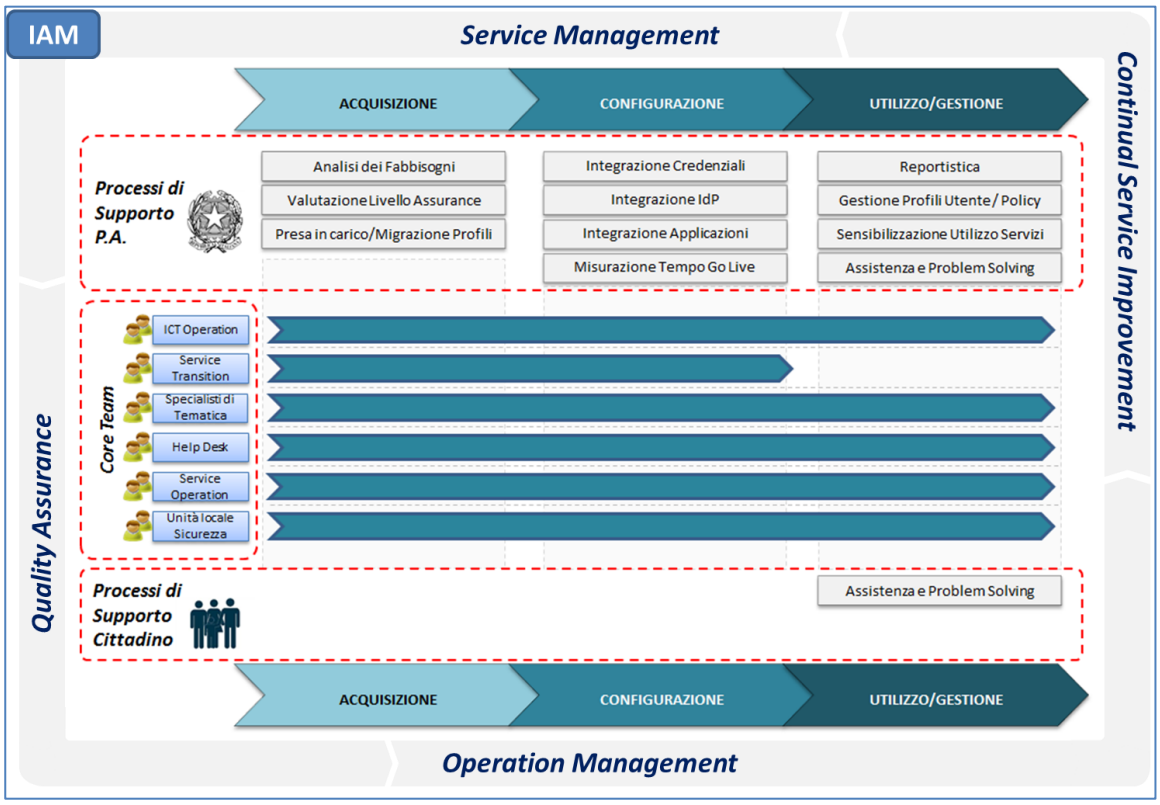
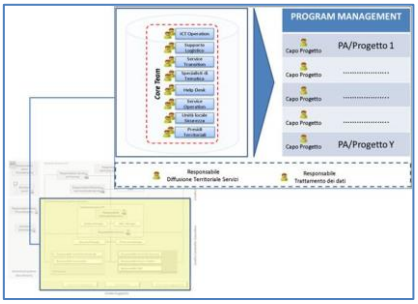


Figura 20: Organizzazione I&AM

In riferimento si veda l'illustrazione riportata nella figura a lato.
L'organizzazione descritta opera in un contesto metodologico, basato su standard e best practice internazionali, prevede attività di Service/Operation Management e Quality Assurance in un'ottica di miglioramento continuo del servizio (Continual Service Improvement).
Di volta in volta, per ogni Amministrazione, verrà nominato un **Capo Progetto** che governerà uno specifico **Team di Progetto** ed opererà in coordinamento con il **Responsabile del Trattamento dei dati personali ed il Responsabile Diffusione Territoriale Servizi.**



4.1.3.1 Team e Figure Professionali

Di seguito i Core Team e le principali figure professionali coinvolte

Figura professionale	Figura profess. RTI	Principali compiti/responsabilità
CAPO PROGETTO	**Responsabile I&AM**	Supervisiona lo svolgimento del servizio e si coordina con i referenti della P.A. e del RTI. E' responsabile della consistenza e dell'adeguatezza sia quantitativa che qualitativa del team di cui dispone, coinvolgendo il Resource Manager qualora necessario.
RESP. Trattamento Dati Personali	**RESP. Trattamento Dati Personali**	Responsabile delle attività secondo quanto stabilito dal Garante per i Dati Personali di cui al d.lgs. 30.06.2003 n° 196

Di seguito i Gruppi e le principali figure professionali coinvolte

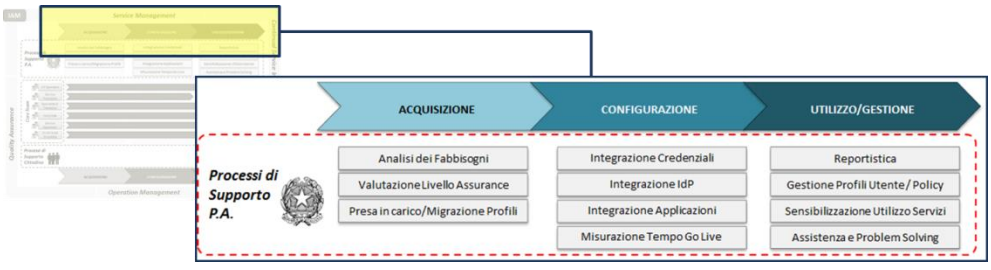
Tabella 10: Team e Figure professionali previste per il servizio di Identity & Access Management

TEAM	Figura profess. del Team RTI	Principali compiti/responsabilità
ICT OPERATION (Conduzione tecnologica infrastruttura)	**Centor Servizi (Rif. § 3.3.2.1.1)**	Conduzione dell'infrastruttura tecnologica
SERVICE TRANSITION (Governo e controllo attività di transizione Servizi)	**Spec. di Change Management**	Esperto di metodologie e soluzioni tecnologiche per quanto concerne le tematiche legate alla portabilità ed interoperabilità
	Analista Funzionale	Responsabile analisi delle funzionalità che il sistema dovrà erogare
	Capacity Manager	Responsabile della produzione e dell'aggiornamento del capacity plan, che include la domanda di servizi attuale e la previsione dei bisogni

		futuri in relazione alla quantità di utenti e profili da gestire e delle relative infrastrutture abilitanti, tenendo aggiornati ed allineati i 3 CED da dove sono erogati i servizi
SPECIALISTI DI TEMATICA (Figure specializzate su tematiche inerenti la realizzazione di servizi di I&AM)	**Specialista di processi**	Specialista di processo
	Analista Funzionale	Responsabile analisi delle funzionalità che il sistema dovrà erogare
	Analista di Sicurezza	Identifica, verifica e garantisce l'efficacia delle misure di sicurezza adottate
	Data Base Architect	Progettazione delle basi dati e sviluppo strategie per l'acquisizione ed il caricamento
	Specialista di prodotto /tecnologia	Possiede una profonda conoscenza delle architetture e delle tecnologie specifiche in tema di I&AM
HELP DESK (SPOC per supporto PA e Cittadino cfr. § 3.4)	**Responsabile HD**	Coordina il team di Help Desk
	Team Leader	Coordina gruppi di operatori organizzati per skill group
	Operatore	Operatore multicanale
SERVICE OPERATION (Conduzione tecnologica infrastruttura specialistica di I&AM)	**Technical Service Manager**	Responsabile tecnico dei servizi e delle risorse necessarie all'erogazione del servizio nel rispetto degli indicatori di qualità previsti
	Data Analyst	Analisi dei dati sull'utilizzo dei servizi, trend e contenuti
	System Architect	Cura l'approccio tecnologico e la produzione dei risultati di progetto, garantendo livelli elevati di capacità analitica e di risultato in fase di analisi delle informazioni.
	Specialista di processi di I&AM	Specialista di processo in ambito I&AM
	Specialista di prodotto /tecnologia	Possiede una profonda conoscenza delle tecnologie e delle problematiche di natura tecnica connesse con la realizzazione dei servizi di I&AM
UNITA' LOCALE SICUREZZA	**Resp. ULS**	Responsabile dell'Unità (rif. § 3.3.2.1.2)
	Addetto	Personale di supporto alle attività

4.1.3.2 Modalità Operative di Processo e Strumenti a supporto della PA

Al fine di individuare la migliore modalità operativa di processo per il servizio di I&AM, il RTI ha portato a fattor comune quanto realizzato con successo nella Pubblica Amministrazione ed in aziende con complessità similare a quella oggetto di Gara fa riferimento. In particolare, nell'area PA, in ambito sia domestico sia internazionale, il RTI vanta referenze di estremo valore (§ 4.1.2), di cui ha riutilizzato il valore aggiunto per la definizione della presente proposta, con particolare attenzione al servizio di Identity Provider. Si ricorda infatti che il servizio di I&AM dovrà interagire con il/i servizio/i di Identity Provider disponibili e conformi a SPID.



Nel seguito del documento le fasi di acquisizione, configurazione e utilizzo/gestione del servizio, saranno declinate negli specifici processi, dettagliando per ognuno gli elementi salienti (descrizione, deliverable e team del RTI coinvolti). In ogni processo è previsto il coinvolgimento del RTI e della PA.

FASE	ACQUISIZIONE
TO ALLA PUBBLICA	**Analisi dei fabbisogni** Deliverable: Piano/Progetto dei fabbisogni Team RTI coinvolti: Service Transition, Specialisti di Tematica Descrizione: Il RTI condivide con l'Amministrazione il quadro normativo vigente al momento dell'acquisizione del

FASE	ACQUISIZIONE
	servizio e relativo alla gestione delle identità e dei relativi attributi (ad es. elenco Attribute Authority SPID). Identifica gli eventuali Identity Provider già esistenti e le loro "caratteristiche" utili al dimensionamento del servizio I&AM, quali ad esempio il numero di utenti già registrati e in che percentuale di distribuzione sono presenti le credenziali "strong" LoA3 o LoA4. Quanto sopra consente una decisione autonoma e consapevole in merito a tipologia e numerosità utenti. Il RTI condivide con l'Amministrazione le caratteristiche tecnologiche che costituiscono pre-requisito per l'integrazione dei servizi telematici della PA all'interno del servizio I&AM (secondo quanto esposto da AgID e più in generale nelle norme di SPID) A supporto della definizione del piano dei fabbisogni, il RTI fornisce una strumentazione (es. cruscotto decisionale) con la quale è possibile simulare scenari alternativi sulla base delle evidenze precedenti (es. dimensionamento, analisi impatti per possibile adeguamento applicativi). **Supporto alla valutazione del Livello di Assurance (LoA2, LoA3 e LoA4)** Deliverable: documento di analisi del rischio LoA2/LoA3/LoA4 Team RTI coinvolti: Service Transition, Specialisti di Tematica Descrizione: Gli unici livelli di assurance ammessi per servizi erogati dalla PA sono i livelli LoA3/LoA4 (rif. Capitolato tecnico 2.2.2.4), salvo differente indicazione come emerge dai chiarimenti alla Gara (*Rif. I tranche-199 - "Il livello di assurance (LoA) viene stabilito dall'amministrazione erogatrice di servizi (o applicazioni) web e può essere diverso da servizio a servizio (ad es. servizi orientati alle consultazioni possono avere associati dei LoA bassi, altri servizi potranno avere dei LoA di tipo 2 o superiore). "*. La corretta attribuzione del livello deve necessariamente passare attraverso una valutazione del rischio, cui sono soggetti i servizi/applicazioni. Il RTI propone pertanto la propria esperienza nell'analisi del rischio specifica, fornendo come risultante di tale attività un documento che permetta alla PA di valutare in autonomia il meccanismo di autenticazione maggiormente adeguato. **Presa in carico e migrazione dei profili utente** Deliverable: report esito caricamento Team RTI coinvolti: Service Transition, Specialisti di Tematica, ICT Operation, Service Operation Descrizione: a. **"migrazione",** L'attività di migrazione si svilupperà attraverso le seguenti fasi di dettaglio: Analisi, Test/Simulazione e Caricamento. L'analisi sarà condotta attraverso l'utilizzo di specifici "manuali di istruzione" e relative "check list" che hanno lo scopo di definire le modalità di individuazione dei dati relativi agli utenti, dei relativi profili e dell'eventuale suddivisione in gruppi omogenei (categorie) già in possesso dell'Amministrazione. Ciò permetterà inoltre di evidenziare le attività necessarie per rendere il dato maggiormente coerente con i fabbisogni della PA (corretta attribuzione e gestione dell'autorizzazione all'accesso delle risorse web dell'amministrazione). L'attività di Test/Simulazione, finalizzata ad una valutazione della numerosità degli utenti e dei profili potenzialmente migrabili, sarà svolta dal RTI mediante l'uso di una soluzione web based, a garanzia del buon fine e dell'esito dell'attività e conseguentemente della "qualità del dato" specifico di migrazione, facilitando il successivo caricamento massivo dei profili utente e la creazione di gruppi omogenei (categorie). La soluzione tecnica proposta supporterà le operazioni di caricamento reale ed operativo, con massima flessibilità ed apertura in merito ai principali standard affermati nel settore dell'Identity and Access Management, oltre che gli "standard de facto" maggiormente in uso presso le PA (LDAP, DB RDBMS, flat file, ecc.). Nel caso in cui l'Amministrazione prima di avviare le attività di migrazione, ritenga necessario effettuare una razionalizzazione dei profili utente esistenti e l'associazione per gruppi omogenei (categorie) il RTI fornirà il proprio supporto specialistico per lo svolgimento di tale attività. Le successive attività di caricamento verranno svolte dal RTI con le stesse modalità sopra descritte, riferite al nuovo perimetro; b. **" ex-novo",** qualora si evidenzi l'esigenza da parte dell'Amministrazione di creare ex-novo i profili utente, il RTI fornirà il proprio supporto specialistico per lo svolgimento di tale attività, definendo in condivisione con l'Amministrazione stessa, il modello di riferimento da utilizzare. Le successive attività di Test/Simulazione e caricamento verranno svolte dal RTI con le stesse modalità sopra descritte.

FASE	CONFIGURAZIONE
SUPPORTO ALLA PUBBLICA	**Integrazione credenziali** Deliverable: report periodico di avanzamento Team RTI coinvolti: Service Transition, Specialisti di Tematica, ICT Operation, Service Operation Descrizione: Qualora l'Amministrazione lo ritenga utilizzabile nel proprio caso d'uso specifico, il RTI propone un processo graduale di transizione dal vecchio modello di autenticazione "locale" a quello erogato per il tramite

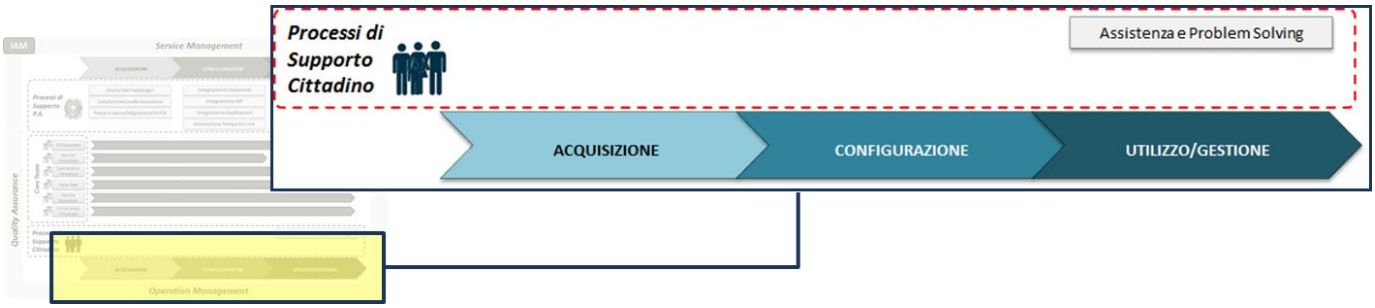
FASE	CONFIGURAZIONE
	dell'IdP interrogato dal nuovo I&AM, garantendo, nella fase intermedia, un parallelismo di funzionamento tra i sistemi di autenticazione. Tale approccio rappresenta un elemento aggiuntivo e di valore alla presente offerta.
	Integrazione con gli Identity Provider Deliverable: report di integrazione IdP Team RTI coinvolti: Service Transition, Specialisti di Tematica, ICT Operation, Service Operation
	Descrizione: Il RTI provvederà alle attività di integrazione con gli Identity Provider o con l'Amministrazione, nel caso sia essa stessa un Identity Provider. Inoltre metterà a disposizione della PA un'infrastruttura di sviluppo aggiuntiva, per effettuare test funzionali al fine di garantire massima efficienza nelle integrazioni. Tale *atout* rappresenta un ulteriore asset disponibile ai fini della qualità complessiva del processo di integrazione con l'identity Provider.
	Integrazione prima applicazione Deliverable: report di integrazione applicazione Team RTI coinvolti: Service Transition, Specialisti di Tematica, ICT Operation, Service Operation, Help Desk, Unità Locale di Sicurezza
	Descrizione: L'integrazione di un'applicazione con il sistema di I&AM comporta potenziali attività di adeguamento dell'infrastruttura applicativa in carico sia dell'Amministrazione sia al RTI. Pertanto per una corretta e funzionale integrazione, dopo una prima fase di condivisione di informazioni il RTI garantirà le necessarie attività sistemistiche e di configurazione, rendendo accessibili nella nuova modalità di autorizzazione le URL comunicate dall'Amministrazione. L'elemento di valore è rappresentato dalla definizione del modello di integrazione che potrà essere utilizzato in occasione di future ulteriori integrazioni, nell'ambito di un processo di miglioramento continuo (Continual Service Improvement). A tale scopo verrà messo a disposizione della PA un ambiente di sviluppo aggiuntivo e dedicato alla PA, con relativa documentazione di progetto specificamente realizzata, nonché tutto quanto necessario al fine di garantire autonomamente la verifica la delle funzionalità. Tale ulteriore ambiente di sviluppo, rispetto all'ambiente di Test Bed, offrirà alla PA un maggiore grado di libertà nelle attività di test e simulazione delle proprie applicazioni. Nel contesto in esame, qualora ritenuto utile, il RTI propone un periodo di parallelismo nel funzionamento dei sistemi, al fine di ridurre ogni eventuale impatto sul servizio e sull'utente finale, fornendo supporto all'Amministrazione grazie alle migliori competenze di system integration/management di cui il RTI dispone.
	Misurazione del tempo di go-live Deliverable: report di sintesi Team RTI coinvolti: Service Transition, Specialisti di Tematica, ICT Operation, Service Operation, HelpDesk
	Descrizione: Il tempo di go-live rappresenta uno degli indicatori fondamentali per l'aggiornamento dell'Amministrazione sullo stato di avanzamento delle attività. Gli strumenti messi a disposizione dal RTI permettono pertanto di misurare e verificare accuratamente gli indicatori ed i tempi condivisi nella fase di acquisizione. Tale indicatore potrà arrivare fino alla stima del periodo di parallelismo al fine di individuare il momento di swap definitivo dei sistemi.

FASE	GESTIONE/UTILIZZO
PROCESSO DI SUPPORTO ALLA PUBBLICA AMMINISTRAZIONE	**Esposizione di report periodici e analisi consuntivi** Deliverable: report Team RTI coinvolti: Specialisti di Tematica, ICT Operation, Service Operation, Help Desk
	Descrizione: Alla PA è garantita la possibilità di verificare in autonomia quale sia lo stato di utilizzo del servizio. A tale scopo è resa disponibile ulteriore reportistica specifica, aggiuntiva a quella prevista, anche in forma aggregata ed accessibile mediante il "Portale di Gestione dello I&AM" e il "Portale di Governo della Fornitura".
	Incentivo all'utilizzo dei servizi della PA Deliverable: Report del trend di utilizzo dei servizi digitali Team RTI coinvolti: Specialisti di Tematica, ICT Operation, Service Operation, Help Desk
	Descrizione: Al fine di agevolare l'Amministrazione nel processo di sensibilizzazione dell'utenza all'uso dei servizi digitali, il RTI mette a disposizione la soluzione OSINT (http:// www.selex-es.com/it/-/cyber-security), erogata dall' infrastruttura di supercalcolo di Selex ES, che sarà orientata alla sentiment analysis e alla brand reputation per fornire informazioni sull'utilizzo dei servizi digitali e relative tendenze dell'utenza. Tale attività rientra nel più ampio obiettivo di riduzione del "digital divide" che si realizza anche tramite automazione dei processi, informatizzazione e dematerializzazione.
	Governo del ciclo di vita dei profili utente e delle policy di accesso Deliverable: processi e procedure tecnico/amministrative Team RTI coinvolti: Specialisti di Tematica, ICT Operation, Service Operation, Help Desk, Unità Locale di Sicurezza

FASE	GESTIONE/UTILIZZO
	Descrizione: Durante le fasi precedenti è stato di fatto delineato un modello di gestione e comunicazione che verrà utilizzato per l'intero ciclo di vita del servizio. Tale modello ha lo scopo di rendere la comunicazione tra l'Amministrazione e il RTI semplice, snella ed efficiente; il Portale di gestione dello I&AM e la strumentazione del Portale di Governo della Fornitura costituiscono gli strumenti necessari per una governance completa del ciclo di vita dei profili utente e delle relative policy di accesso. L'infrastruttura di sviluppo aggiuntiva costituisce inoltre un asset di valore, a disposizione della PA, mediante il quale effettuare simulazioni di contesto per ottimizzare successivamente le attività di erogazione del servizio. A supporto delle attività il RTI garantisce il monitoraggio e la gestione continua della sicurezza mediante il SOC, all'interno del team Unità Locale di Sicurezza, ottemperando agli obblighi del gestore, eventualmente anche mediante segnalazione di utilizzi anomali dell'Identità Digitale. I team coinvolti nell'intero ciclo di vita del servizio opereranno a supporto del Responsabile del Trattamento dei Dati Personali nel rispetto della normativa vigente. **Assistenza e Problem Solving** Deliverable: reportistica di riscontro Team RTI coinvolti: Help Desk, Service Operation, Specialisti di Tematica, Unità Locale di Sicurezza, ICT Operation Il Servizio di Help Desk Telematico costituisce il punto unico di contatto (SPOC) per le Amministrazioni in merito alle tematiche in ambito I&AM. L'Help Desk, attivato tramite una pluralità di canali di contatto dai referenti dell'Amministrazione, dialogherà con gli altri Core Team operativi, provvedendo al loro ingaggio funzionale, al coordinamento ed al monitoraggio delle service request e gestendo le tematiche relative all'autorizzazione e profilazione sulle applicazioni della PA. In tale ambito il Portale di Governo della Fornitura costituirà l'interfaccia di comunicazione in uso all'Amministrazione per le attività di gestione, monitoraggio e reportistica. Per una descrizione di dettaglio si faccia riferimento al capitolo ad esso espressamente dedicato (cfr. § 3.4).

4.1.3.3 Modalità Operative di Processo e Strumenti a supporto del Cittadino

In merito ai servizi di Identity & Access Management e più in dettaglio per quanto concerne i processi di supporto al Cittadino, è possibile individuare il solo processo di Assistenza e Problem Solving in quanto in questa fase il Cittadino non ha interazioni dirette con il gestore del Servizio, salvo quelle legate alle attività di assistenza.



Nella seguente tabella il dettaglio del singolo processo.

FASE	GESTIONE/UTILIZZO
PROCESSO DI SUPPORTO AL CITTADINO	**Assistenza e Problem Solving** Il Servizio di Help Desk Telematico costituisce il punto unico di contatto (SPOC) per le Amministrazioni in merito alle tematiche in ambito I&AM. L'Help Desk dialogherà con gli altri Core Team operativi, provvedendo al loro ingaggio funzionale ed al coordinamento e monitoraggio delle service request. Gestirà inoltre le tematiche relative all'autorizzazione e profilazione sulle applicazioni della PA. In tale ambito il Portale di Governo della Fornitura costituirà l'interfaccia di comunicazione in uso all'Amministrazione per le attività di gestione, monitoraggio e reportistica. Le attività di assistenza e problem solving relative agli aspetti di autenticazione, di competenza del servizio di Identity Provider, saranno gestite dal team di Help desk afferente a tale servizio.

4.1.3.4 Modalità con cui verrà prodotto il documento di analisi del rischio.

Il RTI, come richiesto nel Capitolato, predispone di concerto con l'Amministrazione un documento di analisi del rischio che verrà reso disponibile entro 10 giorni lavorativi dall'effettuazione della richiesta da parte dell'Amministrazione stessa. Saranno descritte le caratteristiche del sistema, la configurazione, la collocazione degli apparati necessari, le procedure organizzative e la delimitazione del contesto, nonché i risultati dell'attività di analisi del rischio. La metodologia di analisi dei rischi adottata si basa sugli elementi distintivi di seguito elencati: ► attinenza al dominio, tramite l'utilizzo di particolari elementi valutativi, quali scenari di minaccia,

vulnerabilità e contromisure di sicurezza, applicabili al contesto tecnologico ed organizzativo definito da un sistema I&AM ► ripetibilità e riproducibilità ► comprensibilità ► riutilizzabilità ► rapidità ► coerenza dei valori attribuiti alle informazioni con quanto stabilito dalle politiche e procedure di sicurezza ► fruibilità e sintesi dei risultati prodotti ► conformità agli standard vigenti appartenenti alla famiglia ISO/IEC 27000 e ISO/IEC 9798:2010 - Entity Authentication (6 parti), ISO/IEC 24760:2011 - A Framework for Identity Management, ISO/IEC 29115:2013 - Entity Authentication Assurance Framework.
La metodologia adottata, calata all'interno del contesto specifico, prevede i seguenti passi operativi:

- individuazione del perimetro di analisi, definendo in maniera formale gli asset interessati. In questa fase verrà costruito un asset model, che correli tra loro processi, servizi, informazioni, dati informatici, moduli applicativi, software di base e hardware. Data la specificità del dominio di analisi, per garantire l'attinenza dei risultati al contesto definito e valutare coerentemente i livelli di esposizione al rischio, in questa fase saranno considerati:
  - particolari tipologie di asset, propri di un sistema I&AM quali, tra gli altri, utenze trattate, profili utente, dati di navigazione in transito, interfacce di autenticazione e flussi di autorizzazione;
  - configurazioni e/o aspetti logistici di eventuali componenti del servizio I&AM, facenti comunque parte del dominio di analisi e attestati – se del caso – presso gli ambienti operativi delle Amministrazioni;
- analisi delle minacce applicabili che determinano la perdita o la riduzione dei livelli di riservatezza, integrità e disponibilità e la valutazione degli impatti. In questa sede saranno valutati scenari di minaccia applicabili al contesto I&AM, quali accessi non autorizzati a dati e sistemi, escalation di privilegi sulle applicazioni, attacchi di tipo DoS e DDoS ai servizi esposti, ecc.;
- valutazione delle vulnerabilità, definendo formalmente, per ogni minaccia applicabile, la probabilità di accadimento e il livello di esposizione di ciascun asset;
- valutazione dei livelli di esposizione al rischio informatico, calcolati in funzione dei valori precedentemente acquisiti;
- definizione del profilo di protezione ottimale, individuato dalle contromisure di sicurezza logica, fisica ed organizzativa, applicate ad un livello di robustezza calcolato in funzione dei livelli di esposizione al rischio. Le contromisure saranno selezionate a partire da una libreria di controlli conforme allo standard ISO/IEC 27002 (Code of Practice for Information Security Controls) e personalizzati in sede di analisi, in base al dominio I&AM esaminato
- determinazione del Livello di Rischio Residuo e del Livello di Rischio Previsto, ossia di quello calcolato tenendo conto delle misure di protezione in atto e di quelle comunque pianificate, in funzione delle strategie di trattamento del rischio precedentemente concordate.

La suddetta metodologia sarà descritta in uno specifico documento facente parte del Sistema Documentale del SGSI, così come descritto al § 5.2.4.3
Come **elemento migliorativo della fornitura**, si precisa inoltre che le attività di analisi dei rischi saranno supportate del tool software MIGRA (Metodologia Integrata per la Gestione del Rischio Aziendale), proprietario della mandataria, tramite il quale gli analisti di sicurezza potranno ottimizzare le fasi di acquisizione dati, di elaborazione, di analisi, di produzione e presentazione degli elaborati documentali.
L'utilizzo di uno strumento software garantirà inoltre la possibilità alla PA di monitorare lo stato di avanzamento delle analisi in corso per un controllo dell'efficacia dell'attività.

4.1.4 Soluzione tecnologica dei servizi Identity Provider e I&AM

Il **Sistema Pubblico per la gestione dell'Identità Digitale (SPID)**, rappresenta un **elemento di trasformazione** della Pubblica Amministrazione di enorme portata, estendendo per cittadini ed imprese la possibilità di accesso ai servizi in rete, anche in mobilità.
Il RTI ha progettato una **soluzione modulare, integrata ed innovativa** per la realizzazione del servizio di Identity Provider e Identity and Access Management sulla base degli obiettivi espressi dalla Gara.
Per la realizzazione della piattaforma del servizio di Identity Provider e Identity and Access Management il RTI ha scelto di utilizzare la competenza **IBM** relativa alla progettazione ed erogazione di soluzioni (servizi e tecnologie proprietarie) per la gestione delle identità e degli accessi federati, reputando di particolare eccellenza il contributo da questa fornito attraverso il contratto relativo alla "progettazione, realizzazione e gestione di Servizi Infrastrutturali di Interoperabilità, Cooperazione ed Accesso (SICA)" (rif. Contratto giugno 2007, CNIPA-R.T.I. IBM-Sistemi Informativi). L'erogazione dei servizi oggetto di quest'ultimo ha rappresentato un passo fondamentale del

percorso verso la interoperabilità sicura tra le Pubbliche Amministrazioni. Questo percorso include l'implementazione del Centro-Gestione SICA e la stesura del modello di Gestione Federata delle Identità Digitali (**GFID**) che ha recentemente trovato una naturale evoluzione nell'attuale SPID. L'approccio deciso dal RTI include anche la proposizione di funzionalità innovative relative al **"Identity Management as a service"** (IDaaS) **e valorizzate anche grazie all'utilizzo delle tecnologie "IBM Lighthouse".** IBM Lighthouse Security Group, è una società acquisita da IBM, leader nei temi "Next-Generation Enterprise Identity and Access Management (IAM) from the Cloud" .
La soluzione tecnologica proposta dal RTI per la realizzazione della piattaforma IdP e IAM consente la gestione sicura dell'intero ciclo di vita delle identità digitali e profili con modalità volte a valorizzarne la facilità d'uso. In particolare: l'utilizzo di strumenti di autenticazione basati su più di un fattore, la possibilità di realizzare il Single Sign On all'interno dei domini applicativi, e l'integrazione dei domini di sicurezza, rappresentano fattori abilitanti sia della componente di sicurezza che della facilità d'uso. Entrambi riducono di fatto le vulnerabilità tipiche dei meccanismi di autenticazione applicativa, come ad esempio la molteplicità di credenziali di autenticazione riferibili al singolo utente.
A completamento della sicurezza tecnologica offerta dalle tecnologie proposte, la struttura SOC dell'Unità Locale di Sicurezza, realizzerà attività continua di monitoraggio mediante rilevamento degli allarmi e degli incidenti di sicurezza. L'ULS utilizzerà tutte le infrastrutture di sicurezza del Centro Servizi descritte nel § 3.3.2.1.2.

Le esigenze di implementare meccanismi di semplificazione e facilità d'uso, ai fini della promozione della cooperazione applicativa, sono state nel tempo declinate in soluzioni che, partendo da una iniziale dimensione aziendale (ovvero interessando l'ambito dei soli domini interni all'azienda), si sono via via ampliati per includere gli aspetti di federazione (ovvero interessando l'ambito dei domini di cooperazione applicativa). La cooperazione applicativa e gli accessi ai sistemi esterni al perimetro dell'Amministrazione avvengono quindi utilizzando le medesime credenziali. Proseguendo l'analisi del modello di evoluzione della cooperazione applicativa, l'ultimo livello è rappresentato dalla introduzione dei paradigmi "Cloud" e "Social Networking" che conducono all'introduzione del modello di "Identity Management as a service", modello oggetto della proposizione del RTI che rappresenta la soluzione di ultima generazione per la gestione ed accesso unificato delle identità digitali. La soluzione tecnologica proposta dal RTI consente di implementare l'utilizzo sicuro di credenziali digitali univoche per l'accesso ai servizi online delle Amministrazioni, applicando il paradigma SPID. La proposizione della tecnologia IBM Lighthouse, uno dei primi "Identity as a Service provider" a livello mondiale, rappresenta un ulteriore elemento di valore in ottica di innovatività, evoluzione e sostenibilità della proposizione. Nel seguito si descrive la soluzione in termini tecnologici nei suoi aspetti generali e complessivi e nelle sue componenti significative di dettaglio. Nella descrizione sono utilizzati i **Tag** al fine di evidenziare gli aspetti più rilevanti della soluzione proposta di seguito proposti.

Adeguatezza	AD	Efficacia	EC	Facilità d'uso	FU	Innovatività	IN	Modularità	MO

Caratteristiche generali della soluzione

Adeguatezza AD

La soluzione, basata su tecnologia IBM Lighthouse, risponde al principio di adeguatezza delle esigenze della PA indirizzando tutti i requisiti di gara presenti nel capitolato tecnico.

Innovatività IN

Gartner individua la soluzione di Identity and Access Management (IDaaS) erogati in modalità Cloud-Based di IBM (**Lighthouse**), come soluzione **differenziante in termini innovativi** in grado di migliorare continuamente con un approccio di leadership visionaria. Secondo quanto analizzato all'interno del "**Magic Quadrant Identity and Access Management as a Service**", le metriche di valutazione utilizzate sono le seguenti:

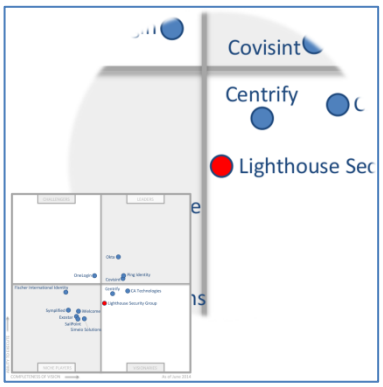


Figura 21: magic quadrant Identity as a service

- Identity Governance and Administration ("IGA") – include, oltre le funzionalità standard di un sistema di IdM quali la gestione del ciclo di vita di un'identità, e la governance amministrativa delle stesse, anche la capacità di sincronizzazione delle identità detenute dal servizio verso le applicazioni target;

- Accesso - include l'autenticazione degli utenti, il single sign-on (SSO) e il "Authorization enforcement" verso applicazioni Web Based mediante gli standard internazionali di federazione delle identità (es. SAML V2.0);
- Intelligenza - include la registrazione degli eventi e le funzionalità di reporting relative a temi che possono includere ad esempio la capacità di rispondere a domande tipo: "Chi ha avuto accesso a quali sistemi e quando?" o "Chi ha dato l'accesso a chi ("who"), a quali sistemi ("what") e quando ("where")?".

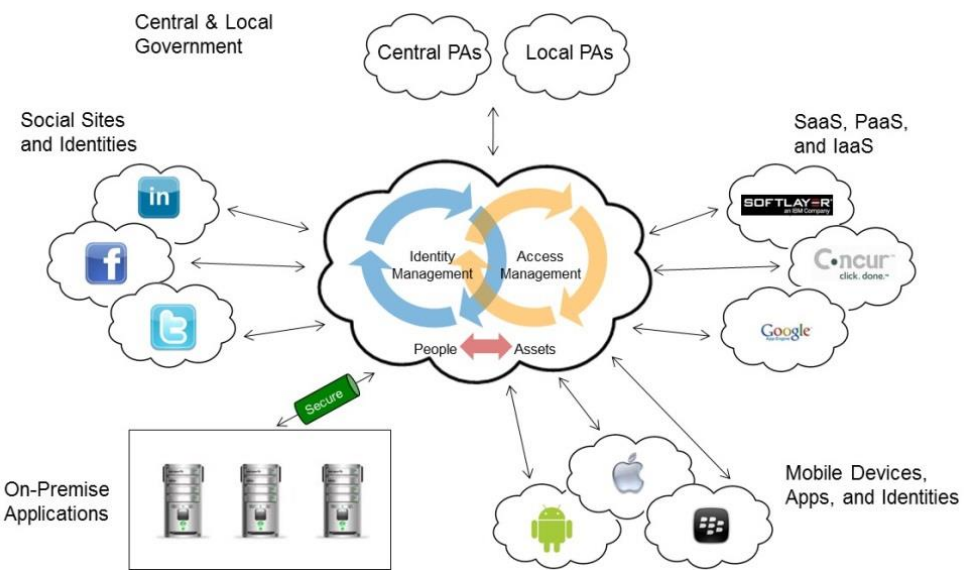


Figura 22: innovatività di Lighthouse

In una soluzione IaaS moderna, quale quella proposta dal nostro RTI, è necessario considerare, oltre a quanto affermato da Gartner, che la gestione sicura delle identità deve essere estesa a **dispositivi mobili, ad applicazioni nate sul Cloud** e soprattutto deve essere in grado, all'occorrenza, di federarsi con identità digitali delle realtà aziendali che prendono parte al percorso di crescita digitale del "sistema Paese". Nella Figura 22 **l'approccio eterogeneo e innovativo** della soluzione proposta.

Ulteriori evidenze oggettive della innovatività della soluzione tecnologica adottata dal RTI è presentata dagli attestati dei maggiori analisti di mercato e dalla partecipazione a gruppi di definizione degli standard riportati nella tabella seguente.

Tabella 11: Riconoscimenti analisti di mercato

FROST & SULLIVAN	IBM riconosciuta per Customer Value leadership in 2014 - **Mobile Identity and Access Management;**
IDC Analyze the Future	**IBM riconosciuta come Market Share leader in 2013** – Identity and Access Management – Federation Identity Management e SSO Market Scope leader in 2014
Gartner	**IBM riconosciuta come Visionary nel Magic Quadrant 2013**
kuppingercole ANALYSTS	**IBM leader nelle discipline di:** – Cloud IAM/IAG (July 2014) – Identity Provisioning, Privileged Identity Management – Access Management & Federation, Enterprise SSO, Dynamic Authorization Management
FORRESTER®	**IBM riconosciuta leader nella prestazioni nel Wave report del 2013 per** – WW Identity and Access Management
OASIS Advancing open standards for the information soci	**IBM membro fondatore di OASIS e partecipa al comitato tecnico per la OASIS Security Services (SAML)** – https://www.oasis-open.org/member-roster – https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

Efficacia EC

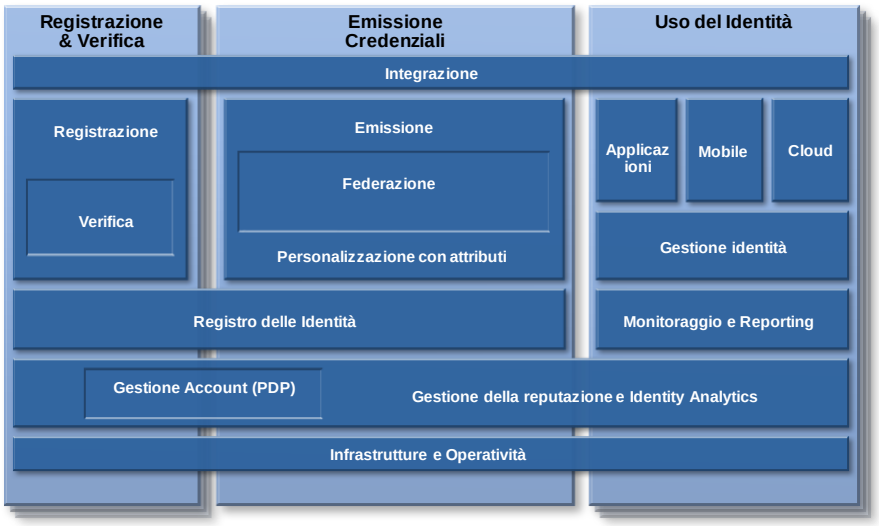


Figura 23: Modularità della soluzione

La realizzazione di un modello operativo frutto della esperienza IBM nel campo della gestione delle identità rende la soluzione efficace e semplice da utilizzare da parte di cittadini ed amministrazioni, a tale scopo la Figura 23 presenta il modello della gestione delle identità. Sviluppato inizialmente da IBM nel progetto **India Unique ID**[3], il modello è stato adottato dal RTI come riferimento per rendere la soluzione di gestione delle identità scalabile, semplice da utilizzare e **completa nella copertura funzionale** di tutte le fasi del ciclo di vita dell'Identità Digitale.

Facilità d'uso FU

Le funzionalità di **Registrazione & Verifica-> Emissione Credenziali -> Uso delle Identità** risultano nativamente **integrate** consentendo alle Amministrazioni e ai cittadini di interagire con una soluzione logicamente unica aumentandone quindi la fruibilità. La **registrazione & verifica** è implementata su un insieme di canali che forniscono

- **Semplicità di gestione ed autonomia d'uso per la Pubblica Amministrazione**: le interfacce amministrative dedicate, particolarmente efficaci, unite ad una piattaforma robusta e consolidata (IBM Directory Integrator) e integrate nel Portale dell'Identità Digitale, consentono di automatizzare le logiche di provisioning per la creazione degli account nei domini di sicurezza, riducendo la complessità e quindi l'impegno di gestione per il personale dell'Amministrazione.

- **Semplicità per l'Utente**: attraverso la gestione multicanale, che consente di accedere ai servizi erogati autenticandosi con le varie forme di credenziali tra quelle accettate dalla PA, e disporre di tutte le funzionalità di self service.

Figura 24: Componenti Lighthouse

Le Credenziali emesse, **personalizzabili** in base agli attributi dell'utente, consentono un accesso federato (**Single Sign-On**) ai servizi delle amministrazioni aumentando quindi l'efficacia nell'utilizzo dei servizi pubblici. L'Identità è utilizzata per accessi da dispositivi multicanale e gestita opportunamente in termini, per esempio, di aggiornamento e dismissione. Infine **componenti di monitoraggio e reporting** assicurano un controllo continuo dell'uso dell'identità. Ultimo elemento della soluzione è la **possibilità di verifica di usi fraudolenti** della identità attraverso una analisi della reputazione basata su algoritmi di Identity Analytics, in grado di verificare se le identità sono utilizzate da persone terze rispetto al reale possessore per usi eventualmente illeciti. L'intera soluzione è gestita dalla professionalità e competenza del personale della RTI su centri in **continuità di servizio e disaster recovery**.

[3] **Unique Identification Authority of India (UIDAI)** agenzia del Governo Indiano che ha commissionato ad IBM uno studio per realizzare un Sistema di Gestione delle Identità in grado di gestire 500 Milioni di identità digitali.

Modularità MO

La soluzione IDaaS presenta un'architettura modulare ed integrata che consente di indirizzare sia le problematiche di gestione dell'identità sia quelle di accesso in modalità federata. Tre livelli funzionali (illustrati nella Figura 24), basati su standard aperti, consentono l'intercambiabilità dei componenti, rendono la stessa aperta e priva di lock-in, garantendo la portabilità della soluzione su qualsiasi architettura conforme allo SPID, senza la necessità di dover cambiare il sistema di gestione degli accessi.

Grazie all'implementazione di standard aperti, la soluzione si integra con le applicazioni attualmente operative nelle Pubbliche Amministrazioni.

Architettura della soluzione

Al fine di garantire la **massima efficacia in termini di usabilità** per l'Amministrazione, la soluzione è stata disegnata con particolare attenzione agli **aspetti operativi di gestione** del ciclo di vita della identità e nella volontà di renderla **aperta**. L'attenzione è stata posta sulla definizione di un'architettura modulare e i cui componenti si integrano attraverso protocolli standard. La Figura 25 presenta l'architettura logica della soluzione.

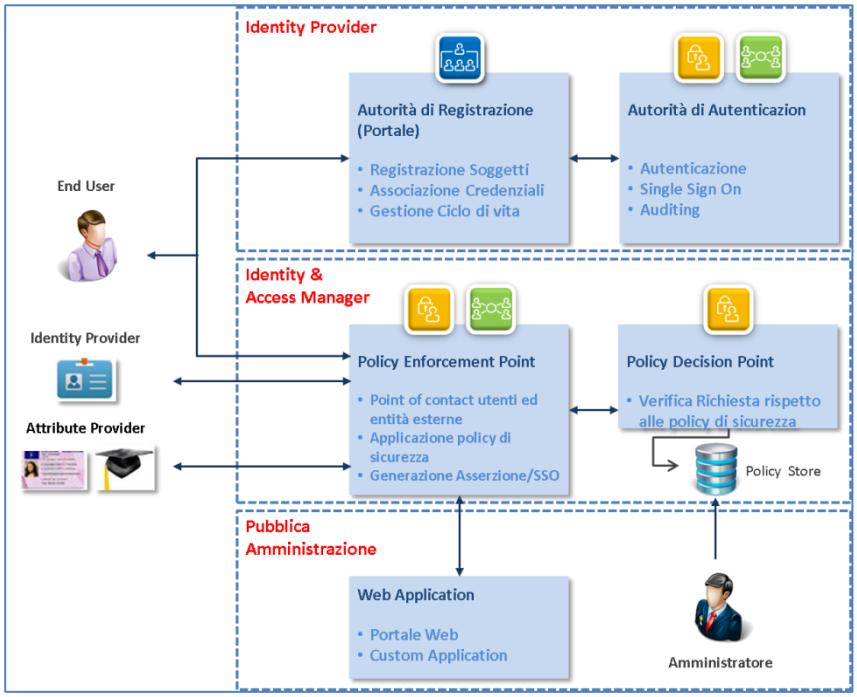


Figura 25: Architettura logica della soluzione

Identity Provider

Autorità di Registrazione, fornisce i servizi tecnologici a supporto dei processi di registrazione del cittadino, dell'associazione degli utenti alle credenziali emesse dall'Identity Provider e della gestione del ciclo di vita dell'identità digitale, comprese la revoca e/o il disconoscimento delle Identità stesse;

Autorità di Autenticazione, fornisce i servizi di autenticazione ed emissione delle asserzioni di autenticazione per permettere l'accesso al Service Provider richiesto. Tale asserzione, rilasciata dall'Autorità di Autenticazione, contiene gli attributi associati all'identità digitale autenticata.

Identity and Access Management

Policy Decision Point (PDP), gestisce la verifica dei diritti di accesso alle risorse richieste nel rispetto delle policy di sicurezza associate e presenti nel policy store;

Policy Enforcement Point (PEP), è il point of contact responsabile del dialogo con gli utenti esterni e le entità di certificazione. Intercetta le richieste di accesso dell'utente verso una data risorsa, colleziona dal PDP la totalità delle informazioni necessarie per l'applicazione delle policy di sicurezza ed infine applica la decisione di accesso, approvato o rifiutato, alla risorsa.

Policy Store, contiene le policy di sicurezza associate alle risorse protette.

4.1.4.1 Identity Provider

In riferimento all'architettura logica della soluzione di Identity Provider e Identity e Access Management basata sulla tecnologia IBM Lighthouse e presentata in precedenza, viene descritto nel seguito l'"Identity Provider" che consente al RTI di indirizzare il **Servizio di Gestione delle Identità Digitali** erogato in modalità "as a service" a tutte le amministrazioni contraenti**.**

Gli elementi distintivi della soluzione tecnologica per l'Identity Provider sono i seguenti:

- ogni area funzionale è nettamente distinguibile da tutte le altre: ciò consente una gestione e manutenzione indipendente della singola componente (MO)

- al crescere della domanda (in termini di nuove Amministrazioni integrate, e/o quantità di utenti gestiti, e/o transazioni Web eseguite) è possibile aumentare, nelle proporzioni adeguate, le risorse software e di sistema, mantenendo così costanti gli standard di servizio erogati (MO, EC)
- la realizzazione del "Portale dell'Identità Digitale" (IN, FU), dove il Cittadino, mediante un sistema semplice e dedicato, possa completamente gestire tutte le fasi del ciclo di vita della propria Identità Digitale e dove l'Amministrazione possa essere autonoma nel riconoscimento del Cittadino (IN, FU)
- possibilità di disporre in modo flessibile dei diversi livelli di Autenticazione (AD)
- la componente "Identity Provider" è basata sull'integrazione di prodotti IBM la cui attuale e comprovata efficacia è il frutto dello sviluppo tecnologico conseguente ad anni di esperienza su disparate e complesse realtà di business, diffuse al livello mondiale (AD)
- il Security Web Gateway Virtual Appliance fornisce inoltre funzioni di protezione dalle minacce, mediante Web Application Firewall. Le regole di protezione sono aggiornate tramite un servizio on-line di update basato sugli input forniti dal team di ricerca e sviluppo IBM X-Force (IN, EC)
- la componente IBM Directory Integrator supporta con flessibilità un ampio spettro di connettori standard per integrarsi con soluzioni di Identity management di terze parti (AD, EC)

Nella Figura 26 è presentata l'architettura logica della soluzione IdP.

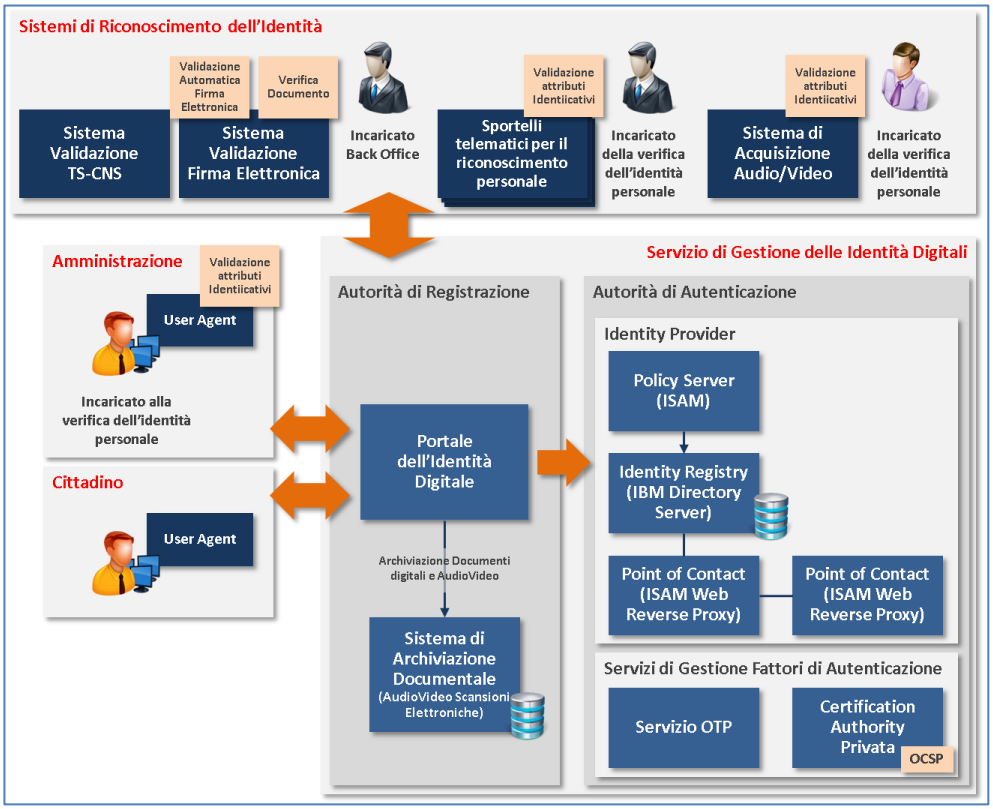


Figura 26: Architettura della Soluzione IdP

In riferimento alla figura si evidenziano le aree funzionali all'intero flusso di funzionamento del servizio di Identity Provider; esse sono "*Sistema di Riconoscimento dell'Identità*", "*Autorità di Registrazione*" e "*Autorità di Autenticazione*" (MO, AD). Verranno di seguito analizzate singolarmente fornendo per ognuna il dettaglio dei moduli da cui è composta:

- **Sistemi di Riconoscimento dell'Identità**: il processo di riconoscimento è eseguito dai seguenti quattro moduli:
  - **Sportelli telematici per il riconoscimento personale (Sportelli di verifica a vista) (AD):** L'incaricato alla verifica a vista dell'identità personale ha accesso tramite le proprie credenziali ad uno specifico servizio che gli consente, a valle dell'avvenuto riconoscimento, di completare il processo di validazione dei dati del cittadino con contestuale sottomissione telematica della scansione del documento che ne certifica l'identità (copia per immagine); al termine del processo può quindi consegnare le credenziali in modalità sicura.
  - **Sistema di Acquisizione Audio/Video (AD, IN, FU)**: in questo modulo è incluso tutto il supporto tecnologico funzionale al riconoscimento tramite sessione audio/video prevista da Capitolato. Il sistema offerto è completamente integrato nel Portale al fine di garantire semplicità d'utilizzo da parte del Cittadino ed indipendenza dalle pluralità di tecnologie disponibili sul mercato. In tale modalità l'identificazione e la registrazione sono effettuate mediante l'ausilio di un sistema di videoconferenza che prevede che il cittadino, o l'Amministrazione stessa nel caso di postazioni totem di ausilio, sia dotata di una webcam correttamente collegata ad un PC con sistema audio funzionante.

- Nel corso della sessione in videoconferenza, l'incaricato seguirà delle particolari procedure, volte a garantire l'autenticità della richiesta del corso della sessione in videoconferenza: in particolare è accertata l'identità del cittadino tramite la verifica di un documento di riconoscimento in corso di validità, purché munito di fotografia recente e riconoscibile del Titolare **(**AD**)**.
- La piattaforma permette di passare velocemente tra due tipologie di visualizzazione (IN, FU): il layout discussione nel quale vengono visualizzate le riprese di entrambe le parti (operatore e richiedente) ed i layout dei documenti nei quali il richiedente ha la possibilità di visualizzare nel dettaglio i moduli proposti, le condizioni accettate inclusa la dichiarazione di volontà del soggetto di essere dotato di Identità Digitale ecc. La tecnologia utilizzata è Aruba PEC.

Figura 27: Soluzione pe il riconoscimento Audio/Video

- **Sistema Validazione TS-CNS, CNS o carte a essa conformi (**IN AD**):** il Portale dell'Identità Digitale è integrato con il sistema di validazione delle carte ritenute valide e trusted dalla PA e quindi offre la possibilità del riconoscimento immediato tramite lettura e validazione della carta già in possesso del cittadino.
- **Sistema Validazione Firma Elettronica (**IN AD**):** in maniera analoga a quanto avviene per la validazione delle carte di cui sopra, il Portale dell'Identità Digitale è in grado di fornire un processo di riconoscimento immediato del cittadino attraverso la validazione della sua firma digitale.

I quattro moduli appena descritti interagiscono con l'" Autorità di Registrazione".

Autorità di Registrazione:

l'Autorità di Registrazione si compone del "Portale dell'identità digitale" che si interfaccia con gli utenti del sistema (per es. Cittadini, Amministrazioni, Sistemi di verifica della identità digitale) e del "Sistema di Archiviazione Documentale" a cui è demandato il compito di custodire le pratiche di registrazione delle identità (AD).

Il Portale dell'Identità Digitale (dettagliato in seguito ed anche denominato semplicemente "Portale", (FU), fornisce i servizi tecnologici a supporto dei processi inerenti la registrazione del cittadino al servizio di Identity Provider e alla gestione del ciclo di vita dell'identità digitale, ivi comprese revoca e/o disconoscimento delle identità stesse.

Il Portale avvia e controlla il flusso di lavoro che conduce al riconoscimento del cittadino che fa richiesta dell'identità digitale nelle quattro modalità come sopra descritto. Al termine del workflow di riconoscimento il Portale interagisce con la "Autorità di Autenticazione" (FU, AD) inserendo l'Identità Digitale nel registro interno dell'Identity Provider.

Come descritto negli aspetti organizzativi della soluzione IdP, il Portale consente inoltre alle Amministrazioni Pubbliche di erogare autonomamente il servizio di riconoscimento a vista (IN, FU).

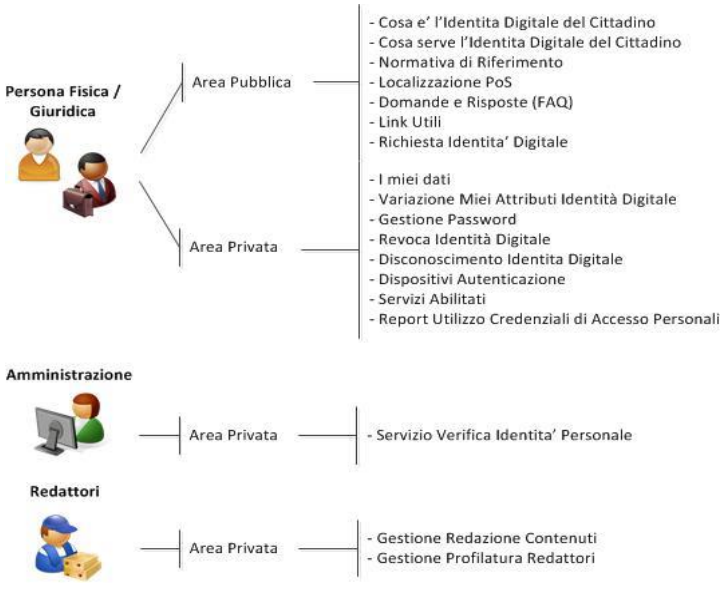


Figura 28: Casi d'uso per il Portale dell'Identità Digitale

- **Portale dell'Identità Digitale**: il Portale ha lo scopo principale di valorizzare l'opportunità che, in un ambito di "cittadinanza digitale", permette al cittadino di avvicinarsi e interagire con la PA, mediante l'utilizzo di tecnologie informatiche e di servizi proattivi (cfr. Linee guida per i siti web della PA, 2011) (FU, AD, IN). In quest'ottica il Portale permette al **cittadino**, mediante un sistema semplice e dedicato, di gestire completamente le problematiche e i processi associati alla gestione della propria Identità Digitale, ed **all'Amministrazione**, in modo efficace e

innovativo, di erogare autonomamente il servizio di riconoscimento a vista, sollevandola dalle attività di approntamento di un'ulteriore soluzione tecnologica.

Gli attori interessati all'accesso al Portale sono differenti in base ai processi di gestione dell'identità nei quali sono coinvolti e quindi alla tipologia d'informazioni e di servizi ai quali possono accedere (AD). In particolare:

- **Cittadino** –persona fisica o giuridica, che consulta le informazioni sui servizi di gestione dell'identità digitale e fruisce dei servizi stessi, previa profilatura laddove richiesta.
- **Amministrazione** –utilizza il Portale in piena autonomia operativa per la verifica dell'identità personale.
- **Redattori** –gestiscono i contenuti di natura redazionale ed informativa del Portale.

Quale strumento rivolto al cittadino e alla Pubblica Amministrazione, il Portale recepisce ed implementa alcuni pilastri fondamentali nella comunicazione verso il pubblico, quali semplicità d'uso e navigabilità del sito, intuitività del layout sviluppato, reperibilità e completezza delle informazioni, fruibilità dei contenuti con tecnologie "assistenti", chiarezza del linguaggio, supporto multicanale, accesso in mobilità (FU, AD, EC)[4].

Organizzazione dei contenuti del Portale: Architettura delle informazioni

Il portale sarà realizzato sulla base di un'architettura delle informazioni costruita a partire dalle indicazioni dell'utente, secondo paradigmi di *User Centered Design* ed *Agile Design*, e con l'uso di un approccio progettuale basato su *Responsive Design*, atto a migliorare la *user experience*, unito all'*Adaptive Design* per garantire personalizzazione e adattabilità dei layout a tutti i device e di conseguenza la visualizzazione ottimale in tutte le situazioni di utilizzo. Per una efficace e innovativa comunicazione tra la Pubblica Amministrazione e il cittadino, garantendo la giusta fruibilità alle minoranze linguistiche riconosciute ed alla popolazione non di madre lingua italiana, il Portale sarà disponibile in italiano, inglese, francese e tedesco; per tutte le altre lingue è sempre prevista l'integrazione grazie alla funzionalità automatiche di traduzione (FU, EC).

Figura 29: Mockup di portale del cittadino

L'architettura delle informazioni proposta organizzerà i contenuti e i servizi per tematica e attività. In particolare sono state identificate le seguenti macro aree:

- **Identità digitale: area informativa** caratterizzata dalla definizione d'identità digitale nel contesto italiano, descrivendone l'utilizzo con i servizi pubblici correlati e gli **attori istituzionali** coinvolti e le modalità per ottenere l'identità digitale. A corredo è riportata l'area di accesso al **Service Desk Telematico** (IN, FU, AD), contenente tutta la normativa pertinente cui il cittadino può accedere con particolare riferimento al D.lgs. del 21 giugno 2013, n. 69 (in S.O. n. 50/L alla Gazzetta Ufficiale - Serie generale - n. 144 del 21 giugno 2013) ed art. 64 comma 2-sexies del D.lgs. 7 marzo 2005, n 82.
- **Per richiedere l'Identità Digitale: area operativa** con acceso diretto al servizio per ottenere il rilascio dell'identità digitale, attraverso l'inserimento **online** dei propri dati; l'elenco dei **Presidi Territoriali** con la possibilità di geo localizzazione dei più vicini; i **moduli** e l'area per **registrazione audio video**(IN, AD, EC).
- **Area riservata:** form di accesso alle funzioni di gestione della propria identità digitale, previo inserimento di credenziali valide (codice identificativo, password e secondo fattore di autenticazione). La richiesta di nuova emissione delle credenziali di accesso (*Hai dimenticato la password?*) e la possibilità di richiedere l'utilizzo di

[4] Linee guida per i siti web della PA, 2011, dal CAD (D.lgs 7 marzo 2005, n. 82 art. 52. art.53 comma 1, art. 54, art.55, art.56, art.57 e relative integrazioni d.lgs 30 dicembre 2010, n. 235, e d.l 13 agosto 2011, n. 138) e da quanto stabilito in materia di usabilità (ISO 9241-11:1998, ISO/IEC 9126-4, ISO 20282-2) e accessibilità (Legge 9 gennaio 2004; Decreto del Presidente della Repubblica, 1 marzo 2005, n. 75; Decreto Ministeriale 8 luglio 2005)

un altro dispositivo in caso di smarrimento (*Hai smarrito il dispositivo?*) sono entrambe funzionalità soggette a meccanismi di *challenge* (IN, AD).

All'interno di quest'area (denominata "area pubblica") sono inoltre disponibili **strumenti** a supporto dell'utente (FU), sia di tipo applicativo (motore di ricerca, form inserimento dati identità digitale, mappa con geolocalizzazione, ricerca a *faccette*) sia redazionale (mappa, sito, privacy e informativa trattamento dati personali, FAQ, Service Desk Telematico, link utili, accessibilità).

L'architettura delle informazioni proposta per "l'area privata" del Portale potrà tenere traccia dei contenuti informativi dell'"area pubblica" e si focalizza sulla gestione della singola identità digitale (FU, AD):

- **I miei dati** - area con i dati personali del cittadino che permette la consultazione e la modifica dei soli attributi identificativi e non. Le variazioni sottomesse saranno tempestivamente verificate sulla base di documenti e dati ottenibili da fonti affidabili e indipendenti, consultabili tramite cooperazione applicativa, secondo le modalità concordate con AgID**.**
- **Gestione Revoca Identità Digitale**– è possibile richiedere la revoca dell'Identità Digitale.
- **Gestione Dispositivi Autenticazione** – è possibile verificare lo stato e la configurazione del proprio dispositivo di autorizzazione LoA3/4.
- **Servizi Abilitati** – cruscotto informativo che permette di visualizzare i servizi delle Amministrazioni ai quali la propria identità ha accesso (se disponibili).
- **Utilizzo Credenziali di Accesso Personali** – lista degli ultimi accessi ai servizi delle Amministrazioni con la propria identità digitale. E' possibile inviare tale lista a uno degli attributi non identificativi individuato dall'utente stesso secondo le modalità definite all'articolo 4 del Capitolato Tecnico.

L'interfaccia grafica **rispecchia i più innovativi paradigmi nell'ambito della user interface** ***(FU, EC)***. Il registro comunicativo è emotivo, efficace, e garantisce facilità d'uso delle informazioni e maneggevolezza dell'interfaccia.

Questa soluzione presenta una **digital identity** efficace nell'erogazione dell'informazione, garantendo autonomia operativa nella fruizione dei servizi.

All'interno del portale sono presenti alcuni elementi distintivi ed a valore aggiunto per l'Amministrazione, in linea con le nuove tendenze e con quanto suggerito in merito dalla PA stessa quali il "Responsive Design" (ottimizzazione della struttura dell'interfaccia alle dimensioni dello schermo con cui è visualizzata, tra smart TV, tablet, netbook, ecc.), la "Interfaccia Adattiva" (personalizzazione dei contenuti e dell'interfaccia da parte dell'utente, per una migliore facilità d'uso) e la "Classificazioni di contenuti e funzionalità" (es. messa a disposizione di dati geo-referenziati per trovare il Presidio Territoriale più vicino all'utente anche se in mobilità).

- **Sistema di Archiviazione Documentale (AD):** tale sistema attiene alle funzioni di archiviazione elettronica di tutti i documenti di riconoscimento inerenti l'identità, le registrazioni audio/video trattate, i log delle transazioni effettuate e i moduli di adesione firmati. I dati personali e la documentazione raccolti per la verifica dell'identità personale sono trattati e conservati nel rispetto della normativa in materia di tutela dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196**.** Tutta la documentazione è conservata per un periodo non inferiore ai venti anni decorrenti dalla scadenza, dalla disattivazione o dalla revoca dell'identità digitale e sarà successivamente trasmessa alla scadenza contrattuale ad AgID o a soggetto da quest'ultima indicato**.** Tale sistema è implementato su piattaforma IBM FileNet. IBM FileNet è la soluzione per la gestione dei documenti che integra funzioni di workflow predefinite per l'automatizzazione dei processi documentali.

Autorità di Autenticazione (AD)

il modulo interno **"Identity Provider"** espone le interfacce SAML e permette agli utenti l'autenticazione ai servizi online delle Amministrazioni. È l'area che afferisce alla funzionalità di autenticazione intesa come servizio conforme allo standard SAML v2.0 come descritto da specifiche OASIS e seguendo i paradigmi di autenticazione definiti all'interno della normativa SPID e quindi conforme ai requisiti dal punto 3.1 al punto 3.5 del Capitolato Tecnico Lotto 2 (IN, AD).

Il servizio è fornito ad una entità esterna caratterizzata come Service Provider (l'Amministrazione), anch'essa utilizzante analoghi paradigmi dello standard SAML v2.0. L'intera area è basata su tecnologia IBM, in particolare sono presenti i seguenti moduli (MO, IN):

- **Point of Contact:** è il Web Reverse Proxy della soluzione "IBM Security Access Manager for Web" (ISAM) cui perviene la richiesta di autenticazione su protocollo http/https contenente la SAML authentication request generata dal Service Provider esterno. Esso ha il compito di proporre all'utente il challenge di autenticazione con il livello di LoA indicato nell'Authentication Request.

- **Policy Server:** componente della soluzione ISAM che svolge le funzioni di Policy Decision Point autorizzando o meno l'accesso alle risorse Web Protette da ISAM.
- **Identity Registry:** è il registro delle identità realizzato tramite la tecnologia IBM Directory Server che memorizza le informazioni relative all'identità digitale sotto forma di attributi (identificativi e non), e la password per l'autenticazione di livello LoA2. Il prodotto, che realizza lo standard del protocollo LDAP, offre in maniera nativa funzionalità di "scalabilità orizzontale" e sostiene l'aumento dei volumi delle identità da gestire senza modificare l'architettura ma semplicemente aggiungendo risorse hardware (MQ).
- **SAML Federation Gateway:** realizzato tramite la soluzione IBM Security Federated Identity Manager (IFIM), fornisce lo strato applicativo necessario per la gestione dei servizi utili, nel caso specifico, alla realizzazione delle dinamiche dello standard SAML v2.0, supportando tutti i formati ammessi in merito alle asserzioni, alle richieste <authnrequest> con relative risposte <response> e del binding. In particolare garantisce le primitive necessarie per allestire un Single Sign On federato e quindi il trust tra partner qualificati come Identity Provider o Service Provider. Consente inoltre la gestione di token di sicurezza e, nel caso specifico, la validazione e il consumo della SAML Authentication Request proveniente dal Service Provider. A valle della riuscita autenticazione, lo stesso modulo genera la SAML Authenticaton Response, che è restituita tramite il Point of Contact al Service Provider.

Altro modulo contenuto nell'Autorità di registrazione è quello dei **"Servizi di Gestione Fattori di Autenticazione"** comprendente i sistemi complementari che consentono l'autenticazione a più fattori di livello LoA3 e LoA4 come da standard ISO/IEC DIS 29115 (AD, IN).

La sempre maggiore diffusione degli strumenti di comunicazione mobile (telefoni, smartphone e tablet) consente attualmente di disporre praticamente sempre di un dispositivo adatto ad ospitare strumenti che possono essere utilizzati per questo tipo di autenticazione. Il fornitore metterà a disposizione i seguenti supporti (IN AD):

- **LoA2**: sistemi di autenticazione informatica ad un fattore (password); nel sistema proposto verrà utilizzata la coppia username (identificativo univoco) e password[5].
- **LoA3**: sistemi di autenticazione informatica a due fattori non basati necessariamente su certificati digitali le cui chiavi private siano custodite su dispositivi che soddisfano i requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo; nel sistema proposto verranno utilizzati gli attributi username, password statica e OTP (one time password) (IN). Nel dettaglio i sistemi OTP forniti saranno i seguenti:

  ► **Email** ► **OTP Software**, disponibile come App Mobile negli store ufficiali (Android, iOS, Blackberry e Windows Phone (IN) per smartphone e tablet) ► **Callback telefonica** con ultime 4 cifre comunicate dal gestore da utilizzare come PIN per il secondo fattore di accesso.

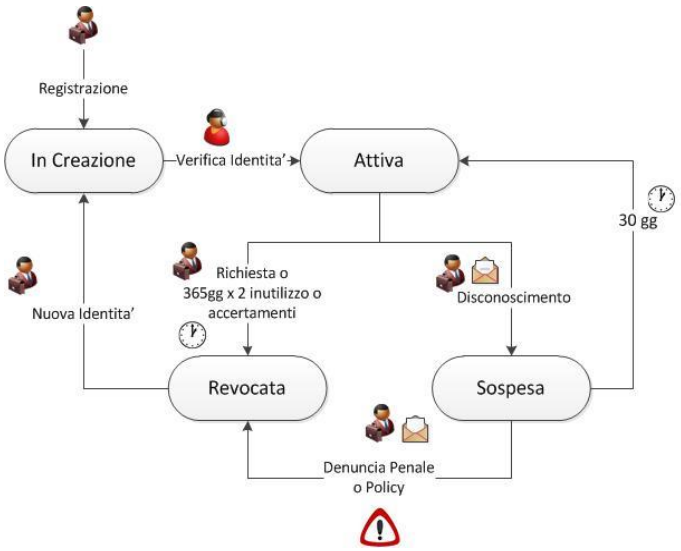
  Le tecnologie proposte hanno carattere di innovatività e praticità, in quanto combinano l'autenticazione in modalità sicura con l'utilizzo di un dispositivo personale e comodo, che l'utente ha sempre con sé.

- **LoA4 (IN)**: sistemi di autenticazione informatica a due fattori basati su certificati digitali, le cui chiavi private siano custodite su dispositivi che soddisfano i requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo; nel sistema proposto saranno utilizzate Smart Card certificate Common Criteria EAL4+ e conformi al DE 1999/93/CE e DPCM 22/2/2013. Il sistema esporrà il servizio OCSP (Online Certificate Status Protocol) per la verifica immediata della revoca o sospensione del certificato da parte dell'IdP. Esso autenticherà ogni cittadino che sia in possesso di un certificato personale emesso dalla PKI privata, fornita dal RTI, che non sia nello stato revocato o sospeso. Potranno essere valutate, in accordo con le Amministrazioni, dispositivi microSD, sempre conformi alle normative, da installare nei lettori SD di dispositivi mobile e personal computer.

Ciclo di vita dell'identità digitale (AD)

I processi e la soluzione tecnologica proposta sono in grado di supportare in maniera adeguata ed efficace il ciclo di vita e l'aggiornamento delle Identità Digitali. Lo schema che segue è una rappresentazione grafica degli stati dell'Identità e delle transazioni che intercorrono tra di esse. Nel diagramma sono inseriti sia gli "attori" sia le" azioni".

[5] La password policy verrà concordata con le Amministrazioni alla stesura dei piani di fabbisogno.



In particolare si evidenziano le seguenti azioni:

a) ***Registrazione Identità Digitale***: Il Cittadino accede all'interfaccia Web (FU) del Portale e sottomette una richiesta di creazione della propria Identità Digitale, precompilando i propri attributi identificativi e non**;** contestualmente sceglie uno dei metodi di riconoscimento disponibili. Al termine del processo di riconoscimento e verifica**,** controllato dal relativo workflow autorizzativo allineato con le procedure previste dai regolamenti e dall'Amministrazione, le credenziali dell'Identità Digitale vengono create nel sistema di autenticazione e consegnate per via sicura al cittadino **(**AD**).**

b) ***Revoca per inutilizzo o per accertamenti***: l'identità digitale, sottoposta ad un predefinito workflow che effettua le verifiche e le notifica al gestore per le azioni del caso, è revocata se si riscontra l'inattività della stessa per un periodo continuativo superiore a ventiquattro mesi o se, mediante servizi di cooperazione applicativa, si riscontrino le cause riconducibili alla cessazione o revoca di una identità digitale **(**AD**)**.

c) ***Disconoscimento*****:** l'Identità Digitale, anch'essa sottoposta al suo specifico workflow, è sospesa a seguito di esplicita richiesta da parte dell'utente nel caso in cui questi ritenga sia stata utilizzata abusivamente o fraudolentemente da un terzo. Secondo i requisiti indicati nel Capitolato, l'azione è innescata a mezzo posta elettronica mediante la quale l'utente dichiara il disconoscimento della propria identità al gestore **(**AD**)**. Qualora vengano indicate altre modalità di disconoscimento, esse saranno integrate nel workflow. Di seguito un caso d'uso relativo al disconoscimento:

1. Invio a mezzo mail della dichiarazione di disconoscimento dell'Identità Digitale al gestore del servizio. Tale dichiarazione se non firmata digitalmente deve avere come allegato copia di un documento di riconoscimento valido,
2. verifica da parte dell'incaricato della correttezza delle informazioni fornite e conseguente sospensione immediata dell'identità, in tal caso saranno gestiti i due scenari alternativi:
    a. revoca dell'Identità Digitale se entro 30 giorni perviene al gestore a mezzo posta elettronica copia della denuncia penale presentata all'autorità giudiziaria per gli stessi fatti su cui è basata la dichiarazione di disconoscimento
    b. ripristino automatico da parte del gestore se entro 30 giorni non perviene la denuncia di cui sopra.

Continuità operativa, funzionalità e architettura fisica del servizio di Identity Provider

L'architettura logica precedentemente descritta è realizzata tramite l'integrazione di tecnologie eterogenee, hardware e software, progettate per operare in sinergia rispondendo, oltre ai requisiti funzionali già descritti, a quelli non funzionali di alta affidabilità, scalabilità, performance, Business Continuity e Disaster Recovery.

A tale scopo, in conformità con l'approccio sostenuto per tutti gli altri servizi, si è scelto di distribuire la tecnologia su due siti in Business Continuity e un sito di Disaster Recovery (MO, EC, AD, IN). Per i dettagli in merito alla dislocazione geografica e all'architettura dei siti si rimanda alla documentazione del centro servizi (rif. §3.4).

Per le attività di collaudo sarà predisposto l'ambiente di Test-Bed strutturato secondo il principio della replica in termini di risorse hardware e software aventi le stesse caratteristiche funzionali di base dell'ambiente di Business Continuity, ivi compresa l'alta affidabilità.

Come elemento migliorativo il RTI metterà a disposizione per tutta la durata del contratto un ambiente ulteriore di Test/Sviluppo avente le medesime caratteristiche funzionali dell'Ambiente di Business Continuity supportando le attività del Team di Innovazione Tecnologica dettagliato nel paragrafo "Organizzazione Ruoli e Responsabilità per il governo del contratto quadro" (rif. § 3.2.2.1).

In funzione del numero di identità gestite, il criterio principale adottato nel dimensionamento delle risorse di sistema e software è stato quello di garantire il massimo rendimento in termini di: ► capacità di elaborazione delle richieste in parallelo ► capacità di accodamento del sistema ► tempi di risposta del sistema.

Nel grafico è presentata l'architettura fisica (IN, AD). Ogni blocco elementare corrisponde a nodi virtuali di tipo appliance o software. I tre siti di riferimento avranno la stessa distribuzione delle componenti.

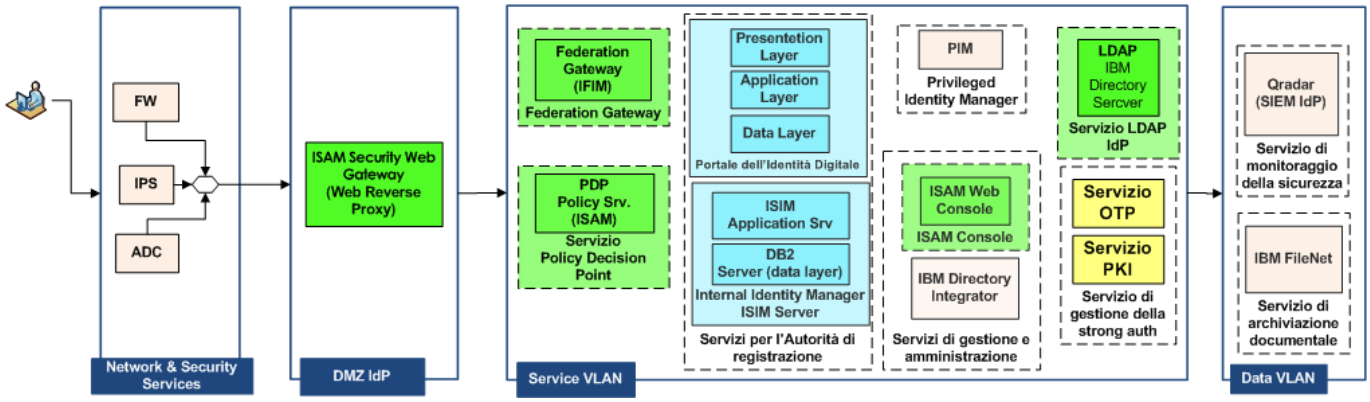


Figura 30: Architettura fisica IdP

L'alta affidabilità è realizzata geograficamente tra i due siti di business continuity (BC) i quali sono contemporaneamente attivi. In condizioni di normale operatività, è gestito il bilanciamento del carico di lavoro tra i due siti di BC consente un ulteriore incremento delle prestazioni. Il singolo sito è in ogni caso dimensionato in modo da sostenere autonomamente il massimo carico di lavoro nominale previsto (AD).

L'area funzionale denominata come "**Autorità di Autenticazione**" (contraddistinta in verde), integralmente basata su tecnologia IBM, ha come fulcro l'utilizzo di un Web reverse proxy (altrimenti nominato WebSEAL), fornito all'interno dell'appliance virtuale **ISAM Security Web Gateway** responsabile dell'autenticazione degli utenti dietro verifica di una valida userid registrata nella directory LDAP; esso applica le politiche di controllo degli accessi alle richieste degli utenti, e installato in zona demilitarizzata (DMZ), consente di aumentare sicurezza e protezione delle risorse web (IN, AD).

Il Security Web Gateway Virtual Appliance fornisce inoltre funzioni, aggiuntive a quanto previsto dal capitolato, relative alla protezione dalle minacce, mediante Web Application Firewall. Le regole di protezione sono aggiornate tramite un servizio on-line di update basato sugli input forniti dal team di ricerca e sviluppo IBM X-Force(IN).

La soluzione proposta è pienamente compatibile con gli scenari sempre più diffusi che vedono gli utenti internet accedere ai servizi Web mediante browser http fruiti da dispositivi mobile (smartphone/tablet)(IN).

L'area "**Autorità di Registrazione**" è indicata in celeste e comprende il Portale dell'Identità Digitale, i servizi di front-end e back-end per i singoli attori (Amministrazione, Cittadino, Redattori). La soluzione proposta è basata sulla piattaforma jAPS 4.0 Entando, una piattaforma web open source con licenza GPL v2, in tecnologia Java EE, che nasce in Italia e ne rispetta pienamente la normativa (CAD, Legge Stanca, Privacy, Trasparenza e partecipazione attiva del cittadino) (IN). Esso combina gli elementi di un portale di classe Enterprise, di un Content Management System e di un framework per applicazioni web in un unico prodotto. All'interno della stessa area è presente anche l'ISIM Server (IBM Security Identity Manager) per implementare le funzionalità di workflow autorizzativo.

L'area "**Servizi di Gestione Fattori di Autenticazione**" (blocchi in giallo) è sintetizzata rispettivamente nei blocchi:

- Servizio OTP: infrastruttura per l'emissione e gestione del ciclo di vita del token OTP (IN)
- Internal PKI: componente abilitante alla emissione e gestione del ciclo di vita dei certificati personali (IN, AD).

In aggiunta a quanto direttamente associabile al disegno funzionale si evidenziano i seguenti componenti di software: un cruscotto di monitoraggio della sicurezza (Security Information and Event Management, SIEM) implementato tramite tecnologia IBM Security QRadar (AD), un sistema di Privileged Identity Management per la gestione del ciclo di vita degli utenti con privilegi di amministrazione per quanto riguarda l'accesso a qualsiasi componente del sistema di Identity Provider (AD) e strumenti che facilitano le attività di porting e migrazione: IBM Directory Integrator per il caricamento massivo di identità digitali nell'LDAP a valle del processo di migrazione (AD).

La tabella evidenzia come il criterio principale adottato nel dimensionamento delle risorse di sistema e software viene applicato nella simulazione di un caso reale di utenti pari a **2 milioni**. Il dimensionamento di cui alla tabella deve essere considerato al netto di ulteriori macchine di Test Bed e Sviluppo previste all'interno del servizio, e dell'Infrastruttura prevista per la sicurezza e controllo del servizio.

Tabella 12: Tabella riepilogativa della fornitura HW/SW per IdP - simulazione per carico 2 mln utenti

Tabella riepilogativa della fornitura HW/SW per IdP - simulazione per carico 2 mln utenti					
Software servizio IdP	**CPU core per server**	**RAM (GB) per server**	**Disk (GB) per server**	**Disk (TB) SAN**	**n° macchine**
IBM Security Access Manager Reverse Proxy	8	16	50	0,5	4
IBM Federated Identity Manager	8	16	50		2
ISAM Policy Server	4	8	50		2
ISAM Console	8	16	50		2
IBM Directory Server	16	24	200		4
IBM Security Identity Manager	8	16	50		2
IBM ISIM Data Base	16	64	50		2
IBM QRadar SIEM	8	16	100	10	2
IBM Directory Integrator	8	16	50	0,5	2
Portale dell'Identità Digitale (presentation)	8	16	50		3
Portale dell'Identità Digitale (application)	8	16	100		2
Portale dell'Identità Digitale (dati)	8	16	200		3
Privileged Identity Manager System	8	16	50		2
PKI Systems	8	16	50		2
Servizio OTP	8	16	100		3
IBM FileNet (archiviazione documentale)	8	16	50	20	3
Riepilogo per singolo sito e globalmente sui tre siti					
Totali	**CPU core totali**	**RAM (GB) totali**	**Disk (TB) totali (server)**	**Disk (TB) totali (SAN)**	**n° macchine totali**
Totale per singolo sito	360	752	3,4	31[6]	40
Totale per sito principale, Business Continuity e Disaster Recovery	1080	2256	10,2	93	120

4.1.4.2 Identity e Access Management

Il servizio di I&AM fornito dal RTI è erogato in modalità "as a service" e gestisce le attività di identificazione, autenticazione e autorizzazione all'accesso ai portali delle Amministrazione e alla fruizione dei servizi da esse erogati ai propri utenti esterni (AD).

Le caratteristiche distintive del servizio includono:

- Ogni area funzionale è nettamente distinguibile da tutte le altre: ciò consente una gestione e manutenzione indipendente della singola componente (MO)
- al crescere della domanda (in termini di nuove Amministrazioni integrate, e/o quantità di utenti gestiti, e/o transazioni Web eseguite) è possibile aumentare, nelle proporzioni adeguate, le risorse software e di sistema, mantenendo così costanti gli standard di servizio erogati (MO, EC).
- possibilità di integrare Applicazioni Web presso le Amministrazioni basate su tecnologie eterogene in modalità "Unauthenticated" e/o "Authenticated" (FU)
- la modalità "Authenticated" consente all'Amministrazione di configurare i propri sistemi in modo che, in un periodo transitorio, coesistano contemporaneamente il vecchio modello di autenticazione tramite il sistema di sicurezza locale e il nuovo tramite IdP (FU)
- la modalità "Authenticated" consente di applicare delle policy autorizzative di particolare dettaglio ("grana fine") alle applicazioni Web delle Amministrazioni che ne abbiano necessità (FU)
- segregazione degli spazi Web e delle policy d'accesso tra le varie Amministrazioni che partecipano al servizio in modalità *multitenant*: ciò consente di fornire alla singola Amministrazione una vista limitata

[6] Di cui il 10% in tecnologia SSD – Solid State Disk

esclusivamente sul proprio dominio e un controllo puntuale della propria policy di accesso oltre che degli utenti abilitati ai propri servizi **(AD)**

- disponibilità di una interfaccia Web di gestione del ciclo di vita dell'utenza e dei suoi profili autorizzativi. Con tale strumento si intende dare controllo e autonomia di gestione all'Amministrazione sulle politiche d'accesso, pur svincolandole dal dover gestire nel proprio sito web le identità e i profili autorizzativi (IN, FU)
- tutte le componenti dell'architettura fanno parte di una soluzione integrata IBM, il cui valore è frutto dello sviluppo tecnologico e dell'esperienza su numerose e complesse realtà di business, diffuse a livello mondiale (AD).
- indipendenza dai sistemi operativi e dalle applicazioni: versatilità nell'integrazione di tecnologie eterogenee. Per la maggioranza delle applicazioni Web fondate su tecnologie proprietarie sono disponibili best practice d'integrazione (AD,MO)
- disponibilità di un cruscotto unificato, per la verifica in tempo reale delle statistiche circa l'utilizzo puntuale di risorse dello I&AM per ogni servizio gestito. Esso segnalerà il superamento di soglie di attenzione definite, consentendo l'attivazione di contromisure a garanzia della disponibilità delle risorse (EC).
- la gestione del ciclo di vita dei profili autorizzativi può avvenire in più modalità sia agendo puntualmente sul singolo utente sia associandolo automaticamente, sulla base della valutazione dei suoi attributi qualificati, a categorie predefinite di utenti (AD,IN).

Per l'autenticazione dei propri utenti il servizio è abilitato all'interazione con Identity Provider esterni all'Amministrazione **(AD,MO)**. Per la verifica degli attributi associati al profilo di un utente, non certificabili dalla stessa Amministrazione contraente, il servizio farà ricorso ad **Attribute Authority** esterne. Le fonti delle informazioni relative agli Identity Provider ed alle Attribute Authority esterne saranno indicate dall'Amministrazione. Il servizio è fornito in modo indipendente dai sistemi operativi ed applicativi utilizzati e dalle architetture di rete **(AD, MO).**

Nella Figura 31 è illustrato come i requisiti funzionali espressi per il servizio I&AM siano adeguatamente soddisfatti dall'architettura logica proposta (AD) tramite l'integrazione di tecnologie eterogenee, hardware e software, progettate per operare in sinergia. Sempre la Figura 31 mostra, a partire dal modello logico richiesto dal Capitolato (Rif. figura pag. 17 Cap. Tecn.) il parallelo con la proposta del RTI in termini componenti architetturali del servizio I&AM come erogato del Centro Servizi (cfr. nella figura il blocco denominato "I&AM").

La trattazione che segue è incentrata sugli aspetti funzionali della soluzione. L'architettura fisica scalabile (EC) (MO), dimensionata in base al carico di lavoro previsto ed ai requisiti di Alta Affidabilità e Business Continuity (AD), verrà affrontata in maniera distinta successivamente.

La suite tecnologica adottata prevede l'utilizzo di **IBM Security Access Manager for Web** (ISAMxWeb nel seguito) per implementare le tre funzioni principali richieste: **Policy Enforcement Point** (PEP, implementata dal componente ISAM Web Reverse Proxy), **Policy Decision Point** (PDP, implementata dell'ISAM Policy Server), e **Policy Store** (implementata dall'IBM Directory Server e dal Policy Server)(AD).

In aggiunta al modello di riferimento sono inoltre esplicitati i seguenti blocchi funzionali, tutti necessari per dare massima efficacia al servizio (EC):

1. **SAML Federation Gateway (AD,IN):** realizzato tramite la soluzione IBM Federated Identity Manager (IFIM) fornisce lo strato applicativo necessario per la gestione dei servizi utili alla realizzazione delle dinamiche dello standard SAML v2.0 come descritto nelle specifiche OASIS.
2. **IBM Directory Integrator** (IDI,IN) è il tool programmabile per lo scambio di informazioni tra strutture dati eterogenee. Nell'architettura proposta la sua funzione è quella di implementare la logica di "Just-in-Time Provisioning" necessaria per la creazione dell' account I&AM, nel dominio di sicurezza ISAM, in seguito alla prima autenticazione di una identità.
3. **Web Profiles Manager (IN,AD,FU)**: l'Amministratore locale della PA avrà la possibilità di accedere ad una interfaccia Web di Gestione con visibilità dei soli dati degli utenti accreditati alla propria Amministrazione. Egli avrà facoltà di ricercare le proprie utenze nel Policy Store I&AM, di visualizzarne gli attributi e procedere autonomamente all'assegnazione dei profili autorizzativi. Si ricorda che, come previsto dagli obblighi del servizio di Identità Digitale, da questi attributi si ritengono escluse le componenti riservate delle identità degli utenti.

L'Amministratore avrà la possibilità di dichiarare/definire nuovi profili autorizzativi ed utilizzarli nelle assegnazioni.

La figura seguente riporta l'architettura del sistema I&AM.

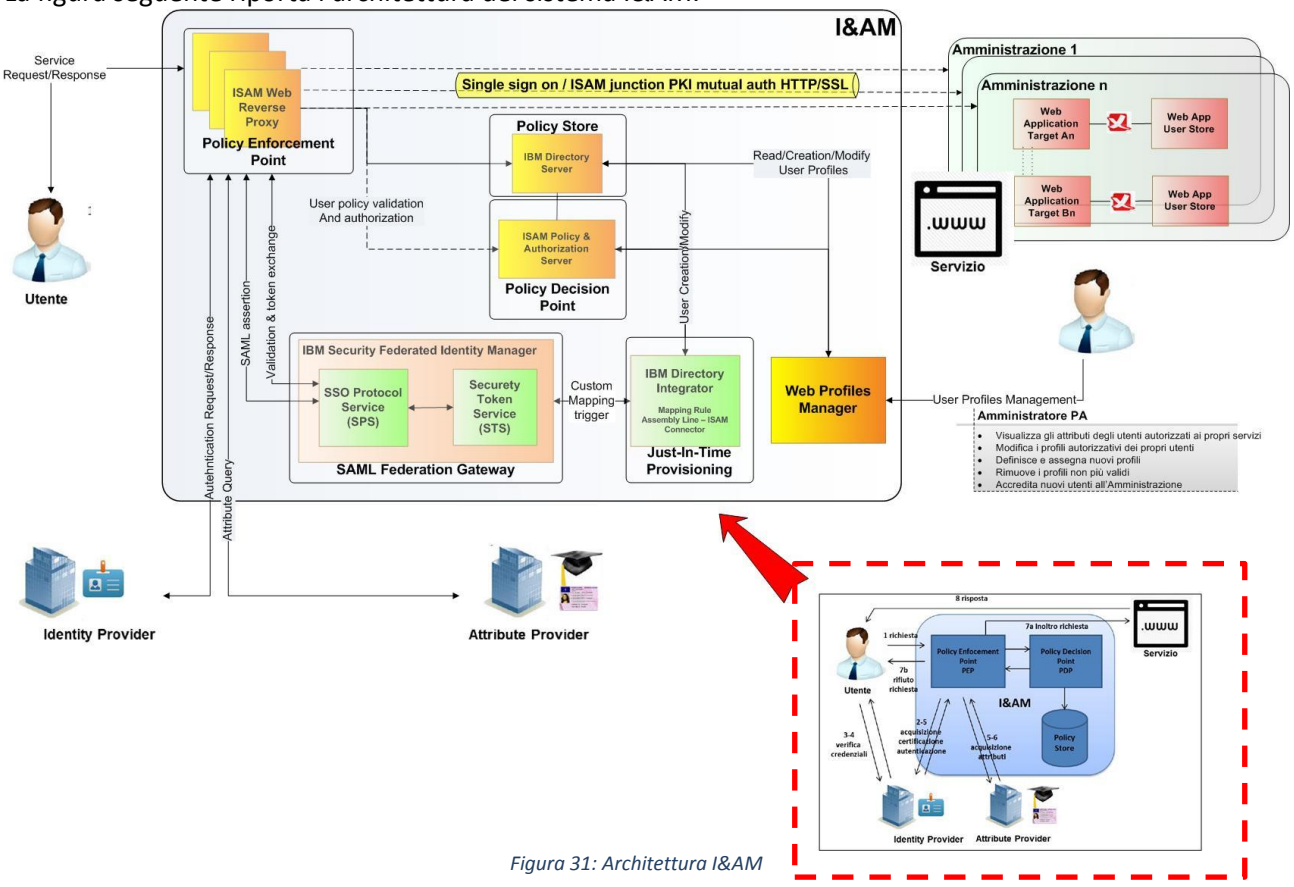


Figura 31: Architettura I&AM

Figura pag. 17 dell'All. 5B

Le funzionalità che saranno realizzate sono le seguenti (IN, AD, EC, FU):

- **Ricerca** di utente accreditato all'Amministrazione e visualizzazione dei suoi attributi e profili autorizzativi;
- **Modifica** della assegnazione dei profili autorizzativi;
- **Definizione** di un nuovo profilo.
- **Cancellazione** profilo.
- **Accreditamento nuovo utente**: in questa fase sarà necessario specificare solamente il codice identificativo univoco dell'identità. Se l'utente è già presente nello I&AM, esso viene visualizzato con tutti i suoi attributi e quindi può essere aggiornato con l'assegnazione di nuovi profili. Se l'utente non è ancora presente, esso sarà creato senza gli attributi personali, che saranno comunque valorizzati dall'IdP e dal Servce provider alla prima richiesta di accesso (*Just-in-Time Provisioning*).
- **Sospensione o revoca dell'utente**: l'utente, indipendentemente dalla valorizzazione dei suoi profili, non sarà più autorizzato ad accedere ai servizi dell'Amministrazione.

Nel modello sono state fatte alcune assunzioni circa due ipotetici scenari tecnologici gestibili presso le Amministrazioni:

1. Scenario "**Unauthenticated**": le Amministrazioni espongono applicazioni Web con strato di sicurezza disabilitato e pertanto affidano integralmente il controllo dell'autenticazione e autorizzazione rispettivamente ad un servizio IdP e al servizio I&AM. Lo I&AM protegge una serie di servizi applicativi delle Amministrazioni presentati sotto forma di URL e agli utenti, superato il processo di autenticazione sull'IdP, è accordato o meno accesso in base al loro profilo autorizzativo. In questo scenario l'accesso sarà controllabile per la specifica URL (servizio Web) e al livello di profilatura e l'Amministrazione dovrà solo specificare se l'autorizzazione sia concessa o meno (MO, IN, FU).
2. Scenario "**Authenticated**" (che costituisce una funzionalità aggiuntiva rispetto alle richieste del Capitolato) (IN): le Amministrazioni espongono applicazioni Web su piattaforma con strato di sicurezza abilitato e pertanto quest'ultimo deve essere configurato per delegare in maniera selettiva autenticazione e autorizzazione a terze parti (l'IdP e lo I&AM rispettivamente). A tale scopo l'applicazione web recupera opportunamente i dati passati dal Web Reverse Proxy (l'identificativo dell'utente ed il suo profilo nominale), creando il mapping con il contesto di

sicurezza locale e così consentendo un'autorizzazione "**Fine-Grained**" (IN). Tale scenario presenta il vantaggio di continuare a permettere la gestione locale dell'autorizzazione di "grana fine" e consente alle amministrazioni, potenzialmente, di gestire un periodo transitorio durante il quale entrambe le possibilità di autenticazione/autorizzazione possano coesistere. È così concessa la libertà ad un utente di scegliere, limitatamente al periodo transitorio, di continuare ad autenticarsi con il vecchio sistema oppure con il nuovo servizio (IdP).

Sono evidenziati di seguito gli aspetti salienti della soluzione tecnologica:

1. La gestione *multitenant* e la segregazione logica degli ambienti, dei dati e delle policy di sicurezza è realizzata tramite la definizione di tante istanze dedicate di *ISAM Web Reverse Proxy* (Policy Enforcement Point) quante sono le Amministrazioni integrate nel SSO federato (AD,MO);
2. Per lo I&AM il *Policy Store* contiene le utenze replicate delle identità registrate sugli IdPs partner che accedono ai servizi I&AM (MO,EC);
3. Il popolamento delle utenze I&AM può avvenire per mezzo di un meccanismo di auto provisioning, denominato "*just-in-time provisioning*" (IN);
4. È possibile eseguire in un qualsiasi momento operazioni di popolamento massivo delle utenze (IN).
5. Le policy a "grana grossa" (Coarse-grained) per l'autorizzazione di accesso alle applicazioni per ogni singola Amministrazione prevedono la definizione di regole d'accesso basate sui gruppi. Le regole d'accesso sono esaminate ed applicate dal Web Reverse Proxy (PEP) (IN,AD,MO).
6. Il modello architetturale richiede interventi minimi sugli ambienti tecnologici delle Amministrazioni garantendo il massimo dell'efficacia (EC). L'unico punto di contatto tra il servizio I&AM e le Amministrazioni è realizzato attraverso la tecnica del collegamento logico con il sistema ISAM, denominato giunzione. La soluzione proposta prevede la componente PEP dislocata presso il centro servizi del fornitore; la flessibilità e modularità delle tecnologie utilizzate ne permettono tuttavia la collocazione presso l'Amministrazione, qualora questa, a seguito di valutazioni oggettive con il RTI, ne suggerisca l'opportunità (IN,MO). La logica di autorizzazione "**Coarse-Grained**" applicata al livello dello I&AM prevede che per ogni utente siano conosciute le applicazioni/servizi dell'Amministrazione cui è titolato ad accedere (AD);
7. La facoltà di scegliere su quale Identity Provider l'utente possa autenticarsi è offerta tramite una funzionalità del IFIM chiamata "*Where Are You From?*" (WAYF?) (AD). Nella fase di adesione dell'Amministrazione al servizio dovrà essere dichiarata la lista degli IdP ad essa associabili (AD);
8. Come elemento migliorativo la soluzione aderisce al profilo standard SAML chiamato "Identity Provider Discovery Profile" (MO,IN). Tale *profilo* permette di rendere trasparente all'utente la scelta dell'IdP (FU);
9. Il popolamento dei profili amministrativi può avvenire con un elevato grado di flessibilità (MO,IN,EC):
   - **Modalità offline schedulata**: l'Amministrazione fornisce file in formato csv o similari contenente la lista delle associazioni <codice identificativo univoco>:<profili>. IBM Directory Integrator è lo strumento per il caricamento dei dati nel Policy Store dello I&AM.
   - **Modalità Interfaccia Web di gestione (FU)**: l'Amministrazione ha la possibilità di caricare i dati delle proprie utenze tramite interfaccia Web dedicata.
   - **Modalità online (IN)**: qualora l'amministrazione agisca da Attribute Authority potrà essere interrogata dallo I&AM per ottenere la lista dei profili applicativi abilitanti.
   - **Modalità automatica per categorie utenti (EC)**: l'Amministrazione può evitare l'assegnazione puntuale dell'utente al proprio profilo autorizzativo, delegando ciò ad un automatismo basato sulla classificazione, in base agli attributi, di categorie di utenti, con conseguente mappatura su gruppi/profili predefiniti. La logica di assegnazione sarà decisa dall'Amministrazione e comunicata al gestore che provvederà a "programmarla" all'interno del servizio I&AM

4.1.4.3 Erogazione del servizio I&AM

Si assume che ogni Amministrazione presenti più applicazioni Web autonome fondate sulla sicurezza di tecnologie proprietarie eterogenee da integrare nel servizio I&AM (WebSphere, IIS, Tomcat, JBoss, Oracle Application Server, etc.). Ogni Applicazione Web presenterà inizialmente il suo sistema di controllo accessi locale abilitato, basato su

un proprio Policy Store locale. L'inclusione dell'applicazione Web nel servizio I&AM presuppone un'attività di configurazione volta a consentire il trusting e quindi l'autenticazione a carico di terze parti (MO,EC). E' inoltre prevista la ricostruzione del contesto di sicurezza dell'utente. A seconda delle tecnologie coinvolte sarà svolto da parte del RTI uno studio preliminare per fornire le best practice di abilitazione del trusting, con lo scopo di agevolare il "change" tecnologico da parte dell'Amministrazione.
La soluzione garantisce il supporto di tutti i formati ammessi dallo standard SAMLv2.0 in merito alle asserzioni, alle richieste di <AuthnRequest> con relative risposte <Response> e del binding (AD).

Continuità operativa, funzionalità e architettura fisica del servizio di I&AM

L'architettura logica precedentemente descritta è realizzata tramite l'integrazione di tecnologie eterogenee, hardware e software, progettate per operare in sinergia rispondendo, oltre ai requisiti funzionali già descritti, a quelli non funzionali di alta affidabilità, scalabilità, performance, Business Continuity e Disaster Recovery.
A tale scopo, in conformità con l'approccio sostenuto per tutti gli altri servizi, si è scelto di distribuire la tecnologia su due siti in Business Continuity e un sito di Disaster Recovery (IN,AD,MO). Per i dettagli in merito alla dislocazione geografica e all'architettura dei siti si rimanda alla documentazione del centro servizi (rif. §3.3).
Per le attività di collaudo sarà predisposto l'ambiente di Test-Bed strutturato secondo il principio della replica in termini di risorse hardware e software aventi le stesse caratteristiche funzionali di base dell'ambiente di Business Continuity, ivi compresa l'alta affidabilità.
Come elemento migliorativo il RTI metterà a disposizione per tutta la durata del contratto un ambiente ulteriore di Test/Sviluppo avente le medesime caratteristiche funzionali dell'Ambiente di Business Continuity supportando le attività del Team di Innovazione Tecnologica dettagliato nel paragrafo "Organizzazione Ruoli e Responsabilità per il governo del contratto quadro" (rif. § 3.3).
In funzione del numero di identità gestite, il criterio principale adottato nel dimensionamento delle risorse di sistema e software è stato quello di garantire il massimo rendimento in termini di: ► capacità di elaborazione delle richieste in parallelo ► capacità di accodamento del sistema ► tempi di risposta del sistema.
Oltre al monitoraggio previsto per assicurare la disponibilità e continuità del servizio sarà predisposto il Monitoraggio delle statistiche circa le prestazioni del servizio erogato per ogni Amministrazione (MO,AD,EC). Attraverso tale strumento sarà possibile avere riferimento misurazioni in tempo reale, visualizzabili in un cruscotto unificato a disposizione del Team di Service Operation e in uso del team di ICT Operation, circa il consumo puntuale di risorse dello I&AM per ogni servizio protetto presso le Amministrazioni (FU). Esso segnalerà il superamento di eventuali soglie di attenzione consentendo delle contromisure ai primi sintomi di degrado, così anticipando l'incorrere di anomalie bloccanti (IN).

Nel grafico è presentata l'architettura fisica (IN,AD). Ogni blocco elementare corrisponde a nodi virtuali di tipo appliance o software. I tre siti di riferimento, avranno la stessa distribuzione delle componenti. Di seguito viene descritto ogni singolo blocco dell'architettura.

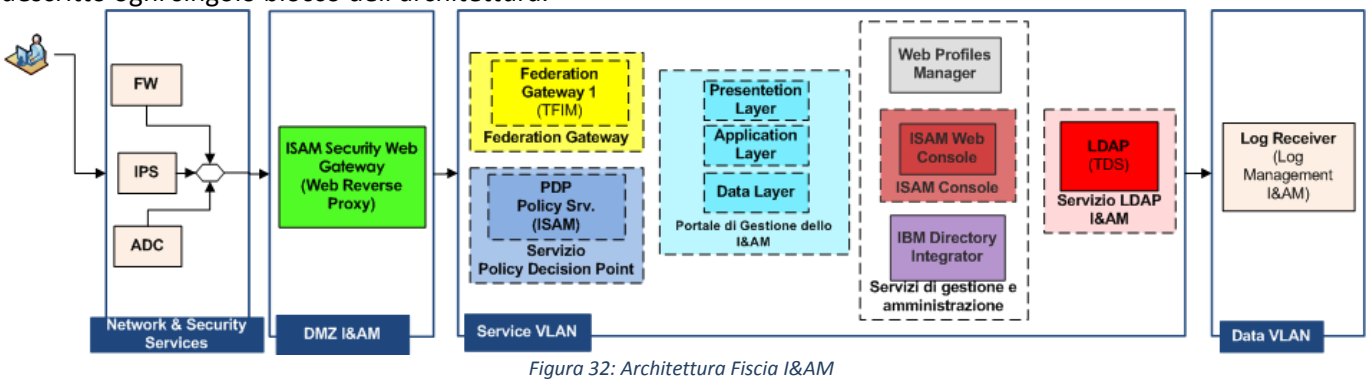


Figura 32: Architettura Fiscia I&AM

L'alta affidabilità è realizzata geograficamente tra i due siti di Business Continuity (BC) i quali sono contemporaneamente attivi. In condizioni di normale operatività, è gestito il bilanciamento del carico di lavoro tra i due siti di BC consentendo un ulteriore incremento delle prestazioni. Come già detto il singolo sito è in ogni caso dimensionato in modo da sostenere autonomamente il massimo carico di lavoro nominale previsto (AD).
I diversi nodi virtuali, ridondati per garantire disponibilità, performance e alta affidabilità, sono strettamente integrati con tutti gli altri (EC,IN,MO) e assolvono alle funzionalità precedentemente descritte nel disegno logico/funzionale, ossia:: ► **Policy Enforcement Point Policy Store ► Policy Decision Point ► SAML Federation Gateway ► Just-In-Time-Provisioning ► Web Profiles Manager**

L'area funzionale denominata "**Policy Enforcement Point**" è implementata dai nodi appliance virtuali **ISAM Security Web Gateway** attraverso il servizio di Web reverse proxy. Esso valida l'utenza registrata nella directory LDAP ("**Policy Store**") implementato su tecnologia Tivoli Directory Server. Il PEP crea le credenziali ed applica le politiche di controllo degli accessi alle richieste degli utenti, gestendo la sessione Web nel suo intero ciclo di vita. Il Security Web Gateway Virtual Appliance fornisce inoltre, come già specificato nella trattazione dell'IdP, funzioni aggiuntive di protezione dalle minacce, mediante Web Application Firewall (IN); tali funzionalità sebbene non richieste nel Capitolato, sono incluse nella soluzione proposta.

Il Web Reverse Proxy (WebSEAL) gestisce l'autorizzazione degli utenti sul dominio protetto e provvede alla realizzazione del Web Single Sign On verso i sistemi di back-end. E' sufficiente configurare l'ISAM e i sistemi target affinché essi possano condividere il contesto di sicurezza. In generale, in un ambito di integrazione che esula dai requisiti del Capitolato, l'ISAM offre ulteriori funzionalità modularità estremamente modulari (MO) quali, ad es. gli *adapter* di integrazione verso sistemi di terze parti (IN). In alcuni casi tali adapter consistono in moduli di integrazione che vengono installati sui sistemi di back-end affinché essi possano consumare le credenziali fornite da ISAM (es. attributi in http header, token). L'elenco delle integrazioni disponibili out-of-the-box è tenuto aggiornato dall'info center della soluzione[7].

Le politiche di accesso sono governate centralmente attraverso il Policy Server, che costituisce funzionalmente il "**Policy Decision Point"** della soluzione. Le modifiche alle policy possono avvenire attraverso la console amministrativa disponibile via Web (ISAM Console), oppure tramite CLI (Command Line Interface); sono inoltre disponibili API di gestione. In ambito autorizzativo la suite proposta fornisce anche funzionalità avanzate di "Risk Based Access" basate sulla valutazione di dati di sessione quali per esempio la geo-localizzazione, l'IP reputation ed il dispositivo di accesso (funzionalità di "fingerprint") (IN). Ad esempio può essere incrementato il livello di LoA con un processo di autenticazione progressiva (*step-up authentication*), oppure negato del tutto l'accesso, nel caso in cui la richiesta provenga da dispositivi utilizzati in aree geografiche a rischio, o con IP appartenenti a liste sospette, oppure da dispositivi sconosciuti (cioè non censiti tra i dispositivi, mantenuti in un DB interno, catalogati nei login passati).

La gestione delle primitive del Federated Single-Sign-On, quindi del protocollo SAML e dei meccanismi di trust con i partner federati (le Amministrazioni) sono a carico del "**SAML Federation Gateway**" implementato tramite la soluzione IBM Federated Identity Manager (EC, AD).

La funzione di **Just-in-time Provisioning (IN)**, più volte citata, è implementata dal tool IBM Directory Integrator (IDI). Attraverso la sua estrema flessibilità, IDI consente l'esecuzione di un flusso logico programmato in grado di eseguire l'auto-provisioning degli utenti prendendo le informazioni in input dal IFIM e inserendo i dati in output sul Policy Decision Point e sul Policy Store, avendo come condizione scatenante il primo accesso di un utente ad un servizio. Tutto questo può avvenire grazie all'utilizzo di connettori predefiniti che consentono la comunicazione tra strutture dati eterogenee. Lo stesso strumento sarà utilizzato, sfruttando ovviamente una diversa programmazione, per il processo di migrazione massivo dei profili utente (MO).

Il **Web Profiles Manager** è una componente applicativa che ha lo scopo di fornire alle Amministrazioni uno strumento di gestione autonoma degli utenti accreditati ai propri servizi, visualizzandone gli attributi che ne costituiscono l'identità digitale e consentendo il controllo sull'intero ciclo di vita dei profili autorizzativi ad essi assegnati. L'applicazione è parte integrante del "**Portale di Gestione dello I&AM" (IN, FU).**

In risposta al requisito che ogni operazione effettuata sui sistemi deve essere riconducibile a soggetti correttamente identificati, autenticati e autorizzati, e alla necessità di rilevare tutti i tentativi di accesso non autorizzato da parte degli utenti, sono predisposti dei server **Log receiver** in qualità di sistemi di Log Management **(AD).** Tali sistemi avranno il compito di raccogliere e archiviare gli eventi di accesso prodotti dal servizio I&AM nelle modalità e nei tempi previsti dalla normativa.

La tabella evidenzia come il criterio principale adottato nel dimensionamento delle risorse di sistema e software viene applicato nella simulazione di un caso reale di utenti pari a 4 milioni. Il Dimensionamento di cui alla tabella deve essere considerato al netto di ulteriori macchine di Test Bed e Sviluppo previste all'interno del servizio, e dell'Infrastruttura prevista per la sicurezza e controllo del servizio.

[7] http://www-01.ibm.com/support/knowledgecenter/SSELE6_8.0.0.4/com.ibm.isam.doc_8.0.0.4/welcome.html#!/SSPREK/welcome

Tabella 13: Tabella riepilogativa della fornitura HW/SW per I&AM - simulazione per carico 4 mln utenti

Tabella riepilogativa della fornitura HW/SW per I&AM - simulazione per carico 4 mln utenti					
Software servizio I&AM	**CPU core per server**	**RAM (GB) per server**	**Disk (GB) per server**	**Disk (TB) SAN[8]**	**n° macchine per 2mln utenti**
IBM Security Access Manager Reverse Proxy	8	16	50	0,5	8
IBM Federated Identity Manager	8	16	50		4
IBM ISAM Policy Server	4	8	50		2
IBM ISAM Console	8	16	50		2
IBM Directory Integrator	8	16	50		2
IBM Directory Server	16	24	200		4
Log Receiver System	8	16	50	3	2
Portale di Gestione dello I&AM (presentation)	8	16	50	0,5	2
Portale di Gestione dello I&AM (application)	8	16	100		2
Portale di Gestione dello I&AM (dati)	8	16	100		2
Riepilogo per singolo sito e globalmente sui tre siti					
Totali	**CPU core totali**	**RAM (GB) totali**	**Disk (TB) totali (server)**	**Disk (TB) totali (SAN)**	
Totale per singolo sito	264	496	2300	11	30
Totale per sito principale, Business Continuity e Disaster Recovery	792	1488	6900	33	90

4.2 Soluzione per l'erogazione di Servizi di Firma Digitale Remota e Timbro Elettronico

Nel presente paragrafo si descrivono i servizi di **firma digitale remota** e **timbro elettronico** proposti dal RTI.
Con "**firma remota**" si intende la firma digitale eseguita con una chiave privata non residente su un dispositivo personale, trasportabile, dell'utente bensì su un dispositivo *remoto*. L'utente deve accedere al servizio utilizzando un sistema di **autenticazione a due fattori** (*conoscenza* e *possesso*) basato su token OTP.
Il "**timbro elettronico**", consente alle Amministrazioni la creazione di documenti informatici che conservano la medesima validità legale anche dopo essere stati stampati su supporto cartaceo.
Nel seguito sono descritte le modalità organizzative e tecnologiche per l'erogazione dei servizi.

4.2.1 Soluzione Organizzativa

Il modello organizzativo per l'erogazione del servizio è costituito dall'insieme di strutture e processi operativi con i relativi flussi informativi, che saranno posti in essere dal RTI al fine di soddisfare i requisiti dell'Amministrazione nel rispetto dei livelli prestazionali previsti dal capitolato di Gara.

[8] Di cui il 10% in tecnologia SSD – Solid State Disk

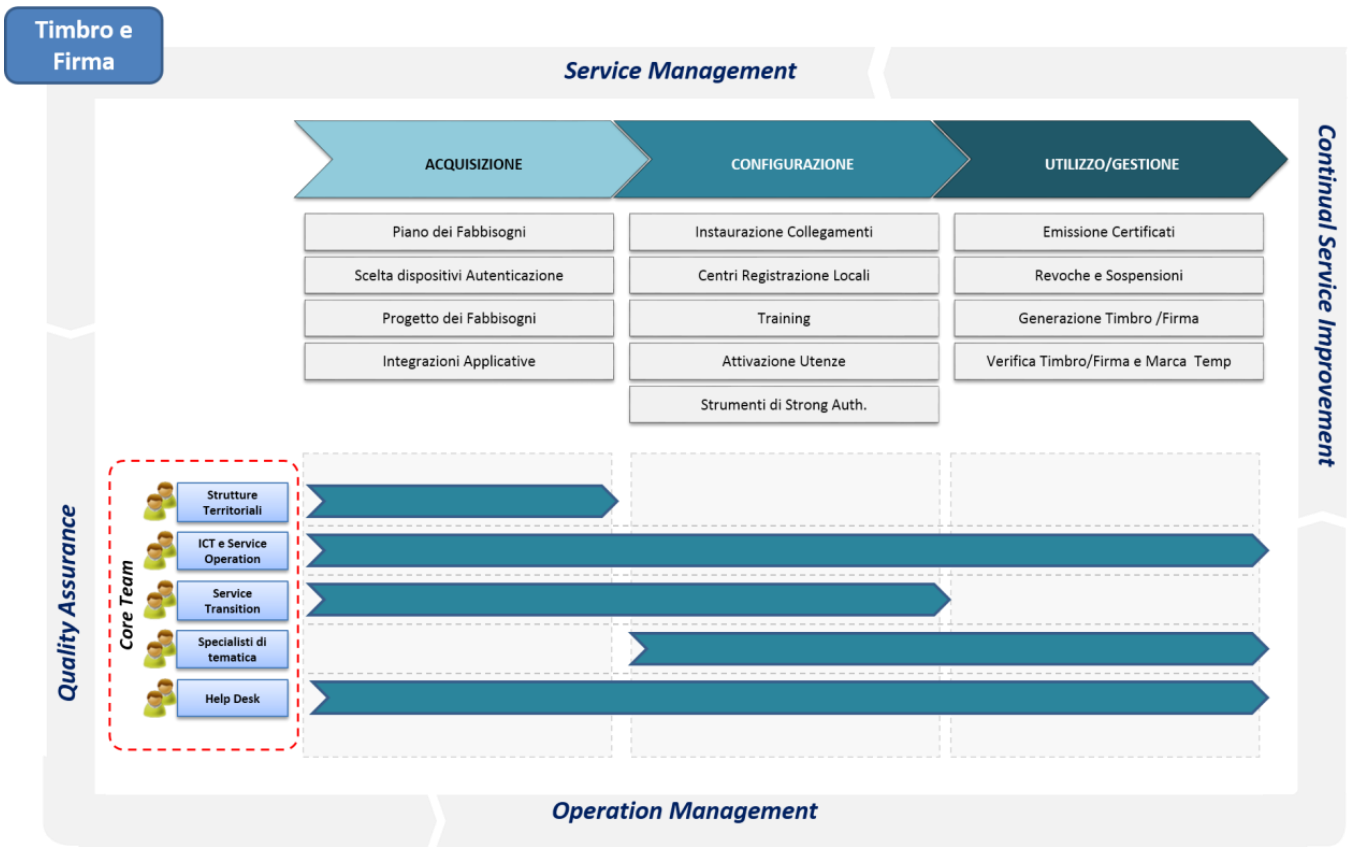


Figura 33: Struttura Organizzativa per il Servizio di Firma/Timbro

La struttura organizzativa proposta per i servizi di Firma digitale Remota e Timbro elettronico è analoga a quella già presentata per i servizi IdP e I&AM (rif. § 4.1.1). Anche i flussi comunicativi, i razionali di ingaggio e di composizione dei team specificatamente coinvolti, sono caratterizzati secondo quanto descritto in occasione dei precedenti servizi in quanto comunque riferiti al contesto di ORM (Organizational Resilient Model), che fa dell'adattività e della resilienza i suoi maggiori punti di forza. In particolare, per ogni Amministrazione verrà istitutito un **Gruppo di Lavoro** nel quale il **Responsabile dei servizi di Firma/Timbro** opererà in coordinamento con il **Responsabile Tecnico,** il **Responsabile Diffusione territoriale dei Servizi** e il **Responsabile del Contratto Esecutivo.**

Il Gruppo di Lavoro opererà inoltre in un contesto metodologico, basato su standard e best practice internazionali che prevede attività di Service/ Operation Management e Quality Assurance, in un'ottica di miglioramento continuo del servizio (Continual Service Improvement). Nella Figura 33 sono dunque sinteticamente riportate le fasi, i processi relativi ad ogni singola fase ed i Core Team che sono coinvolti lungo l'intero ciclo di vita del servizio di Firma e Timbro.

Il modello organizzativo proposto è stato già utilizzato con successo in progetti di Firma Digitale Remota in grandi Amminstrazioni pubbliche.

4.2.1.1 Team e Figure Professionali

I Core Team e le principali figure professionali coinvolte nella gestione e conduzione del servizio di Firma e Timbro sono riassunte nella tabella seguente.

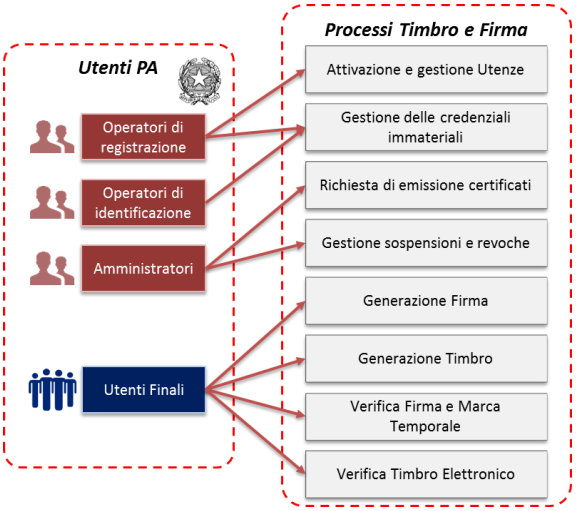
Figura professionale	Figura profess. RTI	Principali compiti/responsabilità
Responsabile Servizio Firma e Timbro	**Resp. Servizio Firma e Timbro**	È responsabile del servizio e si coordina con i referenti della PA e del RTI. E' dotato di certificazione ITIL. E' responsabile della consistenza e dell'adeguatezza sia quantitativa sia qualitativa del team di cui dispone, coinvolgendo il Resource Manager quando necessario.
Responsabile Diffusione territoriale dei Servizi	**Resp. Diffusione territoriale dei Servizi**	Ha il compito di individuare ed organizzare il team con competenze commerciali e tecniche che meglio rappresentano l'iniziativa specifica, all'interno delle strutture territoriali.

Team	Figura profess. del Team RTI	Principali compiti/responsabilità

Service Transition	**Transition Manager**	Supporta la fase di roll out del servizio e fornisce alle amministrazioni tutte le informazioni necessarie per la stima e la realizzazione delle integrazioni applicative e la migrazione delle utenze per scopi di pre-popolamento.
SPECIALISTI DI TEMATICA	**Analisti**	Supportano le amministrazioni nella verifica del corretto utilizzo degli strumenti e supportano le amministrazioni per questioni normative o tecniche riguardanti la Firma o il timbro.
ICT OPERATION e SERVICE OPERATION	**Rif. Centro Servizi**	Partecipano alle fasi di acquisizione, configurazione e utilizzo gestendo le infrastrutture da cui il servizio viene erogato
HELP DESK	**Team di Operatori**	Primo punto di contatto per l'Amministrazione per l'avvio delle attività di Acquisizione del servizio. Supporta inoltre i referenti delle Amministrazioni nelle attività di risoluzione di eventuali problematiche di utilizzo del servizio

Nel seguito del paragrafo verranno dettagliati i servizi di Firma Digitale Remota e Timbro Elettronico, descrivendo nello specifico le macro fasi di Acquisizione, Configurazione e Gestione e dei relativi processi, secondo quanto indicato nella figura a fianco e fornendo evidenza delle modalità operative, dei team coinvolti e degli strumenti a supporto degli utenti.

Gli utenti potranno usufruire dei servizi di Firma Digitale e Timbro sia in modo **semplice ed immediato** attraverso il **Portale di Firma Digitale e Timbro della PA,** che sarà reso disponibile dal Fornitore, sia richiamando direttamente il servizio **dall'interno dei sistemi** delle Amministrazioni grazie alla semplice **integrabilità** della soluzione proposta.



Nella descrizione sono utilizzati i **Tag** al fine di evidenziare gli aspetti più rilevanti della soluzione proposta di seguito proposti.

Adeguatezza	AD	Efficacia	EC	Facilità d'uso	FU	Innovatività	IN	Modularità	MO

ACQUISIZIONE

La fase di acquisizione si svolge come descritto nel § 3.2.3.1.

Le Amministrazioni potranno definire, con il supporto di figure specializzate del fornitore (Responsabile Tecnico, Responsabile dei Servizi di Firma e Timbro, Responsabile Diffusione territoriale dei Servizi), il Piano dei Fabbisogni e il Progetto dei Fabbisogni avviando così la fase di attivazione della soluzione. Grazie all'estrema facilità di installazione e configurazione delle componenti architetturali (non è richiesta installazione di prodotti e/o soluzioni sulle postazioni utente), l'Amministrazione potrà disporre in tempi brevi servizi del servizio. In questa fase saranno eseguite le seguenti attività:

- in accordo con l'Amministrazione e con, la flessibilità consentita dalle diverse modalità offerte dal RTI, sarà scelto il **metodo di autenticazione forte** con il quale gli utenti accederanno al servizio (nel caso di acquisizione del solo servizio di Timbro l'uso di un dispositivo di autenticazione forte è a discrezione dell'Amministrazione non essendo normativamente richiesto)
- saranno illustrate all'Amministrazione le modalità con le quali è possibile utilizzare un servizio di Firma e Timbro **integrato a livello applicativo**; il servizio potrà quindi essere direttamente configurato ed attivato dall'Amministrazione interessata
- sarà valutata la necessità di fornire agli utenti finali, oltre al portale web, applicazioni client di firma e timbro per dispositivi **fissi** o **mobili**; l'installazione di tali applicazioni sulle postazioni di lavoro degli utenti sarà a cura dell'Amministrazione, con il supporto del RTI ed offre il vantaggio di limitare l'uso di banda da parte del servizio in quanto viene evitato il trasferimento al Centro Servizi del documento

CONFIGURAZIONE

La fase di Configurazione si svolge come descritto nel § 3.2.3.2 e prevede le seguenti attività:

- instaurazione di collegamenti sicuri tra Amministrazione e Centro Servizi via INFRANET o Internet
- istituzione dei Centri di Registrazione Locale (CDRL) presso le Amministrazioni e nomina di dipendenti delle stesse quali Operatori Di Riconoscimento (ODR), Identificazione (ODI) ed amministratori

- erogazione di training specifico per l'utilizzo del Portale di Firma Digitale e Timbro a favore del personale dell'Amministrazione (utenti finali, incaricati di registrazione/identificazione, amministratori). Le sessioni di formazione potranno essere erogate in modalità e-learning (con conseguente consegna di questionario di feedback) o in aula da parte del RTI offrendo massima flessibilità temporale e di copertura del territorio
- esecuzione delle attività di Collaudo
- consegna alle Amministrazioni della documentazione relativa alle **procedure di Identificazione** degli utenti, di **attivazione** delle Credenziali e di **utilizzo** del servizio. Per facilitare il reperimento della documentazione, questa sarà resa disponibile anche sul Portale di Firma Digitale e Timbro.

Per permettere all'Amministrazione di accelerare il processo di adozione del servizio, il Fornitore darà supporto in eventuali attività di **prepopolamento** delle utenze.

Ad avvenuta abilitazione dell'Amministrazione ad operare sul sistema, questa **sarà totalmente autonoma** nello svolgimento di tutte le operazioni di attivazione, configurazione e gestione del servizio di firma digitale e timbro tramite il Portale dedicato. In particolare gli ODR potranno:

- rilasciare ed attivare i certificati di firma remota in completa autonomia
- eseguire facilmente tutte le operazioni di gestione delle utenze e di attribuzione agli utenti dei **dispositivi di autenticazione** forte (es. token OTP).

Il Fornitore approvvigionerà ciascuna Amministrazione del quantitativo e tipologia di dispositivi OTP necessari, secondo piani di approvvigionamento concordati.

UTILIZZO/GESTIONE

Ad avvenuto collaudo, l'Amministrazione usufruirà del servizio di Firma Digitale Remota e Timbro elettronico attraverso il Portale.

Attraverso il **Portale di Firma Digitale e Timbro della PA**, gli utenti finali avranno a disposizione tutte le funzionalità previste dal Capitolato. Le principali sono di seguito elencate:

- **Attivazione** della propria **utenza** di firma remota
- **Attivazione** della propria **utenza** per le operazioni di timbro
- **Modifica** della **password** e dati anagrafici, ri-sincronizzazione del token OTP, recupero username/password.
- **Generazione** e **gestione** delle richieste di emissione dei certificati di firma digitale
- **Sottomissione** e **gestione** revoche e sospensioni dei certificati di firma digitale remota
- **Apposizione** di Firma o Timbro Elettronico
- **Verifica** di Firma, Marcatura Temporale o Timbro.

Il RTI fornirà il monitoraggio della piattaforma di erogazione, il supporto specialistico e l'**Help Desk** per tutta la durata del servizio come definito nel § 3.4

IL PORTALE DI FIRMA DIGITALE E TIMBRO DELLA PA

Il "**Portale di Firma Digitale e Timbro della PA**"(FU), consente agli utenti delle Amministrazioni di *richiedere i servizi in modo semplice ed immediato*, senza bisogno di installare SW specifici sulle postazioni di lavoro o nei data center delle PA. Le operazioni di generazione firma, timbro, verifica firma e timbro potranno dunque essere svolte interamente "on-line", attraverso il portale. L'approccio **innovativo** di utilizzo dei servizi via Web (IN) permetterà agli utenti delle Amministrazioni di firmare e timbrare documenti tramite un browser senza dover installare nulla sulle loro postazioni di lavoro .

Essendo il Portale riservato alle PA, *gli utenti dovranno autenticarsi* inserendo le proprie credenziali (user e password - vedi figura a fianco). L'uso di credenziali di autenticazione forte è necessario solo per le operazioni di inserimento della firma digitale e, se richiesto dalla Amministrazione, per il timbro dei documenti (AD). Altre aree e funzionalità del Portale saranno ad accesso libero, per es. l'area informativa nella quale saranno pubblicate le norme di legge rilevanti, eventuali manuali, news, ecc.

Vi sarà inoltre un accesso al Portale

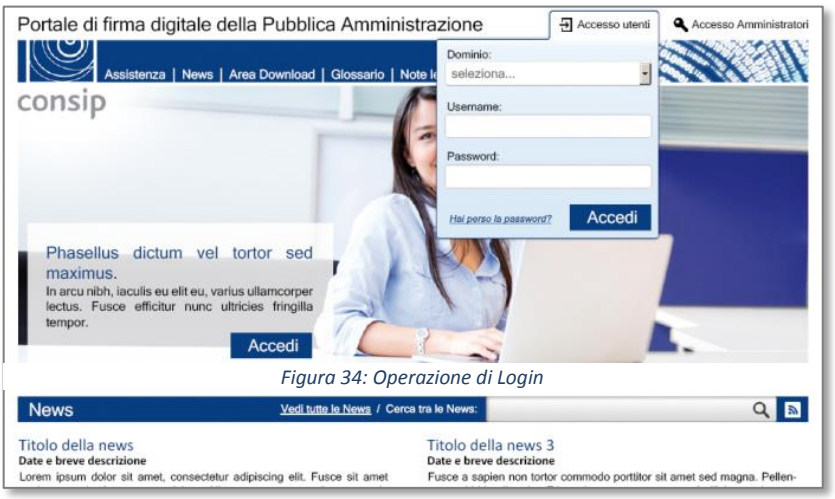


Figura 34: Operazione di Login

riservato agli "**amministratori**" delle varie Amministrazioni.
Il Portale è conforme alle normative vigenti relative alla comunicazione verso il pubblico e rispetta le Linee guida per i siti web della PA, 2011, dal CAD (D.lgs 7 marzo 2005, n. 82 art. 52. art.53 comma 1, art. 54, art.55, art.56, art.57 e relative integrazioni d.lgs 30 dicembre 2010, n. 235, e d.l 13 agosto 2011, n. 138). Inoltre risponde a standard di usabilità (ISO 9241-11:1998, ISO/IEC 9126-4, ISO 20282-2) e a norme di accessibilità (Legge 9 gennaio 2004; Decreto del Presidente della Repubblica, 1 marzo 2005, n. 75; Decreto Ministeriale 8 luglio 2005).
Si riporta di seguito il dettaglio delle funzionalità erogate dal "Portale di Firma Digitale e Timbro".

Generazione della firma digitale e del timbro elettronico

Con un interfaccia intuitiva (EC, FU) gli utenti delle Amministrazioni potranno generare la firma digitale o il timbro elettronico su qualsiasi documento in modo estremamente efficiente e semplice previa autenticazione. Gli utenti potranno effettuare il caricamento del documento sul Portale tramite inserimento guidato o con una semplice operazione di Drag&Drop (FU) e ottenere immediatamente il documento firmato digitalmente (scaricabile, e rinominabile).

Verifica della firma digitale e marcatura temporale

Gli utenti delle Amministrazioni potranno eseguire la verifica di Firma Digitale e Marcatura Temporale di un qualsiasi documento, in modo semplice ed efficiente, caricando il documento sul Portale con una procedura analoga a quella usata per l'operazione di firma (EC, FU).
La funzionalità di verifica include, se consentito dal formato la possibilità di scaricare sul proprio PC il documento nella sua forma "originale" (non firmata).

Verifica del timbro elettronico e della conformità del documento stampato rispetto all'originale informatico

Gli utenti delle Amministrazioni potranno verificare il timbro di un documento digitale (tipicamente in formato PDF) o di uno in formato cartaceo. Nel secondo caso sarà necessaria una scansione a toni di grigio ad almeno a 600 dpi e la generazione di un PDF/TIFF/PNG/ecc.
Per la verifica del timbro, l'utente effettua il caricamento del documento sul portale. La soluzione verifica se è presente il timbro elettronico e la firma digitale presente nei codici bidimensionali (glifi). Procede quindi con la verifica della corrispondenza tra documento visualizzabile dall'utente (potenzialmente falsificabile) e quello contenuto nei glifi o nel repository della soluzione evidenziandone eventuali differenze.

INTEGRABILITÀ DEI SISTEMI ESTERNI

- Le PA potranno **integrare i propri applicativi** (IN) col sistema di firma remota e di timbro attraverso l'invocazione di semplici e ben documentati **Web Services (WS) in standard SOAP** (partendo dal WSDL è infatti possibile realizzare una chiamata di firma remota in brevissimo tempo, con qualsiasi ambiente di sviluppo WS-aware come Visual Studio, Eclipse, ecc.). Il RTI metterà a disposizione parti di codice "**plug & play**" utilizzabili in maniera rapida ed efficace da parte delle Amministrazioni, all'interno delle loro applicazioni (FU).
- È inoltre possibile utilizzare interfacce di firma installate su dispositivi mobili per le operazioni di firma e avvio di batch di firma massiva.

4.2.2 Soluzione tecnologica dei servizi di Firma e Timbro

Di seguito viene descritta la soluzione Tecnologica a Supporto dei servizi di Firma e Timbro.
Nella descrizione sono utilizzati i **Tag** introdotti nella sezione Glossario, al fine di evidenziare gli aspetti più rilevanti della soluzione proposta.
Il servizio di Firma Digitale remota e Timbro soddisfa tutti i requisiti del capitolato (AD) e in particolare supporta:

- la generazione di Firma digitale remota e massiva / automatica in tutti formati previsti dalla normativa, **CAdES-BES** anche **"detached"**, **PAdES-Basic** e **PAdES-BES** e **XAdES-BES "enveloping"**, **"enveloped" e "detached"**; è compatibile con i principali formati di documenti, tra cui quelli richiesti da Capitolato (rif. 1.2.1 Cap. Tec.);
- la generazione di firme multiple sullo stesso documento (parallele o controfirme);
- la **verifica di documenti firmati** in tutti i formati previsti dalla normativa, inclusa la verifica delle eventuali marche temporali associate alle firme, con possibilità di specificare la data-ora di riferimento (c.d. "**verifica alla data**") eventualmente desunta dalla marca temporale, ove presente.

Per tutti i tipi di firma digitale sopra elencati, è possibile inoltre ottenere una "**firma verificata**" ai sensi della Determinazione Commissariale n. 63/2014 dell'AgID.
Nel caso della firma **PAdES** (per documenti PDF), è supportata la versione "invisibile" oppure "visibile".
Per la firma visibile, è supportata la completa **parametrizzazione** (configurabilità) dell'aspetto grafico della firma.

4.2.3 Architettura tecnologica

La soluzione si basa sulle tecnologie **Aruba PEC** per la Firma e **Land** per il Timbro, disponibili in modalità integrata. Tali soluzioni sono utilizzate con successo all'interno di numerose Amministrazioni.
Essa è costituita dei seguenti layer architetturali:

Front End – costituito dal SW applicativo del Portale di Firma remota e Timbro e dalle librerie dei servizi, oltre che dalle interfacce WS per l'eventuale integrazione con gli applicativi delle Amministrazioni.

Back End, che comprende gli HSM (apparato crittografico hardware a norma di legge), il Sistema di Strong Authentication, il sistema di gestione dei certificati, sistemi di Monitor e Backup (che consentono il monitoraggio del sistema ed implementano funzioni necessarie a garantire l'alta disponibilità del servizio).

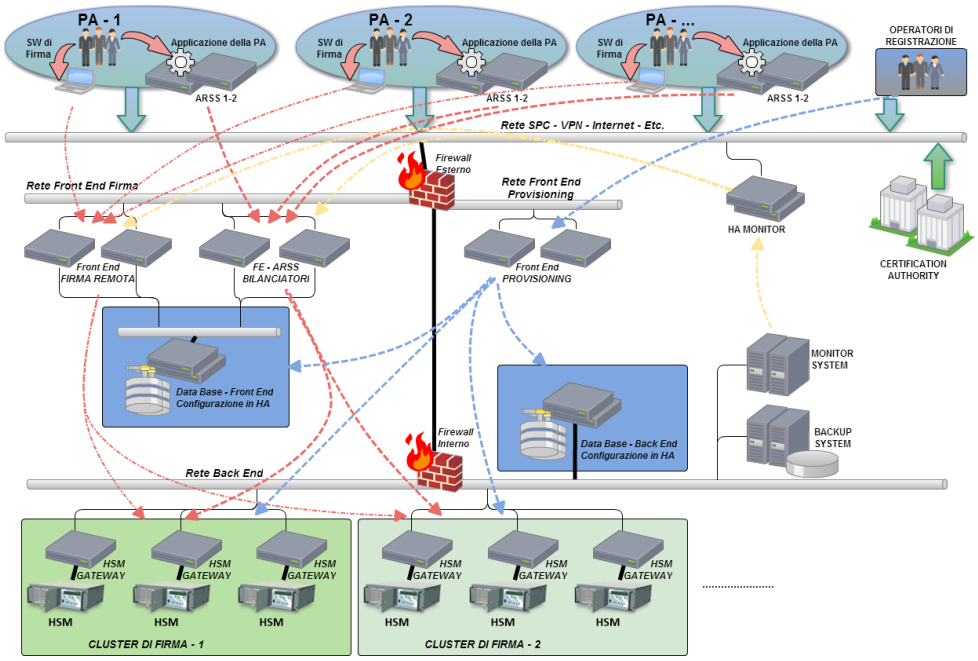


Figura 35: Architettura Sistema di Firma e Timbro

La Disponibilità Operativa

I sistemi di Back End sono raggruppati in "**Cluster Applicativi**" (MQ). Ogni Cluster Applicativo è composto da almeno due catene costituite da un HSM **CoSign** ed un server con le funzioni di Back End e Gateway (Front End facing). In collegamento con le Identità Digitali per cui vengono richiesti sono generati Certificati Digitali all'interno di tutti i dispositivi HSM per Cluster, così da ovviare nel caso di indisponibilità di alcuni. Sistemi di controllo e di ripristino garantiscono il ripopolamento di un HSM in caso di rottura e/o sostituzione di uno dei componenti di sicurezza all'interno di uno stesso Cluster. Le chiavi private non vengono mai duplicate o esportate dall'HSM, ma un fermo di un Cluster non ha alcun effetto sul sistema, se non sulle operazioni in atto al momento del blocco dell'apparato, poiché gli altri Cluster dispongono comunque di Certificati riferiti a tutte le Identità interessate, garantendo di fatto l'**Alta Affidabilità**.
Il servizio richiede l'instaurazione di una connessione sicura fra il sito dell'Amministrazione e i Centri Servizi. La connessione sarà instaurata sulle reti sia INFRANET sia Internet per disporre di una ridondanza in caso di indisponibilità di una delle due.

L'Efficienza

Le funzionalità di timbro sono erogate con **efficienza**, in quanto le operazioni di firma e timbro effettuate dagli utenti tramite Portale hanno la priorità rispetto a quelle applicative, in modo che l'utente finale non percepisca il carico del sistema, anche in presenza di batch di firma massiva in corso.
Il sistema offre **scalabilità** e **modularità**, in quanto i Cluster Applicativi possono essere aumentati su necessità, garantendo di fatto il supporto ad un numero illimitato di utenti.

Autenticazione Forte degli Utenti

L'accesso al Portale da parte dell'utente è controllato mediante un meccanismo di autenticazione a due fattori.
Il servizio prevede la fornitura di un **dispositivo OTP** classico a Display LCD.

Meccanismi alternativi che possono essere resi disponibili sono:

- una **Mobile app** (per gli utenti delle amministrazioni che hanno in dotazione smartphone o tablet aziendali) (IN, FU),
- un servizio di **Callback telefonico** al cellulare dell'utente (in questo caso la OTP è rappresentata dalle ultime 4 cifre XXXX del n. chiamante) (IN)
- un soluzione tipo **Battlecard** basata su una "grid card" del tipo comunemente usato in ambito bancario.

Formati di Timbro

Il servizio di Timbro elettronico proposto dal RTI è basato sulla soluzione SecurePaper™ che mette a disposizione entrambe le tipologie di Timbro Elettronico disponibili sul mercato: "AutoContenuta" e "Copia Conforme".

Aspetti di sicurezza

Il sistema di firma remota supporta chiavi di lunghezza di 1024 bit e 2048 bit. N*ell'ambito della fornitura proposta le chiavi di firma degli utenti avranno sempre una lunghezza di **2048 bit*** come richiesto dalla certificazione dello HSM.
L'accesso al Portale di Firma digitale e Timbro della PA avverrà su canale sicuro SSL/TLS (quindi su HTTPS), con server authentication e cifratura della sessione con chiavi di lunghezza ≥ 128 bit.
Sul Portale e nei sistemi di Back End, sarà assicurata la segregazione logica dei dati delle diverse PA grazie alla qualifica del parametro "dominio" univoco per le utenze del portale.
Gli HSM utilizzati dal sistema di firma remota sono il modello **CoSign 7.1** della **ARX**.
Tutte le operazioni critiche dal punto di vista della sicurezza (generazione delle chiavi, utilizzo delle chiavi private per la generazione delle firme, conservazione e confidenzialità delle chiavi private) avvengono esclusivamente all'interno degli apparati **CoSign,** la cui operatività è protetta da numerose funzioni di sicurezza a livello sia hardware (es. anti-tampering) che software.
L'apparato CoSign ha ottenuto dall'**OCSI** (EC, IN) (Organismo di Certificazione della Sicurezza Informatica) la **certificazione CC EAL4+** richiesta dalla normativa vigente (cfr. http://www.ocsi.isticom.it/index.php/elenchi-certificazioni/prodotti-certificati) oltre che, sempre in OCSI, ha **concluso con successo la Procedura di Accertamento** di Conformità di un Dispositivo per la creazione di Firme Elettroniche ai Requisiti di Sicurezza previsti dall'Allegato III della Direttiva 1999/93/CE (cfr. http://www.ocsi.isticom.it/index.php/dispositivi-di-firma/dispositivi-accertati).

4.3 Soluzione per l'erogazione di Servizi di Sicurezza

I servizi di sicurezza erogati dal RTI supporteranno le Amministrazioni nella prevenzione e gestione degli incidenti informatici e nell'analisi delle vulnerabilità delle componenti hardware e software dei sistemi informativi.
L'insieme dei servizi erogati in modalità "as a service" ed "on premise" possono essere raggruppati nelle seguenti tre macro categorie:

- **Gestione delle Vulnerabilità**: include i servizi di "Static Application Security Testing", "Dynamic Application Security Testing", "Mobile Application Security Testing" e dai servizi di "Vulnerability Assessment", volti alla rilevazione delle eventuali vulnerabilità delle applicazioni tramite analisi, eliminazione di falsi positivi, classificazione e reporting. Tali servizi sono erogati centralmente dal RTI e sono fruibili attraverso il "**Portale dei Servizi di Sicurezza**"; per il caso in cui siano presenti componenti HW e SW installati presso l'Amministrazione si faccia riferimento ai "Servizi Professionali in modalità *on premise*".

In generale i servizi relativi alla "Gestione delle Vulnerabilità", sono realizzati all'interno del Ciclo di Vita di Sviluppo delle Applicazioni (SDLC) delle Amministrazioni. Tali servizi, si possono collocare in due momenti temporalmente distinti:

- prima del rilascio delle applicazioni in produzione;
- periodicamente, per verifica del livello di sicurezza delle applicazioni in produzione;

L'esito delle verifiche di analisi e scansione delle vulnerabilità , le "remediation" definite e l'ampia collezione di best practice di settore, continuamente aggiornata a disposizione del RTI, costituiscono una vera base dati incrementale in grado di apportare valore all'intero SDLC.

- **Protezione** delle infrastrutture e dei sistemi: include i servizi di "Data Base Security", "Data Leak/Loss Prevention", "Web Application/Next Generation Firewall Management" e "Secure Web Gateway", finalizzati alla rilevazione di anomalie, minacce ed attacchi alle infrastrutture ed ai sistemi delle Amministrazioni. Tali servizi sono fruibili attraverso il "**Portale dei Servizi di Sicurezza**". In funzione del contesto specifico e delle necessità dell'Amministrazione, è prevista la possibilità di installare componenti "on premise" presso l'Amministrazione o in modalità centralizzata all'interno del Centro Servizi.
- Servizi **Professionali:** saranno erogati dal RTI in modalità "on premise" utilizzando strumenti HW/SW presenti all'interno dell'Amministrazione.

Strumenti a supporto

I seguenti strumenti di Gestione del Servizio sono a supporto di tutte le attività, permettendo la tracciatura e le notifiche necessarie di tutti gli eventi rilevanti durante tutte le fasi del ciclo di vita del servizio:

- **Portale di governo della fornitura** descritto nel paragrafo § 5.2.4.1;
- **Portale dei Servizi di Sicurezza** che espone le interfacce di Help Desk, Trouble Ticketing e Reporting, descritte nel paragrafo § 3.4;
- Strumenti di **Service Management**, descritti nel paragrafo § 3.3, e cioè, Monitoraggio, Asset Management, Configuration Management, Service Desk, Backup.

4.3.1 Referenze

Le referenze di seguito riportate sono quelle maggiormente significative rispetto alle specificità delle attività di cui al paragrafo. Oltre ai servizi più rilevanti di sicurezza gestita, Selex ES ha realizzato progetti di implementazione di infrastrutture di sicurezza per la NATO (NCIRC) e le forze armate (Esercito, Marina), oltre al centro di comando e controllo interforze del ministero della difesa.

Tabella 14: Referenze Servizi di Sicurezza

Cliente	Progetto e Descrizione
INPS	Presidi di sicurezza a supporto delle ULS
ENAV	Sistema di Sicurezza Integrato e Security Operation Center
Pres. Cons Ministri	Sistema di monitoraggio NIDS e Security Operation Center per l'evento G8.
Corte Dei Conti	Servizi di Sicurezza Gestita
S-RIPA	Security Operation Center della rete Internazionale S-RIPA
Ministero Difesa	Event&Log Management per il SOC C4D

4.3.2 Soluzione Organizzativa

L'organizzazione dei servizi di sicurezza è strutturata per garantire il massimo livello di efficienza nell'erogazione, e facilitando la comunicazione e quindi lo scambio di informazioni tra l'Amministrazione e il RTI, anche mediante strumenti informatici a supporto. Nella Figura 36 sono illustrati i processi relativi ai servizi di sicurezza (inclusi i team coinvolti per l'erogazione), con riferimento alle tre macro categorie ed alle relative fasi di Acquisizione, Configurazione ed Utilizzo/Gestione.

La soluzione organizzativa, incluse le componenti operative dei processi è frutto dell'applicazione di metodologie basate su standard e best practice internazionali, valorizzando le componenti di Service Management, Operation Management e Quality Assurance in un'ottica di miglioramento continuo del servizio attraverso il Continual Service Improvement.

Le metodologie applicate sono descritte all'interno del paragrafo §3.2.3.5. in particolare per la gestione delle vulnerabilità sono utilizzate da parte delle aziende del RTI le metodologie **OWASP** e **OSSTMM**.

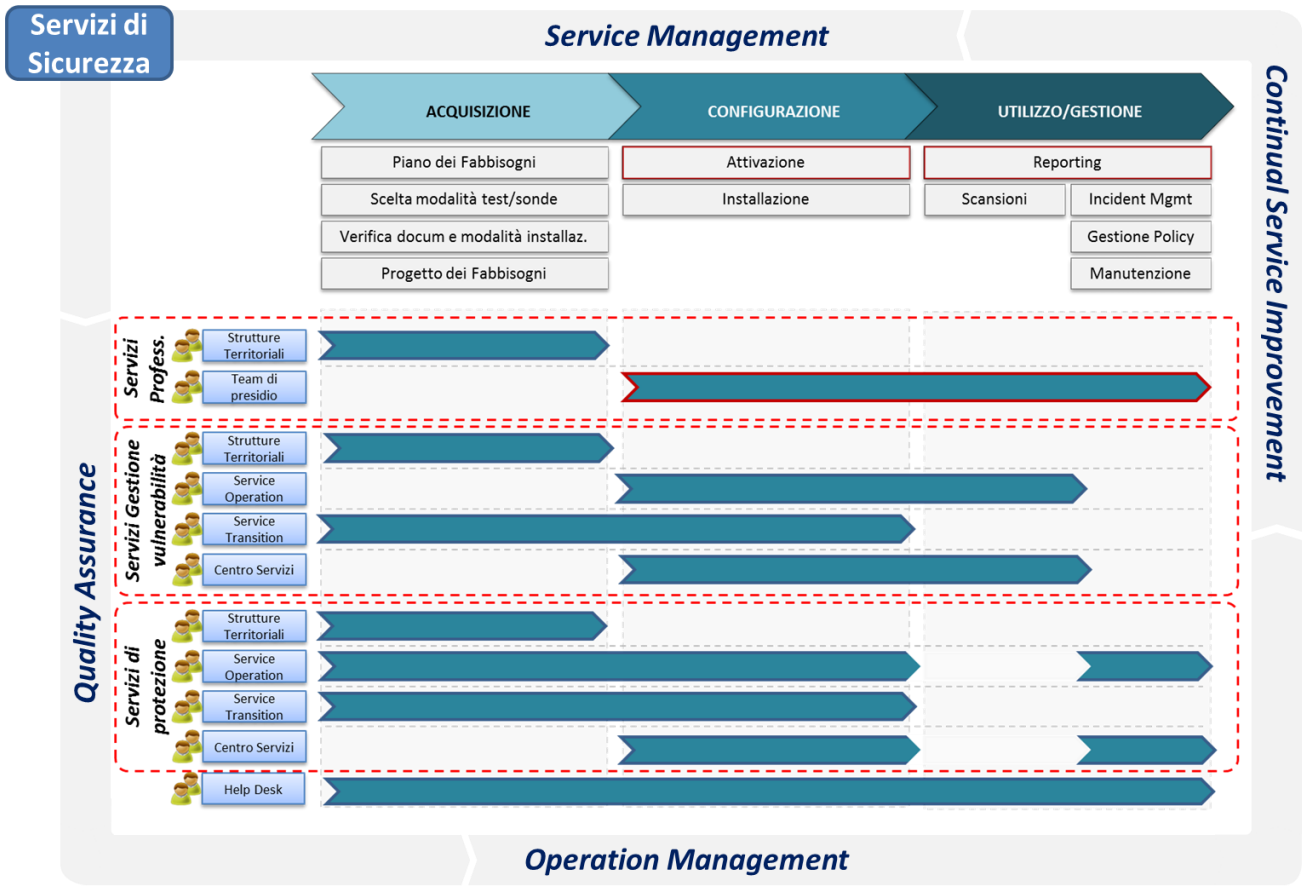


Figura 36: modello organizzativo Servizi di Sicurezza

Il modello organizzativo per l'erogazione dei servizi è descritto nelle sue linee generali nel paragrafo § 3.2.2.2 e prevede l'impiego di Team di lavoro, come sintetizzato nella seguente tabella:

Figura professionale	Figura profess. RTI	Principali compiti/responsabilità
Responsabile Diffusione territoriale dei Servizi	**Resp. Diffusione territoriale dei Servizi**	Ha il compito di individuare ed organizzare il team con competenze commerciali e tecniche che meglio rappresentano l'iniziativa specifica, all'interno delle strutture territoriali.

TEAM	Figura profess. RTI	Principali compiti/responsabilità
Strutture Territoriali	**Responsabile Diffusione territoriale dei Servizi**	Supportano la redazione del piano dei fabbisogni e del progetto dei fabbisogni in accordo con i referenti delle Amministrazioni.
ICT OPERATION	**Rif. Centro Servizi**	Conduzione dell'infrastruttura tecnologica del Centro Servizi
SERVICE TRANSITION	**Spec. di Change Management**	Esperto di metodologie e soluzioni tecnologiche per quanto concerne le tematiche legate alla portabilità ed interoperabilità
	Resp. Progettazione	Responsabile delle fasi di attivazione ed installazione delle componenti che andranno installate presso le Amministrazioni
	Capacity Manager	Responsabile della produzione e dell'aggiornamento del capacity plan, che include la domanda di servizi attuale e la previsione dei bisogni futuri in relazione ai servizi erogabili
SUPPORTO LOGISTICO	**Responsabile Logistica**	Responsabile attività di approvvigionamento e movimentazione materiali e scorte
	Addetto	Personale di supporto alle attività logistiche (Logistica, trasporti, capacity planning, gestione scorte e materiali)
SERVICE OPERATION	**Responsabile dei Servizi di Sicurezza**	Nella funzione di Service Operation (§ 3.3.2.1.1) è il responsabile del Servizio (indicato nel § 3.2.2.2) verso l'Amministrazione e svolge attività di coordinamento e supervisione delle azioni eseguite dal personale del Centro Servizi durante la fase di configurazione e gestione. E' responsabile inoltre della consistenza e dell'adeguatezza sia quantitativa sia qualitativa del team di cui dispone, coinvolgendo il Resource Manager qualora necessario.

	Operatore di Sicurezza	Riporta al Responsabile dei Servizio, ha il compito, oltre che di verificare il corretto funzionamento degli apparati di sicurezza, di gestire rapidamente ed efficacemente gli incidenti di sicurezza noti, supportando il personale e le funzioni coinvolte nella realizzazione delle azioni di contrasto da adottare e nelle attività di ripristino degli asset colpiti.
	Analista di Sicurezza	Riporta al Responsabile dei Servizi, analizza gli incidenti provenienti dai dispositivi di sicurezza monitorati, esamina le cause, identifica le azioni di contrasto più opportune. Esamina i rapporti di scansione generati dagli strumenti automatici, effettua analisi di secondo livello allo scopo di ridurre e eliminare i falsi positivi, verifica la sfruttabilità delle vulnerabilità identificate ("vulnerability exploitation"), ricerca, per quanto possibile, la presenza di falsi negativi.
	Specialista di prodotto /tecnologia	Possiede una profonda conoscenza delle tecnologie e delle problematiche di natura tecnica connesse con la realizzazione dei servizi di sicurezza
HELP DESK	**Responsabile HD**	Coordina il team di Help Desk
	Team Leader	Coordina gruppi di operatori organizzati per skill group
	Operatore	Operatore multicanale

Nel seguito saranno dettagliate le attività svolte durante le fasi di acquisizione, configurazione e utilizzo/gestione per i servizi di Gestione delle Vulnerabilità e per i servizi di Protezione. Vista la natura differente dei servizi professionali, essi saranno trattati in un apposito paragrafo (rif § 4.3.4)

4.3.2.1 Acquisizione

Tale fase, caratterizzata dalle attività di definizione del Piano di Progetto e del Progetto dei Fabbisogni, è descritta nel paragrafo § 3.2.3.1. Le attività previste sono elencate nella matrice RASCI, di seguito esposta, che rappresenta un'estensione della tradizionale matrice RACI, in cui la partecipazione a livello di "Responsabile" viene a sua volta suddivisa in "Responsabile" e "Supporta".

Attività	Responsabile del servizio	Resp. Progettazione	Resp. Diffusione Territoriale	PA
Attività comuni				
Analisi e redazione del Piano dei Fabbisogni	C	C	S	R
Verifica e scelta delle modalità di collegamento tra centro servizi e sito dell'Amministrazione		S	R	I
Servizi di Gestione delle Vulnerabilità				
Raccolta di informazioni sulle Applicazioni			R	S
Verifica della soluzione e redazione del Progetto dei Fabbisogni		R	S	C
Definizione di elenco e modalità dei test di collaudo condivisi con l'Amministrazione	A	R		I
Servizi di Protezione				
Scelta della modalità di installazione delle sonde (centralizzata/on premise)	C	S		R
Definizione delle procedure di escalation per le attività di Gestione degli Incidenti	S			R
Esecuzione Attività di Sopralluogo concordate con l'Amministrazione	A	R		C
Verifica della necessità di Migrazione e Parallelo operativo	I	R		C
Verifica della soluzione e redazione del Progetto dei Fabbisogni	I	R		S

Definizione un elenco accurato dei test di collaudo condivisi con l'Amministrazione	R	S	I

Il RTI supporta l'Amministrazione nella redazione del **Piano dei Fabbisogni** e redige il **Progetto dei Fabbisogni** con le modalità indicate nella matrice precedente.
Per quanto riguarda specificamente il **Servizio di Gestione delle Vulnerabilità**, saranno raccolte le informazioni sul tipo di applicazioni da scansionare e sulle modalità di esecuzione (ad esempio: integrazione con repository, sottomissione di codice o artefatti, servizio continuativo o "one-time").
Per i **Servizi di Protezione** il RTI supporterà l'Amministrazione nella scelta delle modalità di installazione delle componenti ("on premise" o centralizzata presso il Centro Servizi) e nella definizione delle relative procedure di escalation.
Prima dell'attivazione del Servizio, sarà concordata con l'Amministrazione l'attività di sopralluogo per verificare le caratteristiche del sito e la compatibilità tecnologica. L'attività sarà realizzata dalle **Strutture Territoriali** e dal **Responsabile della Progettazione**, coordinati dal **Responsabile della Diffusione Tecnologica**. A valle delle attività di sopralluogo, sarà verificata la necessità di effettuare migrazioni e/o paralleli operativi.

4.3.2.2 Configurazione

Questa fase è descritta nelle sue linee guide generali nel paragrafo § 3.2.3.2
Nella fase di Configurazione, per ottimizzare i tempi di subentro, realizzare l'eventuale parallelo operativo e ridurre al minimo i possibili disagi, il RTI supporterà l'Amministrazione nel reperimento delle informazioni necessarie per la migrazione dei servizi, tra cui, ad esempio: dati di configurazione o altri dati provenienti da eventuali fornitori / terze parti. Fatte salve le attività di sopralluogo, per aumentare l'efficienza e la produttività si utilizzeranno anche metodologie di interazione o collaborazione remota (Es. video o web conferencing).
Il RTI identificherà con i referenti dell'Amministrazione le finestre di intervento per le attività di installazione, anche fuori orario lavorativo, nell'ottica della massima flessibilità.

Fase di CONFIGURAZIONE per i servizi di "Gestione delle Vulnerabilità"
Durante la fase di Configurazione il RTI realizzerà le seguenti attività:

- **Raccolta di Informazioni** - In questa fase il Responsabile Tecnico e il Responsabile del Servizio concordano con il Direttore dei Lavori le modalità di esecuzione delle scansioni; in particolare:
  - l'ambiente su cui effettuare le scansioni (produzione/pre-produzione);
  - il/i target su cui effettuare le scansioni (es.: URL, host o virtual host per test dinamici; IP o hostname per il servizio di Vulnerability Assessment; software baseline in caso di analisi statica di applicazioni con repository sincronizzato o software package in caso di analisi statica di codice sorgente o binario con repository applicativo non sincronizzato);
  - le finestre orarie di scansione entro cui preferibilmente/obbligatoriamente effettuare le scansioni.

Figura 37: Ciclo di Vita dello Sviluppo Software

- **Consegna di best practice** – Il RTI renderà disponibile all'Amministrazione informazioni e documenti (che saranno continuamente aggiornati anche durante la fase di utilizzo / gestione) con l'obiettivo di consentire all'Amministrazione stessa il miglioramento del proprio SDLC. La documentazione è relativa a tematiche specifiche di sicurezza quali a titolo di esempio:
  - la sicurezza delle applicazioni e la realizzazione di un piano di sicurezza dedicato;
  - la sicurezza dei Software di base (Oracle, WebLogic, WebSphere, Tomcat, Apache, JBoss, etc);
  - la configurazione sicura dei dispositivi di rete (Router, Switch, Firewall);

- lo sviluppo sicuro di codice (concetti generali e specifici per i principali linguaggi: ad es. C/C++, PHP, Java, PERL, PL/SQL, Ruby);
- Le best practice saranno facilmente reperibili all'utenza mediante il portale dei Servizi di Sicurezza

La matrice RASCI di seguito descritta evidenzia le attività previste nella fase di configurazione.

Attività	Responsabile del Servizio	Resp Progettazione	Resp. Diffusione Territoriale	PA
Servizi di Gestione delle Vulnerabilità				
Analisi e rilevazione di eventuali vincoli tecnici e/o organizzativi	R	C	C	I
Instaurazione della connettività tra Centri Servizi e Amministrazione	A	R		S
Raccolta di informazioni	R			S
Definizione delle Modalità di integrazione ai repository	I	S		R
Definizione e Consegna Best Practice	R	S		I
Definizione delle regole di ingaggio e manleva	R			C

Fase di CONFIGURAZIONE per i "Servizi di Protezione"

Durante la fase di Configurazione il RTI realizzerà le seguenti attività:

- Definizione delle modalità di installazione delle componenti, che possono consistere in Agent software da installarsi sulle macchine dell'Amministrazione stessa (Server, PDL), sonde o apparati da posizionare presso siti o CED. La scelta della modalità di installazione sarà concordata con l'Amministrazione e basata su criteri condivisi, quali la dimensione e livelli prestazionali delle componenti (Metriche in Fasce 1/2/3/4).
- Definizione del piano dei lavori in accordo con l'Amministrazione, da inserire nel Progetto Esecutivo, a cura del RTI.

La matrice RASCI di seguito descritta evidenzia le attività previste nella fase di configurazione.

Fase	Responsabile del servizio	Resp Progettazione	Resp. Diffusione Territoriale	PA
Servizi di Protezione				
Definizione delle modalità di installazione di componenti (es. Agent, sonde).	S	R		C
Definizione condivisa del Piano lavori	I	R		C
Istallazione delle sonde / appliance / agent		R		C
Attività di parallelo operativo		R		I

Installazione di Appliance

Durante questa fase sarà prestata particolare attenzione alle modalità di installazione delle componenti (Agent/Appliance) presso le Amministrazioni.

L'attività di **Installazione** sarà svolta sulla base delle specifiche tecniche definite nel Progetto dei Fabbisogni. Il RTI dovrà contattare i referenti delle sedi impattate e concordare i modi e i tempi dell'intervento, preceduto da un'attività di sopralluogo, laddove definito necessario. Allo scopo di contenere ad un livello minimo l'impatto dei lavori pianificati, particolare cura sarà posta da parte del RTI alla pianificazione con l'Amministrazione degli intervalli temporali idonei. A ulteriore garanzia delle attività, saranno preventivamente effettuati back-up delle configurazioni attive per consentire eventuali procedure di rollback.

Il RTI verificherà il corretto funzionamento del parallelo operativo (che sarà mantenuto attivo fino alle operazioni di collaudo) e ne darà comunicazione all'Amministrazione.

Le appliance installate saranno tutte conformi agli standard di consumo energetico e interferenze elettromagnetiche, oltrechè a tutte le normative vigenti. Allo scopo di efficientare al massimo i processi di istallazione a beneficio dell'Amministrazione saranno verificati preventivamente tutti i requisiti tecnici e

comunicati alle Amministrazioni i dati tecnico/ambientali per la corretta collocazione delle appliance nei locali delle Amministrazioni, prestando particolare attenzione agli aspetti di impatto ambientale e consumo energetico.

4.3.2.3 Utilizzo/Gestione

Nel seguito saranno dettagliate le attività eseguite durante la fase di Utilizzo/Gestione dei servizi di Sicurezza. L'esposizione di seguito della presente fase viene articolata in due sezioni, una per i Servizi di gestione delle vulnerabilità e una per i servizi di Sicurezza.

Fase di UTILIZZO/GESTIONE per i servizi di gestione delle vulnerabilità

Nella Figura 38 è descritta la modalità operativa di gestione delle vulnerabilità che sarà comune a tutti i servizi compresi nella relativa categoria, riducendo la complessità per l'Amministrazione che si troverà a gestire interfacce e processi comuni. Il Referente individuato dall'Amministrazione potrà effettuare in maniera completamente autonoma, tramite un'interfaccia intuitiva, le richieste di scansione al Centro Servizi, visualizzarne lo stato di avanzamento e ricevere il report nelle modalità concordate.

Il processo, conforme allo standard ITIL, attraverso il "Request fulfillment", offre un modello che si può riassumere nei seguenti passi numerati in figura e ripercorsi nel seguito.

- **Richiesta di scansione** 1 – Il referente dell'Amministrazione (utente) richiede la scansione tramite Portale web, inserendo in appositi form tutte le informazioni richieste (software package o artefatto nel caso di analisi statica o mobile, URL o link nel caso di analisi dinamica o mobile);
- **Ricezione della richiesta** Il Centro Servizi prende in carico la richiesta e registra l'avanzamento 2, sempre disponibile all'utenza ed aggiornato in tempo reale;
- **Conferma** 3 **della schedulazione**: l'utente riceve conferma o notifica di nuova pianificazione;
- **Esecuzione delle scansioni** 4 - all'avvio della scansione l'utente viene avvisato via e-mail ed il relativo stato di completamento viene reso disponibile sul portale in tempo reale;
- **Esecuzione dell'analisi di secondo livello** 5 - terminata la scansione è aggiornato lo stato del ticket e si avvia l'analisi di secondo livello per la verifica delle vulnerabilità riscontrate all'interno del contesto specifico dell'Amministrazione, per ottenere il miglioramento continuo del livello di affidabilità delle analisi. Tale obiettivo è perseguito nel tempo lavorando per cicli successivi attraverso la manutenzione 6 delle liste di esclusione al fine di migliorare l'efficacia del servizio;

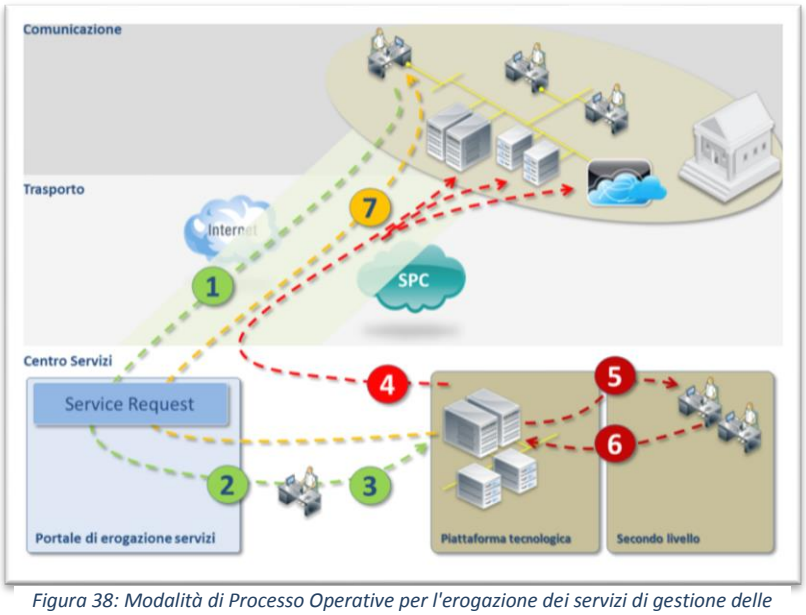


Figura 38: Modalità di Processo Operative per l'erogazione dei servizi di gestione delle Vulnerabilità

- **Produzione della reportistica e consegna dei Rapporti**- In aggiunta a quanto prodotto e reso disponibile al termine delle singole scansioni dei vari servizi, saranno pubblicati 7 e resi disponibili all'Amministrazione i report integrati. A seguito di tale azione si considererà chiusa la richiesta e ne sarà data comunicazione ai referenti dell'Amministrazione attraverso il Portale e via e-mail.

Responsabilità

Nella tabella (RASCI) seguente vengono riepilogate le responsabilità dei singoli ruoli coinvolti nel flusso descritto.

Attivata	Responsabile del servizio	Analista di Sicurezza	Operatore di Sicurezza	PA
Richiesta di scansione	I			R
Ricezione ed Elaborazione	I		R	

Esecuzione delle scansioni		C	R	I
Analisi di II Livello		R		
Consegna rapporti	I	R		I

Fase di UTILIZZO/GESTIONE per i servizi di Protezione

Questa fase è composta principalmente da due tipi di attività: Gestione Operativa e Gestione degli Incidenti. Per garantire l'efficacia del servizio, in ottica di Segregation of Duty, tali attività saranno erogate da due team specializzati, dedicati e separati. Il team di Gestione Operativa si occuperà della gestione dei sistemi tecnologici e della relativa *manutenzione* per garantire la continuità operativa, della *gestione delle policy* per garantire la continua aderenza delle configurazioni alle policy concordate con l'Amministrazione e in ultimo del *reporting*. La visione / richiesta di modifica delle policy potrà essere fatta dall'Amministrazione tramite Portale o Help Desk.
Il team di Gestione Incidenti è descritto in dettaglio nel paragrafo successivo.

Gestione Operativa

Nella tabella (RASCI) seguente sono riepilogate le responsabilità dei ruoli coinvolti nella Gestione Operativa.

Attività	Responsabile del servizio	Analista di Sicurezza	Operatore di Sicurezza	PA
Richiesta di visione/modifica policy			I	R
Modifica/invio delle Policy	I	C	R	I
Manutenzione	I		R	I
Consegna rapporti	I		R	

Gestione Incidenti

Per i Servizi di Protezione il RTI fornirà un servizio di Gestione degli incidenti come richiesto da capitolato. Il servizio sarà erogato con finestre H24x7 dai Centri Servizi del RTI.
Il processo di scambio di informazioni del processo di gestione degli incidenti vedrà coinvolti i seguenti attori:

- **ULS** (Unità Locale di Sicurezza) dell'Amministrazione;
- Team di Gestione Incidenti del Centro Servizi del RTI.

La rilevazione degli incidenti è realizzata dal Centro Servizi utilizzando gli strumenti di gestione e monitoraggio rappresentati dalle Sonde / Appliance installate presso l'Amministrazione e/o quelle centralizzate presso il Centro Servizi. Per migliorare l'efficacia e la completezza del servizio i referenti dell'Amministrazione potranno aprire incidenti di sicurezza tramite Ticket/Help Desk.
Il processo di gestione di un incidente si comporrà delle seguenti fasi:

- **Rilevamento**: attivato dal Centro Servizi a seguito della ricezione di un allarme generato dagli stessi dispositivi di sicurezza o dall'Amministrazione tramite segnalazione all'Help Desk;
- **Classificazione**: il Centro Servizi effettua l'analisi di primo livello con rimozione dei **falsi positivi** e successivo approfondimento per classificare con precisione l'incidente in atto (Triage);
- **Notifica:** l'incidente è notificato dal Centro Servizi all'ULS tramite apertura di un ticket che contiene le informazioni descrittive dell'incidente e indicazione di eventuali azioni di contenimento;
- **Risposta**: è la fase di implementazione delle azioni predefinite nelle procedure di escalation sulla base della classificazione dell'incidente. Nel caso siano previste azioni di contenimento è **responsabilità** del RTI implementare la fase di risposta sui dispositivi da lui gestiti. Nell'eventualità in cui le attività malevole segnalate come incidente di sicurezza abbiano portato alla compromissione di uno o più sistemi dell'Amministrazione, il RTI fornirà tutti i dettagli dell'incidente utili alle operazioni di ripristino;
- **Chiusura**: una volta rimossa la minaccia e ripristinata la situazione, l'incidente ha esaurito il proprio effetto dannoso e viene chiuso dal Centro Servizi. Contestualmente viene notificato il referente dell'Amministrazione e prodotto il rapporto di incidente;

- **Follow-Up:** all'interno del servizio, se richiesto dall'Amministrazione, il RTI fornirà, i dati e i log delle piattaforme da lui gestite al fine di individuare possibili migliorie tecniche ed organizzative (ad esempio per analisi post mortem).

Nella tabella (RASCI) seguente sono riepilogate le responsabilità dei ruoli coinvolti nella Gestione Incidenti.

Attività	Responsabile del servizio	Analista di Sicurezza	Operatore di Sicurezza	PA
Rilevamento			R	
Classificazione		R	C	
Notifica	A	R		I
Risposta (per sistemi gestiti dall'Amministrazione)	I	I		R
Risposta (per sistemi gestiti dal RTI)	I	I	R	I
Chiusura	I	R		I
Follow-Up	I	R		I

A maggior chiarimento della sequenza delle azioni e delle relative correlazioni, la Figura 39 riporta il workflow di gestione incidenti, con l'individuazione delle fasi e degli attori coinvolti.

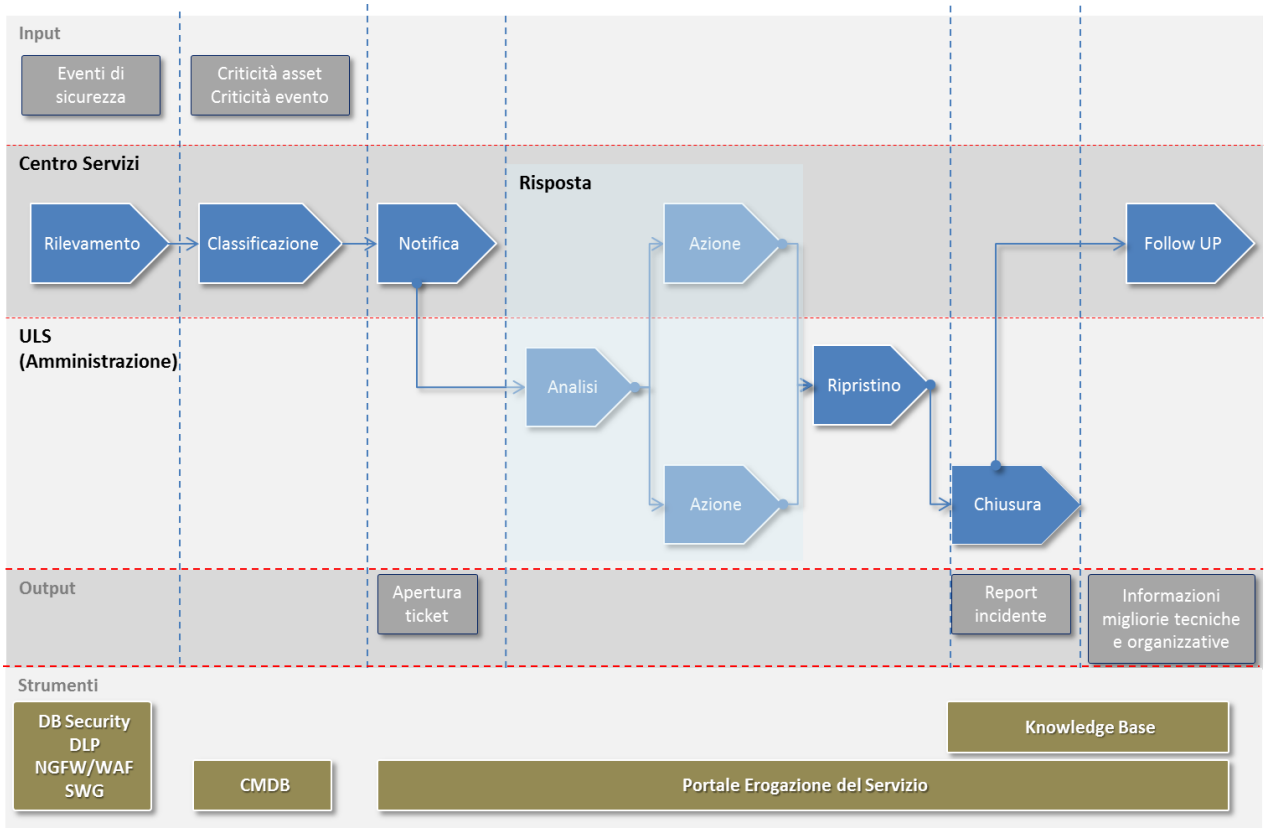


Figura 39: Flusso di gestione incidenti

Per ogni incidente sarà redatto e quindi reso disponibile all'Amministrazione un report di sintesi (**incident report**) in cui saranno indicate le seguenti informazioni: sorgente, tipologia, descrizione, severità dell'evento/allarme; riferimento temporale in cui l'evento si è verificato; azioni intraprese (es. modifiche alle policy) per la risoluzione o mitigazione del problema;
Il livello di allarme (o impatto) di un attacco sarà determinato dal personale del Centro Servizi attraverso un approccio qualitativo sulla base dei seguenti elementi:

- Categoria e livello di gravità della vulnerabilità/minaccia identificata come severità;
- Criticità delle risorse IT coinvolte (se disponibili le informazioni) in termini di valore Asset.

A titolo esemplificativo la Figura 40 riporta un esempio di matrice di correlazione tra i livelli di severità di una vulnerabilità/minaccia, le principali categorie di attacco ed il relativo livello di gravità e la criticità delle risorse IT coinvolte.

SORGENTE ATTACCO				Valore Asset		
Classificazione Risorsa IT Oggetto di Attacco (Riservatezza, Integrità, Disponibilità)				Basso	Medio	Alto
Categoria Attacco	Descrizione	Severità		IMPATTO		
(D)DoS High Volume	La presente categoria include gli allarmi frutto di attacchi intenzionali volti a rallentare l'operatività di un sistema, saturando le risorse fino al collasso del sistema stesso (inibendo la disponibilità dei dati e dei servizi erogati).	percentuale di risorse impegnate	Livello 1	Basso	Medio	Medio
			Livello 2	Basso	Medio	Medio
			Livello 3	Medio	Medio	Alto
IRC Botnet	Indica la presenza su un sistema di un Eggdrop, utilizzato sulle reti ircnet per vari scopi. L'attacco pertanto presuppone una concatenazione di incindenti, ed indica una possibile l'intrusione sul sistema da parte di un attaccante.	diffusione e tipo	Livello 1	Medio	Medio	Medio
			Livello 2	Medio	Alto	Alto
			Livello 3	Alto	Alto	Alto

Figura 40: Matrice di correlazione

4.3.2.4 Reporting

Le attività di reporting sono relative alla produzione e consegna dei report, nei modi concordati con ciascuna Amministrazione. I report conterranno tutte le informazioni previste da Capitolate.
Il reporting prevede:

- Invio di e-mail ai destinatari con indicazione del link al Portale dei servizi (con protocollo cifrato) che consente di scaricare il report (previa autenticazione) o, in alternativa, inviare e-mail cifrata e firmata con report incluso;
- Consegna su un repository di proprietà dell'Amministrazione tramite protocollo cifrato (FTPS/SFTP/HTTPS) e previa autenticazione da parte degli operatori del RTI.

I rapporti oggetto di fornitura saranno conservati in repository documentali che utilizzano robuste tecniche di cifratura conformi allo standard **FIPS 140-2**.
Tali repository sono accessibili solo da terminali in tecnologia VDI e previa autenticazione a due fattori. Per la descrizione delle tecnologie e procedure di sicurezza dei Centri Servizi si rimanda al § 3.3. Non è prevista la conservazione dei report, da parte del RTI, al di fuori dei dispositivi di memorizzazione e archiviazione del Centro Servizi.

4.3.3 Soluzione Tecnologica

Le piattaforme tecnologiche previste per l'erogazione dei servizi ospitate all'interno dei Centri Servizi del RTI ne ereditano le caratteristiche di resilienza, continuità nell'efficienza e disponibilità operativa descritte nel capitolo § 3.3.
Nella descrizione sono utilizzati i **Tag** al fine di evidenziare gli aspetti più rilevanti della soluzione proposta di seguito proposti.

Adeguatezza	AD	Efficacia	EC	Facilità d'uso	FU	Innovatività	IN	Modularità	MO

Per chiarezza, nelle immagini seguenti ci si riferirà con gli acronimi **SAST**, **DAST**, **MAST** e **VA** in luogo di Static, Dynamic, Mobile Application Security Testing e Vulnerability Assessment.
Le piattaforme centrali di gestione sono ridondate a livello fisico e logico e distribuite geograficamente su diversi siti. Gli eventuali apparati dislocati "on premise" presso le Amministrazioni saranno configurati in alta affidabilità; in tal caso, la gestione di tali apparati da parte dei Centri Servizi avverrà tramite collegamento VPN sicuro verso il Data Center / sito locale dell'Amministrazione contraente (AD).

Continuità nell'efficienza (AD)

Il RTI garantirà la continuità nell'efficienza dell'erogazione del servizio, prendendosi carico di tutte le attività che concorrono a mantenere e migliorare l'erogazione e i processi del servizio. In particolare, per garantire il massimo dell'efficienza, il RTI realizzerà attività di:

- Monitoraggio e Gestione dei Guasti: controllo della raggiungibilità di rete e applicativa dei dispositivi e la verifica dei corretti livelli di funzionamento H24x7;
- Manutenzione Preventiva/Straordinaria: per il mantenimento costante del livello di servizio previsto con attività di revisione parziale/totale dei dispositivi;
- Upgrade e Patching/Hotfix: installazione programmata di Upgrade/Patching/Hotfix. Tali attività potranno richiedere anche il Pre Test in ambiente di Test Bed, descritto nel § 3.3;

- Back-up della configurazione e delle Policy: la gestione operativa include il backup, il restore e le operazioni di manutenzione generale dei sistemi di tutti i dispositivi gestiti;
- Revisione periodica delle policy di sicurezza: concordate con l'Amministrazione allo scopo di verificarne l'applicabilità/adattabilità alla mutevolezza del contesto.
- Verifica periodica degli SLA, dei KPI per identificare eventuali debolezze e punti di attenzione in ottica di miglioramento continuo del servizio.

Tali attività, con l'aggiunta di un processo autorizzativo di gestione Policy che prevede la verifica di ogni richiesta di modifica, permettono il mantenimento e il miglioramento costante del livello di servizio richiesto in ottica di efficienza.

Continuità nella disponibilità operativa (AD)

La Disponibilità Operativa è indirizzata attraverso la completa ridondanza sia dei Data Center sia dei collegamenti tra Centro Servizi ed Amministrazione.

In particolare il Centro Servizi, come descritto in §3.3.2.1.3, distribuisce geograficamente le proprie capacità computazionali e infrastrutturali su siti distinti in continuità operativa tra loro (più un sito per DR). I siti sono connessi tra loro da un backbone in fibra ottica ad alte prestazioni.

In particolare, i servizi di Sicurezza sono erogati da Data Center in configurazione di Business Continuity (active-active) e interconnessi in maniera dedicata. L'interconnessione verso l'Amministrazione sarà realizzata in configurazione ridondata utilizzando come collegamento primario la rete Infranet (dove possibile) e, come secondario, la rete Internet.

Questo consente, in caso di indisponibilità di uno dei due canali, di mantenere attiva la connessione tra i due siti. In ogni caso il traffico tra il Centro Servizi e Amministrazione avviene all'interno di VPN sicure e configurate per supportare destinazioni multiple.

In caso di indisponibilità del Data Center primario, sarà automaticamente ripristinato il collegamento VPN con il secondario, senza alcuna interruzione di servizio, mantenendo attive le configurazioni originali.

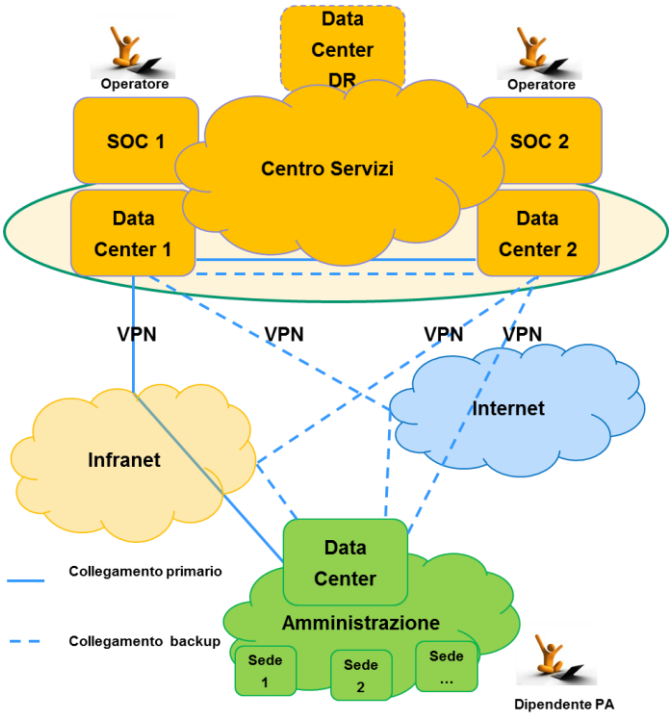


Figura 41: Architettura del Centro Servizi

Inoltre le tecnologie selezionate e l'architettura proposta garantiscono per i Servizi di Protezione (con installazione di appliance on premise):

- **elevati livelli di affidabilità** attraverso l'utilizzo di server con componentistica HW ridondata (alimentazione, dischi, rete).
- **continuità operativa** con l'utilizzo di appliance configurate in alta affidabilità.

Inoltre l'infrastruttura del Centro Servizi viene sottoposta a test periodici (carta e simulazioni) di attivazione del piano di Disaster Recovery, come specificato nel § 3.3.2.1.3, che permette al RTI di mantenere il piano sempre allineato e efficiente, allo scopo di essere pronti per un eventuale necessità.

4.3.3.1 Soluzione tecnologica per i servizi di Gestione delle Vulnerabilità

I servizi di gestione delle Vulnerabilità sono erogati con prodotti della suite IBM Security Appscan, leader nel **Quadrante Magico di Gartner** nell'ambito **della Sicurezza Applicativa** (AST) (vedi Figura 42).La suite copre tutti i requisiti tecnici e funzionali richiesti (AD) ed è conforme alle best practice internazionali e agli standard OWASP (AD) per i servizi di Analisi Statica, Dinamica e Mobile, oltre che per il Vulnerability Assessment, introducendo inoltre aspetti migliorativi.

Al fine di garantire la massima efficacia e scalabilità le componenti SW saranno installate sulla infrastruttura virtuale (EC, IN) del Centro Servizi, descritta nel § 3.3; la virtualizzazione permette l'utilizzo di tecniche di scalabilità e modularità per far fronte all'incremento stimato di richieste di scansione nel corso degli anni (MO). La figura rappresenta l'integrazione funzionale delle varie componenti tecnologiche.

La soluzione integrata:

- permette di classificare gli asset gestiti definendo le priorità in base all'impatto sul business favorendo l'identificazione delle aree a rischio e la gestione del piano di rientro (EC). Inoltre, offre una vista chiara sui gap di conformità rilevati, rispetto alle policy definite anche attingendo ai controlli di standard internazionali già nativamente presenti negli strumenti utilizzati (IBM Appscan), indicando puntualmente la mancata aderenza ai controlli di conformità definiti per le applicazioni analizzate e mostrando i progressi tramite le tendenze e le metriche prestazionali. Sono disponibili in modalità nativa oltre 40 modelli di report di conformità, allineati ai più recenti standard di sicurezza (IN), inclusi PCI Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), ISO 27001 e ISO 27002, HIPAA, Gramm–Leach–Bliley Act (GLBA), Sarbanes-Oxley Act (SOX) e Basel II;

Figura 42: Magic Quadrant Gartner di Sicurezza Applicativa

- sviluppa una metodologia di test innovativa detta IAST (IN) (Interactive Application Security Testing) che combina le due tipologie di analisi statica e dinamica verificando l'ambiente applicativo durante la simulazione di un attacco per fornire risultati di test più accurati che identificano maggiori vulnerabilità e facilitano l'indirizzamento delle attività di remediation.
- effettuare test diversi (analisi statica/dinamica/mobile/VA) sulla stessa applicazione per analizzare diversi aspetti e ottenere risultanze integrate (EC), verificare, una volta individuata una vulnerabilità, la sua effettiva pericolosità attraverso definiti test di "exploit", ovvero di verifica del grado di "sfruttabilità" delle vulnerabilità da parte di un potenziale utente malevolo.

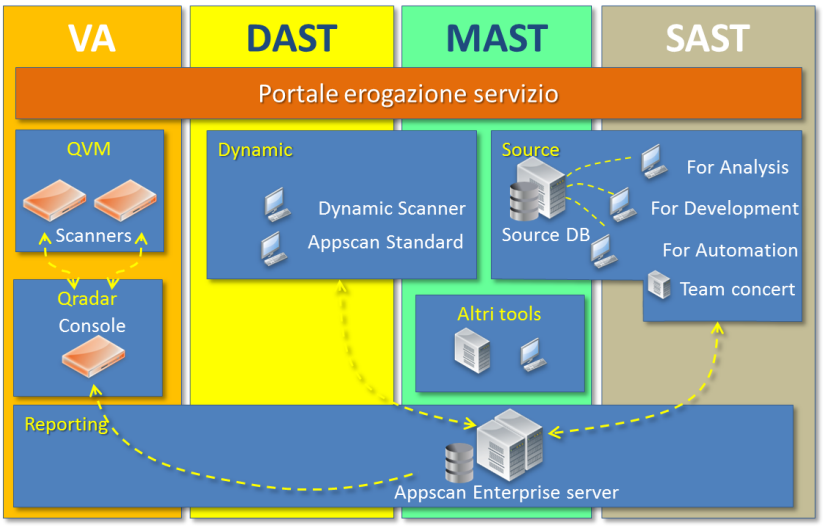


Figura 43: Architettata della Soluzione IBM per la Sicurezza Applicativa

- basa il suo modello di analisi sulle conoscenze che vengono costantemente aggiornate dai laboratori IBM e dal team di ricerca di IBM **X-Force** offrendo informazioni sempre aggiornate in grado di indirizzare efficacemente le contromisure (IN).

Reporting

Per ogni servizio saranno disponibili report di vulnerabilità dedicati ai quali il referente dell'Amministrazione potrà accedere in completa autonomia (AD); inoltre, quale elemento migliorativo della proposta, l'Amministrazione che vorrà dotarsi di più di un servizio riceverà la reportistica integrata (comprensiva di livello di rischio e del piano di rientro) e la gestione centralizzata di tutti i risultati dei test provenienti dalle piattaforme SAST, DAST e MAST e VA (EC, AD). La reportistica evoluta con cruscotti (dashboard) per il reporting di tipo executive, e di dettaglio è integrata per tutti i servizi tramite la componente IBM Security AppScan Enterprise, che si appoggia su un Database Microsoft SQL Server, che consente ulteriori integrazioni con le piattaforme di reportistica più diffuse.
Nel seguito sono indicate, per ogni servizio, le principali caratteristiche tecniche delle relative componenti utilizzate.

Piattaforma tecnologica Static Application Security Testing

La piattaforma effettua test di vulnerabilità del codice sorgente classificando le rilevanze per livello di criticità, identificando le porzioni di codice interessate e indirizzando gli interventi volti alla loro risoluzione.

La componente a supporto è l'"Appscan Source" della suite IBM Security AppScan.

L'architettura è costituita da una componente server database per la storicizzazione locale di tutti i profili di scansione e dei risultati dei test effettuati dalle tre tipologie di client: Appscan Source for Analysis, Source for Development e Source for Automation. Secondo le caratteristiche e le specifiche esigenze della singola Amministrazione, il codice sorgente può essere condiviso (1) tramite il Portale del Centro Servizi oppure caricato su un repository software dell'Amministrazione che potrà essere integrato (2) attraverso la componente di "IBM Rational Team Concert"(AD).

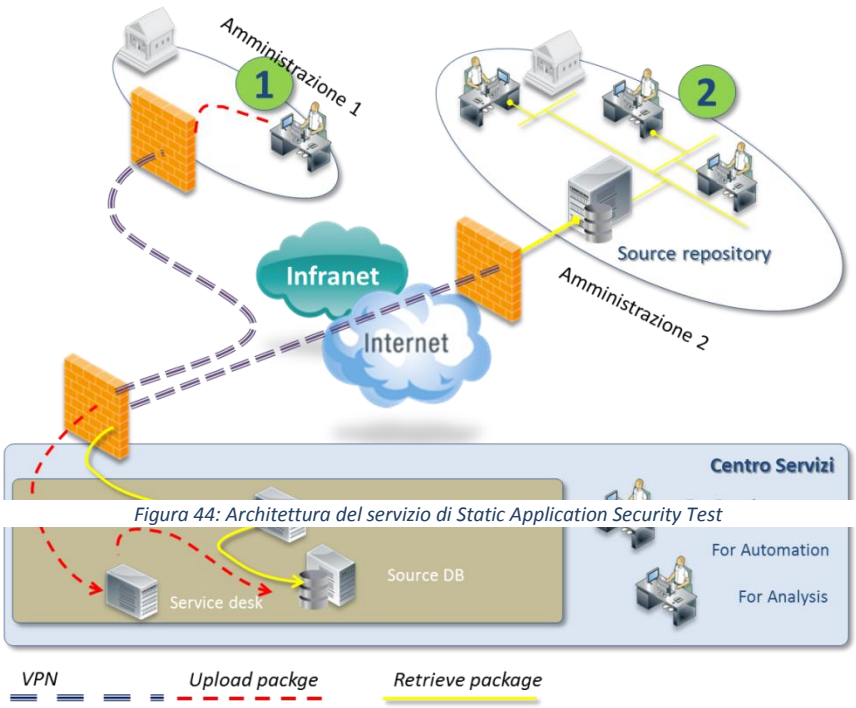


Figura 44: Architettura del servizio di Static Application Security Test

La piattaforma proposta soddisfa tutti i requisiti tecnici e funzionali ed è conforme alle best practice internazionali e agli standard OWASP, eseguendo nelle varie fasi di test controlli come nel seguito riportato a titolo esemplificativo e non esaustivo (AD , EC):

- per la ***"Data Validation"*** è verificata l'esposizione a cross-site scripting, SQL injection, e corruzione di dati applicativi;
- per il ***"Control Flow"*** è verificata la corretta sequenza delle operazioni tramite tracciatura del flusso attraverso l'applicazione, tra moduli e funzioni e visualizza i percorsi di dati potenzialmente pericolosi all'interno di un grafico delle chiamate ed indica le aree in cui l'applicazione potrebbe essere suscettibile a vulnerabilità;
- per la ***"Verifica Semantica"*** è eseguita la rilevazione di problematiche legate all'uso di particolari funzioni, ad esempio viene evidenziato se l'applicazione richiama un metodo dichiarato obsoleto (deprecated);
- per l'analisi delle ***configurazioni*** il prodotto fornisce informazioni sull'uso di elementi esterni, framework o librerie, potenzialmente vulnerabili;
- Per la ***"Buffer Validation"*** vengono verificate le situazioni di buffer overflow che si verificano quando si spostano dati superiori alla capacità del buffer che deve gestirli.

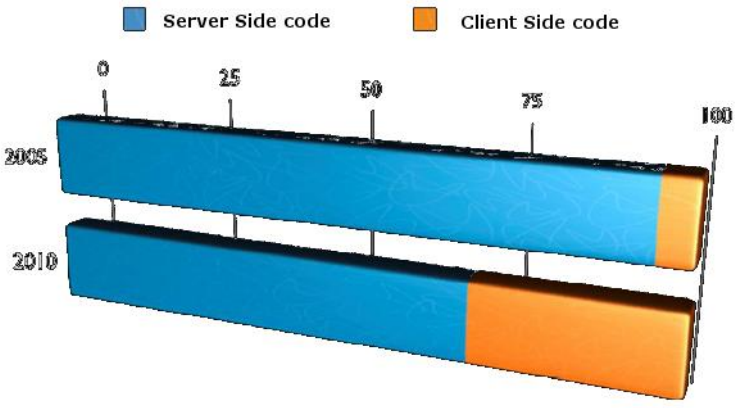


Figura 45: Utilizzo delle tecnologie Client-Side

La piattaforma introduce particolari controlli per i linguaggi utilizzati lato Client, il cui utilizzo è in forte aumento negli ultimi anni (IN). (cfr. Figura 45)

IBM Appscan fornisce la funzionalità di discovery automatica (EC) del codice sorgente e delle sue dipendenze partendo dal folder principale dell'applicazione per costruire un profilo di scansione in modalità semplice e veloce. Inoltre offre la funzionalità di test detta "String Analysis" (IN) che controlla la manipolazione di stringhe nei progetti che utilizzano le più recenti tecnologie come Java e Microsoft .Net, riducendo i falsi positivi. In ambito JavaScript, IBM Appscan permette di effettuare analisi statica nel contesto di una scansione dinamica permettendo una visione concorrente e di maggior completezza (EC) dei rischi correlati.

Piattaforma tecnologica Dynamic Application Security Testing

La piattaforma tecnologica permette l'esecuzione dei test dinamici fornendo anche gli strumenti per l'analisi dei risultati e la verifica delle vulnerabilità tenendo conto dell'esposizione al rischio (AD). Per l'avvio delle attività di scansione l'input è rappresentato dalle informazioni relative ai target da analizzare e le relative modalità attuative che potranno essere comunicate attraverso l'interfaccia offerta dal portale di erogazione del servizio. L'architettura con cui sarà erogato il servizio è basata su IBM Security AppScan Standard.

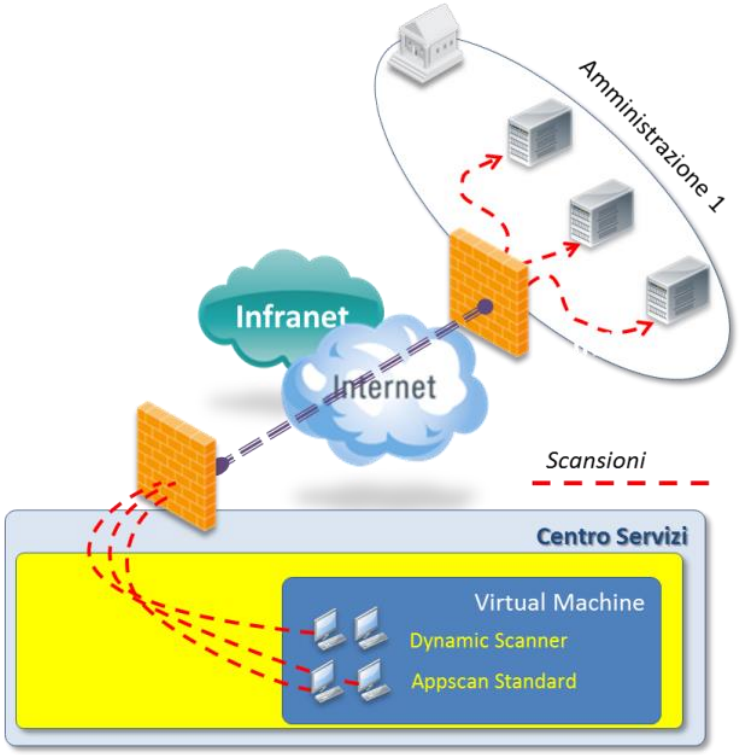


Figura 46: Architettura del servizio di Dynamic Application Security Test

La piattaforma di Analisi Dinamica si integra con la piattaforma di Gestione-Reportistica (EC) per la centralizzazione dei profili di scansione e dei risultati dei test. L'esecuzione delle scansioni è a carico degli agent Appscan Standard e Appscan Dynamic Analysis Scanner, che permettono di effettuare in modalità automatica una serie di test di sicurezza dinamici e automatizzati detti "black box" per le nuove vulnerabilità web, come web service, Web 2.0 (IN) e applicazioni Internet complesse come JavaScript, Ajax e Adobe Flash (IN);

La piattaforma proposta soddisfa tutti i requisiti tecnici e funzionali richiesti da capitolato effettuando tutte le verifiche previste per tutti gli ambiti e le vulnerabilità indicate dal Capitolato Tecnico oltre alle funzioni innovative già prima descritte(AD, EC);

- per la ***Configurazione*** si effettua l'analisi delle pagine web presenti partendo dall'URL base fornito creando una alberatura dell'applicazione;
- per l'***Autenticazione*** viene effettuata una ricerca delle vulnerabilità sulla fase di autenticazione che oltre al controllo sui login e sulla sessione (cifrata) aggiunge la verifica dei meccanismi di sicurezza previsti dall'applicazione come il controllo sulla generazione delle password (lunghezza, complessità, storico, ecc.). Inoltre utilizzando l'utility "Authentication Tester", vengono testati i principali tipi di attacco applicabili: come "brute force", "attacchi a dizionario" utilizzando un dizionario opportunamente creato, ecc.
- per l'***Autorizzazione*** vengono testate applicazioni web alla ricerca di problematiche inerenti la "Privileged Escalation" dove, fornendo le utenze/progetti di scansione per i vari ruoli compreso l'utente non autorizzato (guest), prova ad effettuare attività atte a verificare se sia possibile, per una certa utenza, elevare i privilegi assegnati
- per la ***Validazione dei dati*** la soluzione è in grado di verificare, mediante l'inserimento di opportune stringhe, l'eventuale presenza di vulnerabilità dovute alla mancanza di opportuni controlli di sicurezza. Inoltre i controlli effettuati consentiranno di (AD):
  - verificare i meccanismi di gestione delle sessioni e della loro robustezza
  - analizzare il sistema di gestione degli errori dell'applicazione
  - controllare, laddove applicabile, i meccanismi di crittografia, i meccanismi di logging e il metodo di gestione delle informazioni;
  - verificare le comunicazioni dell'applicativo con soggetti esterni come client, DB, Ldap, ecc..

E' possibile gestire profili di scansioni multiple e differenziate per applicazione, consentendo pertanto di ottimizzare le attività di test differenziando il livello e la tipologia di test cosi da ottenere funzionalità differenziate per ciascuno dei profili **Bronze**, **Silver** e **Gold**.

La soluzione offre diverse funzionalità innovative tra cui:

- la tecnica di test **Glass-box** fornisce un valore aggiunto ai test eseguiti sull'applicazione, in quanto rivela vulnerabilità non evidenziate dai test classici, ovvero la logica nascosta(IN) (link nascosti di entrata all'applicazione, cookies, etc.) ;

- il supporto per web service e service-oriented architecture (SOA), inclusi SOAP e XML (IN) permette personalizzazioni ed ampliamento attraverso IBM Security AppScan eXtensions Framework, che consente di sviluppare e condividere add-on open source;
- esiste un processo di test adattivo che simula in modo intelligente la logica umana (IN) per individuare i test rilevanti (EC);
- sono disponibili strumenti di test manuali, inclusi utility avanzate per i test di sicurezza personalizzati (EC)con gli script Pyscan.

Piattaforma tecnologica di Mobile Analysis

La piattaforma fornisce gli strumenti per l'esecuzione di test mirati alle applicazioni di tipo mobile e permette la rilevazione delle vulnerabilità di sicurezza che possono essere sfruttate da un attaccante per compromettere i dati delle **mobile app**, la logica di business o il framework del dispositivo mobile identificando qualsiasi minaccia che mette a rischio l'applicazione e/o l'infrastruttura.

La piattaforma tecnologica afferisce al servizio di Mobile Analysis Security Testing (MAST) e le tecnologie a supporto sono le suite IBM Security Appscan Source e Appscan Standard, già descritte per le piattaforme di Analisi Statica e Analisi Dinamica, integrate con altre piattaforme verticali che ne estendono le funzionalità nello specifico ambito dell'analisi Mobile. La soluzione supporta i Sistemi Operativi IoS, Android, Windows e Blackberry.

Appscan Mobile esegue un'analisi completa sulle app richieste in quanto copre tre differenti tipologie di test: statico, dinamico ed in emulazione software (EC, IN). In particolare, durante la fase di analisi statica è necessario fornire il codice sorgente dell'app mobile da testare, comprensivo di tutte le eventuali informazioni aggiuntive necessarie per il processo di build. Per la parte inerente l'analisi dinamica è possibile eseguire test specifici sulle "web app" che prevedono l'accesso ad un sito web da un device mobile. In questo caso è necessario fornire come input le informazioni relative a URL da testare, agent da simulare e credenziali di eventuali utenti. Infine, per il test di emulazione, la piattaforma tecnologica utilizza come input l'app stessa (IN); il test consiste nel caricamento della app in un emulatore per effettuare un'analisi definita runtime. Il back-end dell'ecosistema mobile è analizzato ricercando gli specifici URL coinvolti nelle transazioni client-server.

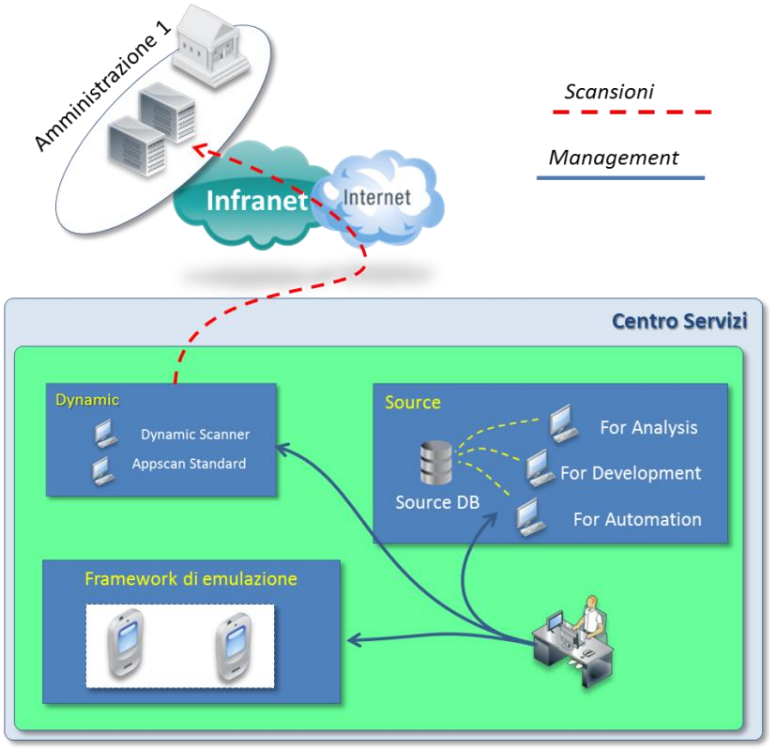


Figura 47: Architettura di Sistema del servizio di Mobile Application Security test

La piattaforma proposta soddisfa tutti i requisiti tecnici e funzionali richiesti da capitolato (AD) comprese le verifiche dei permessi che le mobile App richiedono ai dispositivi, come richieste di **Accesso ad Internet**, ai **contatti/rubrica**, al **telefono**, o altri.

La soluzione opera in conformità alle best practice internazionali e fornisce copertura delle criticità pubblicate nella lista Mobile Top 10 di OWASP. Attraverso il mobile, l'hacker, potenziale utente malevolo, potrebbe accedere ai sistemi legacy, ai siti web aziendali o accedere ai dati di localizzazione. Al fine di assicurare un'analisi completa, i test sono diversificati e mirano a rilevare le configurazioni locali del device (configurazioni specifiche del sistema operativo di ciascun supporto mobile), le vulnerabilità del codice e le interazioni con i server centrali e con il mondo Internet.

Vengono offerte ulteriori funzionalità di test (IN) in ambito web app mobile, dove la soluzione utilizza componenti dette user-agent per eseguire test diversi tra cui ad esempio: Microsoft IE 7 for mobile, Ipad Safari, Iphone Safari, Google Android, Opera mini e Opera mobile (IN). Ulteriori funzionalità includono la possibilità di eseguire test sulle app sviluppate con il framework IBM Worklight ed eseguire test web services basati sui protocolli SOAP e REST. Ulteriore valore ai test eseguiti viene apportato dall'esecuzione di una serie di controlli mirati in modo specifico alla verifica de rischi di integrità delle app e suggerendo, conseguentemente, le protezioni necessarie.

Piattaforma tecnologica Vulnerability Assessment

La piattaforma fornisce gli strumenti per la gestione delle vulnerabilità relative ai servizi, all'architettura e alle configurazioni dei sistemi oggetto dell'analisi, eseguendo una serie di test in grado di coprire le esigenze di sistemi complessi. La soluzione è basata su una componente centralizzata di gestione che governa e raccoglie i flussi informativi provenienti dalle istanze scanner dedicate alla realizzazione dei test. La soluzione si basa su IBM QRadar Vulnerability Manager quale componente specializzato della piattaforma IBM Qradar, posizionata come leader nel Gartner Magic Quadrant 2014 delle piattaforme SIEM.

la piattaforma proposta soddisfa tutti i requisiti tecnici e funzionali richiesti dal capitolato (AD) supportando pienamente l'erogazione del servizio nello svolgimento delle fasi di:

- Raccolta delle informazioni: realizzando la scansione del perimetro indicato rilevando la presenza di asset (discovery) e identificando tipologie e caratteristiche hardware e software,
- Individuazione delle vulnerabilità: collezionando le vulnerabilità presenti nelle varie componenti del sistema target eseguendo test dal livello network al livello applicativo,
- Prioritizzazione delle vulnerabilità: organizzando le vulnerabilità rilevate in funzione del rischio che esse rappresentano per l'Amministrazione. Ai fini di una appropriata classificazione, il RTI promuove una stretta collaborazione e comunicazione con l'Amministrazione sul tema, anche a supporto della realizzazione delle policy.

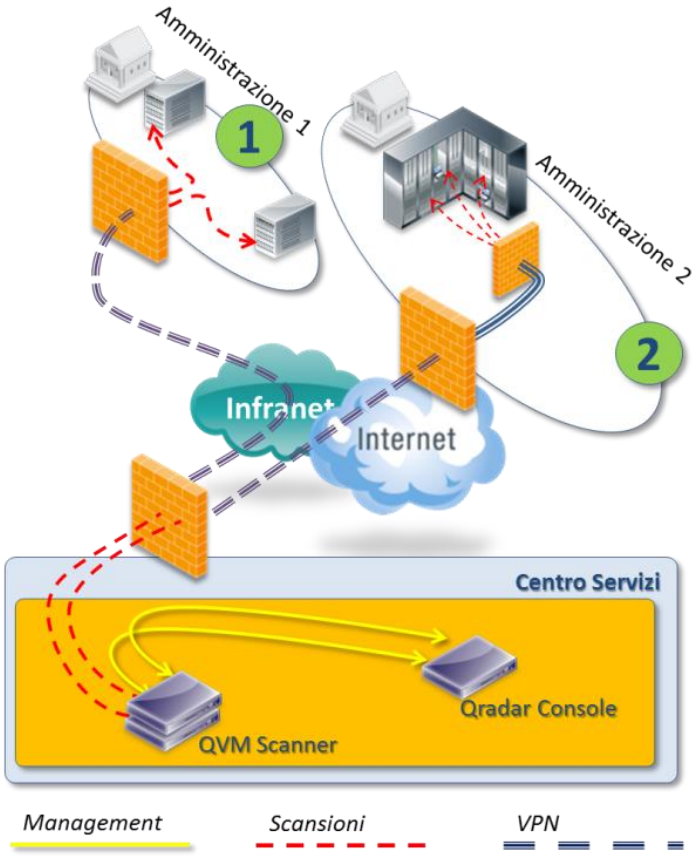


Figura 48: Architettura del servizio di Vulnerability Assessment

Tutte le scansioni saranno eseguite attraverso un canale sicuro instaurato tra gli apparati di sicurezza perimetrale del Centro Servizi e quelli del Cliente. La Figura 48 riporta un esempio di deploy della Piattaforma tecnologica in uno scenario composito dove nel caso (1) le scansioni saranno effettuate attraverso lo scanner posizionato nel Centro Servizi e comunicante con gli IP esposti in DMZ mentre nel caso (2), in funzione della numerosità dei target o per il loro posizionamento all'interno della rete cliente, l'Amministrazione potrà optare per collegare la VPN in prossimità dei target (EC).

l'Amministrazione può beneficiare di una completa ed aggiornata visione delle proprie vulnerabilità e dei relativi rischi connessi che costituiscono fattore abilitante alla gestione proattiva della sicurezza. Grazie alla capacità di integrare sul singolo asset le informazioni provenienti dalle scansioni con i flussi dei laboratori IBM X-Force (IN) la reportistica ed eventuali comunicazioni aggiuntive potranno essere corredate delle necessarie istruzioni per la realizzazione di virtual patch (EC) per la rapida protezione del patrimonio informativo.

4.3.3.2 Soluzione Tecnologica per i Servizi di Protezione

I servizi di **Data Loss/Leak Prevention**, **Database Security**, **Web Application/Next Generation Firewall Management** e **Secure Web Gateway** descritti in soluzione unica, sono supportati dalle architetture e tecnologie descritte all'interno dei seguenti paragrafi. Le tecnologie descritte sono quelle richieste dal Capitolato Tecnico per i singoli servizi, fermo restando che in ottica di maggior flessibilità e di massimo supporto, per allinearsi al rapido tasso di evoluzione delle tecnologie, il RTI potrà proporre l'utilizzo di tecnologie alternative, valutate di volta in volta con l'Amministrazione. (AD, IN, EC) Tutte le componenti (appliance / sonde / agenti) installate "on-premise" sono gestite centralmente dal Centro Servizi con le modalità sicure già precedentemente descritte.

Data Loss/Leak Prevention

La piattaforma tecnologica a supporto del servizio "data loss/leak prevention" (DLP) consentirà all' Amministrazione di proteggere i propri dati da accessi non autorizzati o violazioni delle policy di sicurezza, riducendo il rischio di estrusione di informazioni. Tale soluzione è basata sulla tecnologia leader nel Quadrante **Gartner** di Content aware DLP, Websense Data Security Suite (DSS), ed è in grado di effettuare il monitoraggio e la protezione dei dati *at rest* (sui supporti di memorizzazione), *in use* (accesso tramite endpoint), *in motion* (traffico di rete).

Figura 49: Gartner Magic Quadrant DLP

La soluzione è caratterizzata da una console di gestione dislocata presso i Centri Servizi del RTI e dalle componenti: DLP server per la raccolta centralizzata dei log, software **agent** per gli endpoint e **gateway** per il traffico in motion dislocate "on premise" presso le Amministrazione per l'attuazione delle policy.

La piattaforma proposta soddisfa tutti i requisiti tecnici e funzionali richiesti dal capitolato (AD).

Permette inoltre la rilevazione dei dati che transitano nell'organizzazione ovunque siano archiviati (AD) e supporta l'Amministrazione nella definizione della migliore configurazione di sicurezza possibile mediante:

- la componente endpoint in grado di monitorare tutti i canali di uscita (AD) legati all'endpoint e proteggere i dati all'interno delle periferiche di archiviazione (AD) sia all'interno della rete che in roaming (disconnessa dalla rete aziendale) e consente l'applicazione di regole predefinite in base alla periferica (AD); l'installazione delle componenti agent della soluzione sarà realizzata utilizzando le piattaforme di SW deployment dell'Amministrazione con il supporto del RTI;
- la componente di DLP gateway consente di includere nel perimetro di sicurezza anche gli utenti che non utilizzano un endpoint e i canali di uscita delle informazioni dal perimetro logico;
- funzionalità evolute di analisi e classificazione (AD) dei dati quali il **Machine Learning Documentale (EC, IN)** che consente di analizzare una grande quantità di dati testuali e di estrapolare un dizionario personalizzato da riutilizzare per definire delle politiche di controllo e monitoraggio;
- funzionalità di "**application awareness**" (EC, IN), ovvero la capacità di riconoscere le applicazioni e definire diverse azioni possibili da parte di queste, in modo da gestire in maniera selettiva e sicura quali dati possono essere trattati e verso quali periferiche o destinazioni esterne;
- Generazione automatica di alert quando le policy vengono violate, report (sintesi/dettaglio) e audit trail (AD);

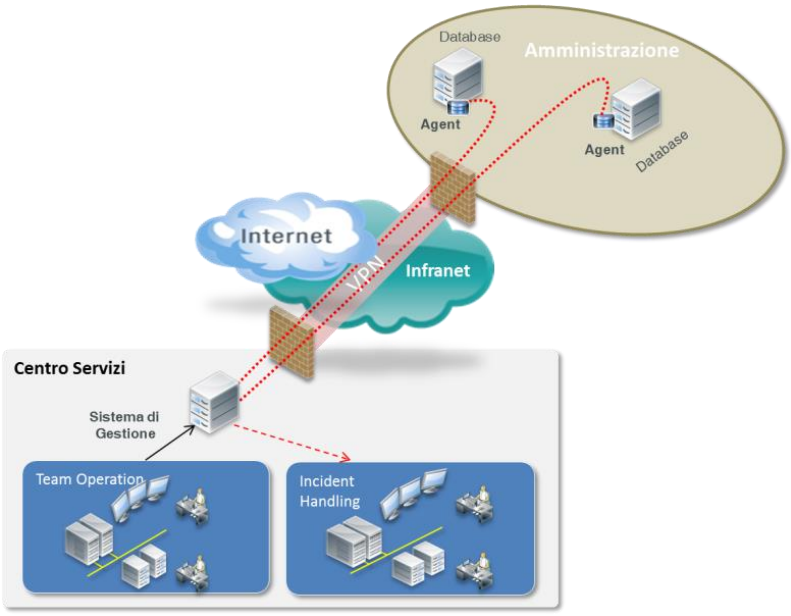


Figura 50: Architettura del servizio di Database Security

Sono previste ulteriori funzionalità innovative che consentono di riconoscere i dati confidenziali in base al contenuto piuttosto che a semplici parole chiave. Di seguito una lista delle funzionalità a valore aggiunto:

- **Drip DLP:** per segnalare potenziali incidenti al ripetersi di un evento in una specifica finestra temporale;
- **Data Theft Protection:** (EC) per bloccare pattern di furto dati da parte di malware riconosciuti;
- **Rilevazione testo per immagini OCR:** (IN) possibilità di analizzare il contenuto informativo all'interno di file immagine, quali scansioni di documenti, bloccandone l'eventuale trasmissione (come allegato email, upload web, etc.) qualora non conforme alle policy DLP. Questa funzionalità non è presente per gli endpoint e richiede un server dedicato per analisi OCR;
- **Fingeprint Documentale:** (IN, EC) per creare una rappresentazione matematica di un documento o contenuto confidenziale da riutilizzare poi come un'impronta digitale del dato per tracciarne gli spostamenti;

- **Policy DLP WEB per Geolocalizzazione:** (EC) tramite integrazione con Websense Web Security Gateway (piattaforma prevista per l'erogazione dei servizio "Secure web Gateway") è possibile implementare policy per GeoLocalizzazione, ovvero bloccare l'upload di dati verso indirizzi IP appartenenti a nazioni considerate a rischio. Questa funzionalità non è presente per gli endpoint.

DataBase Security

La piattaforma tecnologica a supporto del servizio "Database Security" consentirà all'Amministrazione la protezione in tempo reale delle basi dati da minacce esterne o interne mediante la configurazione di policy "ad hoc" in grado di generare alerting su attività sospette fino al suo eventuale blocco.

Tale soluzione è basata sulla tecnologia leader di mercato **McAfee DSS** ed è in grado di impostare una vasta gamma di controlli per la protezione del database nel suo complesso (dati, procedure o funzioni stored, il sistema di gestione, i server ed i collegamenti di rete associati) allo scopo di salvaguardarne la riservatezza, integrità e disponibilità.

L'architettura prevede l'installazione di un agent "on premise" sulle macchine DB dell'Amministrazione incluse nel perimetro di monitoraggio come attuatore delle policy e la presenza di un sistema di gestione all'interno del Centro Servizi, che avrà il triplice ruolo di: **1.** raccogliere in maniera centralizzata e attraverso canali cifrati (SSL) i log generati dagli agent; **2.** gestire la soluzione nelle sue funzioni di sicurezza previste dal servizio comprese la gestione delle configurazioni di policy, le scansioni delle vulnerabilità, la definizione degli alert e report; **3.** rendere disponibile ad un team di specialistici per la gestione degli incidenti, un cruscotto (dashboard) per il monitoraggio.

La piattaforma proposta soddisfa tutti i requisiti tecnici e funzionali richiesti dal capitolato (AD). La tecnologia selezionata per l'erogazione del servizio consentirà di realizzare:

- monitoraggio e audit in tempo reale di tutte le transazioni del database (AD, EC), incluse quelle generate da procedure interne, triggers, views, stored procedures, dati nascosti o criptati.
- definizione di regole di sicurezza personalizzate costruite "ad hoc" e /o basate su standard / normative di settore (AD) e **blocco** in tempo reale di attività **non autorizzate** (AD) con la possibilità di relegare gli utenti sospetti in aree di quarantena**;**
- identificazione e classificazione delle **vulnerabilità** e delle **minacce** e valutazione del relativo rischio con indicazione delle azioni correttive (AD) tramite un modulo dedicato che consente di attuare delle scansioni mirate sulla base di 4700 controlli (EC).

Sono previste ulteriori funzionalità innovative quali il monitoraggio dei database in ambienti virtuali, incluso l'accesso di dati tra Virtual Machine (VM) operanti sulla stessa piattaforma HW fisica (EC, IN).

Web Application/Next Generation Firewall Management

La piattaforma tecnologica a supporto del servizio "Web Application Firewall e Next Generation Firewall Management" consentirà all'Amministrazione di proteggere le applicazioni web da attacchi esterni agendo da filtro del traffico di rete dello strato applicativo e fornendo una visione completa e in tempo reale di tutte le attività, con funzionalità avanzate di reporting. Tale soluzione è basata sulla tecnologia leader di mercato **FortiGate** di **Fortinet** ed è caratterizzata da una componente centrale di gestione e raccolta dei log dislocata presso i Centri Servizi del RTI e dalle componenti gateway (fisiche o virtuali), che possono essere dislocate "on premise" presso l'Amministrazione oppure presso i Centri Servizi del RTI, concordandolo con l'Amministrazione.

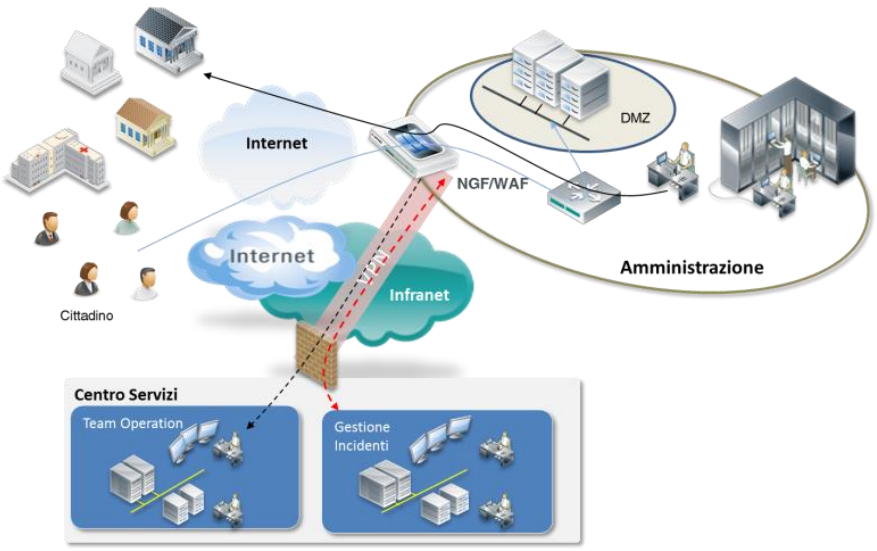


Figura 51: Architettura di Database Security

Pur non esistendo un quadrante Gartner di Next Generation Firewall, Fortinet è presente nei quadranti UTM, Enterprise Firewall e WAF, che ne completano le funzionalità.

La piattaforma proposta soddisfa tutti i requisiti tecnici e funzionali richiesti dal capitolato con inclusione delle funzionalità di **Standard Firewall**, **antimalware/spam**, IPS, monitoraggio del livello di sicurezza degli applicativi web (**WAF**), **prevenzione avanzata** contro le intrusioni/filtraggio dei contenuti, **deep packet inspection**, e **reporting**. (AD).
La soluzione supporta l'Amministrazione nella definizione della migliore configurazione di sicurezza possibile mediante:

- l'infrastruttura di gestione centralizzata, costituita da: un sistema per la gestione delle configurazioni e del monitoraggio e un sistema per il logging e il reporting. Tale infrastruttura è caratterizzata dalla notevole capacità di gestione (scalabilità per migliaia di apparati) ed è *multitenant* attraverso la realizzazione degli Administrative Domain (AD), che permettono la creazione di ambienti indipendenti dal punto di vista sia della gestione, sia dell'accesso amministrativo, con un controllo granulare dei permessi di accesso. Nel Centro Servizi sarà inoltre presente un sistema per il logging e reporting centralizzato deputato alla raccolta dei messaggi syslog da tutti gli apparati attivi, con la possibilità di produrre report a diversi livelli di sintesi.
- l'ispezione del livello applicativo (**Application Control**) (IN), permette una accurata identificazione delle applicazioni (EC) che generano traffico all'interno della rete senza comprometterne le performance; una volta che il traffico applicativo è stato individuato, è possibile bloccare le applicazioni indesiderate o controllarne l'accesso, limitare/garantire la relativa banda (Traffic Shaping feature);
- elevate performance e bassa latenza grazie alla tecnologia **ASIC** (Application Specific Integrated Circuit) proprietaria di **Fortinet**.

La tecnologia adottata prevede caratteristiche innovative che consentono di:

- implementare funzionalità *anti-botnet* (IN), rilevando eventuale traffico anomalo generato da sistemi interni;
- monitorare il livello di sicurezza degli applicativi web; attraverso l'utilizzo contemporaneo delle funzionalità di W*eb Server Protection* introdotte *dal modulo **WAF** di Fortinet per il contrasto di attacchi di tipo Injection, Cross-Site Scripting (XSS), XML, SOAP and SQL vulnerabilities solo per citarne alcuni* (IN);
- applicare tecniche di prevenzione avanzata contro le intrusioni tramite la funzionalità *Threat Detection* per individuare attacchi avanzati e mirati - Advanced Persistent Threat (APT) (IN);
- Selezionare con granularità adeguata il livello di interazione degli utenti con le piattaforme di Social Networking più diffuse (IN) (Facebook, Google, Twitter).

Secure Web Gateway

La piattaforma tecnologica a supporto del servizio "Secure web gateway" consentirà di bloccare l'accesso a siti web potenzialmente malevoli in tempo reale, aggiornando la propria base dati in maniera automatica, e quindi riconoscere il download di applicazioni potenzialmente dannose. Tale soluzione è basata sulla tecnologia leader di mercato **WebSecurity di Websense** (Leader nel quadrante Gartner dei Secure Web Gateway) ed è caratterizzata da una componente centrale di gestione dislocata presso i Centri Servizi del RTI e dalle componenti gateway (fisiche o virtuali) che possono essere dislocate "on premise" presso l'Amministrazione, oppure presso i Centri Servizi del RTI, definendolo come Proxy o Default Gateway.

Figura 52: Gratner Magic Quadrant per Secure Web gateway

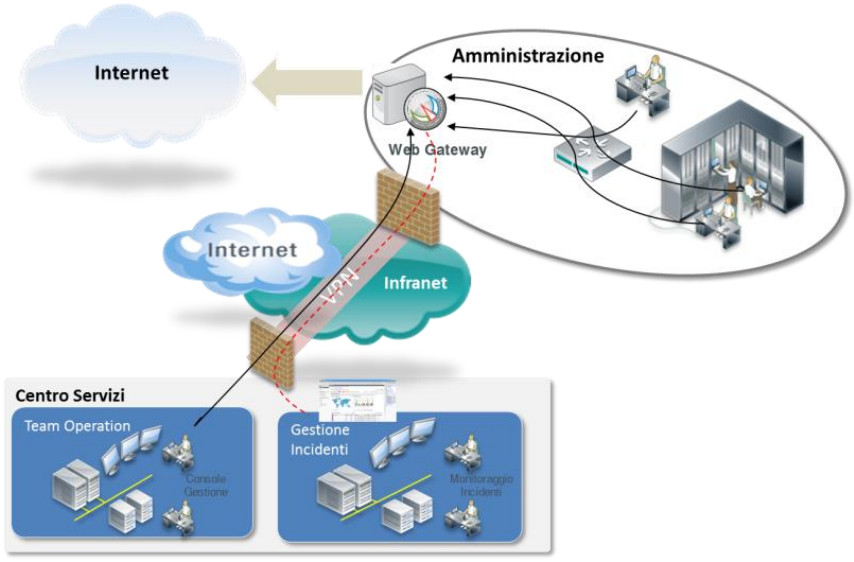


Figura 53:Architettura di Secure Web Gateway

La piattaforma proposta soddisfa tutti i requisiti tecnici e funzionali richiesti dal capitolato, quali: analisi del traffico, rilevazione e

blocco dei comportamenti dannosi, aggiornamento delle liste dei siti (ogni 24 ore per il database dei contenuti, 5 minuti per il Real Time update e 15 minuti per l'Antivirus) (EC) e reporting. (AD)
La soluzione consente la realizzazione di un sistema di "Web Security" estremamente efficace in quanto:

- i controlli sia di sicurezza sia di content filtering vengono effettuati in tempo reale (EC), l'esperienza utente nella navigazione rimane quindi invariata a meno che la risorsa non debba essere bloccata; in questo caso l'utente visualizza tramite browser un messaggio di notifica
- in aggiunta alla classica soluzione Web Security and Web Filter, aggiunge la capacità di eseguire l'analisi in tempo reale del contenuto del traffico Web e SSL (**HTTPS inspection**) (AD) consentendo la catalogazione istantanea dei nuovi siti e del contenuto dinamico, oltre al rilevamento proattivo dei rischi per la sicurezza e al blocco del malware pericoloso;
- il security gateway si presenta al client come un servizio di proxy che, configurato in modo esplicito o trasparente, diventa il punto unico di uscita per la navigazione Internet,
- dispone di un motore di nuova generazione che combina una serie di tecniche che sono progettate per rilevare gli attacchi conosciuti, sconosciuti e "zero-day" propagati in diversi modi (EC). L'analisi in linea, sia testuale sia binaria, consente di riconoscere profili di attacco a prescindere dal codice utilizzato (e dalla signature) grazie a tecniche di analisi innovative: script analysis, de-obfuscation di codice criptato, analisi di embedded link ed iFrame, analisi di exploit, analisi di shell code. Motori dedicati a contenuti Rich Internet Application (Flash), JavaScript e Adobe Reader consentono di gestire anche infezioni che tentano di propagarsi sfruttando vulnerabilità dei plug-in dei browser, spesso non aggiornati.

La tecnologia selezionata fornisce inoltre una serie di funzionalità a valore aggiunto rispetto ai requisiti che consentono ulteriori opzioni di personalizzazione del servizio in tema di gestione e sicurezza:

- **Policy per Quota Tempo/Conferma:** oltre ai classici "Permetti" o "Blocca" è possibile sfruttare diverse opzioni avanzate per la gestione del tempo di navigazione concesso agli utenti :
  - **Quota Time**: gli utenti ricevono una quantità variabile di gettoni di tempo di 10 minuti che possono spendere durante l'arco della giornata.
  - **Confirm**: l'utente visualizza una pagina di blocco dove è presente un messaggio di avviso personalizzato.
- **Categorizzazione di Siti e Applicazioni Web 2.0:** è resa disponibile una funzione di analisi del contenuto del sito Web che, a fronte di un download di una pagina Web, effettua un'analisi in tempo reale per verificare che il contenuto corrisponda realmente alla categoria del sito Web (Real Time Classification). Tale funzione è attiva per tutti i siti non categorizzati, per i siti a contenuto dinamico e siti con tecnologia web 2.0 (IN).
- **Social Web 2.0 Controls:** I Social Web controls permettono all'amministratore di controllare in modo molto granulare (IN) alcuni tra i portali Web 2.0 più importanti, tra cui Facebook, Twitter, YouTube e LinkedIn consentendo ad esempio di garantire l'accesso ma bloccando specifiche azioni (EC).
- **Data Theft Protection:** (EC) Consente di bloccare pattern noti di furto dati da parte di malware, in particolare: custom encrypted upload, file containing password, C&C back channel.

4.3.4 Servizi Professionali

Il RTI metterà a disposizione dell'Amministrazione servizi Professionali erogati attraverso l'impiego di figure professionali di comprovata esperienza, maturata nel corso degli anni per le tematiche oggetto del servizio e con riferimento a progetti realizzati presso PA e organizzazioni private, sia nel territorio nazionale sia internazionale.
Tali servizi saranno erogati esclusivamente nella modalità "on premise" con gli strumenti hardware e software presenti presso l'Amministrazione.
Per il soddisfacimento dei requisiti minimi indicati nell'Appendice 2 del Capitolato tecnico si veda il § 4.6 e § 4.7
Acquisizione.
Le modalità di acquisizione sono descritte nel § 3.2.3.1. In particolare il Responsabile dell'Innovazione ed i Presidi Territoriali supporteranno l'Amministrazione nella redazione del Piano dei Fabbisogni.
Configurazione
Le modalità di configurazione sono descritte nel § 3.2.3.2. Durante questa fase sarà eseguita la selezione delle risorse a cura del Resource Manager e del Responsabile dei servizi on-premise, come indicato nei § 3.2.2.2 e § 4.8.2.
Utilizzo/Gestione

Il personale sarà disponibile on-site presso l'Amministrazione negli orari richiesti (il servizio potrà essere erogato in modalità H8 o H24 a seconda del servizio e della richiesta). I team di presidio saranno coordinati da un team leader che ne curerà la gestione operativa.
Le attività in ambito dei Servizi professionali includeranno i servizi di consulenza, il supporto Generico alle ULS, le attività di supporto per la gestione del CERT e delle Unità Locali di Sicurezza o strutture equivalenti delle Pubbliche Amministrazioni per la prevenzione e gestione degli incidenti informatici e l'analisi delle vulnerabilità dei sistemi hardware e software, penetration test di tipo applicativo e infrastrutturale e servizi di Encryption per le postazioni di lavoro.

Reporting

Saranno prodotti report di gestione atti alla consuntivazione delle giornate di servizi professionali erogate.

4.4 Servizi di Sicurezza - Miglioramento Requisiti Tecnici

Di seguito nella tabella sono indicati, per ciascuna tecnologia sottesa ai servizi, i requisiti tecnici di base e migliorativi.

Tabella 15: Confronto tra i requisiti tecnici richiesti, soddisfatti e migliorativi per i singoli servizi di sicurezza.

Servizi di sicurezza	***Requisiti soddisfatti***	***Requisiti migliorativi***
Static Application Security Testing	Compatibilità con .NET, PHP, C/C++, Java, J2EE, ASP	COBOL, JSP, ASP, JavaScript, ColdFusion, Perl, Visual Basic 6, PL/SQL, T-SQL
	Integrazione con almeno due dei seguenti repository del software SVN, CVS, Git, TVFC	N/A
Dynamic Application Security Testing	Compatibilità con .NET, PHP, C/C++, Java, J2EE, ASP.	HTML5, Java-script, WEB 2.0; Adobe Flash, Flex, AJAX, JQuery, Dojo, ICEfaces, Action Script 2.0/3.0; Supporto Web services (JSON, RESTful)
Mobile application security testing	Compatibilità con Android e iOS.	Blackberry e Microsoft Windows Mobile
Vulnerability assessment	Compatibilità con FTP, SFTP, FTPS, SMTP, HTTP, HTTPS,	SNMP, ODBC, etc.
Data loss/leak prevention	Compatibilità con (FTP/SFTP/FTPS, HTTP/HTTPS, SMTP) e (IP, UDP, TCP)	N/A
	Compatibilità con Windows e Linux	Sistema operativo MAC OSX. Tramite Active Sync anche con OS mobile (Android, , iOS e Microsoft Windows Mobile).
Database security	Compatibilità con Oracle, Microsoft SQL Server, IBM DB2	SAP Sybase, MySQL
WAF e NGF	Compatibilità FTP/SFTP/FTPS, HTTP/HTTPS.	N/A
Secure web gateway	compatibilità con FTP/SFTP/FTPS, HTTP/HTTPS.	N/A

Punteggio tecnico Associato: punti 3 (**tre**).

4.5 Soluzione proposta per le modalità di affiancamento di fine fornitura (Phase Out)

L'obiettivo del processo di Phase Out è trasferire know-how, documentazione e dati **all'Amministrazione** e/o **terzi** da essa designati (di seguito identificati con **Nuovo Operatore**), in modo tale da garantire ► la continuità dell'operatività dei servizi erogati nell'ambito della Fornitura; ► la dismissione sicura dei dati, che risiedono nei sistemi ubicati presso i Centri Servizi del RTI. Per il raggiungimento di tale obiettivo il RTI ritiene necessario adottare un processo di Phase Out strutturato e condiviso tra il RTI ed il Nuovo Operatore. L'attivazione di tale processo metterà il Nuovo Operatore nelle condizioni ottimali per proseguire nell'erogazione dei servizi. In particolare il RTI fornirà un accesso completo ai dati ed alla documentazione prodotta nell'ambito della fornitura e predisporrà, di comune accordo, le modalità operative ritenute più efficienti per il trasferimento di know-how ed il passaggio di consegne. L'esperienza pluriennale maturata in anni di operatività in ambienti PAC e PAL e

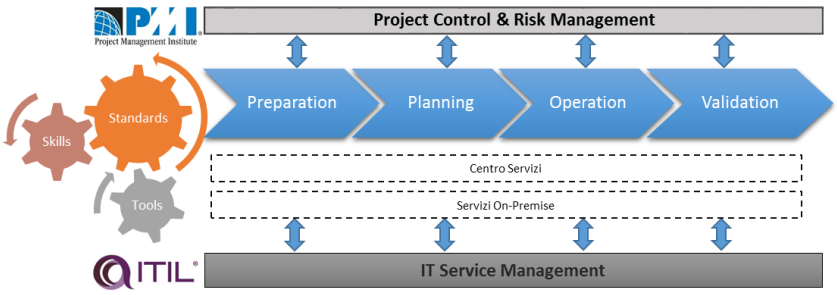
contesti tecnologici analoghi a quelli della presente Fornitura, consente al RTI di affrontare il Phase Out dei servizi applicativi e delle infrastrutture, erogati "on premise" e "as a service", in maniera organizzata e consapevole. Nello specifico, il RTI propone di utilizzare la metodologia "**SMOOTH TRANSITION**", di proprietà della Mandataria, che fornisce un approccio strutturato e completo al processo di transizione, ma allo stesso tempo si rende disponibile ad adattarsi alla metodologia di presa in carico, eventualmente proposta, dal Nuovo Operatore.
Le operazioni di Phase Out saranno realizzate nel rispetto dei requisiti di capitolato per tutti i servizi oggetto di fornitura. Nei successivi paragrafi, a titolo esemplificativo, sono descritte le attività per i Servizi di Identity & Access Management (S1.2) ed i Servizi Professionali (S3.9), specificando l'organizzazione, la metodologia, gli strumenti e la documentazione che si intende adottare a supporto di tale processo. La seguente tabella elenca in maniera schematica i criteri di valutazione e i razionali di sostenibilità della proposta del RTI.

Tabella 16: Razionali di sostenibilità del Phase Out.

Ambito	Caratteristica	Valore
Modalità operative	Il Piano di Trasferimento conterrà una pianificazione di dettaglio delle attività da svolgere, organizzate secondo l'approccio metodologico SMOOTH TRANSITION.	Completezza, efficacia della pianificazione
Risorse	Il RTI dimensionerà le risorse richieste per l'erogazione dei servizi, al fine di garantire la piena operatività e la continuità dei servizi. Inoltre saranno messe a disposizione ove necessario Risorse aggiuntive provenienti dal Pool di Figure professionali del RTI (rif. § 4.8), già formate e facilmente integrabili nei team, per far fronte agli eventuali picchi generati dall'attività e/o sostituire risorse in caso di necessità.	Dimensionamento delle risorse e continuità del servizio
Organizzazione	Il RTI propone una struttura organizzativa efficiente e flessibile, sotto la guida del Transition manager, che si presta in modo ottimale al conseguimento degli obiettivi. Inoltre metterà a disposizione del Nuovo Operatore diverse modalità formative (online e in aula), allo scopo di ottimizzare il processo di trasferimento di know-how.	Struttura organizzativa e formazione dedicate
Strumenti	Il RTI propone di adottare strumenti automatici o semi-automatici a supporto dell'operatività. In particolare sarà impiegato il PGGF come strumento principale per gestire la governance, le comunicazioni, la documentazione e la formazione on-line.	Strumenti di migrazione per ogni tipologia di servizio
Dati ed Informazioni	Il RTI garantisce di eseguire un efficiente trasferimento dei dati e delle informazioni della PA al Nuovo Operatore, **secondo i formati standard definiti dall'Amministrazione**.	Salvaguardia dei dati e delle informazioni

4.5.1 La metodologia "SMOOTH TRANSITION"

La metodologia "**SMOOTH TRANSITION**" si basa sulle best practice internazionali ITIL V3 per il Service Management e PMI per il Project Management. Il processo di transizione è suddiviso in fasi. Lo stato di avanzamento e i rischi associati sono verificati attraverso un processo continuo di *Project Control & Risk Management*. La metodologia definisce puntualmente quali sono le risorse coinvolte, le attività da svolgere, le tempistiche di esecuzione e i deliverable da produrre. Inoltre, la presenza di milestone di verifica intermedie garantisce ► il corretto raggiungimento degli obiettivi pertinenti l'attività, ► la drastica riduzione dei rischi (es. formazione inadeguata, baseline incompleta, mancanza di documentazione,...) e ►l'efficacia di eventuali azioni correttive o proattive.



I seguenti processi della fase di Service Transition del framework ITIL V3 e di ITUP risultano particolarmente utili nella gestione del processo di Phase Out: ► **Knowledge Management (KM)** che ha l'obiettivo di accentrare e trasferire le informazioni e le procedure operative esistenti alle risorse coinvolte nei vari servizi; ► **Release and Deployment Management (RDM)** che ha lo scopo di gestire correttamente i rilasci in ambiente di produzione; ► **Service Asset and Configuration Management (SACM)** che ha lo scopo di definire tutti gli elementi del servizio e di tenerne aggiornata la configurazione (es. versione del prodotto); ► **Change Management (CM)** che ha lo scopo di assicurare che i cambiamenti siano registrati, valutati, autorizzati, pianificati, testati, documentati e revisionati in modo controllato.

Su tali basi, il RTI descrive nel seguito l'organizzazione, le attività e gli strumenti che intende adottare a supporto del processo.

4.5.2 Organizzazione a supporto del processo di Phase Out

La struttura organizzativa generale prevede le figure di Transition manager (a livello di Contratto Esecutivo) e di Responsabile Transition (a livello di Contratto Quadro) al fine di: governare il processo di transizione a livello sia di Contratto Quadro sia di singolo CE, gestire con efficacia attività di transizione relativamente ai servizi erogati "as a service" dai Centri Servizi ed ai servizi erogati in modalità "on premise" alle varie Amministrazioni, annullare o minimizzare eventuali discontinuità di servizio nel passaggio di responsabilità del RTI al Nuovo Operatore, garantire l'identificazione univoca delle interfacce interessate alla conduzione dei servizi rilasciati.
Si sottolinea che la figura di Transition manager è di particolare rilevanza in quanto garantisce che tutti i processi di Service Transition elencati precedentemente vengano gestiti e monitorati in modo continuativo durante l'intera durata di Contratto e non solo durante la fase di Phase out, a garanzia di una massimizzazione dell'efficacia della transizione e di riduzione dei rischi di subentro.

4.5.3 Piano dei lavori proposto (GANTT)

Il RTI si impegna a garantire al Nuovo Operatore un periodo di **supporto alla transizione della durata di 3 mesi** (rif. Capitolato Parte generale 7.4), posizionati indicativamente al termine del CE o del Contratto Quadro (CQ). La Figura 55 propone un possibile piano di dimensionamento, qualora sia previsto un passaggio di consegne al Nuovo Operatore. Al fine di garantire la continuità operativa ed il rispetto dei livelli di servizio contrattuali, il RTI ritiene necessario introdurre, a supporto delle risorse operative a regime, ulteriori risorse aggiuntive già formate, specializzate su prodotti/tecnologie già presenti e con esperienza in ambito PA.
La Figura 54 presenta una ipotesi di Gantt del Piano di Trasferimento, con evidenza delle fasi e dei meccanismi operativi / di controllo atti a rispettare i vincoli contrattuali in termini di rilasci temporali, milestone e deliverable.
Tali risorse, selezionate dal Responsabile Resource Management, provengono dal Pool di Figure professionali del RTI (rif. § 4.8)e saranno impiegate, oltre che per garantire la piena operatività dei servizi anche per svolgere seminari formativi alle risorse entranti del Nuovo Fornitore (es. Team di KA).

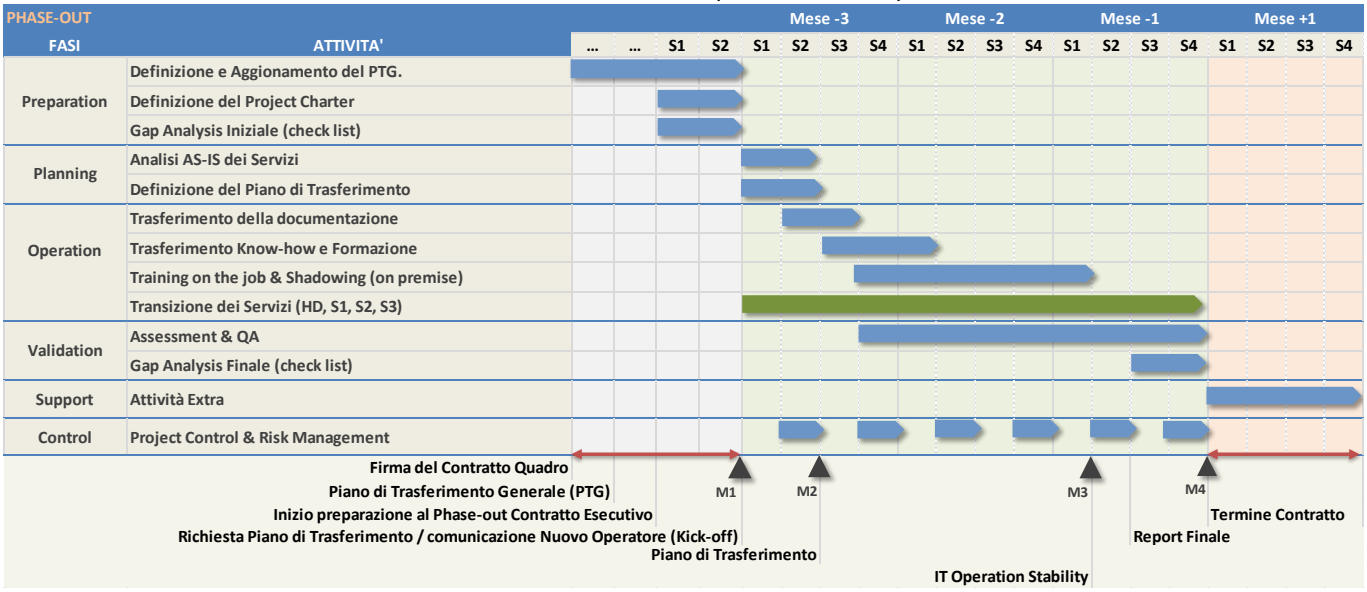


Figura 54: Piano di Progetto di Phase Out

Per quanto concerne, invece, l'attività di affiancamento/addestramento sulle procedure operative di gestione dei servizi, questa sarà svolta dalle risorse già operative del RTI. Tali risorse saranno offerte, sebbene non richieste, dal RTI per un periodo di almeno 2 mesi antecedenti la data di scadenza del singolo CE. Saranno allocate circa dal 10% fino al 30% delle risorse in aggiunta a quelle già presenti nell'erogazione del servizio.

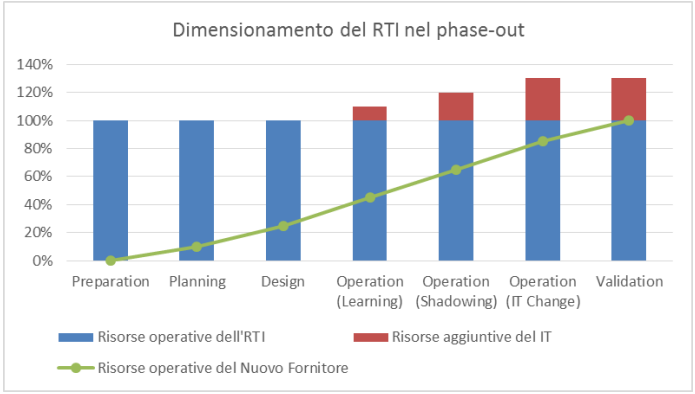


Figura 55: Incremento dell'effort nella fase di phase-out

4.5.4 Preparation

Al fine di rispettare le tempistiche di attuazione richieste dall'Amministrazione, il RTI attiverà una fase di Preparation che sarà propedeutica alla transizione. A livello di Contratto Esecutivo (CE), tale fase avrà una durata di circa 10gg lavorativi, con termine posto al momento del ricevimento della richiesta del Piano di Trasferimento da parte dell'Amministrazione. La seguente tabella mostra le attività tipiche di questa fase.

Tabella 17: Descrizione delle attività relative alla fase di Preparation.

Task	Deliverable
Definizione e Aggiornamento del Piano di Trasferimento Globale *Servizi interessati: Tutti i servizi della fornitura* Entro 30gg dall'avvio del Contratto Quadro, il Responsabile Transition redigerà e metterà a disposizione dell'Amministrazione un "Piano di Trasferimento Globale" con la descrizione di processi, metodi, approcci, soluzioni tecnologiche proposte e indicazione di come saranno prodotti e formalizzati i piani di Trasferimento per le singole Amministrazioni. Il RTI ritiene particolarmente importante tale strumento, poiché fornendo delle linee guida operative, permetterà al RTI di poter trasferire un servizio "as a service" in qualunque momento della fornitura.	Piano di Trasferimento Globale
Definizione Project Charter *Servizi interessati: Tutti i servizi della fornitura* Una volta ricevuta notifica da parte dell'Amministrazione, il Transition manager indirà una riunione tra i Responsabili dei Servizi del RTI per presentare quali sono gli obiettivi ed i servizi oggetto della transizione. Inoltre saranno identificati tutti gli stakeholder del processo, a valle delle comunicazioni ricevute dall'Amministrazione. Tutte le informazioni saranno formalizzate nel Project Charter.	Project Charter
Gap Analysis Iniziale *Servizi interessati: Tutti i servizi della fornitura* Il Transition manager, a livello di CE, compila una check list in formato tabellare di tutti i servizi da migrare, delle varie attività da svolgere e delle deliverable principali del processo. Ogni servizio viene classificato in termini di complessità per rappresentarne la criticità in termini di Phase Out. Analogamente a quanto avviene a livello di CE, Il Responsabile Transition , a livello di CQ, compila una check list dove vengono elencati tutti i contratti in scadenza, associando ad ognuno un livello di criticità. Quelli ritenuti più critici vengono sottoposti all'attenzione del Comitato Esecutivo al fine di intraprendere azioni proattive.	Check List, Check List di Contratto Quadro
Review del Roll-back Plan (on premise) *Servizi interessati: I&AM* Nel caso in cui il servizio abbia richiesto componenti presso le sedi dell'Amministrazione, il Transition manager esegue una review del piano di roll-back. Tale piano fornirà informazioni utili per procedere al piano di transizione.	Roll-back Plan

4.5.5 Planning

L'obiettivo della fase di Planning è elaborare una pianificazione in dettaglio delle attività e delle risorse coinvolte nel processo di transizione e contestualmente eseguire un'analisi AS-IS dei servizi. La durata prevista per tale fase è pari a circa di 20gg a partire dalla data di richiesta dell'Amministrazione di presentare il Piano di Trasferimento o Piano di *phase out*.

Tabella 18: Descrizione delle attività relative alla fase di Planning.

Task	Deliverable
Definizione del Piano di Trasferimento o Piano di phase out. *Servizi interessati: Tutti i servizi della fornitura* Entro i 10gg lavorativi (migliorativo rispetto ai 20gg richiesti) successivi alla richiesta dell'Amministrazione, il Transition manager presenterà il Piano di Trasferimento all'Amministrazione. Tale piano sarà prodotto congiuntamente tra i Responsabili dei Servizi del RTI ed il Nuovo Operatore, tenendo conto del Piano di Trasferimento Globale. Il piano conterrà una pianificazione delle attività da svolgere per eseguire la transizione di ognuno dei servizi richiesti nell'ambito del CE. Il documento conterrà, al fine di articolare puntualmente scadenze di inizio e fine, responsabilità, contenuti e risultati, almeno i seguenti elementi: gli obiettivi, l'elenco dei servizi da migrare, le attività da svolgere (WBS), una pianificazione delle attività (diagramma di Gantt), le deliverables previste, i responsabili delle attività, le risorse coinvolte ed il loro impegno in giorni/uomo. In allegato al Piano di Trasferimento, saranno consegnati anche il Piano di Formazione ed il Piano di Qualità.	Piano di Trasferimento (include Piano di Trasferimento del Servizio di I&AM, …), Piano di Qualità, Piano di Formazione

Logical Assessment *Servizi interessati: I&AM* Il Responsabile Tecnico, supportato dai responsabili dei vari servizi, provvede a fornire un elenco esaustivo delle procedure/ processi di dettaglio utilizzati nell'ambito dei servizi erogati, da considerarsi in aggiunta rispetto alla documentazione già esplicitata nel Capitolato, ad es. verrà indicato il dettaglio delle strutture organizzative e le modalità di comunicazione tra gli attori coinvolti.	Analisi delle procedure e dei processi per servizio.

4.5.6 Operation

La fase di Operation ha come obiettivo quello di trasferire tutto il complesso del know-how acquisito nell'ambito della fornitura al Nuovo Operatore ed eseguire le eventuali attività di migrazione dei servizi. Il RTI svolgerà tali attività, raggruppando i servizi in cluster di sistemi e applicazioni omogenei in termini di funzionalità, utenti coinvolti e scenari di integrazione. Tale segmentazione sarà utile per pianificare le attività di transizione in maniera graduale e in parallelo, mantenendo comunque un elevato livello di controllo e di verifica costante dei risultati raggiunti. La tabella seguente riporta le attività tipiche di questa fase (rif. Par. 7.4 del Capitolato Tecnico).

Tabella 19: Descrizione delle attività relative alla fase di Operation.

Task	***Deliverable***
Trasferimento della documentazione *Servizi interessati: Tutti i servizi della fornitura* Il Transition manager renderà disponibile all'Amministrazione e/o al Nuovo Operatore tutta la documentazione prodotta nell'ambito della fornitura all'interno del PGGF. Tale documentazione include: documentazione tecnica e funzionale dei servizi; manualistica utente; elenco degli utilizzatori interni all'Amministrazione; procedure operative di erogazione dei servizi; reportistica sull'andamento dei servizi; verbali di collaudo, di fine lavori etc… . I contenuti saranno catalogati per contratti/area/servizi e saranno resi accessibili in base al profilo di utenza.	Piani di progetto, manualistica, documenti tecnici, reportistica
Trasferimento Know-how e Formazione *Servizi interessati: Servizi Professionali* Il Transition manager organizza dei seminari con le persone individuate dall'Amministrazione e dal Nuovo Operatore per trasferire il know-how necessario alla gestione della fornitura. In particolare si tratterrà di seminari, in cui il Referente on premise, con l'eventuale supporto delle persone del RTI coinvolte operativamente nelle attività, procederà per le attività: *Concluse*, *In corso e non ancora completate* e *Pianificate*. Tali sessioni avranno come scopo ulteriore quello di informare il Nuovo Operatore sul dimensionamento dei servizi in oggetto della fornitura e fornire così un quadro completo delle principali problematiche ricorrenti riscontrate e gestite durante l'erogazione.	Sessioni formative, Sessioni di lavoro congiunto, Seminari, presentazioni, tavole rotonde, ecc.
Trasferimento Know-how e Formazione *Servizi interessati: I&AM* Il RTI organizza delle specifiche sessioni di knowledge transfer volte a trasferire competenze relativamente a: aspetti organizzativi rivolti ai gestori del servizio ed ai responsabili della comunicazione verso l'Amministrazione; aspetti tecnologici rivolti agli specialisti del tema tecnologico; aspetti applicativi rivolti agli operatori tecnici; aspetti riguardanti la sicurezza rivolti a tutte le figure coinvolte nel servizio, considerata la sua natura di trasversalità tra processi e tecnologie.	Meeting/Aula
Training on the job & Shadowing (on premise) *Servizi interessati: Servizi Professionali* Le risorse operative del RTI, per le attività in corso e non ancora concluse, affiancheranno il personale del Nuovo Operatore nell'erogazione dei servizi. In una prima fase il personale entrante sarà coinvolto nella presa visione di tutte le operazioni effettuate sui sistemi, reti ed applicazioni senza intervenire direttamente nelle attività (shadowing passivo); successivamente sarà chiesto al Nuovo Operatore di suggerire le operazioni da compiere per verificarne il livello di competenza acquisito (shadowing attivo). Il Fornitore si farà garante che tutte le informazioni in possesso delle Amministrazioni per il corretto svolgimento dei lavori (procedure e istruzioni operative) siano efficacemente trasferite al Nuovo operatore, per minimizzare i rischi di perdita di know-how.	Report degli interventi svolti
Transizione dei servizi	
Mapping Utente/ profili/ applicazione (matrice degli accessi) *Servizi interessati: I&AM* Il RTI provvede a fornire il mapping tra le utenze censite nel sistema I&AM e i profili definiti nel corso del tempo sulle applicazioni dell'Amministrazione e le relative policy di accesso ai servizi.	Export dei dati.
Logging export *Servizi interessati: I&AM* Il RTI provvede a fornire copia intellegibile dei log di accesso degli utenti che accedono ai servizi	Logging file nello standard richiesto.

dell'Amministrazione regolati dallo I&AM, secondo la normativa vigente.	
Migrazione dei Sistemi *Servizi interessati: I&AM* Il personale del RTI supporterà il Nuovo Operatore nel rispetto del Piano di Migrazione. Il personale del RTI provvederà a mantenere attivi i servizi sul proprio Centro Servizi per tutto il periodo di supporto alla transizione, indicato nel Capitolato avere durata massima pari a 3 mesi, salvo completamento anticipato.	Tickets di migrazione
Data Cleaning *Servizi interessati: Tutti i servizi della fornitura* Al termine del trasferimento dei dati, il RTI eliminerà dai propri archivi tutte le informazioni ed i dati relativi all'Amministrazione. Il Responsabile del CE sottoscriverà un verbale da consegnare all'Amministrazione.	Report di Data Cleaning

4.5.7 Validation

La fase di Validation ha il duplice obiettivo di verificare che il personale subentrante abbia ricevuto tutto il know-how tecnico necessario per l'operatività dei servizi e che gli stessi siano correttamente trasferiti al Nuovo Operatore, nella salvaguardia dei dati e delle informazioni delle PA presenti. La seguente tabella mostra le attività tipiche di questa fase.

Tabella 20: Descrizione delle attività relative alla fase di Validation.

Task	***Deliverable***
Assessment & Quality Assurance (QA) *Servizi interessati: Tutti i servizi della fornitura* I responsabili dei servizi produrranno al termine di ogni attività un verbale di fine lavori che indicherà le attività svolte, le modalità e le risorse coinvolte. Tali documenti saranno esaminati dal Transition manager, supportato dal Quality Manager, per verificare la corretta esecuzione dell'attività e l'aderenza agli standard qualitativi dell'Amministrazione.	Verbali di Fine Lavoro, Minute
Report di fine Trasferimento *Servizi interessati: Tutti i servizi della fornitura* Entro 10 giorni dal termine del processo, il Transition manager fornirà un Report finale con i verbali allegati.	Report Finale
Gap Analysis *Servizi interessati: Tutti i servizi della fornitura* Il Transition manager, in collaborazione con il Responsabile Tecnico, fa una gap analysis dei servizi erogati. La gap analysis fornirà al Nuovo Operatore una lista delle richieste/tickets non ancora conclusi.	Pending Issues

4.5.8 Extra Support

La conclusione del rapporto contrattuale ha come potenziale rischio l'esistenza di attività in corso di svolgimento non ancora completate che possono causare difficoltà nella presa in carico al Nuovo Operatore. Con l'obiettivo dunque di assicurare la piena operatività del Nuovo Operatore, sebbene non richiesto, il RTI metterà a disposizione ► un mese ulteriore di supporto da parte del proprio Help Desk di II livello nell'ambito del Centro Servizi per supportare il Nuovo Operatore nella chiusura di tutte le eventuali richieste in sospeso; ► la reperibilità del Responsabile Tecnico e, in casi di rilevante criticità, disponibilità di eventuale intervento on premise presso la sede dell'Amministrazione.

4.5.9 Project Control & Risk Management

Il Transition manager eseguirà puntualmente delle verifiche rispetto alla pianificazione iniziale in termini di raggiungimento degli obiettivi, stato di avanzamento del processo, standard di qualità, SLA e Risk Management. Il deliverable si consolida nell'aggiornamento del Piano di Subentro/Trasferimento.

4.6 Profili Professionali - Miglioramento Anzianità di Servizio

A copertura dei profili professionali richiesti nell'Appendice 2 del Capitolato Tecnico, il RTI si impegna ad offrire risorse in possesso del requisito migliorativo *B11 – Miglioramento anzianità nella funzione*, di cui alla *Lettera di Invito – Lotto 2* pag. 35, nella seguente misura:

Figura Professionale	Requisito migliorativo – miglioramento anzianità	Num. risorse offerte
Capo Progetto	2 anni aggiuntivi di anzianità e 1 anno aggiuntivo nella	7

Specialista di tecnologia/prodotto Senior	funzione	28
Specialista di tecnologia/prodotto		35
	Totale	70

Punteggio Tecnico Associato: **2 punti** (due)

4.7 Profili Professionali – Certificazioni

A copertura dei profili professionali descritti nell'Appendice 2 al Capitolato Tecnico, il RTI si impegna ad offrire risorse in possesso del requisito migliorativo *B 12 – Figure professionali – Presenza di Certificazioni*, di cui alla *Lettera di Invito – Lotto 2* pagina 36, nella seguente misura:

Figura Professionale	Requisito migliorativo – Presenza di certificazioni professionali	Num. risorse offerte
Capo Progetto	ITIL v.3 Foundation	7
	Almeno una certificazione di Project Management PMI-PMP e/o Prince2 Practitioner e/o Senior Project manager Level B-IPMA	
	Almeno una certificazione tra Certified Information Systems Auditor e/o Lead Auditor ISO 27001 e/o Security Adviser Professional EUCIP	
Specialista di tecnologia/prodotto Senior	Almeno una certificazione tra Certified Information Security Manager (CISM) e/o Certified Information Systems Security Professional (CISSP) e/o Certified Ethical Hacker (CEH)	28
	Totale	35

Punteggio Tecnico Associato: **3 punti** (tre)

4.8 Soluzione per la formazione e l'aggiornamento delle risorse

Ambito	Caratteristica	Valore
Soluzione organizzativa	Il RTI ha sviluppato un processo di formazione continua basato su figure professionali dedicate (Resource Manager / Segreteria Didattica), strumenti di supporto alla pianificazione e controllo della formazione, attingendo alle migliori esperienze delle aziende costituenti il RTI	Completezza, efficacia,
Soluzione operativa	La soluzione organizzativa e tecnologica che sarà implementata dal RTI consente di garantire sia la rapida creazione di un pool di figure professionali dotate di professionalità adeguate e formate rispetto al contesto normativo, organizzativo e tecnologico dell'Amministrazione, sia la formazione continua sulle evoluzioni tecnologiche, organizzative e normative, mediante strumenti on-line o mediante formazione in aula, realizzata con un processo di rotazione di risorse che consente di non generare impatti sui servizi erogati nel rispetto dei giorni minimi di formazione da erogare	Efficacia, stabilità dei livelli di servizio

4.8.1 Formazione ed aggiornamento delle risorse

Le esigenze di formazione e aggiornamento delle risorse su contratti quali SPC, assumono una particolare importanza per via della durata del Contratto e della sua ampiezza. Per garantire la formazione e l'aggiornamento continuo e tempestivo delle risorse impiegate il RTI, attraverso le aziende che lo compongono, si è dotato di procedure e strumenti atti a garantire non solo il continuo aggiornamento tecnologico delle risorse (competenze, metodologie, strumenti, modalità operative), ma anche la continuità e la disponibilità delle competenze per far fronte sia ad esigenze di ampliamento dei gruppi di lavoro, sia per fronteggiare eventuali turnover.

Tabella 21: Tipologie di esigenze formative su Contratti complessi di lungo periodo

Formazione per introduzione di nuove risorse	Formazione per risorse già allocate al Contratto
Necessità di Ampliamento Necessità di Sostituzione	Adeguamento / Evoluzione tecnologica Necessità ad hoc (esigenze specifiche / locali)

Il RTI dedica particolare attenzione anche alla fase preliminare alla formazione, ovvero all'efficace identificazione delle risorse adeguate all'erogazione dei servizi previsti ed alla pianificazione anticipata del loro impiego. Ciò permette infatti di minimizzare il Gap di Formazione necessario alla presa in carico dello stesso ed i relativi tempi

di inserimento, potendo prevedere sessioni massive dedicate alle informazioni specifiche (modalità operative, metodologie, piano di comunicazione, aggiornamento sull'avanzamento, ruoli e responsabilità, strumenti di progetto, etc.).

A seguire saranno descritti il processo e la soluzione organizzativa adottati per garantire la formazione e l'aggiornamento continuo per le risorse professionali interessate.

4.8.2 Il modello di gestione Organizzativa ed Operativa

Allo scopo di garantire la disponibilità di risorse opportunamente formate ed aggiornate rispetto sia al contesto del cliente sia alle tecnologie previste nell'erogazione dei servizi professionali, il RTI si doterà di un processo integrato di gestione organizzativa ed operativa di formazione delle risorse impiegate, come rappresentato nella Figura 56.

In particolare: le aziende costituenti il RTI (1) dispongono di unità dedicate alle funzioni di Learning & Development (L&D). Tali unità sono responsabili del processo formativo interno tramite il quale le singole aziende hanno formato e formano le Figure Professionali (2) che vengono messe a disposizione del RTI per la costituzione di un pool specializzato (3) per l'erogazione dei servizi ai clienti.

Le competenze rappresentate nel pool ed i processi di gestione ed evoluzione delle stesse sono gestiti da un Resource Manager, dedicato allo specifico pool e dotato di una sua Segreteria Didattica (4), che dispone di alcune applicazioni – raccolte in una piattaforma di "Knowledge Assurance" (5) - che consentono la gestione delle competenze (Skill Inventory), la pianificazione e gestione dei corsi, la verifica ed evidenza della formazione effettuata (Value learning). Il Resource Manager gestisce il processo continuo di formazione (6) utilizzando la piattaforma di Knowledge Assurance per garantire l'identificazione delle necessità di formazione delle singole risorse, la pianificazione degli interventi - con appropriata rotazione delle risorse o con funzioni di "distance learning" così da non pregiudicare i livelli di servizio previsti per la fornitura, sia nell'ambito del centro servizi che per le risorse on premise - la tracciatura e verifica della formazione on-line ed in aula. La piattaforma sarà anche utilizzata dal Responsabile dei Servizi (7), di concerto con il Resource Manager, per effettuare la migliore scelta delle risorse da allocare alla gestione di uno specifico servizio presso una specifica Amministrazione cliente e per controllare la rotazione delle risorse per formazione. Le informazioni relative alla formazione ed aggiornamento professionale saranno rese disponibili, su richiesta, all'Amministrazione ed alla Committente mediante report.

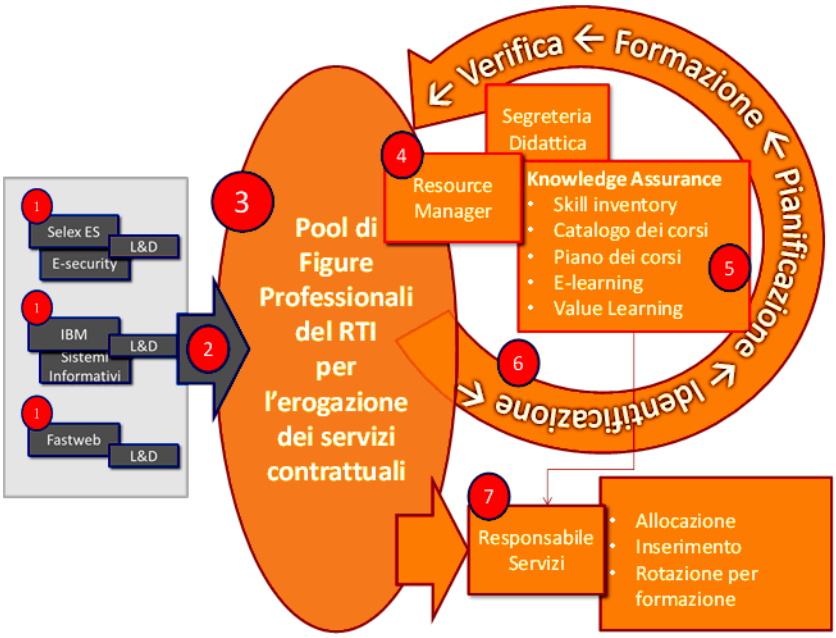


Figura 56: Modello del processo di Resource management

4.8.3 Il funzionamento della Soluzione Organizzativa ed Operativa

Le aziende del RTI adottano un sistema di gestione delle competenze professionali (**Skill Management**) secondo standard e direttive delle specifiche aziende, che prevede la classificazione delle figure professionali sulla base di ruolo/competenze e seniority. Lo Skill Management è strettamente correlato ai Piani di Certificazione professionale, ed alle partnership tecnologiche multi-vendor che coprono le principali tecnologie esistenti presso le Pubbliche Amministrazioni; traccia i percorsi formativi di crescita, segue i percorsi di sviluppo e le esperienze progettuali delle risorse.

La soluzione organizzativa ed operativa proposta dal RTI prevede la messa a disposizione delle informazioni di Skill Management ad una funzione di **Resource Management del RTI**, all'interno di una base dati centralizzata (**Skill Inventory** - sviluppata dalla mandataria Selex ES) tramite la quale sia possibile identificare il pool di figure professionali da ingaggiare sulla base di competenze, certificazioni, esperienze, know-how, posizione geografica per il coinvolgimento nelle sedi periferiche dell'Amministrazione, e consolidare le migliori sinergie organizzative. La base dati conterrà inoltre **l'inventario delle competenze di ogni singolo Contratto Esecutivo**, costruito durante

la fase di presa in carico effettuando una rilevazione, per ogni ambito applicativo di interesse, le funzionalità, le tecnologie, le metodologie e gli aspetti organizzativi specifici. La funzione di Resource Management, con la collaborazione del Responsabile Tecnico e dei Responsabili dei Servizi del Contratto Esecutivo, gestirà centralmente le politiche di inserimento nel pool, gestione delle risorse, allineamento ed adeguamento delle competenze e conoscenze delle risorse sulla base delle esigenze contrattuali, con la responsabilità della pianificazione e dell'utilizzo ottimale delle risorse nell'ambito di ogni Contratto

Tale gestione centralizzata **assicura la crescita, il mantenimento, le sinergie delle competenze messe a disposizione dei Contratti Esecutivi** e contribuisce inoltre a ridurre eventuali emergenze in termini di personale, gestendo in modo efficace i picchi di richieste o altre attività non pianificabili, garantendo un'efficace operatività in tempi immediati di risorse aggiuntive o ausiliarie già formate sui processi, tecniche e tecnologie in uso presso il singolo Contratto Esecutivo.

La funzione di Resource Management sarà coadiuvata da una **Segreteria Didattica** che avrà la funzione di organizzazione logistica delle attività, gestione dei dati relativi alle iscrizioni ai corsi ed alle metriche, la raccolta e l'elaborazione dei questionari, ecc.

Il RTI valorizzerà modalità di formazione alternative, continue e di grande rapidità ed efficienza basate, ad esempio, su **pillole formative** per specifici aggiornamenti fruibili anche in mobilità via podcast, streaming, ecc. nonché su altri **strumenti di condivisione** (piattaforme di e-learning, sistemi di audio-video conferencing, condivisione del desktop, ecc.) già disponibili nei singoli Processi di Formazione delle Aziende costituenti il RTI (ad es: le opportunità di formazione derivanti dai **Centri di Competenza** propri o dei **Partner** tecnologici ed industriali delle aziende costituenti) ed altri strumenti specifici eventualmente previsti dal Contratto o disponibili presso le Amministrazioni. Prevedrà pertanto l'impiego, allo scopo di massimizzare l'efficacia della formazione garantendo la stabilità dei livelli di servizio previsti per la fornitura, di un **ampio spettro di modalità di progettazione ed erogazione** dei percorsi formativi, così come già adottato nei singoli Processi di Formazione Aziendale inclusi corsi in aula, seminari, blended e, vista l'estensione temporale del contratto, anche rotazione per **"Training on the job"** nell'ambito dello stesso Contratto Quadro o su contratti assimilabili e significativi.

Fase di presa in carico a inizio fornitura

Nella fase di **Fase di presa in carico** a inizio fornitura dei servizi e sistemi oggetto di fornitura il RTI, prevede l'impiego **da subito di figure professionali specializzate altamente qualificate**, selezionate in base alle **tematiche funzionali e tecniche** da affrontare e con professionalità e cultura tali da assicurare un rapido apprendimento delle materie oggetto di servizio, con pluriennali esperienze maturate presso le principali Amministrazioni Pubbliche Centrali e Locali ed Enti Pubblici. Tali competenze ed esperienze consentiranno la costituzione, già dalle fasi iniziali dell'Appalto, di un team di lavoro di esperti che potranno svolgere anche **Ruolo di Tutor**, permettendo un efficace orientamento per tutte le nuove risorse inseribili nel team.

Fase di erogazione della fornitura

Nella fase di erogazione dei servizi e sistemi oggetto di fornitura, l'RTI definirà di volta in volta i moduli formativi, gli strumenti formativi, e le collaborazioni più idonee sulla base degli specifici gap da colmare, per la risorsa destinataria e per il servizio o progetto che la risorsa è chiamata ad erogare. Il processo di formazione delle risorse sarà svolto con tempi e modalità che non avranno **alcun impatto sullo svolgimento delle attività contrattuali** e la soluzione **non pregiudicherà quindi in alcun modo i livelli di servizio** previsti. La formazione sarà infatti sviluppata per consentire una semplice ed efficace rotazione delle risorse, soprattutto nel caso di formazione di **risorse impegnate su servizi on premise**, grazie alla modularità del processo formativo; il catalogo dei corsi sarà suddiviso in 3 aree principali:

1. Corsi per la conoscenza dei servizi progettuali e dei servizi operativi del RTI;
2. Corsi per la conoscenza del contesto operativo e tecnico dell'amministrazione cliente;
3. Corsi per aggiornamento continuo su ambienti e tecnologie relative all'erogazione dei servizi professionali.

A tal fine il 100% delle risorse del pool effettuerà i corsi dell'area 1, un numero di risorse pari al 20% al fabbisogno della singola Amministrazione effettuerà i corsi dell'area 2, mentre i corsi dell'area 3 saranno seguiti dai singoli specialisti sulla base del loro specifico dominio di esperienza.

4.8.3.1 Valutazione dell'efficacia e dell'attuazione del piano formativo

Requisito fondamentale per l'attività di formazione è la **qualità della formazione erogata e fruita** che sarà valutata sostanzialmente in termini di incremento delle conoscenze, delle capacità e delle competenze delle risorse in base alle esigenze specifiche.

Tale risultato verrà perseguito con metodologie appropriate volte a misurare l'efficacia degli interventi formativi. L'introduzione di meccanismi di feedback strutturati (colloqui e interviste strutturate, osservazioni attive, somministrazione di questionari e test, …) creerà un flusso di informazioni in grado di monitorare il ritorno formativo sia nel breve (report puntuali del formatore e schede di valutazione) che nel medio periodo (verifiche di apprendimento sul campo, monitoraggio dello sviluppo delle competenze individuali). Le attività di verifica consentiranno di monitorare con cadenza programmata l'avanzamento del processo di acquisizione delle conoscenze e competenze ed effettuare azioni di rimodulazione e reindirizzamento delle attività formative.
La funzione di **Resource Management** implementerà una base dati centralizzata (**Value Learning**- sviluppata dalla mandataria Selex ES), per la raccolta di tutti i dati e le informazioni di dettaglio relative allo svolgimento delle attività formative ed alla rilevazione dei risultati. Sarà così possibile produrre con periodicità costante, tipicamente al termine della fase di presa in carico e poi con cadenza trimestrale, appositi **report e statistiche** contenenti tutta una serie di informazioni quantitative e qualitative, in forma analitica e sintetica, tali da consentire all'Amministrazione la più ampia **possibilità di verifica e validazione** del buon esito delle attività di formazione-addestramento erogate in ogni singolo Contratto Esecutivo

4.8.3.2 Giorni minimi di formazione proposti per ciascuna risorsa impiegata

La tabella seguente riporta il numero di giorni minimi di formazione proposti per ciascuna risorsa impiegata che il RTI prevede annualmente per l'aggiornamento delle competenze professionali del proprio personale, impiegato negli Contratti Esecutivi oggetto dell'Accordo Quadro.

Tabella 22: Giorni minimi di formazione

Modalità didattiche	*Risorse di governance e di coordinamento*	*Figure professionali per i servizi progettuali*	*Figure professionali per i servizi continuativi*
Corsi in aula e blended **Seminari** **Training on the job**	1	6	6
Self training **Corsi on-line**	1	6	6
TOTALE	2	12	12

4.8.4 Esempio del catalogo formativo

Nelle tabelle seguenti viene fornita, a titolo esemplificativo e non esaustivo, un'ipotesi di massima del catalogo formativo previsto per le risorse professionali che l'RTI metterà a disposizione delle Amministrazioni, con la definizione delle finalità e degli strumenti distinti per servizi e/o risorse.

Tabella 22: Area 1 – Conoscenza dei servizi progettuali ed operativi

Risorse	*Finalità*	*Strumenti*
Risorse dei gruppi di lavoro per i servizi progettuali	Aggiornamento e formazione volto agli aspetti prettamente tecnici e metodologici essenziali per l'espletamento della Fornitura (es. metodologia di erogazione e consuntivazione) Aggiornamento e formazione di tipo tematico, finalizzato all'ampliamento e, ove necessario, all'apprendimento delle conoscenze normative e legislative sulle materie di competenza delle varie aree applicative previste	• Self training con documentazione • Corsi (on-line, in aula e blended) • Training on the job, affiancamento ai gruppi operativi • Seminari tenuti da consulenti esperti
Risorse dei gruppi di lavoro per i servizi continuativi	Aggiornamento e formazione volte ad aspetti prettamente tecnologici e metodologici essenziali per l'espletamento della Fornitura; Presa in carico di nuovi obiettivi progettuali; Strategie di cambiamento ed innovazione di strumenti a supporto della erogazione dei servizi;	• Self training con document. • Corsi (on-line, in aula e blended) • Training on the job, affiancamento ai gruppi operativi

Tabella 23: Area 2 – Conoscenza del contesto operativo e tecnico dell'amministrazione cliente

Scopo	*Contenuti*	*Strumenti*
Contesto organizzativo: conoscere l'organizzazione del Committente, dell'Amministrazione e le	• Organizzazione dell'Amministrazione.	• Self training con doc

interazioni con RTI	• Interazione con il Committente • Pianificazione e rendicontazione • Adempimenti contrattuali. Livelli di servizio e indicatori di qualità
Contesto funzionale ed operativo: conoscere le metodologie, gli standard e le modalità operative adottate dal Committente e dall'Amministrazione	• Funzionalità offerte dai servizi • Metodologie, standard, strumenti • Modalità operative, di accesso ed uso
Sessione Contesto architetturale e tecnologico: conoscere le principali architetture e tecnologie di riferimento per il Committente e l'Amministrazione	• Architetture e configurazione dei sistemi • Interazioni e i flussi di scambio con eventuali altre aree funzionali

Area 3 – Aggiornamento continuo su ambienti e tecnologie per l'erogazione dei servizi professionali

La formazione specialistica delle risorse impiegate coprirà gli ambiti **applicativi, tecnologici ed infrastrutturali di tutti i servizi oggetto dell'Accordo Quadro** e, inoltre, tutti gli **ambiti normativi di riferimento** per la gestione delle **Identità Digitali** e la **Digitalizzazione della Pubblica Amministrazione** (es.: SPID, CAD, Agenda Digitale, ecc.).

5 QUALITÀ

5.1 Miglioramento degli indicatori di qualità

Il 'RTI propone i miglioramenti agli indicatori di qualità descritti nella tabella seguente.

Indicatore di Qualità	Miglioramento della soglia/valore	Punteggio tecnico associato
RTO (IQ07)	< 4 (quattro) ore	**4**
RPO (IQ08)	< 1 (una) ora	
IQ12a – "Tempo di risoluzione problemi di priorità 1"	Miglioramento del 1% (uno percento)	**1**
IQ15 – "Uptime dei servizi oggetto di fornitura e degli strumenti a supporto"	Miglioramento del 0,02% (zero virgola zero due percento).	**1**
Totale Punteggio tecnico associato		**6**

5.2 Monitoraggio e governo della fornitura

L'obiettivo del modello di Governance proposto dal RTI è quello di garantire, sia dal punto di vista operativo che amministrativo, **efficacia ed efficienza** nel presidio dei servizi erogati, **monitorando costantemente** il raggiungimento dei KPI previsti e dando attuazione a tutte le **azioni correttive e migliorative** affinché siano finalizzate alla massima soddisfazione da parte degli utilizzatori dei servizi.

La soluzione che il RTI propone prevede che il governo dell'intero Contratto Quadro sia demandato al **Comitato Direttivo RTI** (cfr. § 3.2.2.1), funzione organizzativa rappresentante tutte le aziende costituenti il RTI, che lavora in conformità al quadro metodologico basato su COBIT, ITIL e PMI come anticipato nei precedenti capitoli.

A supporto delle attività di monitoraggio e governo, il RTI adotterà una soluzione informatica, integrata ed allo stato dell'arte, che prevede, oltre ai componenti richiesti dal capitolato, anche ulteriori elementi distintivi tra cui piattaforme di Collaboration, di Portfolio Management e di eLearning/Knowledge Management. Il RTI ritiene di poter fornire un curriculum di competenze di alto livello su queste tematiche, grazie alle esperienze maturate in contratti quadro similari (cfr. tabella a lato).

Principali esperienze RTI
SPC Lotto 1
S-RIPA
Convenzione Consip Manutenzione Centrali Telefoniche (CT6 Lotto 2)
Convenzione Consip Fonia e connettività IP (TF4)
DigitPA SPConn (Sistema Pubblico di Connettività)
Convenzione SCR Piemonte

5.2.1 Razionali della proposta

Per il monitoraggio e governo della fornitura il RTI prevede i razionali descritti in Tabella 23:

Tabella 23: Razionali della proposta del RTI.

Ambito	Caratteristica	Valore
Modello di Governance	Il RTI prevede **un modello di Governance** nel quale il Responsabile Contratto Quadro, le funzioni a Staff del Comitato Direttivo RTI e i Responsabili dei Contratti esecutivi hanno il compito di monitorare l'andamento complessivo del Contratto Quadro e dei Contratti Esecutivi, con ruoli e responsabilità precise (cfr. §.5.2.2).	Completezza Coerenza
Framework	Il RTI prevede un **Framework Operativo** che ha l'obiettivo principale di garantire efficacia	Efficacia

operativo	ed efficienza nel presidio dei servizi erogati e di monitorare costantemente il raggiungimento dei KPI, sia dal punto di vista operativo che amministrativo grazie al quale i processi di gestione e controllo della fornitura ed in particolare dei servizi/progetti integrano aspetti di Gestione della Qualità, Project Management e Gestione del Rischio, garantendo una visibilità sistematica ed organica di tutti i punti critici (cfr. § 5.2.3).	
Sistema Integrato di Governo e Gestione della Fornitura	Il RTI rende disponibili, in un unico ambiente integrato (cfr. § 5.2.4): ►**Portale di Governo e Gestione della Fornitura;** ►**Cruscotto sull'andamento dei servizi erogati**; ►**Sistema di Gestione Documentale.** La soluzione include anche i seguenti strumenti che il RTI ritiene indispensabili ai fini della completezza ed efficacia della soluzione offerta: ►**Componente di Project Portfolio Management (PPM)**; ►**Piattaforma integrata di Knowledge Sharing**.	Disponibilità di strumenti Efficienza

5.2.2 Soluzione organizzativa

In coerenza con quanto previsto dal Capitolato, il RTI propone un modello di *Governance,* mutuato dal Sistema di Qualità della Mandataria*,* nel quale **il Responsabile Contratto Quadro** e **le funzioni a Staff (Comitato Direttivo di RTI)** hanno il compito di:

- **monitorare l'andamento complessivo** del Contratto Quadro e dei Contratti Esecutivi;
- supportare a 360° le Amministrazioni nella fase di redazione del Piano dei Fabbisogni, anche nell'ottica di impostare un percorso condiviso ed efficiente per la **pianificazione delle attività**;
- verificare con le Amministrazioni, laddove richiesto, le **priorità di realizzazione** di Obiettivi e/o Interventi nell'ottica di ottimizzare il bilanciamento delle risorse (servizi) sin dalla fase di set-up ed eventualmente rimodulare, anche in corsa, l'impegno delle stesse durante la fase di esecuzione degli interventi;

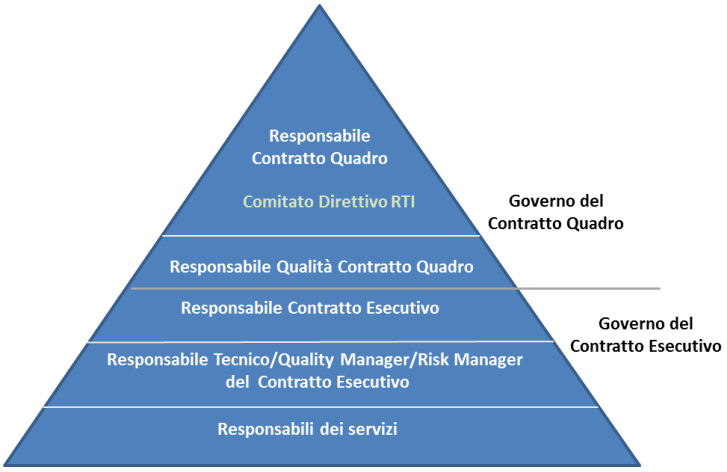


Figura 57: Stakeholder monitoraggio e controllo

- instaurare un rapporto trasparente con le Amministrazioni, attuando politiche di condivisione e di proattività — sia rispetto alle modalità di erogazione dei servizi che alle modalità di monitoraggio della fornitura — che siano propositive nei confronti dei vari Stakeholder (il RTI diventa **business partner** dell'Amministrazione).

Nel corso dell'erogazione della fornitura, il Responsabile Qualità per il Contratto Quadro, e i Quality Manager per i Contratti Esecutivi, pianificheranno degli audit interni alla Fornitura allo scopo di verificare la conformità della stessa ai requisiti espressi nella documentazione contrattuale, nel Piano della Qualità generale e di ogni altro documento di riferimento specificato.

La pianificazione, l'esecuzione e la rendicontazione degli audit saranno condotti in accordo alle procedure del Sistema di Gestione Qualità della mandataria , che definiscono le modalità e le relative responsabilità per la gestione Audit Interni, in accordo alla norma UNI EN ISO 19011.

Di seguito vengono descritti gli attori principali previsti dal modello organizzativo proposto dal RTI (cfr. §. 3.2.2) ed il loro contributo al monitoraggio e governo della fornitura.

Tabella 24: Gli attori previsti nel modello organizzativo.

Governo del Contratto Esecutivo
Responsabili dei Servizi: forniscono al Quality Manager del proprio Contratto Esecutivo dati di sintesi e informazioni di dettaglio relative all'andamento del proprio servizio.
Risk Manager: supporta il Responsabile del Contratto Esecutivo nell'identificare e gestire i potenziali rischi associati alla fornitura dei servizi oggetto del proprio contratto per prevenirli, mitigarli e monitorarli.
Quality Manager: supporta il Responsabile del Contratto Esecutivo nella gestione degli aspetti di qualità relativi agli specifici servizi oggetto del Contratto Esecutivo (indicatori, SAL, ecc.). Interagisce e riporta al Responsabile della Qualità a livello di Contratto Quadro.
Responsabile Contratto Esecutivo: si allinea di norma con cadenza settimanale con il Comitato Direttivo di RTI con l'obiettivo di mantenere informato il Responsabile del Contratto Quadro e le funzioni di staff rispetto all'andamento dei servizi oggetto del contratto stesso, eventuali scostamenti dei livelli di servizio e azioni volte a gestire (mitigare o sfruttare)

eventuali rischi futuri. Convoca SAL di allineamento interno al RTI di contratto esecutivo con cadenza settimanale e SAL con cadenza almeno mensile o secondo le tempistiche concordate/definite con la PA contraente.

Governo del Contratto Quadro

Comitato Direttivo RTI: coordinato dal **Responsabile del Contratto Quadro**, si riunisce con cadenza almeno mensile per la verifica degli andamenti dei contratti utilizzando il Portale di Governo per le verifiche sui dati aggregati dei contratti.

Responsabile Qualità: coordina la raccolta della reportistica contrattuale (consuntivo attività e risorse, rilevazione indicatori di qualità, SLA) e di servizio (volumi, utilizzo dell'infrastruttura, altri indicatori). Pianifica ed effettua le azioni di audit interno al RTI e condivide con il Responsabile del Contratto Quadro e con le Amministrazioni Beneficiarie le misure e le regole per la rilevazione dei Livelli di Servizio. Utilizza il Cruscotto sull'andamento dei servizi erogati (cfr. §. 5.2.4)

5.2.3 Framework operativo

Nel Framework Operativo proposto nella Figura 58, i processi di gestione e controllo della fornitura, ed in particolare dei servizi/progetti, integrano aspetti di Gestione della Qualità, Project Management e Gestione del Rischio, garantendo una visibilità sistematica ed organica di tutti i punti critici dei diversi Contratti Esecutivi.

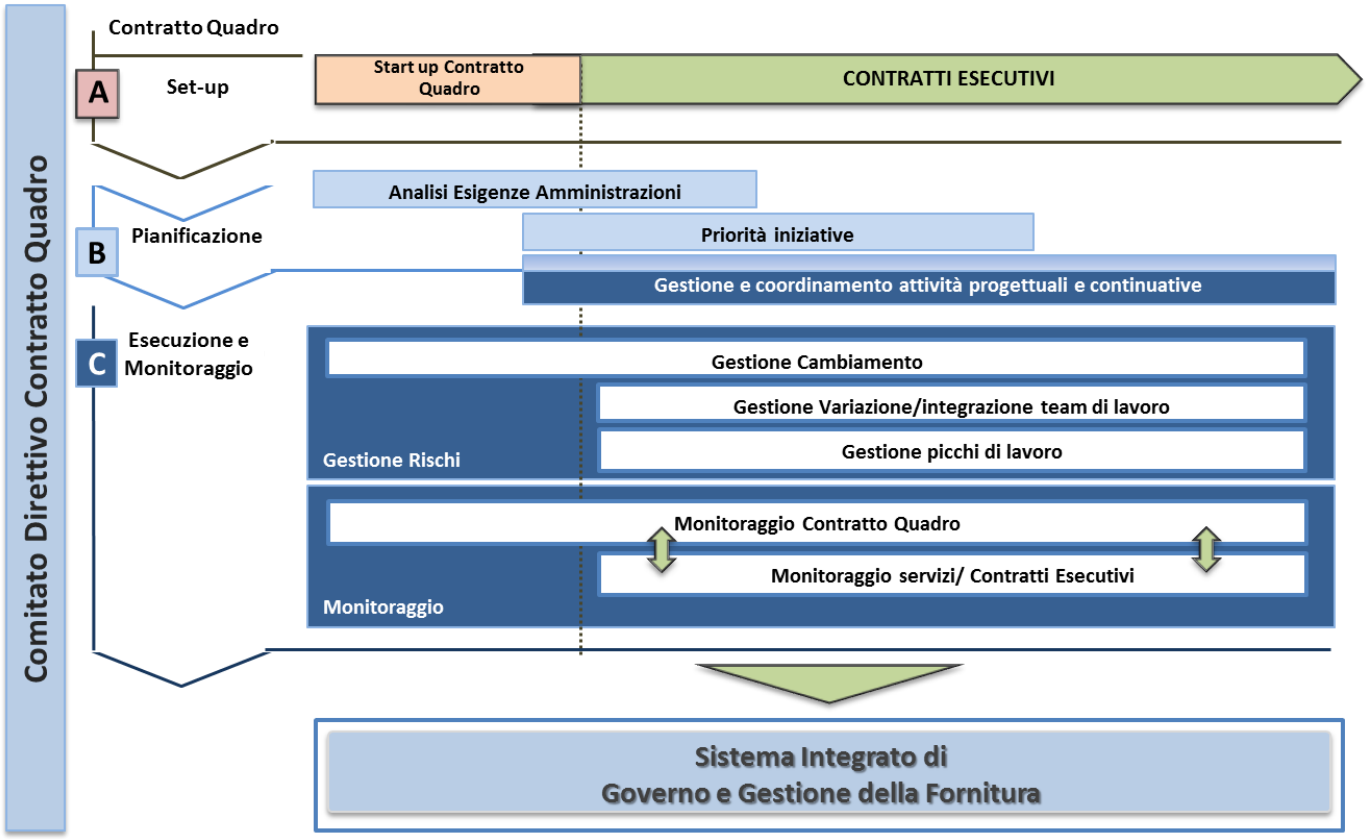


Figura 58: Framework Operativo per il governo e il monitoraggio.

Il contesto metodologico nel quale saranno erogati i servizi, e in particolare i processi di governo sia del Contratto Quadro sia dei Contratti Esecutivi, è un insieme collaudato ed utilizzato con successo dalla Mandataria di metodi e processi in grado di assicurare efficacia ed efficienza nell'esecuzione e governo delle attività, garantendo al contempo l'adattabilità al contesto, flessibilità operativa e il monitoraggio costante del raggiungimento dei KPI previsti.

FASE A – SETUP

Nella fase A di setup il RTI realizzerà il framework operativo per il governo e il monitoraggio del Contratto Quadro e, all'acquisizione dei contratti esecutivi, quello per il governo e il monitoraggio dei singoli Contratti Esecutivi.

Start up del Contratto Quadro

La Fase di Start up del Contratto Quadro verrà avviata dal RTI sin dalla fase di presa in carico, in modo da essere operativo sin dalla stipula del Contratto Quadro.

Contratti Esecutivi

All'acquisizione di ogni Contratto Esecutivo il RTI attiverà il framework in Figura 58 per il governo e il monitoraggio sia dei servizi con modalità di erogazione **Continuativa** (rif. ITIL). sia per quelli **in modalità progettuale**

(scomposizione delle attività progettuali in Fasi) per garantire il monitoraggio dinamico della qualità della fornitura:

- condivisione della scelta degli indicatori addizionali
- della modalità di misura,
- del sistema di monitoraggio e rendicontazione.

In ciascuna fase del ciclo di erogazione del servizio sono dettagliati, tra l'altro: ►obiettivi e fasi dell'attività di Program/Project Management; ►strumenti (software e non) a supporto delle suddette attività di Program/Project Management e di esecuzione dei servizi; ►**modalità operative di monitoraggio della fornitura**; ►strumenti e relative modalità di archiviazione, aggiornamento e storicizzazione dei *deliverable* progettuali.

FASE B – PIANIFICAZIONE

Contestualmente alla fase di set-up il Comitato Direttivo di RTI—prima—e il Responsabile del Contratto Esecutivo—poi—procederanno a:

- rilevare/integrare le esigenze dell'Amministrazione nell'ottica di aiutare a definire compiutamente e a mantenere sempre attuale il Piano dei Fabbisogni;
- aiutare a definire livelli di priorità delle singole iniziative costituenti gli specifici obiettivi/interventi.

Nella fase di pianificazione, gli obiettivi/interventi prioritari potranno essere schematizzati attraverso Project Charter, formalizzando così le finalità, l'organizzazione, i vincoli e le regole progettuali che dovranno regolare le interazioni tra tutti gli attori. A completamento di ciò si procede alla formale **identificazione, quantificazione e mitigazione dei Rischi.**

Da subito, poi, dovranno essere definite le **Regole di governo dei servizi**, in coerenza alle linee guida previste dal Contratto Quadro, dallo specifico Contratto Esecutivo e dal Piano di Qualità, rispetto alle modalità di approvazione dei deliverable, alla definizione delle modalità di gestione delle eventuali varianti in corso d'opera ed alla modalità di intervento a fronte di criticità/urgenze.

FASE C – ESECUZIONE E MONITORAGGIO

Il processo di monitoraggio, proposto dal RTI, prevede:

- **il monitoraggio della Fornitura** nel suo complesso (monitoraggio del Contratto Quadro);
- **il monitoraggio dei singoli Contratti Esecutivi** (anche individuando e concordando con l'Amministrazione eventuali indicatori addizionali per ogni contratto).

Nell'ambito del **monitoraggio del Contratto Quadro e dei Contratti Esecutivi**, il RTI ha la responsabilità:

- della gestione continuativa dei contratti, garantendo il presidio delle informazioni e dei documenti a supporto.
- della prevenzione e gestione dei rischi: ogni rischio individuato sarà condiviso con l'Amministrazione, monitorato e revisionato, nel corso dell'erogazione del servizio, attraverso opportune azioni di mitigazione;
- della gestione del cambiamento: ciascuna modifica, indipendentemente dalla sua origine, correzione o evoluzione, sarà valutata per definirne l'impatto, la fattibilità, la soluzione tecnica e le modalità di esecuzione/realizzazione;
- del monitoraggio dei servizi in termini di volumi, dati economici e raggiungimento degli obiettivi fissati sia di risultato che di qualità.

Di seguito viene presentata una tabella con i principali output del monitoraggio RTI nelle diverse fasi del ciclo di vita del Contratto Quadro.

Tabella 25: Principali output del monitoraggio RTI nelle diverse fasi del ciclo di vita del Contratto Quadro

Fasi del ciclo di vita del Contratto Quadro	Output Monitoraggio RTI	Committenza e Benefici
Stipula Contratto Quadro	Consegna documenti previsti alla stipula entro 30 gg per quanto concerne il Documento Programmatico della Sicurezza.	**Consip**, **AgID**
Monitoraggio Dati Economici	• Fatturato globale • Ordinato • Consumo Medio • …	**Consip** – Evidenza in tempo reale di Forecast e Consuntivo a livello di CQ e CE.

Proposizione Servizi alle PA	Numero Richieste adesioni al Contratto Quadro a livello geografico, numero e tipologia PA richiedenti, numero iniziative di supporto alla redazione Piano dei Fabbisogni.	**Consip** – Evidenza dell'andamento in tempo reale del Contratto Quadro in termini di richieste da parte della PA
	Richieste servizi dalla PA in termini di aderenza agli obiettivi e linee guida di AgID	**AgID** – Verifica e rispetto degli indirizzi standard, linee guida e metodologie in termini di sicurezza, procedure e standard.
	Numero richieste assistenza aspetti amministrativi e contrattuali propedeutiche alla stipula dei Contratti Esecutivi, …	**Referenti Amministrazioni per aspetti amministrativi** – stato di avanzamento richieste PA.
Supporto al Piano dei Fabbisogni Redazione Progetto dei Fabbisogni	Numero iniziative aperte per supporto alle PA per tipologia di Servizio richiesto, stato avanzamento, …	**Consip**, **AgID** – Evidenza attività PA in corso
Redazione Progetto dei Fabbisogni	• Andamento redazione progetto fabbisogni richiesto. • Numero Progetti di Fabbisogno in lavorazione e stato avanzamento.	**Responsabile Procedimento Amministrazione** – Stato avanzamento Progetto dei Fabbisogni
Contrattualizzazione Contratti Esecutivi	• Numero Progetti di Fabbisogno approvati, in corso di stipula e conclusi. • Adesioni al Contratto Quadro a livello geografico, numero PA sottoscrittrici dei Contratti Esecutivi, totale ammontare contratti, valore del consuntivato, tipologia di PA sottoscrittrice, servizi attivati (tipologia e quantità), percentuale sul volume complessivo del Contratto Quadro, valori economici dei consuntivi rispetto al Piano dei Fabbisogni. • Adesioni al Contratto Quadro con periodo di riferimento, numero contratti chiusi, numero contratti aperti • Report di Contratto Quadro sull'andamento indicatori aggregato per tipologia di servizio, tipologia PA, tipologia rilievo,… • Rendicontazioni, avanzamenti contrattuali, revisioni contrattuali, …	**Consip** – Evidenza andamento Contratti in corso di contrattualizzazione e stipulati verso il RTI
Erogazione Contratti Esecutivi	• Report sull'andamento KPI e SLA di dettaglio per contratto esecutivo per tipologia di servizio, numerosità dei rilievi sul contratto, numero di turn-over del personale, ecc. • Report Rendicontazioni, avanzamenti contrattuali, revisioni contrattuali, … • Valori economici dei consuntivi rispetto al Piano dei Fabbisogni, eventuale massimale contrattuale (canone), ecc. • Stato di Avanzamento dei Lavori per ciascun Contratto Esecutivo …	**Consip**, **Amministrazione** – Evidenza andamento Contratto Esecutivo
Phase Out Contratto Quadro	• Andamento Contratti Esecutivi di cui effettuare il phase out. • Rendicontazione con frequenza da concordare (es. settimanale) sul phase out dei singoli Contratti Esecutivi.	**Consip**, **AgID** – Stato della fase conclusiva del Contratto Quadro. Dettaglio phase out su singolo Contratto.

Uno degli obiettivi principali del monitoraggio è il **miglioramento continuo della fornitura**: evidenziare trend negativi in modo da individuare, con largo anticipo, possibili scostamenti (o non conformità) e garantire l'attivazione delle opportune azioni correttive/preventive e/o di miglioramento della soluzione informatica e della sua gestione, revisione degli strumenti di controllo, indici di valutazione ed eventualmente corrispettivi economici; questo è un punto fondamentale in quanto è qui che verranno, in particolare, prese quelle azioni che consentiranno di invertire "trend" che vanno verso lo sforamento dei KPI.

Ad esempio nel caso in cui si rilevi un incremento nel tempo dell'indicatore IQ 13 (Numerosità richieste riaperte) il RTI metterà in atto, prima del superamento della soglia, delle azioni volte ad incrementare la quantità

e la qualità della Knowledge Base a disposizione degli operatori oppure valuterà l'utilizzo di ulteriori strumenti a supporto degli stessi oppure ancora, se necessario, il ricorso all'ampliamento del numero delle risorse.
Questo con l'obiettivo di anticipare efficacemente eventuali "sofferenze" da parte del RTI nell'erogazione dei servizi.

Customer Satisfaction	**Principali attività del processo di monitoraggio**
Fondamentale, ai fini del modello di Governance proposto, è la Customer Satisfaction che il RTI propone come ulteriore misura della qualità dei servizi offerti, rappresentata dal risultato del confronto tra ciò che l'Amministrazione ritiene che il Fornitore debba offrire (Qualità Attesa) e quanto la stessa Amministrazione ritiene di avere realmente ricevuto (Qualità Percepita). La rilevazione (tramite questionari, interviste, ritorni dell'Help Desk) e la valutazione della Qualità Percepita, relativamente al servizio erogato, consente, quindi, di determinare la percezione che il Cliente ha del servizio ricevuto. Il processo proposto in coerenza con lo standard UNI 11098 (linee guida per la rilevazione della soddisfazione del cliente) prevede: ►Individuazione, con il coinvolgimento dell'Amministrazione, di tempi, periodicità delle misurazioni e tecniche di campionatura; ►Individuazione dei modelli di analisi pertinenti i servizi erogati; ►Verifica della misura rilevata.	►**raccolta delle informazioni utili** sul monitoraggio delle lavorazioni svolte e sul controllo del rispetto dei tempi di lavorazione previsti per ogni singola fase; ►**raccolta (automatica o manuale) e caricamento dei dati elementari** nel formato e con periodicità stabilita congiuntamente all'Amministrazione; ►calcolo degli indicatori (livelli di servizio) stabiliti; ►**produzione della reportistica** di rendicontazione nei formati di maggiore diffusione (Excel, PDF, Word, ecc.) ; ►**analisi, verifica ed approvazione** del rapporto da parte del RTI, con una prima valutazione sugli andamenti. I risultati di questa analisi sono tracciati nel report insieme ai commenti ed eventuali azioni correttive. Nel caso siano presenti valori con scostamenti in negativo rispetto ai valori attesi, sarà indicata un'azione correttiva da intraprendere; ►**predisposizione della condivisione delle informazioni** fra l'Amministrazione ed il RTI, per l'anticipazione della **gestione degli eventuali scostamenti** e per la verifica della conformità dei servizi rispetto a quanto richiesto/proposto; ►pubblicazione degli indicatori sul Portale di Governo e Gestione.

5.2.4 Strumenti a supporto del governo e monitoraggio

Gli strumenti a supporto del monitoraggio della fornitura derivano dalle esperienze pregresse che i componenti del RTI hanno maturato nella gestione di forniture per la PA di entità paragonabile. Un **Sistema Integrato di Governo e Gestione della Fornitura (SIGGF)** rende disponibili—in un unico ambiente integrato e coerente—gli strumenti deputati a supportare tutti gli stakeholder. La maggior parte delle funzionalità del sistema verrà erogata su multicanale. La soluzione è **realizzata con prodotti IBM** e prevede:

Portale di Governo e Gestione della Fornitura che rende disponibile in modalità unificata ed integrata la fruizione delle funzionalità operative, di presentazione e di condivisione dei contenuti informativi su pianificazione, andamento, rendicontazione e monitoraggio dei servizi e delle attività progettuali oggetto della fornitura;
Piattaforma di SLA Management, **Business Intelligence e Reporting**, per il calcolo e la presentazione degli indicatori di fornitura (Cruscotto sull'andamento dei servizi erogati);
Sistema di Gestione Documentale per ogni esigenza di archiviazione, conservazione, indicizzazione;
Componente di **Project Portfolio Management** (PPM) per supportare il processo decisionale e la centralizzazione e condivisione del Portafoglio Progetti;
Piattaforma integrata di Knowledge Sharing: **Knowledge & eLearning Management System** per la tesaurizzazione e la condivisione delle conoscenze all'interno del RTI;
Accesso al Sistema di Trouble Ticketing Management.

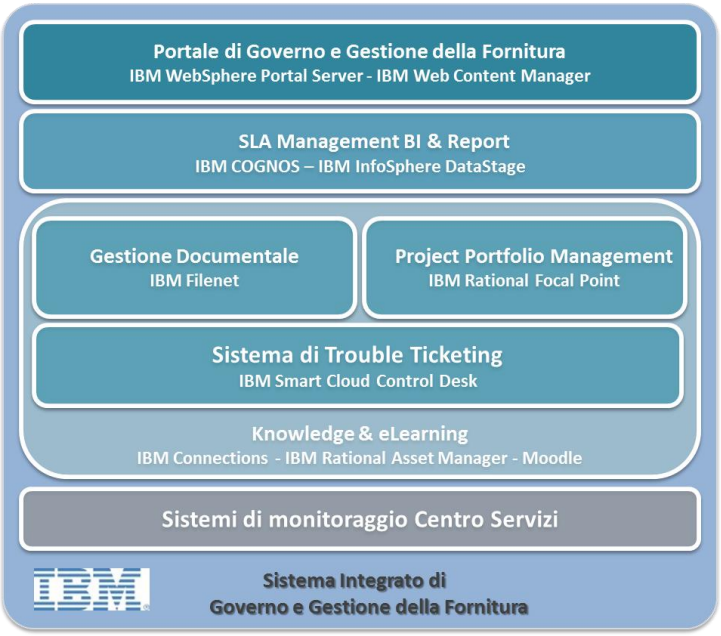


Figura 59: Sistema Integrato di Governo e Gestione della Fornitura (SIGGF)

5.2.4.1 Il Portale di Governo e Gestione della Fornitura

Il Portale di Governo e Gestione della Fornitura rappresenta lo strumento necessario per garantire la costante e puntuale condivisione della conoscenza tra i Referenti della Fornitura, le Amministrazioni e AgID/Consip; inoltre permette di potenziare la comunicazione e la relazione tra le parti coinvolte e di garantire la trasparenza nella gestione del governo della fornitura.

Oltre a ciò, fino all'attivazione dei servizi di governance sulla piattaforma delle Infrastrutture Condivise-SPC, il Portale erogherà tutti i servizi richiesti dal Capitolato generale (par. 6.1) di **SGAC**, **SGQS** e **SGPW**. In particolare le funzionalità richieste per lo SGAC verranno implementate nella sezione Documentale del Portale di Governo del RTI; per le funzionalità del sistema SGQS ci si avvarrà anche delle funzionalità rese disponibili dalla piattaforma di Business Intelligence; per le funzionalità richieste per il sistema SGPW, queste saranno erogate dallo stesso Portale di Governo.

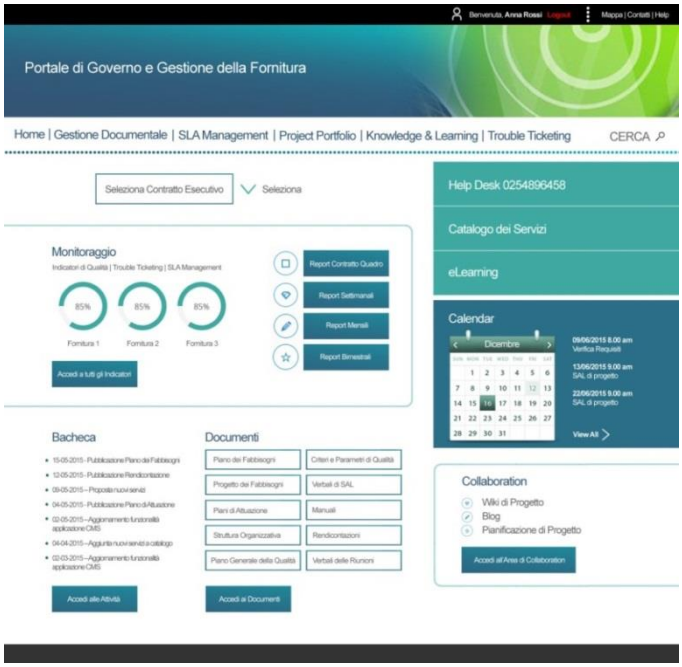


Figura 60: Mockup Portale di Governo della Fornitura

5.2.4.2 Piattaforma di SLA Management, Business Intelligence e Reporting

Il RTI propone la realizzazione di un **Cruscotto sull'andamento dei servizi** erogati avente funzione di monitoraggio continuo di tutte le attività contrattuali, al fine di garantire sia una visione di insieme dell'andamento del contratto quadro sia una visione analitica delle singole forniture previste all'interno dei contratti esecutivi.

La soluzione presentata nasce da diverse esperienze pregresse e propone **la realizzazione di un vero e proprio sistema di Data Warehouse** che ha il compito di raccogliere i dati di tutti gli obiettivi/interventi, elaborarli e prospettarli sia in maniera verticale sui singoli Contratti Esecutivi che in maniera aggregata per l'intero Contratto Quadro per porzioni di esso, permettendone la consultazione nel Portale di Governo della Fornitura.

►**Accounting**: Area funzionale in cui vengono lavorate le misurazioni dei servizi erogati. ►**Charging**: Area funzionale del data warehouse in cui vengono contabilizzati i servizi erogati. ►**Analytics & Report:** implementa la raccolta delle informazioni, la loro organizzazione e la costruzione di reportistica o cruscotti. ►**Monitoring KPI/SLA**: Area funzionale deputata alla vista sintetica sui servizi erogati con indicatori di performance (e penali) correlati ai livelli di servizio dei contratti, anche attraverso **indicatori grafici di immediata comprensione (tachimetri, semafori, serie storiche)**. Tale approccio consente una notevole flessibilità permettendo di valutare situazioni potenzialmente critiche e di produrre analisi di trend in maniera efficace ed intuitiva. Ogni report proposto potrà essere interrogato specificando la "data di osservazione" delle informazioni, potendo in tal modo visualizzare lo stato degli indicatori sia nei momenti di verifica contrattuale (definiti nel Capitolato) che in qualsiasi altro momento temporale. **Tutta la reportistica potrà essere visionata dal Portale e scaricata in formato Excel, PDF, HTML e Rich Text Format**.

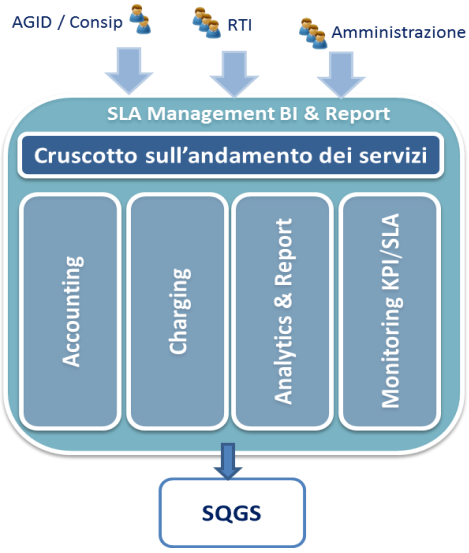
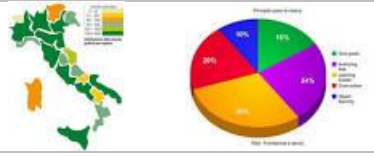
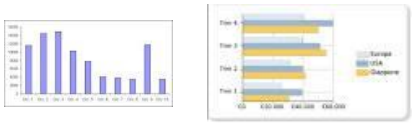


Figura 61: Cruscotto andamento dei servizi

La soluzione proposta dal RTI, come previsto da capitolato, si occuperà dell'alimentazione del sistema **SQGS**, al fine di fornire, con le tempistiche necessarie, gli indicatori necessari alla qualità.

Tabella 26: Esempio di reportistica proposto per l'analisi del monitoraggio del Contratto Quadro.

Modalità di rappresentazione	Dati prospettati
	Adesioni al Contratto Quadro a livello geografico, numero PA sottoscrittrici dei Contratti Esecutivi, totale ammontare contratti, valore del consuntivato, tipologia di PA sottoscrittrice, servizi attivati (tipologia e quantità), percentuale sul volume complessivo del Contratto Quadro.
	Adesioni al Contratto Quadro con periodo di riferimento, numero contratti chiusi, numero contratti aperti, eventuale massimale contrattuale (canone), valori economici dei consuntivi rispetto al Piano dei Fabbisogni, numerosità dei rilievi sul contratto, numero di turn-over del personale, ecc.

Le informazioni necessarie all'alimentazione del sistema sono derivate principalmente dalle seguenti fonti: ►**Sistema di Gestione Documentale** (Contratto Quadro, Catalogo Servizi, Piani dei Fabbisogni, Contratti esecutivi e servizi in essi previsti); ►**Sistema di Trouble Ticketing** (IT Service Management – cfr § 3.3.2.2.4); ►**Form** di **Data**

Entry per le informazioni prelevate da Piani di lavoro, logiche di calcolo dei KPI, penali. Per quelle informazioni su cui non è possibile avere un caricamento automatico (es. rilievi sugli obiettivi e sulla fornitura comunicati attraverso apposite lettere e note ovvero slittamenti nell'inserimento/sostituzione del personale, rilevabili da eventuali fogli presenza, e-mail, ecc.) la soluzione predispone l'uso di opportuni Form di Data Entry alimentati manualmente dal RTI.
Il RTI garantirà l'allineamento costante del Sistema alla situazione corrente. Per tale motivo, il sistema di monitoraggio sarà alimentato giornalmente con tutte le informazioni gestite con procedure automatiche e entro 7 giorni dall'evento che ha generato l'informazione per quei dati non direttamente automatizzabili.

5.2.4.3 Il Sistema di Gestione Documentale

La soluzione presentata dal RTI prevede la realizzazione di un vero e proprio sistema di Enterprise Content Management finalizzato alla raccolta centralizzata, l'archiviazione, la classificazione, la gestione e la consultazione di tutta la documentazione amministrativa ed operativa relativa al Contratto Quadro e ai Contratti Esecutivi, generata sia dal RTI sia dalle PA.
Il sistema di Gestione documentale assicura inoltre la corretta implementazione della "sequenza logica che regola i legami tra le informazioni contenute nell'anagrafica degli utenti e fornitori, nei contratti esecutivi, piani e progetti dei fabbisogni" così come richiesto da Capitolato Generale. Nei vari step contrattuali **il sistema provvederà all'invio di alert** via sms/email di opportune informative (es. all'atto della stipula Contratto Esecutivo) ai Referenti coinvolti delle Amministrazioni beneficiarie e ad Agid/Consip.
La piattaforma si articola in diversi componenti funzionali: ►Servizi di AAA, Single Sign-On tra il sistema documentale e il portale di Governo della fornitura; ►Funzioni di inserimento e classificazione dei documenti (upload) nel repository documentale; ►Gestione del versioning, check-in, check-out; ►Ricerca dei documenti per metadati e per contenuto dei documenti; ►Gestione dei workflow per l'approvazione dei documenti.

5.2.4.4 Le componenti di Project Portfolio Management (PPM)

La componente di PPM prevista dal RTI permette all'Amministrazione una visione sintetica dei propri progetti su cui si può fare "Drill Down" sui vari aspetti della realizzazione; supporta il processo decisionale attraverso la centralizzazione e condivisione delle informazioni del portafoglio IT quali esigenze, progetti, servizi, applicazioni, ecc. e semplifica la valutazione degli effetti delle decisioni attraverso semplici strumenti grafici di analisi, definizione delle priorità, roadmap e dipendenze. La componente inoltre fornisce strumenti per la pianificazione e gestione delle attività progettuali secondo paradigmi tradizionali e Agili consentendo un allineamento automatico delle informazioni a livello di portafoglio progetti e una integrazione nativa con le soluzioni per la gestione del ciclo di vita del Software per un allineamento continuo e in tempo reale di pianificazione ed esecuzione delle attività.

5.2.4.5 La componente di Condivisione della conoscenza (K&LMS)

Il sistema di condivisione della conoscenza (Knowledge and eLearning Management System (K&LMS) si basa su: ►una **Knowlegde Base centralizzata** in cui sono censite ed organizzate tutte le conoscenze (comunicazioni, informazioni, documenti, dati, ecc.); ►un **insieme di procedure** decisionali, di validazione, di comunicazione ecc.
La componente include funzionalità di *Messaggistica, Files, Wiki, Forum, Bookmark, Blog, Ideation Blog, etc.*, di gestione degli asset, offre funzionalità specifiche che favoriscono la produzione e condivisione degli asset relativi ai servizi di Lotto. La componente K&LMS prevede inoltre la piattaforma di eLearning **Moodle** al fine di effettuare l'attività di informazione e condivisione anche nei confronti delle Amministrazioni e di altri soggetti.
Il K&LMS permetterà quindi di tesaurizzare e condividere le conoscenze sia all'interno del RTI che con le PA contraenti; inoltre permetterà di erogare, a supporto delle aule, **i corsi richiesti sulle evoluzioni tecnologiche dei servizi richiesti dall'Amministrazione**.

6 DOCUMENTAZIONE COPERTA DA RISERVATEZZA

Il contenuto della presente offerta non è coperto da riservatezza.

Selex ES S.p.A. Andrea Campora	E-Security S.r.l. Andrea Biraghi	IBM S.p.A. Massimo De Lucia	Sistemi Informativi S.r.l. Carla Monguzzi	Fastweb S.p.A. Claudio Pellegrini	Fastweb S.p.A. Emidio Romano
_____	_____	_____	_____	_____	_____