Identificativo: GOVM-220298 Rev. 1.0
LDO/CYS/P/0034417/22

Data: 05/08/2022

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

Società Regionale per la Sanità

Progetto dei fabbisogni

LEONARDO
IBM
SISTEMI INFORMATIVI
An IBM Company
FASTWEB

Costituito
Raggruppamento Temporaneo di Imprese
composto da:
Leonardo S.p.A. - Cyber & Security Solutions division
IBM SpA
Sistemi Informativi srl
Fastweb SpA

	Nome e Ruolo	Firma
Autore		
	Mirco Rampazzo	
Verifica		
	Germano Matteuzzi	
Approvazione		
	Massimo Farinelli	
Autorizzazione		
	Claudio Rando	

Approvazioni Aggiuntive

Azienda	Nome e Ruolo	Firma

Lista di Distribuzione

Rev.	Data	Destinatario	Azienda
1.0	Vedi Copertina	Società Regionale per la Sanità	

Registro delle Revisioni

Rev.	Data	Descrizione delle modifiche	Autori
1.0	Vedi Copertina	Prima emissione	Mirco Rampazzo

Il Progetto dei fabbisogni si compone dei seguenti documenti:

Volume principale	Documento nel quale si intende raccogliere e dettagliare le richieste dell'Amministrazione contraente contenute nel Piano dei Fabbisogni e formulare una proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nel Contratto Quadro e nei relativi allegati.
Appendice A, Progetto di attuazione	Per ciascun servizio richiesto dal Piano dei fabbisogni, l'appendice contiene i seguenti dettagli: identificativo del servizio; configurazione (ove applicabile); quantità; costi; indirizzo/i di dispiegamento (nel caso di servizi centralizzati si riporterà il solo indirizzo della sede centrale); data prevista di attivazione; impegno delle eventuali risorse professionali previste; descrizione della struttura funzionale ed organizzativa del centro servizi, completa dei nomi e dei ruoli delle figure responsabili per ciascuno dei servizi.
Appendice B, Piano di lavoro	Appendice che contiene l'elenco delle attività/fasi previste con le relative date di inizio e fine. Tutte la fasi previste dal piano indicano gli obiettivi, i tempi necessari comprensivi delle date da garantire, i deliverable prodotti e le date di consegna.
Allegato 1, Modalità di presentazione e approvazione degli Stati di avanzamento mensili	Documento che definisce nei modi e nei tempi come sarà presentato lo stato di avanzamento dei Lavori (SAL). Da consegnarsi in fase di avvio dei lavori.
Allegato2, Documento programmatico di gestione della sicurezza dell'Amministrazione	Da consegnarsi su richiesta dell'Amministrazione
Allegato 3, Piano della qualità	Vedere piano di qualità generale, Documento [DA-7]

= questo documento

SOMMARIO

LISTA DELLE TABELLE

1 INTRODUZIONE

1.1 Ambito

Nel dicembre 2013 CONSIP ha bandito una procedura ristretta, suddivisa in quattro lotti, 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)" nota come Gara SPC Cloud. Il Lotto 2, inerente i Servizi di Identità Digitale e Sicurezza Applicativa, è stato assegnato al Raggruppamento la cui mandataria è Leonardo S.p.A. e le società mandanti sono IBM, Sistemi Informativi e Fastweb.

La durata del contratto è di cinque anni. Nell'arco di tale periodo ogni Pubblica Amministrazione potrà acquisire i servizi offerti dalle "Convenzioni" tramite la stipula di "Contratti Esecutivi" dimensionati tecnicamente in un Piano dei fabbisogni prodotto in base alle proprie esigenze.

In virtù dell'Addendum nr. 4 al Contratto Quadro DA.[1] sottoscritto tra CONSIP ed il RTI in data 26/3/2021 il Contratto Quadro è stato prorogato di ulteriori 12 (dodici) mesi sino alla scadenza al 20 luglio 2022.

Infine in virtù del DL 17 maggio 2022, n. 50 (GU Serie Generale n.114 del 17-05-2022) Art. 31-bis (Proroga di accordi quadro e convenzioni delle centrali di committenza in ambito digitale) il Contratto Quadro è stato prorogato fino al 31 dicembre 2022.

Il presente documento costituisce il progetto dei fabbisogni che comprende l'insieme di servizi e di infrastrutture tecnologiche dedicate alla sicurezza dei sistemi informativi preposti al trattamento dei dati della Pubblica Amministrazione (PA), in conformità alle esigenze dell'Amministrazione stessa espresse attraverso il proprio piano di fabbisogni. Esso raccoglie e dettaglia le richieste della *Società Regionale per la Sanità* (indicata nel documento come Amministrazione contraente o So.Re.Sa.) contenute nel proprio Piano dei fabbisogni [DA-5] in cui l'Amministrazione Contraente manifesta l'esigenza di implementare dei servizi di sicurezza che, come previsto dal Framework Nazionale di Cyber Security e Data Protection, ed alla missione 6 SALUTE del PNRR per l'ammodernamento delle dotazioni tecnologiche del Servizio Sanitario Nazionale (SSN), aumentino la protezione dei propri asset e dei propri servizi digitali ed abilitino le capacità di rilevazione e contrasto degli incidenti di sicurezza (Prevent, Detect & Respond), e descritte sinteticamente in §1.2. Successivamente si formula una proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nel Contratto Quadro "Servizi di gestione delle identità digitali e sicurezza applicativa" e nei relativi allegati.

1.2 Richieste dell'Amministrazione contraente

In questa sezione del Progetto dei fabbisogni l'RTI intende raccogliere e dettagliare le richieste dell'Amministrazione contraente espresse tramite la redazione del Piano dei fabbisogni [DA-5] e da incontri successivi in cui meglio si sono definite le esigenze.

2 RIFERIMENTI

2.1 Documenti Applicabili

Tabella 1: Documenti applicabili.

Rif.	Codice	Titolo
DA-1.	--	Capitolato Tecnico – Parte Generale "Procedura ristretta, suddivisa in 4 lotti, per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (IS SIGEF 1403)"
DA-2.	--	Capitolato Tecnico – Lotto 2 "Procedura ristretta per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (ID SIGEF 1403)"
DA-3.	--	Offerta Tecnica – Lotto 2 "Procedura ristretta per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (ID SIGEF 1403)" del 22 Dicembre 2014
DA-4.	--	Contratto Quadro – Lotto 2 "Procedura ristretta per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (ID SIGEF 1403)" del 20/07/2016
DA-5.		"Piano dei Fabbisogni" – emesso da So.Re.Sa a mezzo PEC il 28/07/2022
DA-6.		Allegato 1 – Listino prezzi - http://www.spc-lotto2-sicurezza.it/
DA-7.	EP4A56001Q01	Piano di Qualità Generale – Lotto 2 "Procedura ristretta per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (ID SIGEF 1403)"
DA-8.		Capitolato Tecnico – Lotto 2 "Procedura ristretta per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (IS SIGEF 1403)" – Appendice 3 – Capitolato Tecnico Servizio di Monitoraggio
DA-9.		Offerta Tecnica – Lotto 2 "Procedura ristretta per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (IS SIGEF 1403)" del 22 Dicembre 2014 - Appendice

2.2 Documenti di Riferimento

Tabella 2: Documenti di riferimento.

Rif.	Codice	Titolo
DR-1.		Guida al Contratto Quadro "Servizi di gestione delle identità digitali e sicurezza applicativa" - http://www.spc-lotto2-sicurezza.it/
DR-2.		Allegato 3 – Schema Progetto dei fabbisogni - http://www.spc-lotto2-sicurezza.it/

3 DEFINIZIONI E ACRONIMI

3.1 Definizioni

La seguente Tabella 3riporta tutte le definizioni adottate nel presente documento.

Tabella 3: Definizioni valide per il presente documento.

Amministrazioni	Pubbliche Amministrazioni.
Amministrazione aggiudicatrice	Consip.
Amministrazione/i Contraente/i	Pubbliche Amministrazioni che hanno siglato un Contratto di Fornitura con il Fornitore per l'erogazione di uno dei servizi in ambito dell'Accordo Quadro.
Fornitore	Vedi Raggruppamento
Modalità "As a Service"	Servizio erogato da remoto attraverso i Centri Servizi dell'RTI.
Modalità "On premise"	Servizio erogato presso le strutture dell'Amministrazione contraente o altre strutture indicate dalla stessa.
Raggruppamento	Raggruppamento Temporaneo di Impresa Leonardo S.p.A. - Cyber & Security Solutions division (nel seguito Leonardo), società mandataria, IBM S.p.A. (mandante), Sistemi Informativi srl (mandante) e Fastweb S.p.A. (mandante).

3.2 Acronimi

La seguente Tabella 4 riporta tutte le abbreviazioni e gli acronimi utilizzati nel presente documento.

Tabella 4: Lista degli acronimi.

ACL	Access Control List
AgID	Agenzia per Italia Digitale
API	Application Programming Interface
BI	Business Intelligence
CA	Certification Authority
CAD	Codice dell'Amministrazione Digitale
CE	Contratto Esecutivo
CED	Centro Elaborazione Dati
CQ	Contratto Quadro
CRL	Certificate Revocation List
CVE	Common Vulnerabilities and Exposures
DAST	Dynamic Application Security Testing
DLP	Data Loss Prevention
DHCP	Dynamic Host Configuration Protocol

DNS	Domain Name System
HSM	Hardware Security Module
HTTP	HyperText Transfer Protocol
HTTPS	HTTP Secure
IAM	Identity & Access Management
LDAP	Lightweight Directory Access Protocol
MAST	Mobile Application Security Testing
OCSP	Online Certificate Status Protocol
PA	Pubblica Amministrazione
PC	Personal Computer
PDF	Portable Document Format
PEC	Posta Elettronica Certificata
RFC	Request for Comments
RPO	Recovery Point Objective
RTI	Raggruppamento Temporaneo di Imprese
RTO	Recovery Time Objective
SAL	Stato Avanzamento Lavori
SAST	Static Application Security Testing
SPC	Sistema Pubblico di Connettività
SPID	Sistema Pubblico di Identità Digitale
URL	Uniform Resource Locator
VA	Vulnerability Assessment
WS	Web Service
XML	eXtensible Markup Language

4 DATI ANAGRAFICI AMMINISTRAZIONE CONTRAENTE

Nelle seguenti tabelle si riportano i dati anagrafici dell'Amministrazione contraente (cfr. Tabella 5) e del suo referente (cfr. Tabella 6).

Tabella 5: Dati anagrafici dell'Amministrazione contraente.

Ragione sociale Amministrazione	So.Re.Sa. S.p.A.
Indirizzo	Centro Direzionale Isola F9
CAP	80143
Comune	Napoli
Provincia	NA
Regione	Campania
Codice Fiscale	04786681215
Codice IPA	Società Regionale per la Sanità
Indirizzo mail	segreteria@soresa.it
PEC	soresa@pec.soresa.it

Tabella 6: Dati anagrafici del referente dell'Amministrazione contraente.

Referente Amministrazione	Alessandro Di Bello
Ruolo	Direttore Generale
Telefono fisso	081 2128174
Indirizzo mail	segreteria@soresa.it
PEC (SI/NO)	soresa@pec.soresa.it

5 PROPOSTA TECNICO-ECONOMICA

Nel dicembre 2013, CONSIP ha bandito una procedura ristretta, suddivisa in 4 Lotti, 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)" meglio nota come Gara SPC Cloud.
In particolare il Lotto 2 riguarda i Servizi di Identità Digitale e Sicurezza Applicativa e tale lotto è stato assegnato a Leonardo S.p.A. che è a capo di un Raggruppamento di Imprese insieme a IBM, Sistemi Informativi e Fastweb. Nel presente capitolo vengono descritti gli ambiti di offerta identificati al momento della stesura del presente progetto dei fabbisogni.
L'esigenza dell'amministrazione si traduce nel seguente catalogo di servizi:

Id Servizio	Titolo	Descrizione
L2.S3.4	VA.01	Vulnerability Assessment Esterno ed Interno
L2.S3.9	SP.01.1	Servizi di supporto per la profilazione del framework Normativo di Riferimento
L2.S3.9	SP.01.2	Servizi di supporto per la profilazione dei requisiti di sicurezza della Supply Chain
L2.S3.9	SP.02	Servizi di supporto per l'assessment ed il miglioramento della postura secondo il Framework individuato
L2.S3.9	SP.03.1	Servizi di Supporto legale per l'assessment ed il miglioramento della compliance alle norme sulla protezione dei dati personali
L2.S3.9	SP.03.2	Servizi professionali formazione e training
L2.S3.9	SP.03.3	Servizi di Supporto per implementazione di un sistema di gestione per la sicurezza delle informazioni
L2.S3.9	PT.01	Servizi di supporto per attività di Penetration Test
L2.S3.9	SP.04	Servizi di supporto per il Monitoraggio Continuativo degli Eventi di Sicurezza
L2.S3.9	SP.05	Servizio specialistico per Tuning servizio di monitoraggio continuativo
L2.S3.9	SP.06	Servizi di Managed Detection & Response
L2.S3.9	SP.07	Servizi di Cyber Threat Intelligence
L2.S3.9	SP.08	Supporto per Design e Progettazione dell'Infrastruttura Green Zone
L2.S3.9	SP.09	Supporto all'attivazione del servizio di Next Generation Firewalling
L2.S3.9	SP.10	Servizi di Protezione perimetrale NGFW
L2.S3.9	SP.11	Supporto Specialistico Cyber Security on Premise

5.1 Servizio di Vulnerability Assessment – VA.01

Il servizio consente la verifica dinamica della sicurezza dei dispositivi di rete allo scopo di identificare eventuali vulnerabilità, configurazioni di sicurezza errate, carenze sui livelli di protezione attivi che espongano il contesto ad attacchi interni ed esterni. Come richiesto nel piano dei fabbisogni, sono eseguite due scansioni annuali attivabili secondo le modalità previste, così come di seguito descritte.

5.1.1 Obiettivi del Servizio VA.01

Il servizio consente di verificare la sicurezza dei sistemi, allo scopo di identificare eventuali vulnerabilità, configurazioni di sicurezza errate, carenze sui livelli di protezione attivi che espongano il contesto ad attacchi interni ed esterni.

5.1.2 Descrizione del Servizio VA.01

Il servizio prevede una *fase di preparazione* con l'esecuzione delle attività sotto elencate:

- redazione documentale: si procede alla redazione dei due documenti di Legal Agreement (LA)1 e di Rules Of Engagement (ROE).2;
- raccolta di informazioni: fase svolta al fine di reperire il maggior numero di informazioni sulla struttura della rete, delle componenti hardware e software dei sistemi oggetto di analisi;
- individuazione delle vulnerabilità: fase svolta al fine di collezionare, tramite un set opportuno di strumenti automatizzati e correttamente configurati, una lista delle potenziali vulnerabilità note a cui potrebbero essere soggetti i sistemi analizzati;
- classificazione delle vulnerabilità: le vulnerabilità individuate saranno classificate in funzione di livelli di priorità d'intervento e saranno classificate secondo lo standard CVSS.

La *fase operativa* del servizio prevede:

- esecuzione periodica di un vulnerability assessment sull'intero spazio di indirizzamento IP (nell'arco dell'intero periodo contrattuale si prevede di portare a termine due cicli completi di vulnerability assessment);
- filtraggio dei risultati ed attività di analisi;
- individuazione delle vulnerabilità attraverso l'esecuzione di test che consentano accertarne l'impatto sui sistemi analizzati;
- assegnazione automatica delle priorità/severità ai rischi di sicurezza sulla base delle policy concordate;
- correlazione dei risultati delle fasi precedenti e la definizione del piano di rientro (remediation plan);
- produzione di reportistica di sintesi (executive summary) e di dettaglio (technical report).

L'architettura di riferimento è indicata nella **Errore. L'origine riferimento non è stata trovata.** sottostante.

[1] Il *Legal Agreement* è un atto legale stabilito tra le parti che autorizza il Red Team dell'RTI a svolgere le attività di VA.

[2] Il *Rules Of Engagement* è un documento riportante le regole d'ingaggio per lo svolgimento delle attività di VA nei confronti del dominio d'intervento nei tempi e nelle modalità ivi contenute. Il ROE fornisce le regole e i limiti cui deve aderire il Red Team che svolge l'attività, per proteggere l'Amministrazione dal rischio d'incidenti, intesi come l'interruzione accidentale del servizio o la divulgazione involontaria d'informazioni critiche per l'Amministrazione.

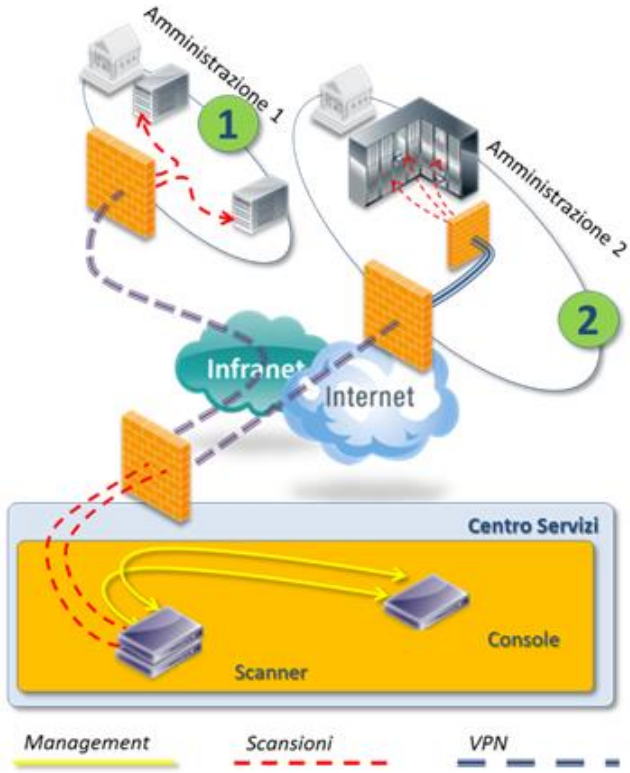

Figura 1: Architettura di riferimento per l'erogazione del Servizio L2.S3.4

A fronte di una verifica dei requisiti tecnici è possibile decentralizzare alcune componenti applicative presso il CED dell'Amministrazione contraente, per far fronte ad eventuali vincoli tecnici e/o organizzativi.

Tutte le scansioni saranno eseguite attraverso un canale sicuro instaurato tra gli apparati di sicurezza perimetrale del Centro Servizi e quelli dell'Amministrazione contraente. La **Errore. L'origine riferimento non è stata trovata.** 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, l'Amministrazione potrà optare per collegare la VPN in prossimità dei target.

5.1.3 Vincoli e assunzioni del Servizio VA.01

Affinché l'Amministrazione contraente possa usufruire del servizio è necessario che sia interconnessa direttamente alla rete del Sistema Pubblico di Connettività (SPC) — o altre strutture equivalenti individuate da Consip S.p.A. e/o dell'Agenzia per l'Italia Digitale (AgID) — attraverso uno o più Fornitori di connettività, o attraverso Enti autorizzati, in modo tale che il traffico tra il Centro Servizi e l'Amministrazione contraente avvenga all'interno di VPN sicure e configurate per supportare destinazioni multiple. In subordine dovrà comunque avere un punto di accesso a Internet.

Per l'erogazione delle attività del servizio è necessaria quindi anche la creazione di una VPN tra il Centro Servizi del Fornitore e l'Amministrazione Contraente, in mancanza della quale potrebbero non essere erogate alcune attività specifiche.

Il servizio sarà erogato a seguito della sottoscrizione da parte dell'Amministrazione contraente dei documenti redatti in fase di preparazione: Legal Agreement e Rules Of Engagement.

5.1.4 Modalità di erogazione del Servizio VA.01

Il servizio sarà erogato in modalità “as a service” da remoto a canone e con cadenza semestrale dalla firma del contratto.

Per gli SLA, dove applicabili, si fa riferimento all’Appendice 1 al Capitolato tecnico [4] “Indicatori di qualità della fornitura per il Lotto 2”.

5.1.5 Quantità e prezzi del Servizio VA.01

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati in Appendice A, secondo le esigenze espresse dall’Amministrazione contraente nel proprio Piano dei fabbisogni [DA-5].

5.1.6 Attivazione del Servizio VA.01

Si prevede l’avvio del servizio secondo i tempi definiti nell’A.3.1. Il servizio è dimensionato per n. 275 indirizzi IP che l’ Amministrazione ritiene prioritari e suddivisi in:

- Qtà 25 indirizzi IP pubblici;
- Qtà 250 indirizzi IP privati.

5.2 Servizi professionali

In questa sezione si descrivono le attività richieste dall’Amministrazione contraente e svolte come servizi professionali. In tale ambito il fornitore s’impegna ad erogare tutti i servizi descritti nel presente documento ed assicura la disponibilità delle risorse indicate per supportare l’Amministrazione contraente alla loro erogazione.

Le attività a corpo ed a task saranno erogate presso le sedi dell’Amministrazione Contraente, presso le sedi del RTI, o presso altra sede da concordare con l’Amministrazione Stessa.

Nei successivi paragrafi si fornisce l’elenco delle attività e le relative descrizioni per ciascuno dei servizi professionali richiesti.

5.2.1 Servizi di supporto per la definizione del framework Normativo di Riferimento – SP.01.1

Il presente servizio è finalizzato ad individuare un framework normativo applicabile al contesto dell’Amministrazione basandosi sugli standard utilizzati sia a livello nazionale che internazionale.

5.2.1.1 Descrizione del servizio SP.01.1

Il servizio, in linea con gli standard di riferimento, si propone di definire le opportune linee guida che la Società Regionale per la Sanità potrà adottare nei seguenti ambiti:

- *Governance*, che indirizza l’insieme delle pratiche volte a definire le politiche e l’organizzazione necessarie per poter reagire e prevenire, in maniera efficace, alle minacce di sicurezza, in modo da minimizzare l’impatto di possibili danni alle finalità istituzionali dell’Amministrazione dovuti ad incidenti di sicurezza di natura informatica.
- *Prevent*, che esprime la capacità di attuare pratiche e misure di sicurezza per la protezione delle informazioni, delle infrastrutture e dei servizi digitali presso l’Amministrazione.
- *Detect*, che esprime la capacità di individuare tempestivamente potenziali violazioni o eventi che possono influenzare o compromettere la sicurezza dell’Amministrazione.
- *Respond & Recovery*, che esprime la capacità di rispondere efficacemente ad un incidente di sicurezza e possibilmente di ripristinare i servizi impattati dallo stesso.

Nella definizione del framework si prenderanno in considerazione, oltre alla specificità dell'Amministrazione, anche i requisiti previsti dalle Misure minime di sicurezza ICT per le pubbliche amministrazioni dell'Agenzia per l'Italia digitale (AgID) e dalla normativa europea sul General Data Protection Regulation (GDPR), tutte inglobate nel Framework Nazionale sulla Cyber Security e sulla Data Protection(FNCS), emesso dal CINI (Consorzio Interuniversitario Nazionale per l'Informatica) e dalla Università Sapienza di Roma con il supporto dell'Autorità Garante per la Protezione dei Dati Personali e del Dipartimento delle Informazioni per la Sicurezza (DIS) della Presidenza del Consiglio dei Ministri, e preso come riferimento istituzionale per la cybersecurity nelle infrastrutture e organizzazioni nazionali.

5.2.1.2 Vincoli e assunzioni del servizio SP.01.1

In avvio del supporto, si dovrà provvedere alla composizione di un gruppo di lavoro misto formato da personale specialistico dell'RTI e personale dell'Amministrazione contraente, al fine di individuare gli ambiti operativi dell'Amministrazione ed individuare in tal modo i framework normativi e gli standard applicabili al contesto.

5.2.1.3 Modalità di erogazione del servizio SP.01.1

Coerentemente a quanto previsto nel Contratto per i servizi professionali (rif. Capitolato Tecnico [DA-2] par. 1.3.9 Servizio L2.S3.9 – Servizi professionali, pagg. 48–49), si precisa che la modalità di remunerazione di tali servizi è "a task". Per gli SLA, dove applicabili, si fa riferimento all'Appendice 1 al Capitolato tecnico [4] "Indicatori di qualità della fornitura per il Lotto 2"

5.2.1.4 Quantità e prezzi del servizio SP.01.1

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati in Appendice A, calcolati secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni.

5.2.1.5 Attivazione del servizio SP.01.1

Si prevede l'avvio del servizio secondo i tempi definiti nell'Appendice B.

5.2.1.6 Deliverable del servizio SP.01.1

È previsto il rilascio di un documento contenente il framework dei controlli di sicurezza individuati durante le fasi di analisi congiunta con il personale dell'Amministrazione: "Framework dei Controlli di Sicurezza".

5.2.2 Servizi di supporto per la definizione dei requisiti di sicurezza della Supply Chain - SP.01.2

Il presente servizio è finalizzato ad individuare i requisiti da applicare alla supply chain al fine di mettere in sicurezza la catena di fornitura dell'Amministrazione contraente.

5.2.2.1 Descrizione del Servizio SP.01.2

Il servizio, in linea con gli standard di riferimento, si propone di definire gli opportuni requisiti di sicurezza che la supply chain dell'Amministrazione contraente deve rispettare.

Si identificheranno quindi un insieme di requisiti/controlli di sicurezza creando un alibreria di controlli specifici per la supply chain. Tale libreria sarà formalizzata a partire da standard, best practices e framework di settore (es. ENISA, NIST, Framework Nazionale per la Cyber Security e Data Protection, ISO27001, ISO27002, IEC 62443, etc.), adattata rispetto al contesto di riferimento e riportato all'interno di un file Microsoft Excel per una più veloce e pratica fruizione.

5.2.2.2 Vincoli e assunzioni del Servizio SP.01.2

In avvio del task si dovrà provvedere alla composizione di un gruppo di lavoro misto formato da personale specialistico dell'RTI e personale dell'Amministrazione contraente, al fine di individuare gli ambiti operativi dell'Amministrazione, della sua catena di fornitura ed individuare in tal modo i requisiti di sicurezza applicabili al contesto

5.2.2.3 Modalità di erogazione del servizio SP.01.2

Coerentemente a quanto previsto nel Contratto per i servizi professionali (rif. Capitolato Tecnico [DA-2] par. 1.3.9 Servizio L2.S3.9 – Servizi professionali, pagg. 48–49), si precisa che la modalità di remunerazione di tali servizi è "a task". Per gli SLA, dove applicabili, si fa riferimento all'Appendice 1 al Capitolato tecnico [4] "Indicatori di qualità della fornitura per il Lotto 2".

5.2.2.4 Quantità e prezzi del servizio SP.01.2

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati in Appendice A, secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni [DA-5].

5.2.2.5 Attivazione del servizio SP.01.2

Si prevede l'avvio del servizio secondo i tempi definiti nell'A.3.1

5.2.2.6 Deliverable del servizio SP.01.2

È previsto il rilascio di un documento contenente i requisiti di sicurezza: "Requisiti di Sicurezza per la supply chain".

5.2.3 Servizi di supporto per l'assessment ed il miglioramento della postura cyber secondo il Framework individuato - SP.02

5.2.3.1 Descrizione del Servizio SP.02

Il presente servizio è finalizzato ad eseguire un'assessment per verificare la copertura e la maturità dei controlli di sicurezza inerenti gli ambiti identificati e riportati nell'SP.1.1:

- Governance,
- Prevent,
- Detect,
- Respond,
- Recovery.

L'assessment avrà ad oggetto ognuna delle misure di sicurezza previste, per le quali saranno rilevate le informazioni necessarie a definire lo stato di implementazione delle stesse, ivi compreso il loro livello di maturità.

L'approccio, consentirà, verificando il livello di copertura dei controlli di sicurezza definiti nel framework oggetto di SP.1.1, di avere l'indicazione del livello di maturità e la postura dell'Amministrazione contraente rispetto alle tematiche cyber.

La Figura 2 contiene una rappresentazione grafica dell'attività progettuale:

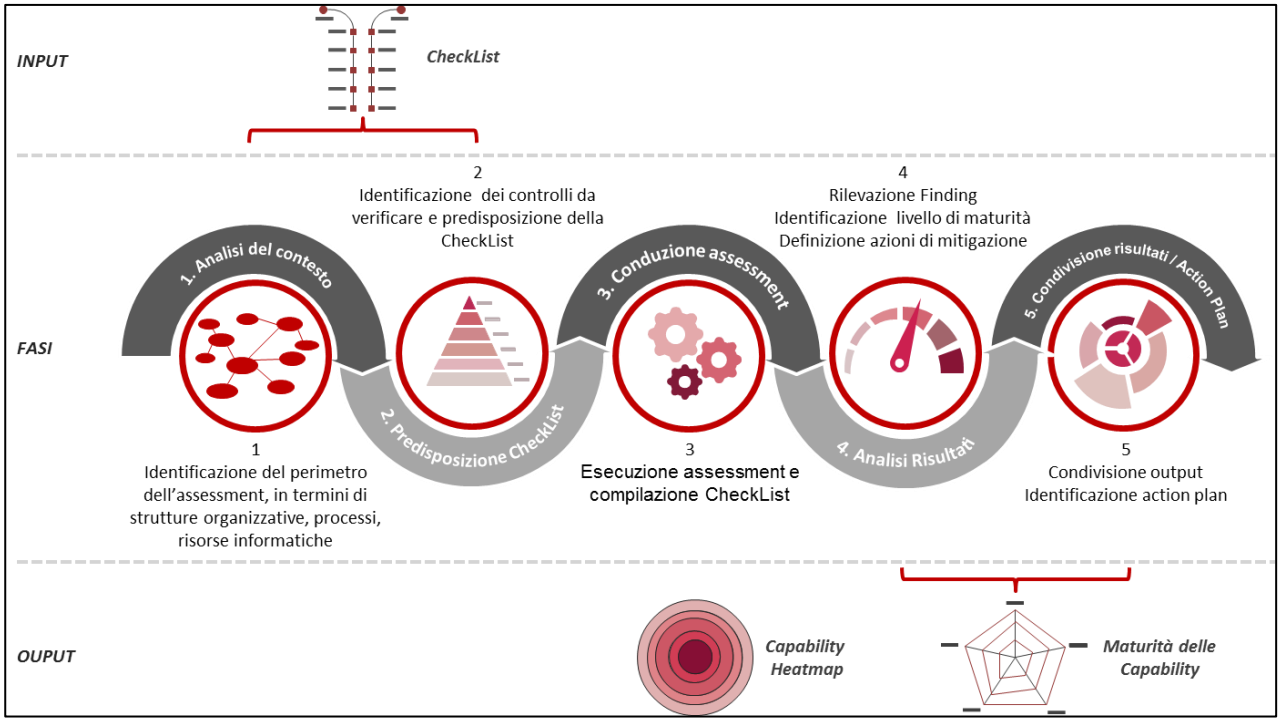

Figura 2 - Assessment maturità dei controlli di sicurezza (SP.1.1 ed SP.0.2)

L'assessment, effettuato basandosi sul Framework, definito nel SP.1.1, prevede in questa attività, una valorizzazione su 5 livelli di maturità di implementazione dei controlli, così suddivisa:

- → - Non Applicabile
- → 0 – Non Implementato;
- → 1 – Iniziale;
- → 2 – Ripetibile;
- → 3 – Definito;
- → 4 – Gestito;
- → 5 - Ottimizzato

I singoli livelli hanno la seguente interpretazione:

CRITERI GENERALI PER LA CONDUZIONE DELL'ASSESSMENT DI SICUREZZA			
Livello	Indicare l'applicabilità o il grado di maturità delle attività afferenti ai processi di sicurezza, secondo la seguente metrica:		
-	Non Applicabile	-	Il controllo non è applicabile al perimetro analizzato
0	Non Implementato	**0**	Controllo non implementato .
1	Iniziale	**1**	L'implementazione del controllo è affidata a processi, procedure e soluzioni tecniche con risultati non prevedibili, non documentati, non organizzati e spesso eseguiti ad-hoc. Il successo della gestione è affidato alle singole competenze del personale e non all'uso comprovato di processi ben definiti.
2	Ripetibile	**2**	L'implementazione del controllo si avvale di processi, procedure e soluzioni tecniche ben definiti e documentati in ciascuna o in un sottoinsieme delle funzioni dell'organizzazione coinvolte, ma in modo non consistente a livello di normativa del soggetto (ciascuna funzione gestisce i propri processi, procedure e soluzioni tecniche in modo indipendente).

CRITERI GENERALI PER LA CONDUZIONE DELL'ASSESSMENT DI SICUREZZA			
Livello	Indicare l'applicabilità o il grado di maturità delle attività afferenti ai processi di sicurezza, secondo la seguente metrica:		
3	Definito	**3**	L'implementazione del controllo si avvale di processi, procedure e soluzioni tecniche ben definiti, documentati e standardizzati a livello di normativa del soggetto. Le varie funzioni possono specializzare i propri processi, partendo da quelli standardizzati a livello di normativa del soggetto.
4	Gestito	**4**	Oltre ad includere gli aspetti del livello di maturità "Definito", sono fissati degli obiettivi quantitativi per quanto riguarda le performance dei processi, delle procedure e delle soluzioni tecniche alla base dell'implementazione del controllo. L'efficacia di processi, procedure e soluzioni tecniche è monitorata e misurata quantitativamente.
5	Ottimizzato	**5**	Oltre ad includere gli aspetti del livello di maturità "Gestito", i processi, le procedure e le soluzioni tecniche alla base dell'implementazione del controllo sono sottoposti a miglioramento continuo in risposta a cambiamenti nell'organizzazione e considerando le esperienze passate.

5.2.3.2 Vincoli e assunzioni del Servizio SP.02

In avvio di progetto si procederà alla composizione di un gruppo di lavoro misto formato da personale specialistico dell'RTI e personale dell'Amministrazione contraente, al fine di individuare le figure da coinvolgere nell'esecuzione dell'assessment e procedere ad una pianificazione di dettaglio.

Dette figure dovranno essere in grado di fornire informazioni in ordine allo stato di implementazione dei controlli di sicurezza presi in considerazione e che potranno essere di tipo logico, fisico e organizzativo.

5.2.3.3 Modalità di erogazione del servizio SP.02

Coerentemente a quanto previsto nel Contratto per i servizi professionali (rif. Capitolato Tecnico [DA-2] par. 1.3.9 Servizio L2.S3.9 – Servizi professionali, pagg. 48–49), si precisa che la modalità di remunerazione di tali servizi è "a task". Per gli SLA, dove applicabili, si fa riferimento all'Appendice 1 al Capitolato tecnico [4] "Indicatori di qualità della fornitura per il Lotto 2".

5.2.3.4 Quantità e prezzi del servizio SP.02

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati in Appendice A, secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni [DA-5].

5.2.3.5 Attivazione del servizio SP.02

Si prevede l'avvio del servizio secondo i tempi definiti nell'A.3.1

5.2.3.6 Deliverable del servizio SP.02

A seguito degli incontri/interviste verranno analizzati, gestiti ed elaborati i dati acquisiti, che avranno particolarmente valore e qualità, in quanto aggiornati allo stato dell'arte.

È previsto il rilascio di un documento contenente i risultati dell'assessment: "Report Risultati e Azioni correttive".

5.2.4 Servizi di Supporto legale per l'assessment ed il miglioramento della compliance alle norme sulla protezione dei dati personali – SP.03.1

5.2.4.1 Descrizione del Servizio SP.03.1

Il servizio prevede la valutazione ex ante -normativa, di processo e tecnica- del gap che separa un soggetto dalla conformità al GDPR e l'individuazione di un percorso di adeguamento. Nello specifico il servizio proposto si compone delle seguenti fasi:

1. **Mappatura** delle attività che comportano un trattamento di dati personali ed Assessment normativo, procedurale e tecnico (fotografia dello stato corrente) al fine di valutare la conformità al Regolamento e fornire l'indirizzamento verso le contromisure organizzative, le politiche e le procedure da adottare sulla base dei rilevamenti effettuati.
2. **Monitoraggio** dei processi di adeguamento al Regolamento.
3. **Check** di conformità al Regolamento a seguito delle azioni correttive intraprese dalla struttura.

Nel corso della durata contrattuale si intende, inoltre, fornire i seguenti servizi accessori:

- supporto nella predisposizione dei Registri delle attività di trattamento, ai sensi dell'art. 30, par. 1 e 2 GDPR;
- supporto alla mappatura dei trattamenti riferibili ai dati personali;
- valutazione della conformità e dell'adeguatezza delle informazioni contenute nei Registri delle attività di trattamento rispetto al Regolamento;
- supporto nella metodologia di costituzione dei Registri ex art. 30 GDPR; o ove richiesto, guida alla selezione e acquisizione del gold standard riferibile allo strumento tecnologico e/o applicazione finalizzata alla migliore gestione dei registri predetti.
- supporto nella predisposizione della modulistica e, nello specifico, delle Informazioni privacy relative ai trattamenti effettuati dalle singole Unit dell'ente, ai sensi degli artt. 13 e 14 GDPR.

Assessment

L'attività di *assessment* si compone delle seguenti fasi:

1. analisi dei trattamenti svolti e delle misure organizzative e tecniche di protezione dei dati personali;
2. predisposizione dell'attività di auditing finalizzati alla comprensione del contesto interno ed esterno dell'ente.
3. definizione dell'Organigramma privacy in relazione ai profili organizzativi e tecnici e definizione della supply chain;
4. eventuali ulteriori approfondimenti nel caso le informazioni non fossero sufficienti;
5. individuazione di un insieme di procedure e regole tecniche di tutela dei dati personali, di cui si consiglia la presa in carico.

Monitoraggio

La fase del monitoraggio consiste nella supervisione dei processi di adeguamento intrapresi dall'ente. Questa fase prevede un raccordo tra la cliente e il *team* di consulenti, in modo da condividere il processo di adeguamento.

Check

La fase di controllo consiste nell'osservazione delle nuove politiche messe in atto, a seguito di un apprezzabile periodo temporale, al fine di verificare gli effetti delle contromisure consigliate e poste in essere ai fini dell'adeguamento normativo e tecnico.

5.2.4.2 Modalità di erogazione del servizio SP.03.1

Coerentemente a quanto previsto nel Contratto per i servizi professionali (rif. Capitolato Tecnico [DA-2] par. 1.3.9 Servizio L2.S3.9 – Servizi professionali, pagg. 48–49), si precisa che la modalità di remunerazione di tali servizi è "a task". Per gli SLA, dove applicabili, si fa riferimento all'Appendice 1 al Capitolato tecnico [4] "Indicatori di qualità della fornitura per il Lotto 2".

5.2.4.3 Quantità e prezzi del servizio SP.03.1

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati in Appendice A, secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni [DA-5].

5.2.4.4 Attivazione del servizio SP.03.1

Si prevede l'avvio del servizio secondo i tempi definiti nell'A.3.1

5.2.4.5 Deliverable del servizio SP.03.1

Non applicabile.

5.2.5 Servizi professionali formazione e training - SP.03.2

5.2.5.1 Descrizione del Servizio SP.03.2

Il servizio prevede la messa a disposizione di contenuti formativi finalizzati alla diffusione della cultura della protezione del dato personale (particolari categorie di dati ex art. 9 e 10 *GDPR*) attraverso una **piattaforma** messa a disposizione dalla scrivente società in modo da consentire l'accesso da remoto dei dipendenti dell'organizzazione, erogare i contenuti ai discenti e **raccogliere i dati di *performance*** registrati dal sistema attraverso la somministrazione di un ***test* finale di apprendimento**.
In particolare, il programma intende approfondire la tematica attraverso i seguenti moduli:

Modulo A) Reg. Ue 2016/679 e nuovo codice *privacy*;
Modulo B) Il *Data Protection Officer*: compiti ed attribuzioni;
Modulo C) La protezione del dato sanitario: le istruzioni del Garante per la Protezione dei dati personali e del EDPB (*European Data Protection Board*);
Modulo D) Obblighi di *compliance* e profili organizzativi;
Modulo E) Valutazione e *Data Protection Impact Assessment*.

Il servizio comprende inoltre **nr. 10** sessioni formative **on site** presso il cliente da svolgersi a cura di primari professionisti operanti in ambito della tutela dei dati personali.
I contenuti interessati dall'erogazione saranno costituiti da tematiche di sicurezza quali, a titolo esemplificativo ma non esaustivo: uso sicuro dei *device* aziendali, uso di periferiche condivise, conservazione dei supporti, corretta conservazione del materiale cartaceo, uso sicuro delle credenziali per l'accesso alle VPN, *clean desk*, accesso alla rete wi-fi interna e rete ospiti, *policy* chiavi fisiche, lavoro fuori sede e *smart working*, configurazione software nei dispositivi individuali, *policy password*, istruzioni operative *mail box*, trasmissione allegati a natura riservata, ritiro dei dispositivi per perdita dei requisiti, riassegnazione dei dispositivi individuali.
Le suddette sessioni formative comprendono lo svolgimento di apposite **esercitazioni pratiche**, aventi ad oggetto la compilazione, l'implementazione e la corretta redazione del Registro delle attività di trattamento ex art. 30 GDPR, le modalità operative e le attività da svolgere per la corretta gestione di eventuali *data breach*, oltre alla individuazione e descrizione delle attività da seguire nell'ambito della prevenzione e nel caso di incidenti sui dati personali.

5.2.5.2 Modalità di erogazione del servizio SP.03.2

Coerentemente a quanto previsto nel Contratto per i servizi professionali (rif. Capitolato Tecnico [DA-2] par. 1.3.9 Servizio L2.S3.9 – Servizi professionali, pagg. 48–49), si precisa che la modalità di remunerazione di tali servizi è "a task". Per gli SLA, dove applicabili, si fa riferimento all'Appendice 1 al Capitolato tecnico [4] "Indicatori di qualità della fornitura per il Lotto 2".

5.2.5.3 Quantità e prezzi del servizio SP.03.2

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati in Appendice A, secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni [DA-5].

5.2.5.4 Attivazione del servizio SP.03.2

Si prevede l'avvio del servizio secondo i tempi definiti nell'A.3.1

5.2.5.5 Deliverable del servizio SP.03.2

Al termine del ciclo formativo, sarà messo a disposizione un **report finale** avente ad oggetto il numero degli effettivi partecipanti al corso e una statistica relativa agli esiti ottenuti.

5.2.6 Servizi di Supporto per implementazione di un sistema di gestione per la sicurezza delle informazioni - SP.03.3

5.2.6.1 Descrizione del Servizio SP.03.3

Il servizio è strumentale all'analisi dell'*as is* e all'implementazione di un sistema di gestione della sicurezza delle informazioni, nonché alla stesura di *policy* e approcci comportamentali applicabili all'infrastruttura tecnologica in linea con la fornitura di beni e servizi fruiti dall'ente attraverso le modalità amministrative consentite dalla legge.
Il servizio prevede lo svolgimento di un sistema di *audit* finalizzati all'individuazione dei Responsabili delle varie divisioni/uffici interni all'organizzazione del cliente.
Questa attività è finalizzata alla comprensione del contesto interno ed esterno all'ente relativamente ai principi finalizzati alla sicurezza delle informazioni. A seguito delle attività di individuazione dei c.d. *Referenti* per la sicurezza delle informazioni (abbreviazione "*Referenti S.I.*") il servizio prevede l'effettuazione di una rilevazione tesa all'"*identificazione e valutazione delle informazioni*", necessaria alla valutazione del sistema ***R.I.D.*** (Riservatezza, Integrità e Disponibilità delle informazioni). Detta azione prevede una serie di *audit* e un opportuno censimento di *asset*, risorse umane e procedure, anche con modalità di rilevamento a distanza oltre che *on site* ove necessità e/o ritenuto opportuno.
L'attività prevede il rilevamento dello stato di situazione in ordine alle misure di sicurezza tecniche, fisiche ed organizzative adottate da ciascuna struttura inserita nell'ambito dell'organigramma di cui all'atto aziendale approvato ed in vigore.
In particolare, il servizio si compone di **5 Step** utili all'implementazione del suddetto Sistema di Gestione.

Lo **Step 1 prevede**:

- Comprensione del contesto interno ed esterno;
- Censimento di tutte le piattaforme interne ed esterne in uso all'Ente;
- Valutazione del Sistema RID (Riservatezza – Integrità – Disponibilità).

Lo **Step 2 prevede tre sottofasi:**

- Individuazione e formazione specifica dei Referenti S.I.;
- Monitoraggio e verifica del livello di conoscenza del personale dell'azienda;
- Misurazione dell'efficacia delle procedure adottate mediante report ed elaborazione delle policy per la sicurezza delle informazioni.

Lo **Step 3 prevede** l'analisi specifica dei rischi riscontrati;
Lo **Step 4 prevede** il trattamento dei rischi riscontrati c.d. attività di *remediation*;

Lo **Step 5 prevede** il monitoraggio finalizzato al miglioramento continuo dell'implementando Sistema di Gestione per la Sicurezza delle Informazioni.

5.2.6.2 Modalità di erogazione del servizio SP.03.3

Coerentemente a quanto previsto nel Contratto per i servizi professionali (rif. Capitolato Tecnico [DA-2] par. 1.3.9 Servizio L2.S3.9 – Servizi professionali, pagg. 48–49), si precisa che la modalità di remunerazione di tali servizi è "a task". Per gli SLA, dove applicabili, si fa riferimento all'Appendice 1 al Capitolato tecnico [4] "Indicatori di qualità della fornitura per il Lotto 2".

5.2.6.3 Quantità e prezzi del servizio SP.03.3

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati in Appendice A, secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni [DA-5].

5.2.6.4 Attivazione del servizio SP.03.3

Si prevede l'avvio del servizio secondo i tempi definiti nell'A.3.1

5.2.6.5 Deliverable del servizio SP.03.3

Non applicabile.

5.2.7 Servizio di supporto ad attività Penetration Test - PT.01

Il presente paragrafo descrive il servizio professionale di Penetration Test che sarà svolto operativamente da remoto One Shot.

Le attività si compongono da un insieme di test manuali ed automatici, volti ad effettuare tentativi di intrusione sui sistemi in scope e le applicazioni concordate. Il servizio prevede strumenti on premise che sono raggiungibili da remoto tramite collegamento in VPN. Su richiesta dell'Amministrazione vengono previste attività di test anche sfruttando le vulnerabilità emerse dal servizio di Vulnerability Assessment descritto nel § 5.1.

5.2.7.1 Descrizione del servizio PT.01

Il servizio prevede l'esecuzione di test puntuali con l'obiettivo di verificare il livello di rischio associato alle vulnerabilità più critiche. Il servizio è erogato su un perimetro massimo di 2 target (host target) concordati con l'Amministrazione.

Operativamente, saranno previste le seguenti attività:

- Tentativi d'intrusione sui sistemi dell'Amministrazione, anche sfruttando le vulnerabilità identificate nell'attività di VA, quali ad esempio utenze o password deboli, uso improprio di script, bug software ed errate configurazioni;
- Tentativi di escalation dei privilegi, nel caso l'accesso ottenuto non fornisca privilegi amministrativi;
- In caso di penetrazione in un sistema, produzione delle relative evidenze al fine di dimostrare l'intrusione effettuata;
- Descrizione dei rischi esistenti relativi alle possibilità di accesso non autorizzato ai suddetti sistemi.

Le attività sono condotte applicando metodologie globalmente riconosciute come standard de-facto per la conduzione di attività di penetration test, e in particolare le metodologie OSSTMM (Open Source Security Testing Methodology Manual) e OWASP (The Open Web Application Security Project) che definiscono le modalità per la conduzione di test completi, accurati, ripetibili e verificabili.

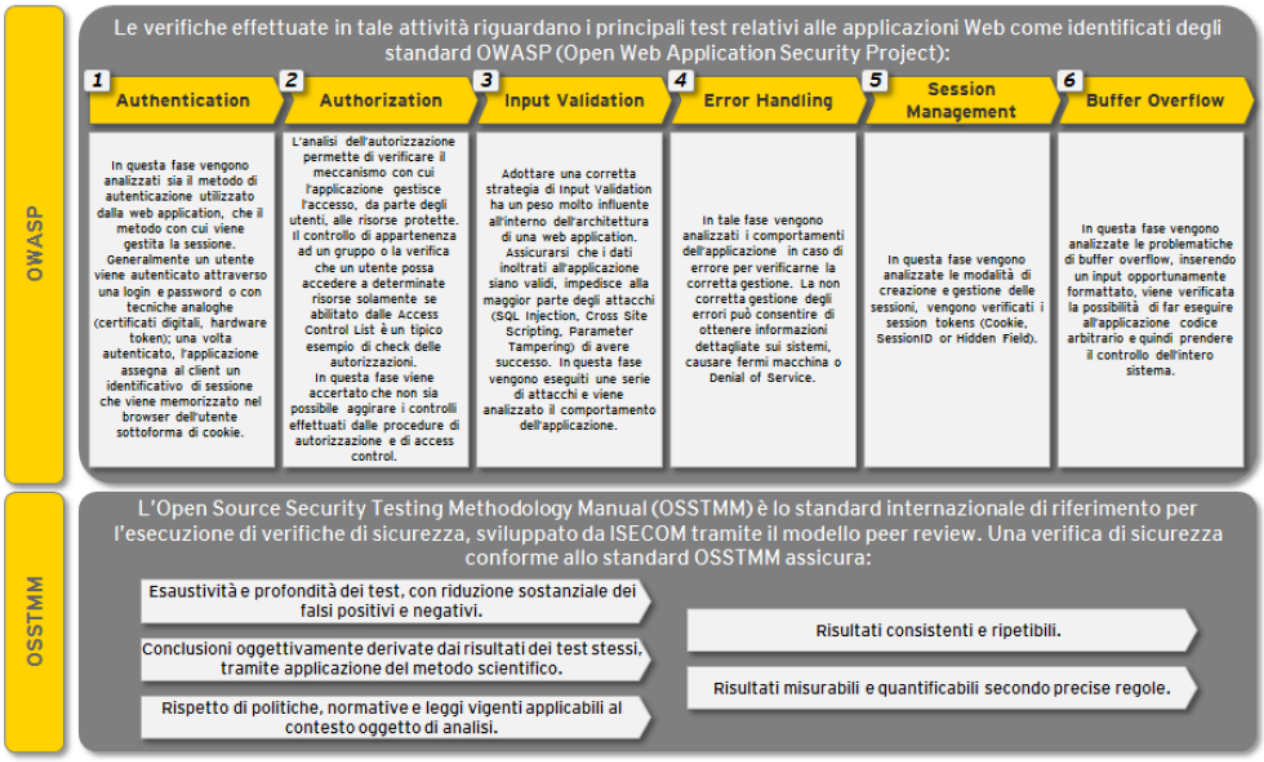

Figura 3: anteprima delle metodologie applicate per lo specifico servizio PT.1

Le verifiche di sicurezza sono effettuate dagli specialisti utilizzando postazioni di hacking appositamente configurate per tali tipologie di assessment.

Di seguito, si riportano i principali strumenti operativi utilizzati a supporto dell'attività:

Strumenti Operativi	Descrizione
NMAP	Network Mapper Tool
Metasploit	Framework di exploiting delle vulnerabilità riscontrate. Utilizzato per realizzare test intrusivi e attacchi DoS mediante l'utilizzo di exploit specifici
Database di exploit (Security Focus, CVE, PacketStorm Security)	Database pubblici di exploit utilizzabili per sfruttare le vulnerabilità rilevate.
Kali OS	Utilizzato per il cracking delle password mediante Attacchi Dizionario, Attacchi BruteForce e cracking basato su Rainbow Tables.
Burpsuite	Piattaforma integrata per l'esecuzione di VAPT di Web Application
OWASP-ZAP	Tool di VAPT per l'esecuzione di VAPT di Web Application
Strumenti sviluppati internamente	Script realizzati ad hoc per sfruttare vulnerabilità riscontrate (ad es. script utilizzati per attacchi di tipo Cross Site Scripting sulle applicazioni web)

Il fornitore si riserva la possibilità di utilizzare ulteriori strumenti alternativi.

5.2.7.2 Vincoli e assunzioni del Servizio PT.01

Affinché l'Amministrazione contraente possa usufruire del servizio, erogato verso gli host interni, è necessario che sia interconnessa direttamente alla rete del Sistema Pubblico di Connettività (SPC) — o altre strutture equivalenti individuate da Consip S.p.A. e/o dell'Agenzia per l'Italia Digitale (AgID) — attraverso uno o più Fornitori di connettività, o attraverso Enti autorizzati, in modo tale che il traffico tra il Centro Servizi e l'Amministrazione contraente avvenga all'interno di VPN sicure e configurate per supportare destinazioni multiple. In subordine dovrà comunque avere un punto di accesso a Internet tramite il quale effettuare l'attività in VPN.

La corretta erogazione del servizio è inoltre subordinata alla fornitura, da parte del cliente, di tutte le informazioni necessarie alla redazione del documento di ROE (Rules of Engagement), nonché all'accettazione della manleva opportunamente firmata dai referenti e responsabili dell'Amministrazione.

5.2.7.3 Componenti del servizio da installare presso l'Amministrazione contraente

Qualora le destination-network dell'Amministrazione siano interne (o distribuite sul territorio), il fornitore si riserva la possibilità di installare una console applicativa di Penetration Test all'interno dell'infrastruttura So.Re.Sa. al fine di erogare il servizio, remotamente, senza interruzioni o potenziali disservizi dati dalla connettività. La console sarà raggiunta dal personale del fornitore, attraverso la connessione VPN citata al § 5.2.7.2. Alternativamente l'attività verrà eseguita su indirizzamento pubblico.

In funzione della disponibilità di risorse, la console potrà essere ospitata sull'infrastruttura virtuale dell'Amministrazione contraente.

5.2.7.4 Modalità di erogazione del servizio PT.01

Coerentemente a quanto previsto nel Contratto per i servizi professionali (rif. Capitolato Tecnico [DA-2] par. 1.3.9 Servizio L2.S3.9 – Servizi professionali, pagg. 48–49), si precisa che la modalità di remunerazione di tali servizi è "a task". Per gli SLA, dove applicabili, si fa riferimento all'Appendice 1 al Capitolato tecnico [4] "Indicatori di qualità della fornitura per il Lotto 2".

5.2.7.5 Quantità e prezzi del servizio PT.01

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati in Appendice A, secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni [DA-5].

5.2.7.6 Attivazione del servizio PT.01

Si prevede l'avvio del servizio secondo i tempi definiti nell'A.3.1.

5.2.7.7 Deliverable del servizio PT.01

È previsto, al termine delle attività previste, il rilascio dei seguenti documenti:

- Technical Report di dettaglio di Penetration Test PT.01
- Executive Report di sintesi di Penetration Test PT.01
- Descrizione di un piano di rientro (remediation plan) con l'indicazione di tutte le possibili contromisure da porre in essere per eliminare le problematiche, le cause di non conformità e/o le vulnerabilità rilevate.

5.2.8 Supporto alle attività di Monitoraggio Continuativo degli Eventi di Sicurezza con Incident Handling - SP.04

Alla luce delle crescenti minacce informatiche per le organizzazioni, diventa fondamentale rivedere l'approccio alla gestione del rischio e individuare strategie per ridurre la vulnerabilità delle infrastrutture informatiche. Quindi per garantire l'adeguato livello di protezione delle reti, dei dati e dei servizi, diventa un fattore di primaria importanza l'individuazione preventiva e la gestione immediata degli incidenti di sicurezza.

In tale ottica il presente servizio effettua attività di monitoraggio continuativo per mezzo di un SOC, messo a disposizione dal Leonardo, presidiato H24 per 365 giorni l'anno e composto da un team di specialisti (analisti, system engineer, security tester e malware specialist).

Il presente servizio utilizzerà la piattaforma di Security Information and Event Management (SIEM) presente presso le infrastrutture Leonardo con attività aggiuntive di Incident Handling remoto.

5.2.8.1 Obiettivi del servizio SP.04

Il servizio viene erogato al fine di anticipare il più possibile il verificarsi di tentativi di attacco, identificando prontamente asset o eventi potenzialmente impattanti.

Il servizio consente di elaborare, correlare ed analizzare i log relativi ai differenti datasource raccolti così da identificare e tracciare l'insieme delle attività sospette rilevate dai singoli sistemi consentendo di:

- correlare e classificare gli eventi di sicurezza ICT in funzione del livello di severità della minaccia, identificando falsi positivi ed incidenti di sicurezza;
- rilevare e segnalare gli Incident ICT tramite Notification ad una opportuna *contact list* fornita da Società Regionale per la Sanità;
- eseguire un reporting accurato degli incidenti di sicurezza, individuando le vulnerabilità sfruttate e suggerendo indicazioni sulla loro risoluzione;
- attuare attività di Incident Handling da remoto (tramite il CSIRT Leonardo) limitatamente ad attività classificate su metrica ENISA per la definizione delle azioni di remediation ed erogabili remotamente con supporto dell'Amministrazione.

5.2.8.2 Descrizione del servizio SP.04

Il servizio di monitoraggio continuativo è erogato dal SOC dislocato all'interno del Centro Servizi Leonardo ed include monitoraggio, correlazione, classificazione ed analisi, nonché la notifica degli eventi di sicurezza relativi all'infrastruttura dell'Amministrazione contraente. Le componenti di servizio sono:

- monitoring & alerting;
- reporting;
- Incident Handling

5.2.8.2.1 Monitoring & Alerting

L'elemento di servizio *monitoring & alerting* viene erogato in modalità H24, per 365 giorni all'anno e prevede:

- Identificazione, ossia la fase in cui un attacco o una presunta violazione viene individuata. In particolare, gli eventi rilevati dai dispositivi di sicurezza (firewall, IDS, EDR, ecc.) sono analizzati al fine di determinare, attraverso la correlazione, se si è effettivamente in presenza di potenziali eventi di intrusione ed incidenti di sicurezza cyber.
- Classificazione degli incidenti in cui viene determinato il livello di severità (conformemente a quanto definito nel Lotto 2 della Gara SPC) e l'impatto del potenziale incidente qualora siano stati forniti in fase di Information Gathering da parte dell'Amministrazione la valorizzazione degli Asset. I

parametri considerati comprendono la tipologia/categoria di attacco (ad esempio DoS, malicious code, misuse, ecc.) e la valutazione delle criticità che riguardano i target coinvolti.

- Notifica di eventuali incidenti e altre anomalie. Stabilita la tassonomia dell'anomalia viene comunicato alle opportune strutture lo stato di allarme (con le informazioni necessarie a qualificarlo) affinché si attivi il processo vero e proprio di contrasto degli incidenti.

5.2.8.2.2 Reporting

È prevista, a seguito della rilevazione di un incidente classificato come reale, l'invio di un *technical report* che contenga tutte le informazioni utili risultanti dall'analisi dell'evento e una descrizione ad alto livello di una *remediation* applicabile.

5.2.8.2.3 Incident Handling

Vengono previste attività di Incident Handling per la definizione delle azioni di immediate relativamente al *containment, eradication e recovery* (ove applicabili), limitatamente ad attività classificate su metrica ENISA. Le attività possono innescare interventi per il governo e supporto dell'incidente informatico secondo quanto definito nei servizi e nei perimetri d'intervento concordati con So.Re.Sa.. Ulteriori analisi vengono demandate all'Amministrazione o a servizi specialistici opportuni.

5.2.8.3 Vincoli e assunzioni del servizio SP.04

Affinché l'Amministrazione contraente possa usufruire del servizio è necessario che sia interconnessa direttamente alla rete del Sistema Pubblico di Connettività (SPC) — o altre strutture equivalenti individuate da Consip S.p.A. e/o dell'Agenzia per l'Italia Digitale (AgID) — attraverso uno o più Fornitori di connettività, o attraverso Enti autorizzati, in modo tale che il traffico tra il Centro Servizi e l'Amministrazione contraente avvenga all'interno di VPN sicure e configurate per supportare destinazioni multiple. In subordine dovrà comunque avere un punto di accesso a Internet.

Per l'erogazione delle attività del servizio è necessaria quindi anche la creazione di una VPN tra il Centro Servizi del Fornitore e l'Amministrazione Contraente, in mancanza della quale potrebbero non essere erogate alcune attività specifiche.

La configurazione oggetto dei servizi di monitoraggio fa riferimento al perimetro dell'Amministrazione contraente. Il dimensionamento dell'architettura utilizzata sarà in grado di gestire *fino a 500 EPS di picco* dei datasource infrastrutturali raccolti. In caso di ampliamento del perimetro/sistemi oggetto di servizio è necessario prevedere un adeguamento dell'offerta economica al fine di coprire gli EPS aggiuntivi. Il SOC è in grado di operare una verifica giornaliera della media EPS del cliente.

Il RTI garantisce esclusivamente l'accesso ad un sistema di interazione e comunicazione (NGS) sviluppato internamente sul quale il cliente potrà verificare lo stato degli incident ed avere informazioni sugli stessi.

In relazione all'integrazione dei datasource, il protocollo/formato preferibile è syslog/CEF per tutte le log source. Qualora questo non sia utilizzabile (vedi sistemi Windows) si renderanno necessarie alternative quali la configurazione di WinRM oppure l'installazione di un agent indipendente (come Snare in versione free ad esempio) oppure di un agent dedicato dipendente dal SIEM (alcuni esempi: RSA NetWitness Endpoint Insights, Splunk Universal forwarder). Non vengono previste integrazioni di sorgenti e/o servizi che non sono nativamente supportati dal sistema SIEM in termini di connettori.

5.2.8.4 Modalità di erogazione del servizio SP.04

Il servizio sarà erogato in modalità «as a service», presso la sede del fornitore. Di seguito viene riportata una tabella relativa alle finestre di servizio:

Tabella 7: Finestre di servizi

Attività	Disponibilità

Attività	Disponibilità
Help Desk (telefonico)	9:00–18:00 dal lunedì al venerdì (escluso festività nazionali)
Help Desk (telematico)	H24
Monitoraggio di sicurezza delle piattaforme	H24
Monitoraggio di disponibilità delle piattaforme	H24

5.2.8.5 Quantità e prezzi del servizio SP.04

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati in Appendice A, secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni [DA-5].

5.2.8.6 Attivazione del servizio SP.04

Si prevede l'avvio del servizio secondo i tempi definiti nell'A.3.1.

5.2.8.7 Deliverable del servizio SP.04

È prevista, a seguito della rilevazione di un incidente classificato come reale, l'invio di un technical report che contenga tutte le informazioni utili risultanti dall'analisi dell'evento e una descrizione ad alto livello di una remediation applicabile.

5.2.9 Supporto specialistico per Tuning del servizio di Monitoraggio Continuativo - SP.05

I servizi professionali richiesti al Fornitore sono finalizzati a supportare la Società Regionale per la Sanità nel *tuning* del servizio di monitoraggio continuativo per tutta la durata contrattuale. Le attività sono organizzate, secondo quanto previsto per il servizio descritto nel § 5.2.1 e sono finalizzate ad eseguire un tuning specifico sulle piattaforme di erogazione del servizio stesso.

5.2.9.1 Vincoli e assunzioni del servizio - SP.05

Affinché l'Amministrazione contraente possa usufruire del servizio è necessario che sia interconnessa direttamente alla rete del Sistema Pubblico di Connettività (SPC) — o altre strutture equivalenti individuate da Consip S.p.A. e/o dell'Agenzia per l'Italia Digitale (AgID) — attraverso uno o più Fornitori di connettività, o attraverso Enti autorizzati, in modo tale che il traffico tra il Centro Servizi e l'Amministrazione contraente avvenga all'interno di VPN sicure e configurate per supportare destinazioni multiple. In subordine dovrà comunque avere un punto di accesso a Internet.

I parser saranno scritti per la presa in carico di tecnologie integrabili esclusivamente tramite protocollo syslog.

5.2.9.2 Modalità di erogazione del servizio - SP.05

Coerentemente a quanto previsto nel Contratto per i servizi professionali (rif. Capitolato Tecnico [DA-2] par. 1.3.9 Servizio L2.S3.9 – Servizi professionali, pagg. 48–49), si precisa che la modalità di remunerazione di tali servizi è "a task". Per gli SLA, dove applicabili, si fa riferimento all'Appendice 1 al Capitolato tecnico [4] "Indicatori di qualità della fornitura per il Lotto 2".

5.2.9.3 Quantità e prezzi del servizio - SP.05

Il fornitore s'impegna a erogare tutti i servizi descritti nella presente offerta e la disponibilità delle risorse per supportare l'Amministrazione contraente per gli scopi sopra dichiarati.

5.2.9.4 Attivazione del servizio - SP.05

Si prevede l'avvio del servizio secondo i tempi definiti nell'A.3.1.

5.2.9.5 Deliverable del servizio - SP.05

La specifica di qualsiasi documento prodotto durante l'esercizio del servizio sarà condiviso di volta in volta con l'Amministrazione in base alle attività effettuate.

5.2.10 Servizi di Managed Detection & Response - SP.06

Nel presente paragrafo è descritto il servizio professionale di supporto alle attività di Managed Detection & Response (MDR) e di seguito rappresentate:

- Ridurre al minimo le possibili finestre d'esposizione a eventuali attacchi informatici per gli endpoint in perimetro (con agent installato);
- Remediation automatica (ove applicabile) per gli incident riconosciuti come "veri positivi" ed a criticità massima;
- Endpoint protetti anche in assenza momentanea di connessione ad internet (dipendente dal tipo di soluzione tecnologica già presente su So.Re.Sa.);
- Possibilità di isolare dalla rete endpoint compromessi conservandone il controllo dalla piattaforma in cloud internet (in funzione del tipo di soluzione tecnologica già presente su So.Re.Sa.);
- Protezione in tempo reale da attacchi sconosciuti e che non utilizzano metodologie e/o indicatori noti internet (limitatamente alle caratteristiche della soluzione tecnologica impiegata);

5.2.10.1 Descrizione del servizio SP.06

Il servizio MDR è erogato dal SOC di Leonardo ed utilizzerà l'attuale soluzione presente presso l'infrastruttura So.Re.Sa.. Pertanto non include le licenze e la gestione degli Endpoint, la cui distribuzione ed installazione non è oggetto del presente servizio.

La gestione centralizzata della soluzione viene fatta attraverso una piattaforma di management resa disponibile con utenze amministrative da So.Re.Sa. e presente su cloud. Tale piattaforma di fatto raccoglie tutte le informazioni di telemetria (metadati) inoltrate dagli agent installati sugli endpoint dell'Amministrazione tramite opportuno collegamento Internet, subordinata alla visibilità continuativa necessaria fra agent e piattaforma di management (e non oggetto della presente fornitura).

Il servizio è erogato as a service ed include un monitoraggio continuativo con finestra di servizio H24 per 365 giorni con notifica degli eventi ritenuti di interesse per l'Amministrazione attraverso il portale di Leonardo NGS, che garantisce discrezionalità nelle comunicazioni e negli accessi.

5.2.10.2 Vincoli e assunzioni del servizio SP.06

Affinché l'Amministrazione contraente possa usufruire del servizio è necessario che sia interconnessa direttamente alla rete del Sistema Pubblico di Connettività (SPC) — o altre strutture equivalenti individuate da Consip S.p.A. e/o dell'Agenzia per l'Italia Digitale (AgID) — attraverso uno o più Fornitori di connettività, o attraverso Enti autorizzati, in modo tale che il traffico tra il Centro Servizi e l'Amministrazione contraente avvenga all'interno di VPN sicure e configurate per supportare destinazioni multiple. In subordine dovrà comunque avere un punto di accesso a Internet.

Per l'erogazione delle attività del servizio è necessaria quindi anche la creazione di una VPN tra il Centro Servizi del Fornitore e l'Amministrazione Contraente, in mancanza della quale potrebbero non essere erogate alcune attività specifiche.

5.2.10.3 Modalità di erogazione del servizio SP.06

Il servizio sarà erogato in modalità as a service, ed utilizzerà la soluzione attualmente presente presso So.Re.Sa. per un numero massimo di 250 endpoint.

5.2.10.4 Quantità e prezzi del servizio SP.06

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati in Appendice A, secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni [DA-5].

5.2.10.5 Attivazione del Servizio SP.06

Si prevede l'avvio del servizio secondo i tempi definiti nell'A.3.1

5.2.10.6 Deliverable del servizio SP.06

Non applicabile.

5.2.11 Servizio di Cyber Threat Intelligence (Early Warning, Data Breach) - SP.07

I servizi di *cyber threat intelligence*, richiesti da Società Regionale per la Sanità nel proprio Piano dei fabbisogni, sono erogati attraverso l'utilizzo di una soluzione tecnologia proprietaria Leonardo, dislocata fisicamente presso il proprio Centro Servizi e che consente l'erogazione delle seguenti tipologie di servizio:

- *Early Warning*
- *Data Breach Discovery*

Le capacità di *cyber threat intelligence* offerte mediante il presente servizio professionale garantiscono una maggiore efficacia dei servizi di monitoraggio di sicurezza descritti al § 5.1.6, grazie alla verifica continua su fonti aperte di eventuali nuove vulnerabilità e/o possibili vettori di attacco che possano impattare l'infrastruttura dell'Amministrazione.

5.2.11.1 Obiettivi del servizio SP.07

I modelli di servizio hanno come obiettivo quello di rilevare e individuare nuove vulnerabilità, indicatori di compromissione ricavati dall'analisi di recenti attacchi informatici, informazioni sottratte illecitamente e/o pubblicate in rete senza autorizzazione. Il servizio è inoltre orientato a fornire conoscenza riguardo attori malevoli operanti in contesti illeciti piuttosto che ad evidenziare elementi di contesto potenzialmente utili a prevenire o mitigare azioni informatiche malevole.

5.2.11.2 Descrizione del servizio SP.07

Il servizio è strutturato da una piattaforma software (Threat Intelligence System - TIS), che è in grado di elaborare in tempo reale grandi quantità di dati grazie al supporto di un'infrastruttura di High Performance Computing (HPC) e da analisti dell'Intelligence Operation Centre, collocato presso il Centro Servizi dell'RTI e attivo H16x7, che svolgono analisi di dettaglio e contestualizzano gli allarmi di sicurezza da notificare all'Amministrazione contraente.

5.2.11.2.1 Early warning

La componente di servizio *Early Warning* ha lo scopo di acquisire, da fonti aperte, elementi informativi tali da individuare nuove vulnerabilità applicative. L'obiettivo è quello segnalare tempestivamente agli operatori impiegati nella sicurezza delle infrastrutture le vulnerabilità rilevate, al fine di prevenire attacchi informatici che sfruttano *malware* idonei ad operare sulle tecnologie in uso presso l'Amministrazione.

Le principali caratteristiche e funzionalità offerte riguardano:

- integrazione di *feed* esterni di sicurezza, potenziando in tal modo le capacità native della piattaforma tecnologica proprietaria;
- monitoraggio in tempo reale delle fonti aperte per la ricerca di possibili nuove vulnerabilità informatiche non ancora note;
- motore di cross correlazione per analizzare le informazioni raccolte rispetto all'elenco delle tecnologie in esame;
- generazioni di *report* basati sulle configurazioni definite.

L'erogazione del servizio prevede una fase di avvio e una fase di esecuzione (gestione, mainteinance e miglioramento continuativo).

Durante la **fase di avvio** sarà attivata un'istanza dedicata del servizio di *Early Warning* sul sistema di *Cyber Threat Intelligence*, sulla quale verranno eseguiti i processi di analisi che realizzano il servizio specifico. Inoltre verrà abilitato un portale Web dedicato (*TIS Disclosure*) ad accesso sicuro sul quale saranno rese disponibili le interfacce per la consultazione dei risultati individuati. In questa fase vengono acquisiti i dati utili all'avvio del servizio e viene concordata con l'Amministrazione contraente la *technology list* per il contesto specifico di osservazione.

Una volta terminata la fase di avvio il servizio entra nella **fase esecutiva**, durante la quale ci si avvarrà in modo intensivo degli *analisti di intelligence* del Centro Servizi dell'RTI che, a partire dalle evidenze fornite dalla piattaforma, estenderanno l'ambito di investigazione al fine di individuare tutti i possibili elementi sensibili eventualmente presenti sulle fonti aperte. In questo modo sarà possibile controllare in modo continuo la rete e generare, di conseguenza, allarmi in base alle evidenze individuate.

All'emergere di informazioni di particolare rilevanza per l'Amministrazione sarà redatto un *Intelligence Allert* ed un *Intelligence Report* con il quale il Centro Servizi dell'RTI segnalerà tempestivamente e con il

dovuto dettaglio le evidenze rilevate e suggerirà eventuali misure da adottare per la risoluzione della problematica. Le due tipologie di deliverable conterranno informazioni relative a:

- categoria di interesse;
- severità;
- data di rilevazione
- Traffic Light protocol - TLP
- dettaglio degli elementi raccolti e dei risultati delle analisi effettuate;
- indicazioni di eventuali raccomandazioni da porre in essere per la risoluzione del «case».

5.2.11.2.2 Data Breach Discovery

La componente di servizio denominata *Data Breach Discovery* ha lo scopo di rilevare attività che mirano a trafugare dati e/o divulgare e rendere pubbliche informazioni da parte di soggetti non autorizzati, relativi a target di interesse, attraverso il monitoraggio continuativo della rete (*surface e deep/dark web*).

Le principali caratteristiche e funzionalità riguardano:

- controllo continuo in tempo reale di fonti aperte alla ricerca di elementi di interesse quali, ad esempio, indirizzi e-mail, documenti, nomi macchina ecc., citati o individuati all'interno di determinate aree della rete;
- generazione di allarmi in base alle evidenze derivanti dall'analisi dei dati;
- produzione di report basati sulle evidenze derivanti dall'analisi dei dati.

L'erogazione del servizio prevede una fase di avvio e una fase di esecuzione (gestione, mainteinance e miglioramento continuativo).

Durante la **fase di avvio** sono definiti, assieme ai referenti individuati dall'Amministrazione, i parametri di configurazione necessari a caratterizzare i *topic d'interesse* e le modalità di condivisione delle informazioni individuate. In particolare, in questa fase sarà attivata un'istanza dedicata sul sistema di *Cyber Threat Intelligence*, sulla quale verranno eseguiti i processi di analisi che realizzano il servizio specifico. Inoltre verrà abilitato un portale Web dedicato (*TIS Disclosure*) ad accesso sicuro sul quale saranno rese disponibili le interfacce per la consultazione dei risultati individuati.

In fase di avvio del servizio sono previste le seguenti attività:

- *assessment* per la raccolta dei requisiti (*information gathering*) che di fatto consistono, a titolo puramente esemplificativo e non esaustivo, in interviste al personale coinvolto e/o referente per l'attività di *cyber threat intelligence* dell'Amministrazione contraente, funzionali alla raccolta, elaborazione e traduzione in requisiti operativi da condividere con il team di intelligence;
- studio e configurazione di fonti, sorgenti, regole, scenari e tag; tale studio prevede la comprensione e l'individuazione del contesto nel quale le entità, le regole e gli scenari devono essere estratti - le configurazioni consistono nella programmazione della piattaforma tecnologica utilizzata a supporto del servizio (anche in linguaggio *regex*);
- configurazione domini e indirizzi IP;
- configurazione indirizzi e-mail;
- nomi dei servizi esposti su rete pubblica dall'Amministrazione;
- configurazione di nomenclature e protocolli relativi ad eventuali documenti prodotti.

Una volta terminata la fase di avvio il servizio entra nella **fase esecutiva**, durante la quale ci si avvarrà in modo intensivo degli *analisti di intelligence* del Centro Servizi dell'RTI che, a partire dalle evidenze fornite dalla piattaforma, estenderanno l'ambito di investigazione al fine di individuare tutti i possibili elementi

sensibili eventualmente presenti sulle fonti aperte. In questo modo sarà possibile controllare in modo continuo la rete e generare, di conseguenza, allarmi in base alle evidenze individuate.

All'emergere di informazioni di particolare rilevanza per l'Amministrazione sarà redatto un *Intelligence Allert* ed un *Intelligence Report* con il quale il Centro Servizi dell'RTI segnalerà tempestivamente e con il dovuto dettaglio le evidenze rilevate e suggerirà eventuali misure da adottare per la risoluzione della problematica. Le due tipologie di deliverable conterranno informazioni relative a:

- categoria di interesse;
- severità;
- data di rilevazione
- Traffic Light protocol - TLP
- dettaglio degli elementi raccolti e dei risultati delle analisi effettuate;
- indicazioni di eventuali raccomandazioni da porre in essere per la risoluzione del «case».

Di seguito si riporta l'elenco delle attività continuative necessarie alla corretta erogazione della componente di servizio *data breach monitoring*:

- allineamento ciclico di information gathering;
- funzioni di collegamento tra l'Amministrazione contraente e lo Intelligence Operation Center al fine di ottimizzazione e tradurre operativamente le informazioni raccolte dell'Amministrazione stessa nella massima riservatezza;
- configurazioni nella piattaforma TIS di altre entità di interesse a richiesta dell'Amministrazione stessa, quali eventi, persone, ecc.;
- fine tuning di regole e scenari inseriti nella piattaforma TIS;
- ricerca e popolamento di nuove fonti e sorgenti;
- stesura di report basati sulle evidenze derivanti dall'analisi dei dati.

5.2.11.3 Modalità di erogazione del servizio SP.07

Nel seguito sono indicate le attività da completarsi in fase di avviamento dei servizi finalizzate al completamento delle attività per la conduzione continuativa.

Sono previste le seguenti attività:

- assessment per la raccolta dei requisiti (*information gathering*) consistenti, a titolo puramente esemplificativo e non esaustivo, con interviste al personale coinvolto e/o referente per l'attività di *threat intelligence* presso l'Amministrazione, funzionali alla raccolta, elaborazione e traduzione, in requisiti *operativi*, da condividere agli analisti;
- studio e configurazione fonti, sorgenti, regole, scenari e tag. Lo studio è previsto per la comprensione e l'individuazione del contesto nel quale le entità, le regole e gli scenari devono essere estratti. Le configurazioni consentiranno la programmazione della piattaforma tecnologica utilizzata a supporto del servizio (in linguaggio *regex*).
- studio e configurazione nella piattaforma della lista delle tecnologie del cliente, che l'Amministrazione contraente si impegna a fornire:
- configurazione delle network IP, che l'Amministrazione si impegna a fornire;
- configurazione dei domini, che l'Amministrazione si impegna a fornire;

Successivamente alla fase preliminare verranno attuate le seguenti attività operative a garanzia della continuità del servizio:

- monitoraggio;

- allineamento ciclico delle *information requirement*;
- aggiornamenti tra l'Amministrazione ed il *team operativo di intelligence* al fine di ottimizzare e tradurre operativamente le *informazioni raccolte* nella massima riservatezza;
- favorire l'interazione tra tecnologie e strumenti in possesso dell'Amministrazione con le tecnologie di cyber *threat intelligence* (piattaforma TIS, NGS);
- configurazioni *ad hoc* della piattaforma TIS a seguito di eventi avvenuti sul perimetro (ad es. campagne malevole);
- approfondimenti in proattività (sia a seguito di un report, sia in autonomia per le attività di *threat intelligence*) per meglio identificare aree di interesse per l'Amministrazione
- fine tuning di regole e scenari inseriti nella piattaforma TIS;
- ricerca e popolamento di nuove fonti e sorgenti;
- stesura di report basati sulle evidenze derivanti dall'analisi dei dati.

5.2.11.4 Quantità e prezzi del servizio SP.07

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati in Appendice A, secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni [DA-5].

5.2.11.5 Attivazione del servizio SP.07

Si prevede l'avvio del servizio secondo i tempi definiti nell'Appendice B.

5.2.11.6 Deliverable del servizio SP.07

Come deliverable del servizio è previsto il rilascio di tre tipi di documenti:

- intelligence report - SP.07
- intelligence alert - SP.07
- report consuntivi periodici - SP.07.

L'Intelligence report sarà un documento, in formato PDF, contenente tutte le informazioni necessarie a capire e contestualizzare una minaccia quali IOCs, descrizione della campagna, gruppo e vulnerabilità trattata, suggerimenti per *remediation* o *mitigation* della minaccia stessa. Ogni report sarà corredato di una classificazione rispetto alla tipologia dello stesso, al Traffic Light Protocol (TLP) e alla severity.

L'*intelligence alert* sarà un documento, in formato PDF, ricevuto contestualmente anche come testo via email, relativo ad una possibile notizia di interesse per l'Amministrazione, che non necessariamente richiede di porre in campo contromisure difensive. L'obiettivo degli *alert* è mantenere per quanto possibile l'Amministrazione contraente allineata su possibili eventi di interesse, fintanto che questi non si traducano in una minaccia fattuale.

Il *report consuntivo* è un report bimestrale, in formato PDF, che riassume le segnalazioni effettuate in un certo periodo, classificandole sia per tipologia che per severity. La periodicità può comunque essere decisa in accordo con l'Amministrazione stessa.

5.2.12 Supporto per Design e Progettazione dell'infrastruttura Green Zone - SP.08

A seguito della richiesta dell'Amministrazione, il RTI intende predisporre un team di specialisti con le competenze e l'esperienza necessarie ad effettuare l'attività di Design e progettazione di una nuova infrastruttura denominata Green Zone per incrementare il livello di sicurezza e raggiungere l'obiettivo desiderato dall'Amministrazione.

L'attività di progettazione della nuova Green Zone rientra nell'ambito del programma di consolidamento delle misure di sicurezza intrapreso dall'Amministrazione.

5.2.12.1 Descrizione del servizio SP.08

Il presente servizio prevede l'avvio di una fase di analisi preliminare volta a comprendere le attuali tecnologie utilizzate e le specifiche caratteristiche al fine di poter predisporre le opportune linee guida o best practice in ambito security by design

In particolare, il modello proposto da Leonardo è basato su un approccio integrato, mediante una metodologia articolata nei seguenti passi (step):

Step 1 – Analisi preliminare

In questa fase verrà eseguita un'analisi preliminare della situazione attuale (in termini di infrastrutture tecnologiche), svolgendo le seguenti attività:

- raccolta delle informazioni sulle tecnologie attualmente utilizzate dall'Amministrazione contraente;
- analisi della fattibilità e classificazione sulla base di livelli di priorità delle tecnologie utilizzate;
- analisi degli impatti di situazioni di indisponibilità, per l'individuazione delle aree problematiche e contromisure tecnologiche da adottare.

Step 2 – Disegno delle linee guida di security by design

In questa fase verranno identificate le linee guida di security by design, propedeutica alla fase di progettazione, svolgendo le seguenti attività:

- predisposizione delle *linee guida di security by design* (sulla base della classificazione delle tecnologie fatta nella fase di assessment);
- ipotesi di progettazione dell'infrastruttura sulla base dei modelli di servizio da erogare;
- condivisione della documentazione predisposta ai referenti coinvolti.

Step 3 – Follow-up & refining

In questa fase verranno condotte le attività follow-up e refining, svolgendo i seguenti passaggi:

- conduzione di specifiche interviste e/o workshop con gli *stakeholder* rilevanti per finalizzare ogni documento e raccogliere feedback;
- completamento della *progettazione dell'infrastruttura* secondo quanto recepito nelle fasi precedenti;
- finalizzazione progetto definitivo e suggerimenti di attuazione e programmazione delle attività con le strutture interessate.

5.2.12.2 Modalità di erogazione del servizio SP.08

Coerentemente a quanto previsto nel Contratto per i servizi professionali (rif. Capitolato Tecnico [DA-2] par. 1.3.9 Servizio L2.S3.9 – Servizi professionali, pagg. 48–49), si precisa che la modalità di remunerazione di tali servizi è "a task". Per gli SLA, dove applicabili, si fa riferimento all'Appendice 1 al Capitolato tecnico [4] "Indicatori di qualità della fornitura per il Lotto 2"

5.2.12.3 Quantità e prezzi del servizio SP.08

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati in Appendice A, calcolati secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni.

5.2.12.4 Attivazione del servizio SP.08

Si prevede l'avvio del servizio secondo i tempi definiti nell'Appendice B.

5.2.12.5 Deliverable del servizio SP.08

Al termine delle attività sarà condiviso con l'Amministrazione il piano progettuale prodotto.

Come deliverable del servizio è previsto il rilascio di un piano progettuale di alto livello ed uno di natura tecnica, con cui ripercorrere e comprendere gli step legati all'attività e come di seguito rappresentato:

- Piano progettuale di dettaglio del SP.08
- Executive Report del SP.08.

5.2.13 Supporto all'attivazione del servizio di Next Generation Firewalling - SP.09

Il servizio professionale richiesto è orientato a supportare l'Amministrazione nella gestione e nel monitoraggio continuativo delle piattaforme previste nella protezione perimetrale della Green Zone secondo quanto previsto nella fase progettuale del paragrafo precedente.

5.2.13.1 Descrizione del Servizio SP.09

Il servizio è erogato a task ed include la prima configurazione degli apparati di protezione perimetrale (per un totale massimo di qtà 2 apparati fisici) finalizzati alla segregazione del traffico (inbound ed outbound) verso la nuova infrastruttura Green Zone per una più appropriata segregazione del traffico previsto in §5.2.12.

5.2.13.2 Vincoli e assunzioni del Servizio SP.09

Affinché l'Amministrazione contraente possa usufruire del servizio è necessario che sia interconnessa direttamente alla rete del Sistema Pubblico di Connettività (SPC) — o altre strutture equivalenti individuate da Consip S.p.A. e/o dell'Agenzia per l'Italia Digitale (AgID) — attraverso uno o più Fornitori di connettività, o attraverso Enti autorizzati, in modo tale che il traffico tra il Centro Servizi e l'Amministrazione contraente avvenga all'interno di VPN sicure e configurate per supportare destinazioni multiple. In subordine dovrà comunque avere un punto di accesso a Internet.

Per l'erogazione delle attività del servizio è necessaria quindi anche la creazione di una VPN tra il Centro Servizi Leonardo e l'Amministrazione Contraente, in mancanza della quale potrebbero non essere erogate alcune attività specifiche.

5.2.13.3 Modalità di erogazione del Servizio SP.09

Coerentemente a quanto previsto nel Contratto per i servizi professionali (rif. Capitolato Tecnico [DA-2] par. 1.3.9 Servizio L2.S3.9 – Servizi professionali, pagg. 48–49), si precisa che la modalità di remunerazione di tali servizi è "a task". Per gli SLA, dove applicabili, si fa riferimento all'Appendice 1 al Capitolato tecnico [4] "Indicatori di qualità della fornitura per il Lotto 2".

5.2.13.4 Quantità e prezzi del Servizio SP.09

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati in Appendice A, secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni [DA-5].

5.2.13.5 Attivazione del Servizio SP.09

Si prevede l'avvio del servizio secondo i tempi definiti nell'A.3.1

5.2.13.6 Deliverable del servizio SP.09

Non applicabile.

5.2.14 Servizi di protezione perimetrale NGFW per nuova area Green Zone – SP.10

I servizi professionali richiesti al Fornitore sono finalizzati a supportare l'Amministrazione nella configurazione finale e gestione continuativa di apparati di sicurezza perimetrali a delimitazione della nuova area Green Zone e di tipologia Next Generation Firewall.

5.2.14.1 Descrizione del servizio SP.10

Il servizio prevede una prima configurazione degli apparati di sicurezza identificati per l'attività specifica, con la presa in carico remota da parte del SOC. in aggiunta vendono definite adeguate politiche di sicurezza in funzione dei servizi erogati e della finalità dell'area di segregazione prevista in fase progettuale nella Green Zone. L'attività prevede anche l'integrazione delle attuali configurazioni presenti su eventuali devices che verranno integrati/sostituiti.

Parallelamente viene garantito il servizio di change policy e di gestione firewall relativamente alla validazione ed implementazione di tutte le richieste di change sui sistemi di sicurezza previsti.

In termini di Device Management sono previste le seguenti fasi:

- Definizione del perimetro di servizio
  - definizione della baseline dei sistemi di sicurezza che saranno oggetto del servizio Security Device Management;
- Definizione delle politiche di sicurezza
  - Partendo dalle considerazioni definite nella fase progettuale prevista nella Green Zone viene attuata un'analisi globale dell'infrastruttura dei sistemi di sicurezza oggetto dei vari servizi in caso di integrazioni di aree gestite da altri apparati di sicurezza;
- Presa in carico dei sistemi, in RW. Nello specifico le attività di presa in carico prevedono:
  - pianificazione temporale delle attività;
  - completa raggiungibilità dei devices e delle relative piattaforme di management ove presenti;
  - configurazione di utenze nominali per gli specialisti del SOC;
- Gestione a regime:
  - ogni richiesta viene validata ed implementata secondo le best practice di sicurezza ed in conformità a quanto definito con i Cliente in relazione anche alle policy aziendali vigenti;
  - i change, ad esempio, possono riguardare aggiunta/rimozione/modifica di policy firewall, creazioni tunnel vpn, modifica routing, /creazione/modifica profili UTM etc.

5.2.14.2 Vincoli e assunzioni del Servizio

Affinché l'Amministrazione contraente possa usufruire del servizio è necessario che sia interconnessa direttamente alla rete del Sistema Pubblico di Connettività (SPC) — o altre strutture equivalenti individuate da Consip S.p.A. e/o dell'Agenzia per l'Italia Digitale (AgID) — attraverso uno o più Fornitori di connettività, o attraverso Enti autorizzati, in modo tale che il traffico tra il Centro Servizi e l'Amministrazione contraente avvenga all'interno di VPN sicure e configurate per supportare destinazioni multiple. In subordine dovrà comunque avere un punto di accesso a Internet.

Per l'erogazione delle attività del servizio è necessaria quindi anche la creazione di una VPN tra il Centro Servizi del Fornitore e l'Amministrazione Contraente, in mancanza della quale potrebbero non essere erogate alcune attività specifiche.

5.2.14.3 Modalità di erogazione del servizio SP.10

Il servizio sarà erogato in modalità as a service, presso la sede del fornitore. Di seguito viene riportata una tabella relativa alle finestre di servizio.

Tabella 6: Finestre di servizi

Attività	Disponibilità
Help Desk (telefonico)	9:00–18:00 dal lunedì al venerdì (escluso festività nazionali)
Help Desk (telematico)	9:00–18:00 dal lunedì al venerdì (escluso festività nazionali)
Monitoraggio di sicurezza delle piattaforme	H24
Monitoraggio di disponibilità delle piattaforme	H24

5.2.14.4 Quantità e prezzi del servizio SP.10

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati in Appendice A, secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni [DA-5].

5.2.14.5 Attivazione del servizio SP.10

Si prevede l'avvio del servizio secondo i tempi definiti nell'A.3.1

5.2.14.6 Deliverable del servizio SP.10

Non applicabile.

5.2.15 Supporto Specialistico Cyber Security on Premise - SP.11

Il presente paragrafo rappresenta la richiesta dell'Amministrazione di supporto specialistico Cyber Security nell'ambito della risposta alle anomalie e minacce informatiche in ambito ICT.

5.2.15.1 Descrizione del Servizio SP.11

Il servizio è erogato in presenza <<on premise>> da personale dell'RTI in orario ordinario (9,00 – 18,00) secondo la modalità di erogazione H8x5. Tale attività si integra e completa quanto previsto dal servizio di monitoraggio erogato tramite il servizio indicato al §5.2.8. In particolare, relativamente alla gestione delle anomalie/minacce informatiche, segnalate attraverso il servizio di monitoraggio *real time*, il personale che si trova presso il cliente interagisce con quello del SOC Leonardo, responsabile della definizione delle attività di gestione delle anomalie, attraverso opportune procedure di gestione delle fasi di contenimento, eradicazione, recovery. Le attività della risorsa in presidio saranno svolte in coordinamento con il personale So.Re.Sa., in modo da favorire l'interazione col personale interno all'Amministrazione contraente, in merito ai processi di gestione degli incidenti di sicurezza e le tecnologie in uso.

5.2.15.2 Vincoli e assunzioni del servizio SP.11

Il perimetro delle attività descritte è da intendersi limitato alle attività del presidio di sicurezza ICT operativo presso il cliente, nell'ambito della risposta alle anomalie e minacce informatiche.

5.2.15.3 Modalità di erogazione del servizio SP.11

Per l'erogazione del servizio sarà garantita la disponibilità presso la sede della So.Re.Sa., per tutta la durata del contratto, delle risorse con competenze idonee alle attività così come previsto nel piano dei fabbisogni.

Coerentemente a quanto previsto nel Contratto per i servizi professionali (rif. Capitolato Tecnico [DA-2] par. 1.3.9 Servizio L2.S3.9 – Servizi professionali, pagg. 48–49), si precisa che la modalità di remunerazione di tali servizi è "a task". Per gli SLA, dove applicabili, si fa riferimento all'Appendice 1 al Capitolato tecnico [4] "Indicatori di qualità della fornitura per il Lotto 2"

5.2.15.4 Quantità e prezzi del servizio SP.11

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati in Appendice A, calcolati secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni.

5.2.15.5 Attivazione del servizio SP.11

Si prevede l'avvio del servizio secondo i tempi definiti nell'Appendice B.

5.2.15.6 Deliverable del servizio SP.11

Non applicabile.

6 RISERVATEZZA

Per l'erogazione della fornitura, il Fornitore non ha necessità trattare e/o accedere a informazioni o materiale classificato ma è comunque tenuto alla sicurezza e alla riservatezza dei dati e della documentazione di cui viene a conoscenza.

APPENDICE A PROGETTO DI ATTUAZIONE

A.1 Struttura organizzativa

La struttura organizzativa completa è descritta nella proposta tecnica (cfr. documento [DA-3]).

Le figure professionali coinvolte nella gestione e conduzione dei servizi oggetto del presente Progetto dei fabbisogni per lo specifico contratto esecutivo sono riassunte nella seguente Tabella 8.

Tabella 8: Figure professionali.

Ruolo	Caratteristiche e responsabilità
Responsabile Contratto Quadro	È il rappresentante del fornitore verso Agid/Consip, garantisce l'omogeneità e l'uniformità di interfaccia verso le parti interessate a livello di Governo del Contratto Quadro 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.
Responsabile Contratto Esecutivo	Costituisce l'interfaccia unica verso il Responsabile del Procedimento dell'Amministrazione Beneficiaria. È responsabile dell'erogazione dei servizi acquistati dall'Amministrazione e della rendicontazione e dei meeting di stato avanzamento lavori. Costituisce l'interfaccia unica verso il Responsabile Unico del Procedimento dell'Amministrazione beneficiaria.
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.
Responsabile del Centro Servizi	È responsabile del Centro servizi da cui vengono erogati i servizi nella modalità "as a service".
Responsabile Servizi 'on premise'	Coincide con il Responsabile Tecnico
HELP DESK	Primo punto di contatto a disposizione dell'Amministrazione per l'avvio delle attività di acquisizione del servizio. Supporta inoltre i referenti dell'Amministrazione contraente nelle attività di risoluzione di eventuali problematiche di utilizzo del servizio. L'Help Desk è contattabile: - per contatti di natura commerciale e informativa al numero verde **800 894 590**. - per contatti di natura tecnica e di problemi di utilizzo del servizio al seguente indirizzo e-mail **sccd@spc-lotto2-sicurezza.it** Ulteriori informazioni sono reperibili al seguente URL: http://www.spc-lotto2-sicurezza.it presso il quale è presente il Portale di Governo e Gestione della Fornitura.

I nominativi delle figure presenti nella tabella soprastante saranno forniti all'Amministrazione entro 10 giorni dalla stipula del contratto.

A.2 Specifiche di collaudo

N.A.

A.3 Quantità e costi

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati di seguito nelle Tabelle successive, secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni [DA-5]. I prezzi tengono conto di quanto riportato nel listino prezzi SPC lotto 2 [DA-6]. In base a quanto richiesto dall'Amministrazione contraente nel Piano dei fabbisogni [DA-5].

A.3.1 Riepilogo Economico

Servizio L2.S3.4 - Vulnerability Assessment Esterno ed Interno - VA.01					
Metrica	**Fascia**	**Prezzo unitario**	**a canone annuo**	**mesi totali**	**TOTALE**
indirizzo IP/anno	Fascia1: n. 1 indirizzo IP	€ 124,00	1	4	€ 41,33
	Fascia 2: da 2 a 15 indirizzi IP	€ 89,00	14	4	€ 415,33
	Fascia 3: oltre 15 indirizzi IP	€ 64,00	260	4	€ 5.546,67
TOT					€ 6.003,33

L2.S3.9 - Servizi di supporto per la profilazione del framework Normativo di Riferimento - SP.01.1				
Metrica	**Figura professionale**	**Prezzo unitario**	**Effort (gg/uomo)**	**Prezzo**
giorno/uomo	Capo progetto	€ 300,00	5,00	**€ 1.500,00**
	Security Architect	€ 372,90	22,00	**€ 8.203,80**
	Specialista di tecnologia/prodotto Senior	€ 295,00	18,00	**€ 5.310,00**
	Specialista di tecnologia/prodotto	€ 235,00	-	**€ 0,00**
TOT				**€ 15.013,80**

L2.S3.9 - Servizi di supporto per la profilazione dei requisiti di sicurezza della Supply Chain - SP.01.2				
Metrica	**Figura professionale**	**Prezzo unitario**	**Effort (gg/uomo)**	**Prezzo**
giorno/uomo	Capo progetto	€ 300,00	5,00	**€ 1.500,00**
	Security Architect	€ 372,90	23,00	**€ 8.576,70**
	Specialista di tecnologia/prodotto Senior	€ 295,00	28,00	**€ 8.260,00**
	Specialista di tecnologia/prodotto	€ 235,00	-	**€ 0,00**
TOT				**€ 18.336,70**

L2.S3.9 - Servizi di supporto per l'assessment ed il miglioramento della postura secondo il Framework individuato - SP.02				
Metrica	**Figura professionale**	**Prezzo unitario**	**Effort (gg/uomo)**	**Prezzo**
giorno/uomo	Capo progetto	€ 300,00	9,00	**€ 2.700,00**
	Security Architect	€ 372,90	6,00	**€ 2.237,40**
	Specialista di tecnologia/prodotto Senior	€ 295,00	85,00	**€ 25.075,00**
	Specialista di tecnologia/prodotto	€ 235,00	-	**€ 0,00**
TOT				**€ 30.012,40**

L2.S3.9 - Servizi di Supporto legale per l'assessment ed il miglioramento della compliance alle norme sulla protezione dei dati personali - SP.03.1				
Metrica	**Figura professionale**	**Prezzo unitario**	**Effort (gg/uomo)**	**Prezzo**
giorno/uomo	Capo progetto	€ 300,00	28,00	**€ 8.400,00**
	Security Architect	€ 372,90	150,00	**€ 55.935,00**
	Specialista di tecnologia/prodotto Senior	€ 295,00	135,00	**€ 39.825,00**
	Specialista di tecnologia/prodotto	€ 235,00	-	**€ 0,00**
TOT				**€ 104.160,00**

L2.S3.9 - Servizi professionali formazione e training - SP.03.2				
Metrica	**Figura professionale**	**Prezzo unitario**	**Effort (gg/uomo)**	**Prezzo**
giorno/uomo	Capo progetto	€ 300,00	47,00	**€ 14.100,00**
	Security Architect	€ 372,90	285,00	**€ 106.276,50**
	Specialista di tecnologia/prodotto Senior	€ 295,00	251,00	**€ 74.045,00**
	Specialista di tecnologia/prodotto	€ 235,00	-	**€ 0,00**
TOT				**€ 194.421,50**

L2.S3.9 - Servizi di Supporto per implementazione di un sistema di gestione per la sicurezza delle informazioni - SP.03.3				
Metrica	**Figura professionale**	**Prezzo unitario**	**Effort (gg/uomo)**	**Prezzo**
giorno/uomo	Capo progetto	€ 300,00	16,00	**€ 4.800,00**
	Security Architect	€ 372,90	159,00	**€ 59.291,10**
	Specialista di tecnologia/prodotto Senior	€ 295,00	-	**€ 0,00**
	Specialista di tecnologia/prodotto	€ 235,00	-	**€ 0,00**
TOT				**€ 64.091,10**

L2.S3.9 - Servizi di supporto per attività di Penetration Test - PT.01				
Metrica	**Figura professionale**	**Prezzo unitario**	**Effort (gg/uomo)**	**Prezzo**
giorno/uomo	Capo progetto	€ 300,00	3,00	**€ 900,00**
	Security Architect	€ 372,90	-	**€ 0,00**
	Specialista di tecnologia/prodotto Senior	€ 295,00	28,00	**€ 8.260,00**
	Specialista di tecnologia/prodotto	€ 235,00	-	**€ 0,00**
TOT				**€ 9.160,00**

L2.S3.9 - Servizi di supporto per il Monitoraggio Continuativo degli Eventi di Sicurezza - SP.04				
Metrica	**Figura professionale**	**Prezzo unitario**	**Effort (gg/uomo)**	**Prezzo**
giorno/uomo	Capo progetto	€ 300,00	4,00	**€ 1.200,00**
	Security Architect	€ 372,90	-	**€ 0,00**
	Specialista di tecnologia/prodotto Senior	€ 295,00	47,00	**€ 13.865,00**
	Specialista di tecnologia/prodotto	€ 235,00	-	**€ 0,00**
TOT				**€ 15.065,00**

L2.S3.9 - Servizio specialistico per Tuning servizio di monitoraggio continuativo - SP.05				
Metrica	**Figura professionale**	**Prezzo unitario**	**Effort (gg/uomo)**	**Prezzo**
giorno/uomo	Capo progetto	€ 300,00	1,00	**€ 300,00**
	Security Architect	€ 372,90	10,00	**€ 3.729,00**
	Specialista di tecnologia/prodotto Senior	€ 295,00	5,00	**€ 1.475,00**
	Specialista di tecnologia/prodotto	€ 235,00	5,00	**€ 1.175,00**
TOT				**€ 6.679,00**

L2.S3.9 - Servizi di Managed Detection & Response - SP.06				
Metrica	**Figura professionale**	**Prezzo unitario**	**Effort (gg/uomo)**	**Prezzo**
giorno/uomo	Capo progetto	€ 300,00	-	**€ 0,00**
	Security Architect	€ 372,90	20,00	**€ 7.458,00**
	Specialista di tecnologia/prodotto Senior	€ 295,00	34,00	**€ 10.030,00**
	Specialista di tecnologia/prodotto	€ 235,00	-	**€ 0,00**
TOT				**€ 17.488,00**

L2.S3.9 - Servizi di Cyber Threat Intelligence - SP.07				
Metrica	**Figura professionale**	**Prezzo unitario**	**Effort (gg/uomo)**	**Prezzo**
giorno/uomo	Capo progetto	€ 300,00	13,00	**€ 3.900,00**
	Security Architect	€ 372,90	89,00	**€ 33.188,10**
	Specialista di tecnologia/prodotto Senior	€ 295,00	45,00	**€ 13.275,00**
	Specialista di tecnologia/prodotto	€ 235,00	-	**€ 0,00**
TOT				**€ 50.363,10**

L2.S3.9 - Supporto per Design e Progettazione dell'Infrastruttura Green Zone - SP.08				
Metrica	**Figura professionale**	**Prezzo unitario**	**Effort (gg/uomo)**	**Prezzo**
giorno/uomo	Capo progetto	€ 300,00	5,00	**€ 1.500,00**
	Security Architect	€ 372,90	20,00	**€ 7.458,00**
	Specialista di tecnologia/prodotto Senior	€ 295,00	33,00	**€ 9.735,00**
	Specialista di tecnologia/prodotto	€ 235,00	-	**€ 0,00**
TOT				**€ 18.693,00**

L2.S3.9 - Supporto all'attivazione del servizio di Next Generation Firewalling - SP.09				
Metrica	**Figura professionale**	**Prezzo unitario**	**Effort (gg/uomo)**	**Prezzo**
giorno/uomo	Capo progetto	€ 300,00	7,00	**€ 2.100,00**
	Security Architect	€ 372,90	52,00	**€ 19.390,80**
	Specialista di tecnologia/prodotto Senior	€ 295,00	46,00	**€ 13.570,00**
	Specialista di tecnologia/prodotto	€ 235,00	-	**€ 0,00**
TOT				**€ 35.060,80**

L2.S3.9 - Servizi di Protezione perimetrale NGFW - SP.10				
Metrica	**Figura professionale**	**Prezzo unitario**	**Effort (gg/uomo)**	**Prezzo**
giorno/uomo	Capo progetto	€ 300,00	2,00	**€ 600,00**
	Security Architect	€ 372,90	-	**€ 0,00**
	Specialista di tecnologia/prodotto Senior	€ 295,00	20,00	**€ 5.900,00**
	Specialista di tecnologia/prodotto	€ 235,00	-	**€ 0,00**
TOT				**€ 6.500,00**

L2.S3.9 - Supporto Specialistico Cyber Security on Premise - SP.11				
Metrica	**Figura professionale**	**Prezzo unitario**	**Effort (gg/uomo)**	**Prezzo**
giorno/uomo	Capo progetto	€ 300,00	15,00	**€ 4.500,00**
	Security Architect	€ 372,90	147,00	**€ 54.816,30**
	Specialista di tecnologia/prodotto Senior	€ 295,00	-	**€ 0,00**
	Specialista di tecnologia/prodotto	€ 235,00	-	**€ 0,00**
TOT				**€ 59.316,30**

Il valore totale dell'iniziativa è pari a € 650.364,03 (IVA esclusa).

A.3.2 Fatturazione L2.S3.9

A valle delle verifiche dell'Amministrazione (art 15 dell'Accordo Quadro), i servizi professionali L2.S3.9 saranno fatturati bimestralmente (art.19 dell'Accordo Quadro), in ragione dei servizi effettivamente prestati nel rispetto del Progetto dei Fabbisogni, ovvero secondo lo stato di avanzamento dei lavori, e nelle misure che si concorderanno ad inizio delle attività o nel piano di lavoro.

APPENDICE B PIANO DI LAVORO

Di seguito si riporta la programmazione delle attività, espressa in giorni lavorativi a partire dalla data di perfezionamento del contratto esecutivo (T0).

B.1 Piano di lavoro

In base a quanto richiesto dall'Amministrazione contraente nel Piano dei fabbisogni [DA-5] la tabella riporta la pianificazione per i servizi contenuti all'interno del presente documento.

Per quanto concerne i servizi professionali erogati in modo continuativo, si indica l'avvio del servizio con T1, corrispondente alla data del 1 Settembre 2022.

Titolo	Descrizione	Inizio	Fine
VA.01	Vulnerability Assessment Esterno ed Interno	T0	31 Dicembre 2022
SP.01.1	Servizi di supporto per la profilazione del framework Normativo di Riferimento	T0	31 Dicembre 2022
SP.01.2	Servizi di supporto per la profilazione dei requisiti di sicurezza della Supply Chain	T0	31 Dicembre 2022
SP.02	Servizi di supporto per l'assessment ed il miglioramento della postura secondo il Framework individuato	T0	31 Dicembre 2022
SP.03.1	Servizi di Supporto legale per l'assessment ed il miglioramento della compliance alle norme sulla protezione dei dati personali	T0	31 Dicembre 2022
SP.03.2	Servizi professionali formazione e training	T0	31 Dicembre 2022
SP.03.3	Servizi di Supporto per implementazione di un sistema di gestione per la sicurezza delle informazioni	T0	31 Dicembre 2022
PT.01	Servizi di supporto per attività di Penetration Test	T0	31 Dicembre 2022
SP.04	Servizi di supporto per il Monitoraggio Continuativo degli Eventi di Sicurezza	T0	31 Dicembre 2022
SP.05	Servizio specialistico per Tuning servizio di monitoraggio continuativo	T0	31 Dicembre 2022
SP.06	Servizi di Managed Detection & Response	T0	31 Dicembre 2022
SP.07	Servizi di Cyber Threat Intelligence	T0	31 Dicembre 2022
SP.08	Supporto per Design e Progettazione dell'Infrastruttura Green Zone	T0	31 Dicembre 2022
SP.09	Supporto all'attivazione del servizio di Next Generation Firewalling	T0	31 Dicembre 2022
SP.10	Servizi di Protezione perimetrale NGFW	T0	31 Dicembre 2022
SP.11	Supporto Specialistico Cyber Security on Premise	T0	31 Dicembre 2022