Identificativo: PRO_GOVM_200101/2212

Data: 07/12/2022

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

AIFA

Progetto dei fabbisogni

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		
	Giorgio Castrucci	
Verifica		
	Germano Matteuzzi	
Approvazione		
	Mauro Pucciarini	
Autorizzazione		
	Claudio Rando	

Approvazioni Aggiuntive

Azienda	Nome e Ruolo	Firma

Lista di Distribuzione

Rev.	Data	Destinatario	Azienda
1.0	Vedi data di copertina	AIFA	

Registro delle Revisioni

Rev.	Data	Descrizione delle modifiche	Autori
1.0	Vedi data di copertina	Prima stesura	RTI

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 dell'Agenzia Italiana del Farmaco (indicata nel documento come AIFA o come Amministrazione contraente) contenute nel proprio Piano dei fabbisogni [DA-5] 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 richiesta di proroga dei servizi finalizzati a supportare l'Amministrazione contraente per implementare tutte le misure che innalzano la qualità dei servizi offerti in termini di sicurezza. Tale Progetto proroga i servizi già previsti nella precedente formulazione con CIG Originario 5518849A42 e CIG derivato 83414427B1 nell'ambito della adesione al Contratto Quadro Consip SPC CLOUD "Sistema Pubblico di Connettività (SPC) – Lotto 2 "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)".

Le iniziative che costituiscono il Progetto dei Fabbisogni sono sostanzialmente composte da servizi in continuità con le attività attualmente in erogazione. Al fine di garantite la continuità di essenziali servizi di Sicurezza Informatica ed un ordinato passaggio di consegne verso il nuovo fornitore, i servizi del presente Progetto dei Fabbisogni vengono prorogati come previsto all'art. 5.2 del Capitolato. Resta comunque inteso che la durata delle proroghe dei singoli servizi è modulata sulla base delle esigenze dell'Amministrazione, che potrà comunicare la cessazione di uno o più servizi a partire dal primo giorno del mese successivo alla comunicazione.

Di seguito vengono elencati in forma sintetica i servizi richiesti:

- Servizio L2.S3.10 - Servizio di Monitoraggio
- Servizio L2.S3.9 - Servizi professionali - Avvio e Supporto al Monitoraggio
- Servizio L2.S3.9 - Servizi professionali - Presidio Operativo

Per la descrizione dei suddetti servizi si rinvia ai successivi paragrafi.

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.		Adesione alla proroga tecnica inviata da AIFA a mezzo PEC il xx/12/2022
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	Agenzia Italiana del Farmaco - AIFA
Indirizzo	Via del Tritone 181
CAP	00187
Comune	Roma
Provincia	Roma
Regione	Lazio
Codice Fiscale	97345810580
Nominativo referente Contratto Esecutivo:	Maurizio Trapanese
Indirizzo mail	protocollo@pec.aifa.gov.it
PEC (SÌ/NO)	SÌ

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

Nome	Maurizio
Cognome	Trapanese
Telefono fisso	06 57984750
Indirizzo mail	m.trapanese@aifa.gov.it
PEC (SÌ/NO)	NO

5 PROPOSTA TECNICO-ECONOMICA

Nella presente sezione del Progetto dei fabbisogni l'RTI intende formulare la proposta tecnico-economica secondo le modalità tecniche e i listini previsti nel Contratto Quadro e per ciascuno dei servizi richiesti dall'Amministrazione nel proprio Piano dei Fabbisogni.

Relativamente alle sedi per lo svolgimento delle attività, si precisa che il personale del RTI assegnato per il Progetto, svolgerà presso gli uffici dell'Amministrazione, previo accordo con la stessa, le sole attività che, per loro natura, richiederanno la presenza presso i suddetti uffici; le altre attività (quali ad esempio l'elaborazione delle informazioni, la stesura documentale) saranno condotte "da remoto" presso gli uffici del fornitore.

In tale ambito il fornitore s'impegna a erogare tutti i servizi descritti nel presente documento e assicura la disponibilità delle risorse indicate per supportare l'Amministrazione contraente alla loro erogazione. La fatturazione avverrà sulla base dello stato dell'avanzamento lavori determinato coerentemente con il piano di lavoro definito ed alla consegna dei deliverable concordati, previo benestare.

Ogni servizio di cui è costituita la fornitura potrà prevedere la vendita di più tipologie di servizi base previsti a listino e completata con l'impegno di risorse professionali (servizio risorse professionali) secondo le esigenze dell'Amministrazione.

Di seguito la matrice dei servizi previsti nel presente Progetto dei Fabbisogni (Matrice di Tracciabilità) a soddisfacimento delle esigenze espresse dal Piano dei Fabbisogni inviato dall'Amministrazione contraente.

Di seguito la lista dei servizi previsti nella fornitura.

Tabella 7: Servizi del Progetto dei Fabisogni

Id	Titolo	Descrizione
SM.1	L2.S3.10 - Servizio di Monitoraggio	Servizio per la prevenzione e gestione degli attacchi informatici attraverso il monitoraggio continuo effettuato dal Security Operation Center (SOC) dell'RTI
SP.3	L2.S3.9 - Servizi professionali - Supporto al Monitoraggio	Servizi professionali a supporto del servizio di Monitoraggio L2.S3.10
SP.4	L2.S3.9 - Servizi professionali - Presidio Operativo	Giornate a consumo

5.1 L2.S3.10 SM1 - Servizi di monitoraggio

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

In tale ottica il seguente Servizio di Monitoraggio effettua attività di monitoraggio real time, per mezzo di un SOC messo a disposizione dal RTI presidiato 24 ore su 24 per 365 giorni l'anno e composto da un team di specialisti (analisti, system engineer, security tester e malware specialist).

5.1.1 Obiettivi del Servizio SM1

Il servizio di monitoraggio si pone i seguenti obiettivi:

- fornire un servizio efficiente per la raccolta ed elaborazione dei log relativi al tracciamento delle attività svolte sui sistemi;

- controllare in maniera attiva l'infrastruttura di sicurezza delle reti e dei sistemi attraverso l'attività di monitoring real-time e supervisione degli apparati di sicurezza prevenendo efficacemente gli incidenti di sicurezza;
- Contribuire al governo ed alla gestione della sicurezza dell'Amministrazione fornendo servizi di installazione, configurazione e manutenzione sia on-site che presso le proprie strutture dei sistemi hardware e software necessari per l'erogazione dei servizi di sicurezza;
- generare allarmi e reportistica per l'auditing sugli eventi raccolti e garantire la conservazione sicura delle evidenze. I risultati di tale attività saranno resi disponibili all'Amministrazione contraente su una piattaforma condivisa al termine delle attività di triage da parte degli analisti di sicurezza.

5.1.2 Architettura di erogazione del Servizio SM1

Il servizio è progettato per anticipare il verificarsi di tentativi di attacco, identificando prontamente asset o eventi potenzialmente impattanti. Il servizio è basato su un monitoraggio continuo in tempo reale e correlazione di eventi di sicurezza della rete (ad es. comportamenti non autorizzati, tentativi di attacco, interruzioni di servizio) con analisi delle anomalie e dei principali trend. Il servizio presuppone l'utilizzo di una piattaforma centralizzata di Security Information and Event Management (SIEM) per la correlazione di eventi, minacce e fornisce allo stesso tempo un potente sistema di intelligence per la sicurezza e gestione continuativa dei log.

La soluzione si articola nelle seguenti componenti:

- Presenti presso il Centro Servizi del RTI:
  - console di gestione, che costituisce il livello di application e presentation presso il Centro Servizi del RTI ad uso esclusivo del team specialistico di monitoraggio. In ogni caso l'RTI mette a disposizione un sistema di ticketing sviluppato internamente sul quale il cliente potrà verificare lo stato degli incident ed avere informazioni sugli stessi;
  - sistema di correlazione e log management, che costituisce il livello di data collecting and storage installato presso il Centro Servizi del RTI;
- Presenti presso l'Amministrazione contraente:
  - sistema di raccolta log (collettori), il quale costituisce il livello di data collecting and forwarding installato «on premise» su infrastrutture dell'Amministrazione contraente.

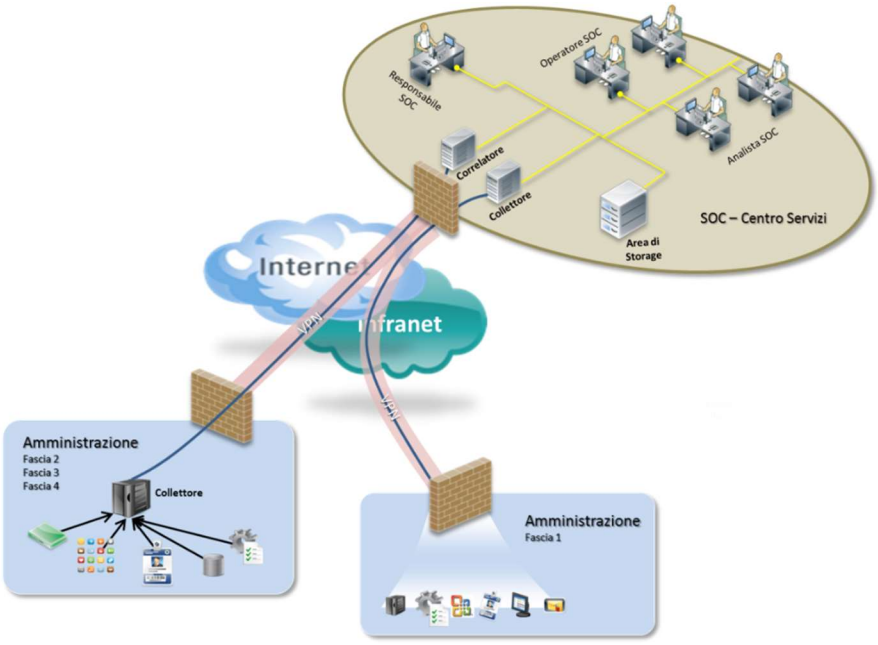

Figura 1: Architettura di riferimento del Servizio di Monitoraggio

Operativamente gli eventi vengono raccolti «on premise» da un collettore VLC (Virtual Log Collector) che integra anche la funzione di *caching dei LOG ricevuti*. Limitatamente all'istanza virtualizzata VLC l'installazione e la manutenzione sono a carico dell'Amministrazione, con il supporto dell'RTI. In caso di indisponibilità della connettività verso la console di gestione centrale, il virtual *collector* è in grado in grado di *mantenere* i LOG in modo da evitarne la perdita definitiva.
La raccolta degli eventi tipicamente avviene in modalità *agentless* e prima di effettuare qualunque elaborazione dei log, il collettore li firma digitalmente, li comprime, ne effettua un hash e li invia verso l'infrastruttura del Centro Servizi dell'RTI, che ha il compito di mantenere i file di log in formato raw inalterati per il tempo di *retention* specificato, che può essere diverso e configurato ad hoc a seconda dei casi da gestire, o più precisamente a seconda delle normative a cui rispondere. La piattaforma effettua l'archiviazione dei log *raw* sullo *storage*. In seguito i log vengono analizzati localmente, normalizzati, indicizzati ed inviati alla piattaforma di analisi. È possibile effettuare copie dei dati indicando una frequenza limite (ad es. una volta al mese) e utilizzando supporti messi a disposizione dal cliente via VPN.
Le estrazioni non sono soggette a SLA.

Nel fare questo, i log vengono anche aggregati: questa fase consente di raggruppare più eventi uguali tra loro verificatisi in un intervallo di tempo prefissato, in modo da ridurre lo spazio occupato da essi all'interno del database. Come conseguenza dell'operazione di aggregazione, nel database saranno conservate le seguenti informazioni: time stamp del primo evento aggregato, numero complessivo di eventi verificatisi nell'intervallo di aggregazione, time stamp e dati contenuti nell'ultimo evento aggregato. Si ribadisce che le elaborazioni effettuate dal collettore sui log sono successive al loro processing (firma digitale, compressione ed hashing) per l'invio ai successivi moduli che devono mantenere i raw log «originali ed inalterabili nel tempo».

5.1.3 Descrizione del Servizio SM1

Il servizi di monitoraggio in ambito di sicurezza informatica sono erogati in modalità «as a service» dal SOC dislocato all'interno del Centro Servizi e includono il monitoraggio, la correlazione, la classificazione e l'analisi, nonché la notifica degli eventi di sicurezza relativi all'infrastruttura dell'Amministrazione contraente. Le fasi di erogazione del servizio si articolano in:

- Monitoring & alerting;
- Reporting;
- Log management.

5.1.3.1 Monitoring & Alerting

L'elemento di servizio monitoring & alerting – erogato in modalità H24, per 365 giorni all'anno – 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, antivirus ecc.) sono analizzati al fine di determinare, attraverso la correlazione, se si è effettivamente in presenza di potenziali eventi anomali ed incidenti di sicurezza.
- **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 (incident response) non previsto in questa voce di fornitura.

Il servizio di monitoraggio è esteso al perimetro di sicurezza dei datacenter, previa analisi sintattica (parsing) delle sorgenti. Il perimetro di monitoraggio sarà individuato di concerto con l'amministrazione nell'ambito dei servizi professionali previsti nel paragrafo 5.2 "Servizio professionale di implementazione e *tuning* del servizio di monitoraggio".

5.1.3.2 Reporting

Per mantenere la massima compatibilità con i deliverable degli altri servizi di sicurezza previsti a catalogo nel Contratto SPC il RTI propone due tipologie di report:

- **Executive Summary**, un rapporto di sintesi destinato prevalentemente al management e al personale non tecnico per una comprensione immediata degli attacchi riscontrati. Si tratta di un elaborato in excel contenente tutti i dati relativi ai KPI di servizio.
- **Technical Report** una scheda incidente con tutte le indicazioni necessarie per la comprensione dei problemi riscontrati, per la loro classificazione in termini di severità e con un suggerimento relativo alle misure più idonee da adottare per la loro risoluzione. Tale rapporto fornirà il dettaglio delle principali vulnerabilità/minacce riscontrate.

5.1.3.3 Log Management

L'elemento di servizio *log management* prevede:

- la raccolta dei dati registrati nei log dei dispositivi controllati;
- la conservazione dei file di log nel formato RAW;
- la conservazione dei log relativi ad eventi correlati in modo da preservarne la disponibilità e l'integrità, in accordo ai requisiti imposti dal testo unico sulla privacy e successive modificazioni;
- la conservazione dei dati delle Amministrazioni contraenti per almeno 180 giorni, con conseguente applicazione delle politiche di rotazione e cancellazione sicura dei dati anteriori al periodo definito;
- la possibilità di estrarre i log secondo specifiche richieste dell'Amministrazione.

E' possibile effettuare copie dei dati indicando una frequenza limite (ad es. una volta al mese) e utilizzando supporti messi a disposizione dal cliente via VPN. Le estrazioni non sono soggette a SLA.

5.1.4 Vincoli e assunzioni del Servizio SM1

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 2500 EPS di picco. In caso di ampliamento del perimetro/sistemi oggetto di servizio RTSM 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 mette a disposizione un sistema di *ticketing (NGS)* sviluppato internamente sul quale il cliente potrà verificare lo stato degli *incident* ed avere informazioni sugli stessi.

5.1.5 Componenti del Servizio SM1 da installare presso l'Amministrazione contraente

Il servizio prevede il deployment della componente di raccolta dei log (collettore) deputato alle funzioni di *data collecting and forwarding* «on premise» c/o l'Amministrazione contraente.

Ciò è infatti necessario al fine di veicolare verso il SIEM gli eventi di sicurezza che provengono dal data centre del cliente. Sarà dunque predisposto un *virtual log collector* (VLC), in formato di *virtual appliance*, che collezionerà e inoltrerà i log provenienti dalle sorgenti verso il SIEM. I log e il contenuto descrittivo verranno archiviati in formato di metadati a servizio delle attività di investigazione e di *reporting*.

La predisposizione delle risorse virtuali necessarie all'implementazione del VLC è a carico dell'Amministrazione (anche nel caso di servizi in Cloud); il VLC dovrà essere ospitato presso il *data centre* del cliente (o in alternativa su un server fisico, sempre presso i CED dell'Amministrazione) e disporre delle risorse qui di seguito elencate in tabella. E' esclusa la fornitura di risorse HW da parte del RTI.

Tabella 8: Requisiti per il VLC presso il data centre del cliente

nr. CPU	Specifiche CPU	RAM	Memoria di massa
4	Intel Xeon CPU @ 2.00 GHz	8 GB	150 GB

La Virtual Appliance richiede un sistema di virtualizzazione basato su Vmware (versioni 5.5/6.0/6.5) poiché non può essere installata su macchine fisiche in modalità stand-alone e viene fornita con un'unica interfaccia di raccolta-log.

Il sistema operativo supportato dal VLC è CentOS 7 (64bit).

Non sono previste integrazioni di sorgenti e/o servizi che non sono nativamente supportati dal sistema SIEM in termini di connettori.

5.1.6 Modalità di erogazione del Servizio SM1

Il servizio sarà erogato in modalità «as a service», come previsto da capitolato tecnico. Di seguito viene riportata una tabella relativa alle finestre di servizio.

Tabella 9: Finestre di servizi

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

5.1.7 Quantità e prezzi del Servizio SM1

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].

5.1.8 Attivazione del Servizio SM1

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

Al fine di garantire una corretta attivazione integrazione del nuovo servizio SPC Cloud Lotto 2 tramite VLC per arrivare alla fase di conduzione, sarà necessario strutturare un processo di attivazione e tuning ad-hoc che preveda il design e l'integrazione delle sorgenti sul SIEM del RTI. Questo richiederà l'utilizzo di Servizi Professionali, più avanti dettagliati nei paragrafi successivi.

5.2 Servizi professionali SP

In questa sezione si descrivono le attività richieste dell'Amministrazione contraente e svolte come servizi professionali. In tale ambito il Fornitore si impegna a erogare tutti i servizi descritti nel presente documento e assicura la disponibilità delle risorse indicate per supportare l'Amministrazione contraente alla loro erogazione.

Per quanto riguarda i servizi a **Task**, coerentemente con 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 corpo". La fatturazione avverrà alla **consegna dei deliverable concordati**, previo benestare sulla base dello stato dell'avanzamento lavori determinato coerentemente con il piano di lavoro definito in Appendice B.

Per quanto riguarda l'erogazione a **Supporto**, coerentemente con 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 corpo". La fatturazione avverrà **periodicamente sulla base dello stato dell'avanzamento lavori** determinato coerentemente con il piano di lavoro definito in Appendice B e sarà riconosciuta bimestralmente come previsto in Allegato 4B – Schema Contratto Esecutivo – Lotto 2.

Le attività potranno essere svolte nelle sedi dell'Amministrazione contraente per quanto riguarda attività che necessitano interfacciamento diretto con l'Amministrazione stessa. A tale scopo devono essere predisposte dall'Amministrazione adeguati spazi e facilities. Le attività che non necessitano di interfacciamento diretto con personale dell'Amministrazione saranno erogate in modalità back office da sedi dell'RTI o da altre sedi operative.

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

5.2.1 L2.S3.9 SP1 - Servizi professionali - Supporto al Monitoraggio

Il servizio professionale di Tuning e Supporto al Monitoraggio SOC è volto a supportare il cliente durante il ciclo di vita del servizio, al fine di eseguire un tuning specifico sulle piattaforme di erogazione del servizio.

5.2.1.1 Descrizione del servizio SP1

Il servizio prevede le seguenti attività specifiche:

- **Applicazione delle regole di retention**, durante tale fase saranno aggiornate, se necessario, le regole di retention applicate e ne sarà verificata l'efficacia;
- **Integrazione delle sorgenti a perimetro,** dove si procederà all'integrazione delle sorgenti nel sistema SIEM, alla verifica del corretto logging e alla verifica dell'interpretazione dei log, fino alla normalizzazione in caso di Custom-Datasource (dove richiesto custom-parsers).
- **Implementazione delle politiche di gestione della memorizzazione dei dati** (Retention e Archiviazione). la soluzione adottata consentirà di definire regole per la retention dei log per 6 mesi Online/Offline;
- **Tuning dei meccanismi di acquisizione e gestione log**. Tale fase riguarderà le operazioni di tuning avanzato della piattaforma rivolte all'implementazione delle configurazioni del livello di acquisizione. Tra le attività principali vanno annoverate:
    - revisione delle fonti e ottimizzazione di tutte le tipologie di sorgente dati;
    - revisione tempistiche e pianificazione dei cicli di raccolta flussi/eventi;

- **Applicazione delle regole di correlazione:** Durante tale fase saranno applicate sia le regole di correlazione standard, proprietarie di Leonardo, sia le regole di correlazione custom specifiche per il contesto Cliente.

5.2.1.2 Deliverable del servizio SP1

Come deliverable del servizio è previsto il rilascio di un documento riassuntivo di alto livello che riassume le regole di correlazione "Custom" (es. nome regola e breve descrizione).

5.2.1.3 Vincoli e assunzioni del servizio SP1

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.

È previsto il rilascio di un massimo di 5 regole di correlazione custom, che saranno rilasciate al Cliente al termine del servizio. Non saranno, in nessun caso, rilasciate le regole di correlazione, proprietarie di Leonardo, utilizzate per l'erogazione del servizio.

Il numero massimo di parser che saranno prodotti in questo servizio è pari a 5. Saranno eventualmente valutate compensazioni tra regole e parser, per un numero totale pari a 10.

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

5.2.1.4 Modalità di erogazione del servizio SP1

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". Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente. La fatturazione avverrà sulla base dello stato dell'avanzamento lavori determinato coerentemente con il piano di lavoro definito in Appendice B, alla consegna dei deliverable concordati, previo benestare.

Le attività a corpo saranno erogate presso le sedi dell'Amministrazione Contraente, presso le sedi del RTI, o presso altra sede da concordare con l'Amministrazione stessa.

5.2.1.5 Quantità e prezzi del servizio SP1

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].

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 corpo".
Si rende noto che non sono previsti e definiti specifici livelli minimi di servizio da garantire e/o meccanismi di penalizzazione da applicare al fornitore, salvo quanto disciplinato in materia di responsabilità contrattuale dalla vigente normativa.

5.2.1.6 Attivazione del servizio SP1

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

5.2.2 L2.S3.9 SP2 - Servizi professionali: Presidio Operativo

I servizi professionali di presidio sono finalizzati alla fornitura di supporto tecnico specialistico nell'ambito delle seguenti aree di competenza:

- Gestione dei bollettini di alert;
- Information Security Policy and Procedure;
- Information Security Specific Policy, Hardening and Configuration Management;
- Supporto alla migrazione dei servizi nell'ambito PSN.

Nei paragrafi successivi sono descritte nel dettaglio le attività sopra elencate.

5.2.2.1 Descrizione del servizio SP2

Gestione Dei Bollettini Di Alert

Il servizio è finalizzato alla fornitura di un supporto tecnico specialistico per la progettazione e pianificazione delle iniziative di contrasto/contenimento delle violazioni di sicurezza segnalate attraverso i bollettini di alert prodotti attraverso il servizio di monitoring and alerting.

Il servizio sarà erogato da un tecnico specializzato con esperienza nella gestione dei processi di incident handling, a cui saranno affidate le seguenti attività:

- analisi dei bollettini e verifiche di riscontro delle condizioni di severità/criticità degli allarmi;
- circoscrizione del perimetro e degli asset informatici interessati dall'allarme;
- supporto alla definizione ed alla pianificazione delle misure di contrasto/contenimento degli incidenti di sicurezza.

Deliverables: il servizio prevede il rilascio delle schede di analisi dei bollettini di alert ricevuti dal gruppo di monitoraggio.

Information Security Policy And Procedure Management

Il servizio è finalizzato alla stesura di documentazione relativa alle Politiche di sicurezza ed alle procedure di gestione applicabili al contesto organizzativo specifico. La documentazione fornisce un quadro di riferimento delle regole, delle modalità operative e delle responsabilità funzionali per tutti i processi di gestione della sicurezza delle informazioni e delle comunicazioni.

Tutta la documentazione prodotta e manutenuta nell'ambito di questo servizio è organizzata secondo i criteri di catalogazione di seguito descritti:

- Politiche o linee guida di indirizzamento;
- Procedure operative che descrivono le modalità di attuazione e le responsabilità organizzative dei processi di gestione della sicurezza.

L'insieme dei documenti così strutturato costituisce il "sistema documentale di riferimento per la gestione della sicurezza" e può assumere per l'Ente valore di direttiva ed è pertanto subordinata all'approvazione del/dei responsabile/i dei processi regolamentati.

In fase implementativa il servizio consiste nella reiterazione delle seguenti attività:

- raccolta delle informazioni utili alla stesura del documento (es. processi interessati, normative applicabili, infrastrutture tecnologiche interessate)
- stesura del documento in bozza;
- condivisione del documento in bozza con il personale interno incaricato di supervisionare il processo di gestione della documentazione di sicurezza;
- condivisione del documento in bozza con i referenti delle funzioni organizzative interessate;
- rilascio del documento nella versione definitiva.

Deliverables: il servizio viene attivato dal Cliente che, in funzione delle esigenze, può richiedere la definizione di politiche, linee guida e procedure attingendo alla seguente lista ovvero proponendo tematiche non presenti:

- Politiche di indirizzamento e linee guida
  - Politica generale per la sicurezza delle informazioni;
  - Politica generale per la classificazione delle informazioni;
  - Politica generale per il trattamento delle informazioni classificate;
  - Linee guida per la conduzione delle verifiche di conformità e adeguatezza della sicurezza delle informazioni;
  - Politica Specifica per gli Amministratori di Sistema;
  - Politica generale per il corretto utilizzo delle risorse informative: istruzioni al personale
  - Politica per la gestione delle utenze;
  - Linea guida per il processo di ICT Risk Management;
  - Linea Guida per il governo della sicurezza informatica;
  - Linea Guida per la raccolta, conservazione e analisi dei dati di tracciamento (log);
- Procedure operative:
  - Procedura operativa per la gestione del sistema documentale per la sicurezza delle informazioni;
  - Procedura per la definizione del ciclo di vita delle identità digitali e delle credenziali di autenticazione associate al personale interno all'Ente;
  - Procedura per la definizione del ciclo di vita delle identità digitali e delle credenziali di autenticazione degli utenti esterni all'Ente;
  - Procedura operativa per la comunicazione degli incidenti di sicurezza informatica;
  - Procedura operativa per la gestione degli incidenti di sicurezza informatica;
  - Procedura operativa per la conduzione delle attività di vulnerability assessment;
  - Procedura operativa per la conduzione dei test di impenetrabilità;
  - Procedura operativa per le attività di change management e patch management sui sistemi critici per la sicurezza delle informazioni e delle comunicazioni.

Information Security Specific Policy, Hardening And Configuration Management

Il servizio è finalizzato alla stesura di documentazione tecnica relativa alla gestione delle configurazioni di sicurezza dei sistemi informatici e delle infrastrutture ICT, al fine di fornire un insieme esaustivo e dettagliato di istruzioni operative di riferimento per il personale tecnico, interno ed esterno, preposto alla gestione ed alla configurazione delle infrastrutture ICT.

Lo scopo ultimo è quello di alimentare il "sistema documentale di riferimento per la gestione della sicurezza", ed ha come finalità quella di creare un insieme di regole tecniche specifiche per determinati ambienti, la cui osservanza è ritenuta obbligatoria (information security baseline).

Di seguito sono descritte delle possibili Specific Policy che possono essere richieste dal Cliente in funzione delle proprie esigenze.

- Definizione dei criteri per la stesura dei requisiti di sicurezza delle applicazioni: l'integrazione delle attività di progettazione delle misure di sicurezza applicative prevede che la stesura dei requisiti di sicurezza sia conforme al conseguimento dei livelli di copertura dei rischi prefissati. A tal fine, nella stesura dei requisiti di sicurezza, deve essere documentato il razionale che attesti la conformità dei requisiti con gli obiettivi stabiliti dalle politiche di sicurezza aziendali. Con questa attività verranno fissati ed opportunamente documentati, i criteri per la stesura dei requisiti di sicurezza, anche conformemente a quanto stabilito dagli standard internazionali, che dovranno essere adottati dalle strutture di sviluppo e/o dai fornitori nella stesura della documentazione di progetto relativa alla sicurezza dell'applicazione.

- Definizione dei criteri per la stesura delle specifiche funzionali di sicurezza applicativa: con questa attività verranno fissati ed opportunamente documentati, i criteri per la stesura delle specifiche funzionali relative alle misure di sicurezza progettate, anche conformemente a quanto stabilito dagli standard internazionali; tali criteri dovranno essere adottati dalle strutture di sviluppo nella stesura della documentazione di progetto relativa alla sicurezza dell'applicazione.
- Definizione dei criteri per l'esecuzione dei test funzionali di sicurezza: o definizione dei livelli e delle tipologie di test: l'introduzione dei test funzionali di sicurezza nel ciclo di sviluppo applicativo consente di eliminare la maggior parte delle vulnerabilità note, potenzialmente insite nell'applicazione. La fase dei test funzionali di sicurezza, eventualmente propedeutica al collaudo dell'applicazione, favorisce la sensibilizzazione degli sviluppatori verso le tematiche di sicurezza, e contribuisce in maniera significativa al miglioramento del grado di robustezza delle applicazioni prodotte. Con questa attività verrà definita la metodologia a supporto dell'esecuzione dei test da svolgere per il controllo della fornitura degli applicativi, dettagliando le fasi di:
    - definizione della strategia di test;
    - definizione delle non conformità ed eliminazione delle vulnerabilità rilevate.
- Definizione delle regole tecniche per lo sviluppo di applicazioni in sicurezza: scopo di queste attività è quello di fornire alle funzioni aziendali preposte allo sviluppo di applicazioni informatiche, i criteri guida e le "best practices" necessarie a contenere l'insorgere di vulnerabilità intrinseche alle applicazioni che, in quanto tali, sono difficilmente rilevabili ed eliminabili in fase di esercizio. L'importanza di adottare particolari accortezze nello sviluppo delle piattaforme applicative, deriva dal crescente numero di violazioni intenzionali della sicurezza, effettuate sfruttando proprio questo tipo di vulnerabilità, rilevabili solo tramite un'attenta analisi della piattaforma applicativa. Nel corso di questa attività saranno quindi individuati i requisiti di base che devono essere rispettati per l'implementazione di applicazioni in sicurezza, indipendentemente dall'ambiente di sviluppo e dalla tecnologia utilizzata per la specifica implementazione software.
- Best practices per lo sviluppo di applicazioni WEB: o Utilizzo sicuro delle sessioni di autenticazione e autorizzazione: questa attività consente di prevenire eventuali vulnerabilità correlate con lo sviluppo di applicazioni web che, allo stato attuale, rappresentano la principale fonte di rischio per la sicurezza delle informazioni gestite. In questa fase saranno definite le raccomandazioni per la prevenzione delle principali vulnerabilità applicabili allo specifico sviluppo, nonché le best practice di programmazione per:
    - Data validation;
    - Error Handling.
- Best practices per lo sviluppo di basi di dati sicure: questa attività consente di prevenire eventuali vulnerabilità correlate con lo sviluppo di basi dati utilizzando piattaforme DBMS.
- Best practices per l'implementazione dei servizi di comunicazione: con questa attività verranno definite le regole da adottare per la sicurezza dei servizi di comunicazione, con particolare riferimento a:
    - Principi di sicurezza logica e architetturale;
    - Requisiti di sicurezza perimetrale.

Deliverables: il servizio viene attivato dal Cliente che, in funzione delle esigenze, può richiedere la definizione di politiche specifiche attingendo alla seguente lista ovvero proponendo tematiche non presenti:

- Politica Specifica per la stesura dei requisiti di sicurezza applicativa;
- Politica Specifica per la stesura delle specifiche funzionali di sicurezza applicativa;
- Politica Specifica per l'esecuzione dei test funzionali di sicurezza;
- Politica specifica per lo sviluppo di applicazioni in sicurezza;
- Politica Specifica per lo sviluppo sicuro di applicazioni web;
- Politica Specifica per lo per lo sviluppo sicuro di basi di dati;
- Politica Specifica per l'implementazione dei servizi di comunicazione.

Supporto alla migrazione dei servizi nell'ambito del PSN

Il servizio ha lo scopo di facilitare il passaggio di consegne dei task citati nel presente Progetto dei Fabbisogni, all'approssimarsi della scadenza della convenzione SPC Lotto 2. Il processo di Trasferimento del Know-How a fine fornitura viene organizzato per assicurare la massima attenzione alla continuità dei servizi erogati. Per il raggiungimento del suddetto obiettivo il RTI ritiene necessario adottare un processo tale da attuare le modalità operative ritenute più efficienti e che garantiscano il miglior risultato. Tale processo prevede anche la garanzia di supporto per la migrazione al PSN ovvero altra struttura Cloud qualificata.

Il servizio è articolato nelle seguenti fasi:

- Nomina di un Transition Manager che ha la responsabilità di tutta la fase di rilascio del servizio compresa la transizione operativa e la migrazione, svolgendo le attività di coordinamento e governo di tutti i processi previsti, identificazione delle interfacce propedeutiche alla continuità dei servizi, supervisione della corretta esecuzione delle attività, coordinamento del team selezionato per supportare le fasi di preparazione e migrazione su cloud delle infrastrutture;
- Identificazione degli obiettivi, degli Stakeholder e dei temi su cui effettuare il passaggio di consegne (servizi e infrastrutture);
- Predisposizione di apposite checklist per la fase di verifica;
- Condivisione con l'Amministrazione di un Piano di Rilascio del Servizio con: pianificazione di dettaglio delle attività, definizione dell'organizzazione, individuazione delle metodologie da utilizzare opportunamente adattate al contesto;
- Condivisione delle configurazioni degli strumenti ad oggi in uso, al fine di facilitare la predisposizione degli ambienti che accoglieranno i servizi di AIFA;
- Supporto alla realizzazione di un Piano di Migrazione verso il PSN, al fine di individuare propedeuticità e criticità legate ai servizi;
- Supporto alla transizione operativa.

5.2.2.2 Deliverable del servizio SP2

I deliverables sono stati descritti nel precedente paragrafo, in correlazione con ognuna delle attività in esso dettagliate.

5.2.2.3 Vincoli e assunzioni del servizio SP2

L'erogazione del servizio presume il supporto attivo di un referente interno AIFA che svolga mansioni di interfaccia tra gli analisti della RTI ed il personale interno o altri fornitori AIFA, provvedendo a convocare le riunioni/interviste ed a fornire la documentazione eventualmente richiesta.

Sono previsti un massimo di 6 documenti richiedibili dall'Amministrazione per gli ambiti previsti dal servizio SP4.

5.2.2.4 Modalità di erogazione del servizio SP2

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". Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente. La fatturazione avverrà sulla base dello stato dell'avanzamento lavori determinato coerentemente con il piano di lavoro definito in Appendice B, alla consegna dei deliverable concordati, previo benestare.

Le attività a corpo saranno erogate presso le sedi dell'Amministrazione Contraente, presso le sedi del RTI, o presso altra sede da concordare con l'Amministrazione stessa.

5.2.2.5 Quantità e prezzi del servizio SP2

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].

5.2.2.6 Attivazione del servizio SP2

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

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 10.

Tabella 10: 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

					2023		
ID SPC	Descrizione	Metrica	Fascia	Prezzo unitario	Nun.tà	Mesi	Prezzo
L2.S3.10	RTSM	Device/anno	Fascia 1 50 Device (max 300 eps)	€ 313,82	0	12	€ 0,00
			Fascia 2 100 Device (max 700 eps)	€ 564,85	0	12	€ 0,00
			Fascia 3 200 Device (max 1.600 eps)	€ 544,30	0	12	€ 0,00
			Fascia 4 500 Device (max 5.000 eps)	€ 508,10	250	12	€ 127.025,00
			Fascia 5 oltre 500 Device (oltre 5.000 eps)	€ 470,00	0	12	€ 0,00
TOTALE							€ 127.025,00

						2023	
ID SPC	Descrizione	Metrica	Servizio	Figura professionale	Prezzo unitario	Nun.tà	Prezzo
L2.S3.9	Serv.Prof.	giorno/uomo	H8	Capo progetto	€ 300,00	21	€ 6.300,00
				Security Architect	€ 372,90	84	€ 31.323,60
				Specialista di tecnologia/prodotto Senior	€ 295,00	110	€ 32.450,00
				Specialista di tecnologia/prodotto	€ 235,00	0	€ 0,00
		giorno/uomo	H24	Specialista di tecnologia/prodotto Senior (H24)	€ 1.180,00	0	€ 0,00
				Specialista di tecnologia/prodotto (H24)	€ 930,00	0	€ 0,00
TOTALE							€ 70.073,60

						2023	
ID SPC	Descrizione	Metrica	Servizio	Figura professionale	Prezzo unitario	Nun.tà	Prezzo
L2.S3.9	Serv.Prof.	giorno/uomo	H8	Capo progetto	€ 300,00	12	€ 3.600,00
				Security Architect	€ 372,90	121	€ 45.120,90
				Specialista di tecnologia/prodotto Senior	€ 295,00	0	€ 0,00
				Specialista di tecnologia/prodotto	€ 235,00	0	€ 0,00
		giorno/uomo	H24	Specialista di tecnologia/prodotto Senior (H24)	€ 1.180,00	0	€ 0,00
				Specialista di tecnologia/prodotto (H24)	€ 930,00	0	€ 0,00
TOTALE							€ 48.720,90

Il valore totale dell'iniziativa è pari a € € 245.819,50 (IVA esclusa), per un valore finale pari a € 299.899,79 comprensivo di IVA.

Su richiesta dell'Amministrazione uno o più servizi in oggetto potranno essere terminati anticipatamente alla fine del mese solare in cui verrà effettuata la richiesta di cessazione.

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

ID Servizio	Attività	Inizio	Fine	Vincoli
SM.1	L2.S3.10 - Servizio di Monitoraggio	T0		
SP.3	L2.S3.9 - Servizi professionali - Avvio e Supporto al Monitoraggio	T0		
SP.4	L2.S3.9 - Servizi professionali - Presidio Operativo	T0		