Comune di Napoli
Data: 30/07/2020, IG/2020/0000927

14-02-2020
LDO/CYS/P/0007117/20

Identificativo: **SRic20180000027775 Rev. 1.1**

Data: **31.01.2020**

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

Comune di Napoli

Progetto dei fabbisogni

Costituito

Raggruppamento Temporaneo di Imprese

composto da:

Leonardo SpA - Divisione Cyber Security

IBM SpA

Sistemi Informativi srl

Fastweb SpA

Pubblico

	Nome e Ruolo	Firma
Autore		
	Carletto Riemma – Sales Engineer Fastweb	
Verifica		
	Oreste Romei - Business Development Fastweb	
Approvazione		
	Giuseppe Nicastro	
Autorizzazione		
	Mauro Magro	

Approvazioni Aggiuntive

Azienda	Nome e Ruolo	Firma

Lista di Distribuzione

Rev.	Data	Destinatario	Azienda

Registro delle Revisioni

Rev.	Data	Descrizione delle modifiche	Autori
1.0	31.01.2020	Prima pubblicazione	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.

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 (indicata nel documento come Amministrazione contraente) contenute nel proprio Piano dei fabbisogni [DA-5]. 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.

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" – *Comune di Napoli del 31.01.2020*
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 Ragruppamento
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 Divisione Cyber Security S.p.A. (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	COMUNE DI NAPOLI
Indirizzo	VIA ADRIANO SNC
CAP	80126
Comune	NAPOLI
Provincia	NA
Regione	CAMPANIA
Codice Fiscale	80014890638
Nominativo referente Contratto Esecutivo:	LUIGI VOLPE
Indirizzo mail	reti.tecnologiche@comune.napoli.it reti.tecnologiche@pec.comune.napoli.it
PEC (SI/NO)	SI

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

Nome	LUIGI
Cognome	VOLPE
Telefono fisso	081.7958800
Indirizzo mail	reti.tecnologiche@comune.napoli.it reti.tecnologiche@pec.comune.napoli.it
PEC (SI/NO)	SI

5 PROPOSTA TECNICO-ECONOMICA

L'estrema eterogeneità tecnologica e delle applicazioni informatiche, in genere riscontrabile presso le Pubbliche Amministrazioni, determina uno scenario di rischio complessivamente elevato, aggravato dall'obsolescenza accelerata delle tecnologie e dal panorama delle minacce informatiche in costante evoluzione.

In questo contesto i Servizi di Protezione forniti sono finalizzati alla rilevazione di anomalie, minacce ed attacchi alle infrastrutture e ai sistemi delle Amministrazioni. In funzione del contesto specifico e delle necessità dell'Amministrazione, è prevista la possibilità di installare componenti "on premise" presso l'Amministrazione o in modalità "as a service" all'interno del Centro Servizi del Fornitore.

I Servizi di Protezione includono i seguenti Servizi di Sicurezza:

- Vulnerability Assessment (VA);
- Monitoraggio (SIEM).

Tali servizi sottintendono una medesima architettura logica e due principali tipi di attività: Gestione Operativa e Gestione degli Incidenti.

Per garantire l'efficacia del servizio, in ottica di Segregation of Duty, tali attività sono erogate da due team specializzati, dedicati e separati. Il team di Gestione Operativa si occupa della gestione dei sistemi tecnologici e della relativa manutenzione per garantire la continuità operativa, della gestione delle policy per garantire la continua aderenza delle configurazioni alle policy concordate con l'Amministrazione e in ultimo del reporting.

Di seguito la lista dei servizi previsti nella fornitura.

Id Servizio	Titolo	Descrizione
L2.S3.4 (VA)	Vulnerability Assessment	Servizio di vulnerability assessment
L2.S3.9 (SP)	Servizi Professionali	Servizi di supporto per la sicurezza
L2.S3.10 (SIEM)	Servizi di monitoraggio	Servizi di monitoraggio

5.1 Vulnerability Assessment - L2.S3.4 (VA)

5.1.1 Obiettivi del Servizio L2.S3.4 VA

L'obiettivo del Servizio è fornire le attività di Vulnerability Assessment (di seguito VA) di tipo infrastrutturale per il perimetro di riferimento dell'Amministrazione per disporre di un quadro completo delle vulnerabilità presenti all'interno della propria infrastruttura IT, tramite lo svolgimento di verifiche tecniche orientate alla sicurezza, al fine di ricavarne indicazioni sulle potenziali debolezze e lacune che potrebbero essere sfruttate e su eventuali ulteriori interventi che occorre porre in essere per aumentarne la robustezza.

L'esecuzione dei test è subordinata a:

- l'ottenimento della manleva da parte dell'Amministrazione;
- la condivisione ed approvazione del piano di test con l'Amministrazione;
- l'ottenimento delle informazioni relative alla configurazione dell'infrastruttura.

5.1.2 Vincoli e assunzioni del Servizio L2.S3.4 VA

Inoltre 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.

5.1.3 Componenti del Servizio L2.S3.4 VA da installare presso l'Amministrazione contraente

Tutte le componenti tecnologiche previste per l'erogazione del servizio saranno installate presso l'Amministrazione contraente.

5.1.4 Modalità di erogazione del Servizio L2.S3.4 VA

Il servizio sarà erogato in modalità "as a service".

5.1.5 Quantità e prezzi del Servizio L2.S3.4 VA

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 L2.S3.4 VA

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

5.2 Servizio di Monitoraggio – L2.S3.10 (SIEM)

L'Amministrazione intende dotarsi delle necessarie contromisure tecniche ed organizzative che consentano il miglioramento della protezione e la mitigazione del rischio di impatti sulla disponibilità in caso di da attacchi informatici mirati. In particolare, il "Servizio di Monitoraggio - L2.S3.10" consente di acquisire informazioni da un insieme eterogeneo di apparati localizzati nella rete del cliente e inviare queste alla piattaforma SIEM presso il SOC RTI che provvederà alla loro catalogazione e correlazione ai fini dell'individuazione di minacce in atto sulla rete.

5.2.1 Obiettivo del servizio L2.S3.10

Il servizio ha l'obiettivo di garantire la capacità di monitoraggio delle reti dell'amministrazione al fine di individuare tempestivamente eventuali attacchi informatici e consentire di disporre le adeguate contromisure.

Il servizio viene erogato tramite piattaforme centralizzate localizzate presso il SOC RTI. Il SOC RTI, dotato di competenze e tecnologie allo stato dell'arte, è stato realizzato espressamente per garantire la fornitura di Servizi Gestiti di Sicurezza alle grandi realtà Aziendali e Organizzazioni nazionali ed internazionali. Competenza e flessibilità rendono possibile personalizzare, su base Cliente e progetto, i principali aspetti di servizio.

Per la realizzazione e la gestione del proprio SOC il RTI ha potuto sfruttare e mettere a fattore comune le proprie esperienze, infrastrutture, metodologie e know-how già presenti presso le strutture di Network Operation Center (NOC), riconosciute di primissimo piano.

Gli obiettivi del SOC sono:

- 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 delle aziende clienti 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;
- Erogare servizi professionali di alto profilo, finalizzati ad aiutare i clienti a definire il proprio livello di sicurezza determinando potenziali problemi e le relative aree di intervento;

Il SOC è organizzato come di seguito descritto:

- Help Desk di I Livello; Tale struttura avrà il compito di fornire assistenza tecnica per tutte le eventuali segnalazioni e richieste provenienti dai referenti dell'Amministrazione.
- Gruppo di Supporto Specialistico di II Livello che si occupa del supporto di secondo livello garantendo la copertura H24 per tutti i servizi erogati dal SOC.

Il SOC risponde ad un unico Coordinatore che ha funzione di centro di competenza ed escalation nei confronti di tutti i clienti/servizi cui si applicano i servizi specialistici relativi alla sicurezza.

5.2.2 Descrizione del Servizio di Monitoraggio L2.S3.10

Il servizio di rilevamento delle minacce complesse si fonda sull'implementazione di capacità di analisi avanzata e reazione ottenute mediante una piattaforma di sicurezza basata su un motore di analisi virtualizzato signature-less, che analizzi in tempo reale eventuali componenti a rischio (email, flussi di rete, eseguibili, documenti, ecc.) per la rilevazione di Advanced Malware e per la protezione attiva dei flussi di comunicazione.

Il Security Operation Center (SOC) è la struttura del centro servizi preposta alla raccolta e correlazione degli eventi provenienti dalle aree operative e tecnologiche dell'Amministrazione al fine di garantire il corretto monitoraggio delle infrastrutture di sicurezza e la tempestiva rilevazione degli incidenti e delle attività sospette.

A livello tecnologico, l'elemento cardine alla base dell'infrastruttura SOC è la piattaforma Security Information Event Management (SIEM) in grado di supportare i servizi di monitoraggio, di detection ed incident management.

Una soluzione di SIEM è un sistema in grado di raccogliere ingenti quantità di eventi di sicurezza provenienti da fonti eterogenee e strategiche dell'infrastruttura dell'Amministrazione (firewall, IPS/IDS, antivirus, endopoint protection, nodi di rete, servizi applicativi, directory aziendali, ecc.), di normalizzarle e di correlarle secondo precise regole di indagine personalizzate rispetto al contesto e agli scenari di attacchi informatici applicabili. Il SIEM abilita l'individuazione "in tempo reale" di eventuali anomalie, attacchi e/o compromissioni sottoponendole all'attenzione dell'operatore di sicurezza del SOC che, attraverso una console di gestione specifica, opera una prima verifica per escludere falsi positivi e successivamente trasferire il caso ad un analista di sicurezza dell'unità competente per la gestione e la risposta all'incidente.

Il RTI valorizzerà le attività di progettazione e realizzazione della piattaforma SIEM, che sarà caratterizzata da un livello di raccolta e correlazione dedicato e posizionato all'interno dell'infrastruttura ICT della singola Amministrazione e da un sistema di gestione centralizzata che, seppur condiviso tra tutte le Amministrazioni che aderiranno al servizio di monitoring, consentirà di mantenere la separazione dei domini di correlazione e una gestione cifrata dei flussi di comunicazione.

Il Servizio di Monitoraggio si compone delle seguenti componenti di attivazione ed erogazione, di seguito descritte:

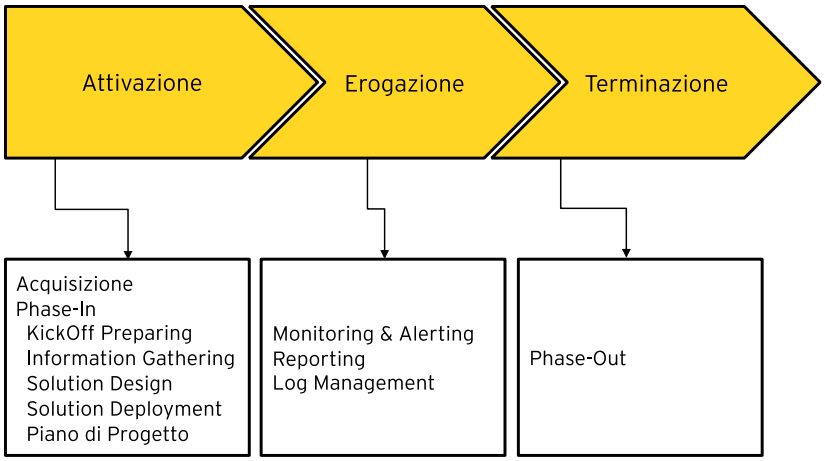

Figura 1 - Componenti del servizio L2.S3.10

5.2.3 Attivazione del servizio L2.S3.10

L'attivazione del Servizio di Monitoraggio è caratterizzata dalle fasi seguono di seguito brevemente descritte.

- **Acquisizione**
  In tale fase saranno definiti i fabbisogni delle Amministrazioni in funzione delle metriche definite in tale documento.
- **Phase-In**
  Conclusa la fase di consolidamento del Piano dei Fabbisogni, il processo di attivazione del Servizio (Phase-in) richiede come prerequisito la progettazione e l'implementazione della Piattaforma SIEM. Il modello architetturale adottato dal RTI prevede di concordare con l'Amministrazione l'eventuale installazione di apparati di raccolta presso le sedi delle stesse. L'analisi degli eventi di Sicurezza sarà gestita tramite console presenti all'interno del Centro Servizi. Tutte le attività di gestione e di monitoraggio afferenti alla piattaforma SIEM saranno quindi erogate da una struttura SOC operante dal Centro Servizi. La progettazione e il deployment della piattaforma SIEM saranno in carico al team specialistico di progettazione e delivery del RTI. L'obiettivo è garantire all'Amministrazione il massimo livello di competenza e di esperienza del personale impiegato rispetto alle problematiche di progettazione, integrazione e realizzazione della soluzione proposta.
  Il progetto di implementazione della piattaforma SIEM sarà organizzato nelle seguenti fasi di lavoro:
  - **Kick Off Preparing**: questa fase assicura che tutte le funzioni e i referenti dell'Amministrazione coinvolti nel progetto condividano le modalità operative e tecniche di esecuzione del progetto stesso. L'avvio del progetto è formalizzato dalla riunione di Kick-off.
  - **Information Gathering**: lo scopo principale di questa fase è la raccolta dei requisiti e di tutte le informazioni di dettaglio per la definizione di un piano di ingegnerizzazione che definisca i tempi, le risorse, l'architettura, e le procedure necessarie per il progetto di implementazione e l'avvio in esercizio della piattaforma SIEM / Log Management.
  - **Solution Design**: terminate le operazioni di Information Gathering, si procederà a quelle di analisi dei requisiti raccolti e modellazione delle varie componenti fisiche, architetturali, di processo e di tuning della piattaforma. L'output di tale fase sarà la redazione del documento di Site Preparation e del Progetto Esecutivo.
- **Solution Deployment**
  Questa fase sarà svolta sulla base delle specifiche tecniche riportate in seguito e include:

- ✓ **Installazione e Configurazione della componente di raccolta della piattaforma SIEM** presso l'infrastruttura dell'Amministrazione al fine di renderla disponibile ed in visibilità sia rispetto alle console di management del Centro Servizi sia alle sorgenti da monitorare nel rispetto dei principi di segmentazione e segregazione della rete condivisi con l'Amministrazione.
- ✓ **Integrazione delle sorgenti a perimetro**: Le operazioni di integrazione delle sorgenti, a seguito delle operazioni di deployment delle componenti della soluzione SIEM finalizzate alla raccolta dei log, saranno eseguite secondo il modello sviluppato nella fase precedente. Il processo di integrazione sarà strutturato, in condivisione con l'Amministrazione.
- ✓ **Tuning dei meccanismi di acquisizione e gestione log**: Tale fase riguarderà le operazioni di tuning avanzato della piattaforma rivolte all'implementazione delle configurazioni al fine di migliorare il livello di acquisizione.
- ✓ **Implementazione delle politiche di gestione della memorizzazione dei dati** (Retention e Archiviazione). La soluzione adottata dovrà consentire di definire regole personalizzate per la retention dei log. In accordo con le esigenze dell'Amministrazione si procederà ad implementare eventuali policy differenziate per la retention degli eventi nel breve e medio periodo, processi automatici di export dei eventi per backup a lungo termine;
- ✓ **Implementazione delle regole di correlazione**: Durante tale fase saranno implementate le regole di correlazione;
- ✓ **Configurazione del Modello di Rischio** associato ai sistemi inclusi nel perimetro di applicazione della soluzione mediante la definizione di un modello di categorizzazione dei sistemi stessi. Il modello di Rischio consente agli analisti di indagare e rispondere alle operazioni classificate come critiche per i servizi erogati dall'Amministrazione;
- ✓ **Implementazione degli allarmi e impostazione dei template di reportistica**. Integrati gli asset e definite le regole, si procederà all'implementazione dei template di reportistica e alla configurazione degli automatismi per la schedulazione dei report e degli allarmi;
- ✓ **Collaudo e rilascio della piattaforma**: L'attività di test prevede la verifica del corretto funzionamento dell'infrastruttura realizzata e l'aderenza ai requisiti. I test comprendono la verifica della corretta acquisizione delle sorgenti e del corretto funzionamento d'insieme. Le specifiche di test saranno definite in modo congiunto tra l'Amministrazione e il RTI durante la fase di analisi dei requisiti;
- ✓ **Documentazione di Progetto**. L'esito positivo del collaudo e il rilascio della documentazione attinente formalizzano la chiusura della prima fase del progetto.

- **Piano di Progetto** sulla base delle specifiche organizzative al fine di fornire le seguenti specifiche:
  - ✓ Sintesi delle caratteristiche del progetto;
  - ✓ Durata complessiva;
  - ✓ Vincoli, tra i quali la disponibilità di risorse dell'Amministrazione coinvolte organizzative e tecniche e le principali milestone per la verifica del corretto avanzamento dei lavori;

5.2.4 Erogazione del servizio L2.S3.10

Il Servizio di Monitoraggio sarà erogato in modalità "as a service" da un Security Operation Center (SOC) dislocato all'interno del Centro Servizi. I servizi saranno erogati dal SOC su base continuativa H24 o nelle fasce orarie concordate a seconda delle esigenze dell'Amministrazione.

I servizi forniti includono i seguenti elementi:

- Monitoring & Alerting
- Reporting
- Log Management

5.2.4.1 Monitoring & Alerting

L'elemento di servizio Monitoring & Alerting prevede:

- L'identificazione di eventuali incidenti, 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;
- La 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;
- La 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).

Il livello di allarme di una severity/minaccia sarà determinato dal personale del SOC attraverso un approccio qualitativo sulla base dei seguenti elementi:

- Categoria e livello di gravità della severity/minaccia (severità);
- Criticità delle risorse IT coinvolte (se disponibili le informazioni).

I valori associati a ciascuno dei due elementi di sicurezza sono assegnati dagli operatori e analisti del SOC sulla base delle informazioni acquisite (eventi pervenuti attraverso la piattaforma SIEM, analisi preliminare effettuata dalle fonti informative, ecc.) e delle specifiche competenze in materia di gestione degli incidenti di sicurezza.

Il servizio di Monitoraggio potrà essere esteso alle seguenti tipologie di dispositivi di sicurezza, elencate in modo esemplificativo e non esaustivo, previa verifica del parsing delle sorgenti:

- **IDS/IPS e dei Firewall**: monitoraggio in tempo reale dei dispositivi IDS/IPS e dei firewall gestiti dal Centro Servizi del RTI (qualora inclusi nei servizi di Sicurezza previsti per il Lotto2) o dalle funzioni dell'Amministrazione. Questo controllo permette la rilevazione in tempo reale delle minacce segnalate dai suddetti dispositivi e la loro tempestiva segnalazione;
- **Antimalware e Antispam**: monitoraggio in tempo reale dei dispositivi antimalware/antispam gestiti dal Centro Servizi del RTI (qualora inclusi nei servizi di Sicurezza previsti per il Lotto2) o dalle funzioni dell'Amministrazione. Questo controllo permette la rilevazione in tempo reale delle minacce segnalate dalle piattaforme antimalware e la loro tempestiva segnalazione;
- **VPN Gateway**: monitoraggio in tempo reale dei VPN Gateway e degli accessi remoti. Questo controllo permette la rilevazione in tempo reale delle minacce o i tentativi di accesso segnalati dai VPN gateway e la loro tempestiva segnalazione;
- **Internet Proxy/Web Security**: monitoraggio in tempo reale del servizio di navigazione Internet via Proxy gestiti dal Centro Servizi del RTI (qualora inclusi nei servizi di Sicurezza previsti per il Lotto2) o dalle funzioni dell'Amministrazione. Questo controllo permette la rilevazione in tempo reale delle minacce segnalate dalle piattaforme proxy, comprese le eventuali violazioni di policy, o navigazione su URL sospette o compromesse, e la loro tempestiva segnalazione;
- **Web content filtering**: monitoraggio in tempo reale del servizio di web content filtering. Questo controllo permette la rilevazione in tempo reale delle minacce segnalate dalle piattaforme di web content management, comprese le eventuali violazioni di policy, o navigazione su URL non consentite o segnalate, e la loro tempestiva segnalazione;
- **Application control**: monitoraggio in tempo reale del servizio di controllo applicazioni. Questo controllo permette la rilevazione in tempo reale delle minacce segnalate dalle piattaforme di

application control, comprese le eventuali violazioni di policy, utilizzo elusivo di applicazioni web non consentite e la loro tempestiva segnalazione;

- **Database Control**: monitoraggio degli accessi ai RDBMS, tramite controllo degli accessi e profili di Audit. Questo controllo permette la rilevazione in tempo reale delle minacce o i tentativi di accesso segnalati RDBMS e la loro tempestiva segnalazione;

Con la finalizzazione della fase di collaudo della soluzione SIEM con esito positivo, viene formalmente attivato il Servizio di Monitoraggio. All'interno del SOC sarà presente un team di specialisti e analisti di sicurezza che controlleranno in maniera continuativa la console di monitoraggio. Tutte le anomalie, laddove previsto dalla classificazione degli eventi/potenziali incidenti, saranno tracciate mediante apertura di un ticket sulla piattaforma di trouble ticketing ad uso del SOC su cui saranno registrate tutte le attività di indagine preliminare atte ad effettuare una prima identificazione e a escludere eventuali falsi positivi. Nel caso di riscontro dell'incidente sarà effettuata la segnalazione alle funzioni preposte alla gestione dell'incidente o a responsabili dell'Amministrazione (in genere a seconda del grado di impatto) secondo apposita procedura di notifica. All'interno della notifica, veicolata mediante vari canali da concordare in fase preliminare, tra cui il canale standard della piattaforma di Trouble Ticket in uso all'Help Desk per la comunicazione con l'Amministrazione, sarà presente un link per accesso diretto al sistema di TT del SOC. Oltre all'accesso al ticket, sicuramente nei casi più critici, il personale dell'Amministrazione dell'Unità Locale di Sicurezza (ULS) e responsabile dei sistemi coinvolti nell'incidente sarà supportato nell'analisi e nella classificazione dell'incidente dall'operatore SOC.

Il Servizio di Monitoraggio prevede oltre all'individuazione e alla comunicazione dell'incidente, anche il continuo miglioramento delle configurazioni delle regole di correlazioni del SIEM (Policy Enforcement) e l'emissione di report periodici.

L'elemento di servizio Monitoring & Alerting sarà erogato in modalità H24, per 365 giorni all'anno.

5.2.4.2 Reporting

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. Illustrerà con tecniche di aggregazione di dati e indicatori grafici in modo esaustivo le principali minacce rilevate dalla piattaforma del servizio.
- **Technical Report** un rapporto tecnico con tutte le indicazioni necessarie per la comprensione dei problemi riscontrati, per la loro classificazione in termini di severità e per l'identificazione delle misure più idonee da adottare per la loro risoluzione. Tale rapporto fornirà il dettaglio delle principali vulnerabilità/minacce riscontrate.

5.2.4.3 Log management

L'elemento di servizio Log Management prevede:

- La raccolta dei dati registrati nei log dei dispositivi controllati;
- La possibilità di conservare i 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 per almeno 180 giorni, con conseguente applicazione delle politiche di rotazione e cancellazione sicura dei dati anteriori al periodo definito;
- L'attività di gestione della piattaforma (Configuration & change management, fault management);
- Un insieme standard di report;
- La possibilità di estrarre i log in modalità concordate con l'Amministrazione.

5.2.5 Terminazione (Phase-out) del Servizio L2.S3.10

Il processo di rilascio del Servizio di Monitoraggio segue i processi di Phase-out previsti per i servizi di Sicurezza e descritto al paragrafo § 4.5 del documento di risposta tecnica alla gara: "PROCEDURA RISTRETTA, SUDDIVISA IN 4 LOTTI, PER L'AFFIDAMENTO DEI SERVIZI DI CLOUD COMPUTING, DI SICUREZZA, DI REALIZZAZIONE DI PORTALE E SERVIZI ONLINE E DI COOPERAZIONE APPLICATIVA PER LE PUBBLICHE AMMINISTRAZIONI" afferente al Lotto 2.

5.2.6 Vincoli e assunzioni del Servizio L2.S3.10

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 dall'Amministrazione 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.

5.2.7 Componenti del Servizio L2.S3.10

Per il Servizio di Monitoraggio (SOC) si utilizza una piattaforma centralizzata di Security Information and Event Management (SIEM). Tale piattaforma consiste in un sistema che associa eventi, minacce e rischi per fornire un potente sistema di intelligence per la sicurezza, risposte rapide in caso di necessità, una ininterrotta gestione dei log. La soluzione è intrinsecamente scalabile e modulare e si presenta sotto forma di appliance, con alcune componenti virtualizzabili.

L'architettura prevista si articola nelle seguenti componenti:

- Console di Gestione che compone il Layer Application e Presentation installato presso il Centro Servizi ad uso del team specialistico di monitoraggio
- Sistema di Correlazione e Log Management (Correlatore)che compone il Layer di Data Collecting e Storage installato presso il Centro Servizi
- Sistema di Raccolta Log (Collettore) che compone il Layer di Data Collecting and Forwarding e che sarà installabile "on premise" previo accordo con le Amministrazioni. Per la tipologia di servizio offerto si prevede la possibilità dell'installazione "on premise" per tutte le Amministrazioni che presentano un numero di log consistenti.

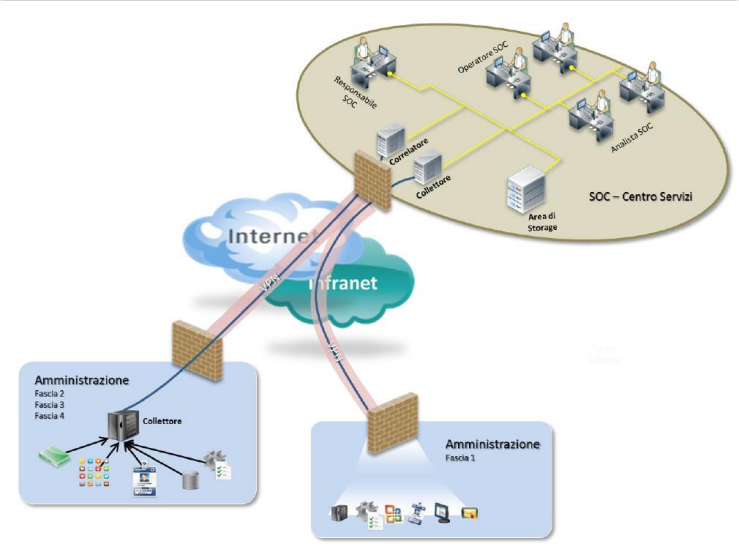

Figura 2 - Architettura di riferimento

Gli eventi sono raccolti dal cluster di Collettori che integrano anche la funzione di Real Time Correlation. La raccolta degli eventi, tipicamente avviene in modalità “agent-less”.

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 che ha il compito di mantenere i file di log “raw” inalterati per il tempo di “retention” specificato. Tale tempo di retention può essere diverso e configurato ad hoc a seconda dei casi da gestire, o più precisamente a seconda delle normative cui rispondere.

La piattaforma effettua poi l’archiviazione dei log raw sullo storage. In seguito i log vengono analizzati localmente, normalizzati, indicizzati ed inviati alla piattaforma di analisi.

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 DB verranno 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.

Le elaborazioni effettuate dal Collettore sui log sono “successive” al loro processamento (firma digitale, compressione ed hashing) per l’invio ai successivi moduli che deve mantenere i raw log “originali ed inalterabili nel tempo”.

Le soluzioni proposte prevedono i moduli Collettori in cluster HA. Si ricorda che tali Collettori sono le componenti cui è demandata la raccolta dei log e, eventualmente, la correlazione degli eventi in real time. Questa configurazione consente di ottenere un meccanismo di alta affidabilità sia per parte di raccolta dei log che per quella di correlazione degli eventi in tempo reale. Il processo di switch-over tra un Collettore e l’altro può essere causato da un fault del Collettore Primario, oppure può essere iniziato manualmente. Nel primo caso è compito del Secondario rilevare il fault del Primario.

5.2.8 Modalità di erogazione del Servizio L2.S3.10

Il servizio viene erogato in modalità “as a service”.

5.2.9 Quantità e prezzi del Servizio L2.S3.10

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].

5.2.10 Attivazione del Servizio L2.S3.10

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

5.3 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 a erogare tutti i servizi descritti nel presente documento e assicura la disponibilità delle risorse indicate per supportare l'Amministrazione contraente alla loro erogazione.

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". 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.

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

5.3.1 Servizio Professionale: Servizi di Supporto alle attività di VA – SP-01

Il servizio supporta l'Amministrazione nelle attività relative al servizio di Vulnerability Assessment.

5.3.1.1 Modalità di erogazione dei Servizi Professionali SP-01

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

5.3.1.2 Attivazione del servizio SP-01

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

5.3.1.3 Deliverable del servizio SP-01

Il servizio prevede il supporto specialistico per le attività relative al servizio di Vulnerability Assessment.

5.3.1.4 Quantità e prezzi del servizio SP-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].

5.3.2 Servizio Professionale: Servizi di Supporto alle attività di Monitoraggio – SP-02

Il servizio supporta l'Amministrazione nelle attività relative al servizio di monitoraggio (SIEM).

5.3.2.1 Modalità di erogazione dei Servizi Professionali SP-02

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

5.3.2.2 Attivazione del servizio SP-02

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

5.3.2.3 Deliverable del servizio SP-02

Il servizio prevede il supporto specialistico per le attività relative al servizio di monitoraggio (SIEM).

5.3.2.4 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].

5.3.3 Servizio Professionale: Servizi di supporto specialistico in ambito sicurezza - SP-03

Il servizio fornisce all'Amministrazione un supporto specialistico avanzato in ambito sicurezza finalizzato a garantire la corretta adozione del sistema di gestione della sicurezza delle informazioni e del sistema di gestione ambientale utili a ottenere il conseguimento delle certificazioni ISO/IEC 27001 e ISO 14001 e a garantire il corretto mantenimento del sistema di gestione privacy, sulla base degli standard di riferimento, attraverso attività tecniche e di natura professionale.

Per raggiungere tale obiettivo le attività individuate sono state suddivise in base a tre stream:

1. Attività per la gestione del sistema della sicurezza delle informazioni e del sistema di gestione ambientale (in riferimento agli standard ISO 27001 e ISO 14001)
    a. Review dei processi e fine tuning delle procedure a supporto della ISO 27001
    b. Review dei processi e fine tuning della documentazione in ambito ISO 27001
    c. Supervisione dei task a supporto ISO 27001
    d. Supervisione delle azioni operative intraprese per l'adeguamento ISO 14001
2. Attività di analisi a supporto dei sistemi di gestione Security / Privacy
    a. Supporto per la gestione del modello GDPR e analisi a supporto
    b. Supporto per l'esecuzione di attività di analisi e di implementazione in ambito ISO 27001
3. Attività di manutenzione ai sistemi di gestione Security / Ambientale / Privacy
    a. Attività integrative Security
    b. Attività integrative Ambientale
    c. Attività integrative Privacy

Si riporta nei paragrafi successivi una descrizione più dettagliata dei singoli stream progettuali e delle specifiche attività a esse correlate.

5.3.3.1 Steam 1: Attività per la gestione del sistema della sicurezza delle informazioni e del sistema di gestione ambientale

Al fine di garantire una corretta gestione del sistema della sicurezza delle informazioni (con riferimento allo standard ISO 27001) e del sistema per la gestione ambientale (con riferimento allo standard ISO 14001), sono state individuate le seguenti attività progettuali:

a. Review dei processi e fine tuning delle procedure a supporto della ISO 27001
b. Review dei processi e fine tuning della documentazione in ambito ISO 27001

c. Supervisione dei task a supporto ISO 27001
d. Supervisione delle azioni operative intraprese per l'adeguamento ISO 14001

Review dei processi e fine tuning delle procedure a supporto della ISO 27001

L'obiettivo di questa attività è eseguire una review delle procedure a oggi adottate dal Comune di Napoli ed eventualmente apportare modifiche e/o integrazione al fine di renderle conformi con i principali standard di settore. In particolare, le procedure interessate nell'ambito del sistema della sicurezza delle informazioni (rif. ISO 27001) riguardano i seguenti processi:

- Gestione degli Accessi fisici e logici;
- Gestione Incidenti di Sicurezza;
- Patch e Vulnerability Management;
- Change Management e Sviluppo sicuro;
- Gestione dei dispositivi mobili e corretto utilizzo dei sistemi informatici;
- Protezione dei dati e cancellazione sicura;
- Gestione Installazione di Software sui Sistemi Operativi;
- Codifica documentale.

Review dei processi e fine tuning della documentazione in ambito ISO 27001

L'obiettivo di questa attività è eseguire una review della documentazione a supporto della certificazione allo standard ISO 27001 ed eventualmente apportare modifiche e/o integrazioni necessarie sulla base degli audit eseguiti precedentemente dal Comune di Napoli. In particolare, la documentazione oggetto di analisi e a supporto della certificazione ISO è la seguente:

- Risk Assessment;
- Compendio Generale della Informazione Documentata;
- Statement of Applicability Summary;

Supervisione dei task a supporto ISO 27001

Attività finalizzate alla supervisione di alcuni task intrapresi dal Comune di Napoli utili a garantire una gestione ottimale dei processi in ambito al sistema della sicurezza delle informazioni. In particolare, durante le attività si garantirà una supervisione dei task operativi affinché siano indirizzati secondo lo standard di riferimento ISO 27001 relativi al processo di Log Management e di Disaster Recovery e Business Continuity.

Supervisione delle azioni operative intraprese per l'adeguamento ISO 14001

Attività finalizzate alla supervisione di alcuni task intrapresi dal Comune di Napoli utili a garantire una gestione ottimale dei processi in ambito al sistema per la gestione ambientale. In particolare, durante le attività si garantirà una supervisione dei task operativi affinché siano indirizzati secondo lo standard di riferimento ISO 14001; inoltre, le attività serviranno a supervisionare i piani di rientro individuati nei precedenti audit nell'ambito del sistema di gestione ambientale e a raccogliere tutte le evidenze necessarie per l'ottenimento della certificazione ISO.

5.3.3.2 Steam 2: Attività di analisi a supporto dei sistemi di gestione Security / Privacy

Al fine di garantire una corretta gestione del sistema della sicurezza delle informazioni (con riferimento allo standard ISO 27001) e del sistema privacy (con riferimento al regolamento GDPR), sono state individuate le seguenti attività di analisi:

a. Supporto per la gestione del modello GDPR e analisi a supporto
b. Supporto per l'esecuzione di attività di analisi e di implementazione in ambito ISO 27001

Supporto per la gestione del modello GDPR e analisi a supporto

Attività finalizzate a garantire un supporto privacy al Titolare del Trattamento, ovvero il Comune di Napoli, per una corretta gestione di tale ambito e per la produzione di tutta la documentazione richiesta dal Regolamento generale sulla protezione dei dati (GDPR). In particolare, i task previsti per l'esecuzione di questa attività riguardano.

- GDPR Assessment e definizione dei piani di rientro
- Supporto per la predisposizione del Registro dei trattamenti
- Data Protection Impact Assessment (max n.5 trattamenti)

Supporto per l'esecuzione di attività di analisi e di implementazione in ambito ISO 27001

Attività di analisi e di implementazione a supporto di alcuni processi considerati particolarmente "critici" in ambito alla gestione del sistema della sicurezza delle informazioni. In particolare, tali attività riguardano i processi di Log Management, Disaster Recovery e Business Continuity e Vulnerability Assessment e Penetration Test e possono essere scorporate nei seguenti task:

- **Log Management:**
  - Assessment dell'attuale processo di Log Management e del relativo tool a supporto
  - Gap analysis e individuazione dei requisiti di remediation
  - Definizione di una procedura di Log Management
- **Disaster Recovery e Business Continuity:**
  - Assessment dei servizi a supporto del business
  - Individuazione dei principali indicatori utili a definire una strategia di BC (es. RTO, RPO, Servizi critici etc.)
  - Definizione di una procedura di Disaster Recovery e Business Continuity
- **Vulnerability Assessment e Penetration Test:**
  - Supporto per l'esecuzione di VAPT
  - Elaborazione dei report delle attività di VAPT
  - Individuazione dei piani di remediation sulla base delle risultanze dei test di VAPT

5.3.3.3 Steam 3: Attività di manutenzione ai sistemi di gestione Security / Ambientale / Privacy

Al fine di garantire una corretta manutenzione del sistema della sicurezza delle informazioni (con riferimento allo standard ISO 27001), del sistema per la gestione ambientale (con riferimento allo standard ISO 14001) e del sistema privacy (con riferimento al regolamento GDPR), sono state individuate le seguenti attività di analisi:

a. Attività integrative in ambito IT Security;
b. Attività integrative in ambito Sistema di Gestione Ambientale;
c. Attività integrative in ambito Privacy.

Attività integrative in ambito IT Security

Attività finalizzate alla corretta manutenzione del sistema di sicurezza delle informazioni tramite task di supporto per la predisposizione e l'esecuzione di Audit ed attività di Formazione, sulla base di quanto previsto dallo standard ISO 27001.

Attività integrative in ambito Sistema di Gestione Ambientale

Attività finalizzate alla corretta manutenzione del sistema di gestione ambientale tramite task di supporto per la predisposizione e l'esecuzione di Audit ed attività di Formazione, sulla base di quanto previsto dallo standard ISO 14001.

Attività integrative in ambito Privacy

Attività finalizzate alla corretta manutenzione del sistema di gestione privacy tramite task di supporto per la predisposizione e l'esecuzione di Audit ed attività di Formazione, sulla base di quanto previsto dallo Regolamento generale sulla protezione dei dati (GDPR).

5.3.3.4 Modalità di erogazione dei Servizi Professionali SP-03

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

5.3.3.5 Attivazione del servizio SP-03

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

5.3.3.6 Deliverable del servizio SP-03

Per ogni steam è prevista la redazione della seguente documentazione:

1. Attività per la gestione del sistema della sicurezza delle informazioni e del sistema di gestione ambientale:
    a. Procedura di Gestione degli Accessi fisici e logici:
    b. Procedura di Gestione Incidenti di Sicurezza;
    c. Procedura di Patch e Vulnerability Management;
    d. Procedura di Change Management e Sviluppo sicuro;
    e. Procedura di Gestione dei dispositivi mobili e corretto utilizzo dei sistemi informatici;
    f. Procedura per la Protezione dei dati e cancellazione sicura;
    g. Procedura di Gestione Installazione di Software nei Sistemi Operativi;
    h. Procedura di Codifica documentale;
    i. Metodologia per l'esecuzione di Risk Assessment;
    j. Compendio Generale della Informazione Documentata;
    k. Statement of Applicability Summary.

2. Attività di analisi a supporto dei sistemi di gestione Security / Privacy:
    a. Documento di Assessment GDPR;
    b. Piani di remediation per la compliance al GDPR;
    c. Template Registro dei trattamenti;
    d. Data Protection Impact Assessment (max n.5);
    e. Procedura di Log Management;
    f. Procedura di Disaster Recovery e Business Continuity;

g. Report di Vulnerability Assessment e Penetration Test.

3. Attività di manutenzione ai sistemi di gestione Security / Ambientale / Privacy:
   a. Rapporto di audit sul sistema di gestione della sicurezza delle informazioni;
   b. Programma di audit sul sistema di gestione della sicurezza delle informazioni;
   c. Piano di dettaglio di audit sul sistema di gestione della sicurezza delle informazioni;
   d. Materiale formativo sul sistema di gestione della sicurezza delle informazioni;
   e. Rapporto di audit sul sistema di gestione ambientale;
   f. Programma di audit sul sistema di gestione ambientale;
   g. Piano di dettaglio di audit sul sistema di gestione ambientale;
   h. Materiale formativo sul sistema di gestione ambientale;
   i. Rapporto di audit sul sistema di gestione Privacy;
   j. Programma di audit sul sistema di gestione Privacy;
   k. Piano di dettaglio di audit sul sistema di gestione Privacy;
   l. Materiale formativo sul sistema di gestione Privacy.

5.3.3.7 Quantità e prezzi del servizio SP-03

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].

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 7.

Tabella 7: 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 Modalità di configurazione

N/A

A.3 Specifiche di collaudo

Le specifiche di collaudo utilizzate per il collaudo della piattaforma saranno fornite separatamente.

A.4 Quantità e prezzi

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati di seguito, 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].

Servizio L2.S3.4 – Vulnerability Assessment (VA)						
Metrica	**Fascia**	**Num.tà I Anno**	**Num.tà II Anno**	**Num.tà III Anno**	**Prezzo unitario**	**Prezzo Totale**
indirizzo IP/anno	1	1	-	-	€ 124,00	€ 133.978,00
	2	14	-	-	€ 89,00	
	3	2.072	-	-	€ 64,00	
Servizio L2.S3.10 – Servizio di monitoraggio (SIEM)						
Metrica	**Fascia**	**Num.tà I Anno**	**Num.tà II Anno**	**Num.tà III Anno**	**Prezzo unitario**	**Prezzo Totale**
Device equivalenti	3	125	-	-	€ 544,30	€ 68.037,50
Servizio Professionale L2.S3.9: Servizi professionali di supporto alle attività VA (SP-01)						
Metrica	**Fig. Prof.**	**Num.tà I Anno**	**Num.tà II Anno**	**Num.tà III Anno**	**Prezzo unitario**	**Prezzo Totale**
Giorno/uomo	Capo Progetto	20	-	-	€ 300,00	€ 32.103,00
	Security Architect	70	-	-	€ 372,90	
Servizio Professionale L2.S3.9: Servizi professionali di supporto alle attività SIEM (SP-02)						
Metrica	**Fig. Prof.**	**Num.tà I Anno**	**Num.tà II Anno**	**Num.tà III Anno**	**Prezzo unitario**	**Prezzo Totale**
Giorno/uomo	Capo Progetto	10	-	-	€ 300,00	€ 10.458,00
	Security Architect	20	-	-	€ 372,90	
Servizio Professionale L2.S3.9: Servizi di supporto specialistico in ambito sicurezza (SP-03 Steam 1)						
Metrica	**Fig. Prof.**	**Num.tà 2019 (4 mesi)**	**Num.tà 2020 (12 mesi)**	**Num.tà 2021 (7 mesi)**	**Prezzo unitario**	**Prezzo Totale**
Giorno/uomo	Capo Progetto	18	-	-	€ 300,00	€ 46.946,50
	Security Architect	35	-	-	€ 372,90	
	Specialista di tecnologia	48	-	-	€ 295,00	

	/prodotto Senior					
	Specialista di tecnologia /prodotto	61	-	-	€ 235,00	
Servizio Professionale L2.S3.9: Servizi di supporto specialistico in ambito sicurezza (SP-03 Steam 2)						
Metrica	**Fig. Prof.**	**Num.tà 2019 (4 mesi)**	**Num.tà 2020 (12 mesi)**	**Num.tà 2021 (7 mesi)**	**Prezzo unitario**	**Prezzo Totale**
Giorno/uomo	Capo Progetto	21	-	-	€ 300,00	€ 105.940,00
	Security Architect	50	-	-	€ 372,90	
	Specialista di tecnologia /prodotto Senior	124	-	-	€ 295,00	
	Specialista di tecnologia /prodotto	189	-	-	€ 235,00	
Servizio Professionale L2.S3.9: Servizi di supporto specialistico in ambito sicurezza (SP-03 Steam 3)						
Metrica	**Fig. Prof.**	**Num.tà 2019 (4 mesi)**	**Num.tà 2020 (12 mesi)**	**Num.tà 2021 (7 mesi)**	**Prezzo unitario**	**Prezzo Totale**
Giorno/uomo	Capo Progetto	20	-	-	€ 300,00	€ 94.220,50
	Security Architect	45	-	-	€ 372,90	
	Specialista di tecnologia /prodotto Senior	94	-	-	€ 295,00	
	Specialista di tecnologia /prodotto	186	-	-	€ 235,00	

Tabella 8: Quantità e costi

Il totale del progetto è pari a **€ 491.683,50** oltre IVA.

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 (T_0).

B.1 Piano di lavoro

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

Nome attività	Durata	Inizio	Fine	Vincoli
L2.S3.5 – Vulnerability Assessment (VA)	12 mesi	T_0	T_0+12 mesi	Rif. par. 5.1.2
L2.S3.10 – Servizio di monitoraggio (SIEM)	12 mesi	T_0	T_0+12 mesi	Rif. par. 5.2.7
L2.S3.9- Servizi professionali (SP-01)	12 mesi	T_0	T_0+12 mesi	
L2.S3.9- Servizi professionali (SP-02)	12 mesi	T_0	T_0+12 mesi	
L2.S3.9- Servizi professionali (SP-03)	12 mesi	T_0	T_0+12 mesi	