Identificativo: MCel20210000082845_3.1

Data: 11/08/2021

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

ASL RIETI

Progetto dei fabbisogni

Costituito

Raggruppamento Temporaneo di Imprese

composto da:

Leonardo SpA - Divisione Cyber Security

IBM SpA

Sistemi Informativi srl

Fastweb SpA

	Nome e Ruolo	Firma
Autore		
	Stefano Guidotti - Presale PAL	Fastweb SpA
Verifica		
	Germano Matteuzzi	
Approvazione		
	Giuseppe Nicastro	
Autorizzazione		
	Claudio Rando	

Approvazioni Aggiuntive

Azienda	Nome e Ruolo	Firma

Lista di Distribuzione

Rev.	Data	Destinatario	Azienda
2.0	09/08/2021	Claudio Rando	Leonardo Societa' per azioni
2.0	09/08/2021	Carlo Coccoli	IBM SpA
2.0	09/08/2021	Danilo Niccolini	FASTWEB SpA
2.0	09/08/2021	Gianfranco Schito	Sistemi Informativi srl

Registro delle Revisioni

Rev.	Data	Descrizione delle modifiche	Autori
1.0	08/01/2019	Prima Emissione	Antonio Pilotti (Fastweb)
2.0	09/08/2021	Seconda Emissione – Estensione contratto	Stefano Guidotti (Fastweb)

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

LISTA DELLE FIGURE

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 dell'Amministrazione contraente) contenute nel proprio Piano dei fabbisogni [DA-5] e descritte sinteticamente in §0. 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.

Questo progetto costituisce l'estensione del contratto in essere con l'Amministrazione sino a luglio 2022.

1.2 Richieste dell'Amministrazione contraente

In questa sezione del Progetto dei fabbisogni l'RTI intende raccogliere e dettagliare le richieste dell'Amministrazione contraente espresse tramite la redazione del Piano dei fabbisogni [DA-5], contenente per ciascuna categoria di servizi indicazioni di tipo quantitativo che la stessa intende sottoscrivere, in continuità con i servizi già presenti nel contratto in essere.

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" – ASL RIETI del **09/08/2021**
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. - Divisione Cyber Security (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	Azienda Sanitaria Locale Rieti
Indirizzo	Via del Terminillo 42
CAP	02100
Comune	Rieti
Provincia	RI
Regione	Lazio
Codice Fiscale	00821180577
Nominativo referente Contratto Esecutivo:	ING. ANTONINO GERMOLE'
Indirizzo mail	a.germole@asl.rieti.it
PEC (SI/NO)	NO

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

Nome	
Cognome	Germolè
Telefono fisso	0746 279779
Indirizzo mail	a.germole@asl.rieti.it
PEC (SI/NO)	NO

5 PROPOSTA TECNICO-ECONOMICA

Di seguito la lista dei servizi previsti nella fornitura.

Id Servizio	Titolo	Descrizione
L2.S3.4	Vulnerability assessment	Servizio di verifica del livello di vulnerabilità dei sistemi dell'Amministrazione.
L2.S3.5	Data loss/leak prevention	Servizio per la protezione dei dati da accessi non autorizzati o violazioni delle policy di sicurezza riducendo il rischio di perdita, danno o svantaggio competitivo.
L2.S3.8	Secure Web Gateway	Servizio per la protezione della navigazione Internet degli utenti da minacce di sicurezza informatica attraverso una capability tecnologica in grado di ridurre considerevolmente la superficie d'attacco rappresentata dagli innumerevoli siti Internet malevoli o pericolosi.
L2.S3.9	Servizi Professionali	Servizi Professionali per l'erogazione di servizi specialistici a supporto delle strutture aziendali per le attività di sicurezza.

5.1 Servizio L2.S3.4 - Vulnerability assessment

5.1.1 Obiettivi del Servizio Servizio L2.S3.4

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 Descrizione del Servizio L2.S3.4

Il servizio si compone di specifiche fasi di seguito dettagliate:

1. ***Information* Gathering** (avviamento al servizio): Durante questa fase viene eseguita la raccolta automatica delle configurazioni e della topologia di rete per la definizione dei profili di scansione, ovvero:
    - Operazione di *network discovery* della rete: rilevazione attiva e passiva di ogni nuovo dispositivo installato nella rete; questo riduce in maniera significativa il rischio associato alle risorse non protette e non governate dalle Amministrazioni collegate alla rete includendo apparati, porte, sistemi, servizi, applicazioni;
    - Valutazione di tutti gli indirizzi IP attivi e non attivi all'interno di un determinato intervallo.
2. ***Individuazione delle vulnerabilità** (Operations):* sono eseguite scansioni rapide condotte in tutta la rete (con cadenza periodica) per trovare le eventuali falle di sicurezza e ridurre i rischi di esposizione, evidenziando l'aderenza o meno alle normative vigenti tramite raccolta, correlazione e reportistica delle informazioni rilevate durante le scansioni. Le scansioni applicano una combinazione di controlli attivi (quali l'invio di pacchetti e l'analisi in remoto) e controlli di correlazione passiva.
3. ***Assegnazione della priorità alle vulnerabilità** (Operations)*: avviene in ottica di risoluzione e mitigazione del rischio attraverso la comprensione dell'intero contesto di rete.
   Il rischio di ogni vulnerabilità è classificato tramite un algoritmo basato su fattori come impatto o facilità di sfruttamento. Le vulnerabilità scoperte possono essere filtrate per asset, rete, servizio o tipo di vulnerabilità permettendo di produrre reportistica personalizzata secondo le esigenze dell'Amministrazione.

L'architettura di riferimento del servizio è rappresentata in Figura 4:

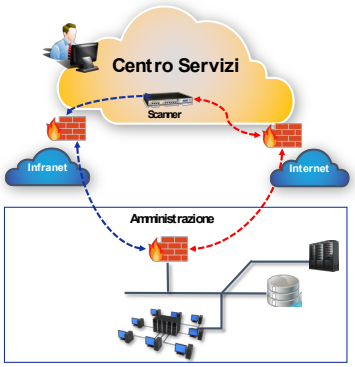

Figura 4 - Architettura di riferimento per l'erogazione del servizio L2.S3.4

L'Amministrazione contraente può beneficiare di una completa e aggiornata visione delle proprie vulnerabilità e dei relativi rischi connessi che costituiscono fattore abilitante alla gestione proattiva della sicurezza.

5.1.3 Vincoli e assunzioni del Servizio L2.S3.4

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.

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

Il servizio è erogato centralmente dal personale RTI. Non è prevista l'installazione di componenti HW/SW presso l'Amministrazione contraente.

5.1.5 Modalità di erogazione del Servizio L2.S3.4

Il servizio sarà erogato in modalità "as a service" in modalità continuativa e da remoto.

5.1.6 Quantità e prezzi del Servizio L2.S3.4

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].

5.1.7 Attivazione del Servizio L2.S3.4

Si prevede l'estensione del servizio in continuità sino a luglio 2022, come da contratto in essere con l'Amministrazione, la cui fatturazione per quanto riportato nel presente progetto partirà da Settembre 2021.

5.2 Servizio L2.S3.5 - Data loss/leak prevention

5.2.1 Obiettivi del Servizio L2.S3.5

Il servizio di "data loss/leak prevention" consente alle Amministrazioni la protezione dei dati da accessi non autorizzati o violazioni delle policy di sicurezza riducendo il rischio di perdita, danno o svantaggio competitivo.

5.2.2 Descrizione del Servizio L2.S3.5

Tecnologia Forcepoint Data Security

La soluzione con tecnologia leader di mercato Forcepoint Data Security Suite (ex Websense) è in grado di effettuare il monitoraggio e la protezione dei dati at rest (sui supporti di memorizzazione), in use (accesso tramite endpoint), in motion (traffico di rete).

Il servizio di compone delle seguenti funzionalità:

- rilevazione dei dati che transitano all'interno dell'amministrazione, ovunque essi siano archiviati;
- analisi e classificazione dei dati facilitata da OCR e Machine Learning Documentale;
- possibilità di creare regole predefinite per la protezione dei dati, identificando i sistemi in cui sono memorizzati (ad es porte USB, DVD, porte COM & LPT, dischi rimovibili, etc..),
- generazione automatica di alert nel caso in cui vengano violate le policy di sicurezza definite, visibilità e controllo sui dati in movimento, sia che si trovino in messaggi e-mail, nella mail sul Web, nell'instant messaging e nei protocolli di comunicazione;
- possibilità di generare report di sintesi (executive summary) e di dettaglio (technical report);

Il servizio prevede l'installazione di SW agent sugli endpoint distribuibili in maniera semi-automatica attraverso piattaforme di sw deployment dell'Amministrazione; è inoltre prevista l'installazione di gateway "on premise" per l'analisi del traffico in motion.

Architettura

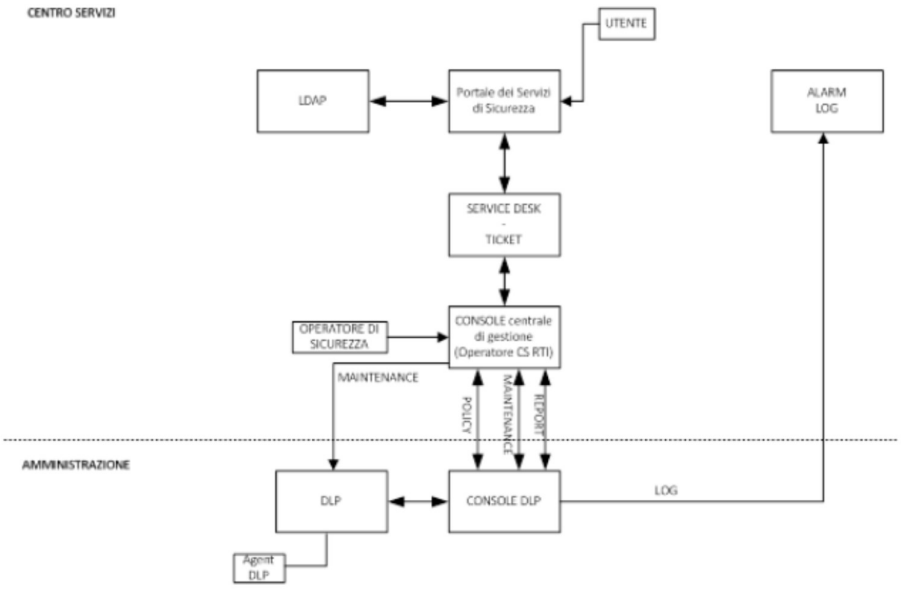

Figura 5 - Architettura servizi Data loss/leak prevention

L'architettura è dislocata presso:

- Centro Servizi;
- Pubblica Amministrazione.

Presso il Centro Servizi sono dislocati:

- Portale dei Servizi di Sicurezza: per effettuare nuove richieste di servizi (es.: creazione o modifica di una policy);
- LDAP: per l'accesso ai servizi con utenza di dominio;
- Service Desk / Ticket: piattaforma di ticketing per la gestione delle richieste;
- Console centrale di gestione: postazione di gestione del servizio;
- Alarm log: per la raccolta degli eventi di sicurezza

Presso la Pubblica Amministrazione:

- Endpoint Controller (DLP): per il controllo e l'invio agli agent DLP delle policy di sicurezza;
- Console DLP: per il deploy delle policy di sicurezza;
- Agent DLP: per la protezione dei dati sulle PdL (Postazione di Lavoro).

5.2.3 Vincoli e assunzioni del Servizio L2.S3.5

Affinché le attività di gestione degli apparati possano essere erogate dal centro servizi del fornitore è necessario instaurare una o più VPN tra i DataCenter di ASL RIETI (o ovunque questi apparati siano attestati) e il centro servizi del fornitore stesso.

5.2.4 Componenti del Servizio L2.S3.5

Tecnologie e prodotti di riferimento

La figura seguente illustra l'architettura applicativa del servizio DLP, con indicazione dei prodotti utilizzati (tecnologia FORCEPOINT).

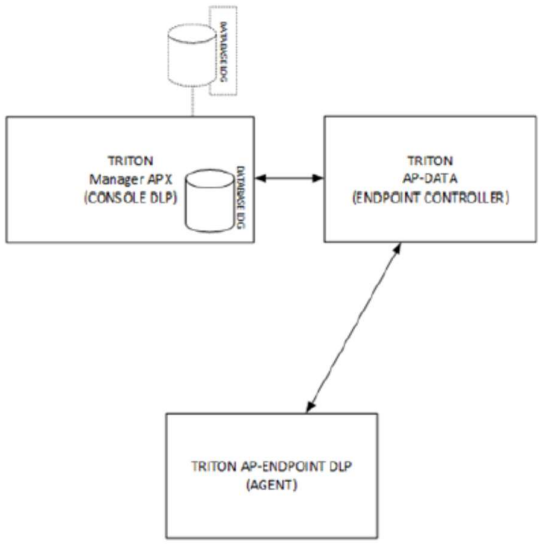

Figura 6 - Schema applicativo servizi data loss/leak prevention

Di seguito il dettaglio sui prodotti che costituiscono l'architettura applicativa:

- TRITON AP-DATA (Endpoint Controller) – si occupa della gestione degli endpoint, controlla la corretta connessione degli endpoint e applica l'enforcement delle policy inviate dal Triton Manager APX (Console DLP);
- TRITON Manager APX (Console DLP) – consente di applicare le policy di sicurezza inviandole al Triton AP-DATA (Endpoint Controller). La Triton Manager APX (Console DLP) è accessibile tramite Web Browser con connessione sicura SSL. La Triton Manager APX (Console DLP) genera logs di allarmi che vengono memorizzati sul DATABASE LOG;
- TRITON AP-ENDPOINT DLP (Agent) – Il Triton AP-ENDPOINT (Agent) monitora in tempo reale la violazione delle policy in vigore e genera log di allarme che vengono inviati al Triton Manager APX (Console DLP). Attraverso tale Agent è possibile controllare costantemente lo spostamento (inteso come copia/invio/ricezione) dei dati nella rete e/o attraverso le periferiche di una postazione di lavoro (pendrive usb, stampanti, cd/dvd, dischi esterni).

5.2.5 Modalità di erogazione del Servizio L2.S3.5

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

5.2.6 Quantità e prezzi del Servizio L2.S3.5

Si veda l'appendice A.3.

5.2.7 Attivazione del Servizio L2.S3.5

Si prevede l'estensione del servizio in continuità sino a luglio 2022, come da contratto in essere con l'Amministrazione, la cui fatturazione per quanto riportato nel presente progetto partirà da Settembre 2021.

5.3 Servizio L2.S3.8 - Secure Web Gateway

5.3.1 Obiettivi del Servizio L2.S3.8

Il servizio "secure web gateway" consente di bloccare l'accesso a siti web potenzialmente malevoli in tempo reale, aggiornando la propria base dati in maniera automatica e quindi riconoscere il download di applicazioni potenzialmente dannose.

5.3.2 Descrizione del Servizio L2.S3.8

Tale soluzione è basata sulla tecnologia leader di mercato Web Security di Forcepoint ed è caratterizzata da una componente centrale di gestione e dalle componenti gateway (fisiche o virtuali) dislocate "on premise" presso l'Amministrazione definendolo come Proxy o Default Gateway.

La piattaforma proposta soddisfa tutti i requisiti tecnici e funzionali richiesti dal capitolato, quali: analisi del traffico, rilevazione e blocco dei comportamenti dannosi, aggiornamento delle liste dei siti (ogni 24 ore per il database dei contenuti, 5 minuti per il Real Time update e 15 minuti per l'Antivirus) e reporting.

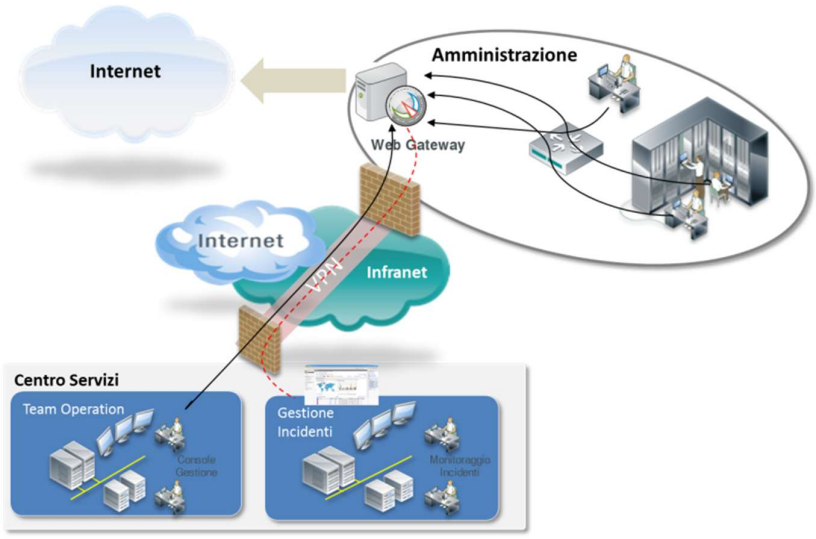

Figura 7 - Architettura di riferimento de servizio L2.S3.8

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

- **Policy per Quota Tempo/Conferma:** oltre ai classici "Permetti" o "Blocca" è possibile sfruttare diverse opzioni avanzate per la gestione del tempo di navigazione concesso agli utenti :
  - **Quota Time**: gli utenti ricevono una quantità variabile di gettoni di tempo di 10minuti che possono spendere durante l'arco della giornata.
  - **Confirm**: l'utente visualizza una pagina di blocco dove è presente un messaggio di avviso personalizzato.
- **Categorizzazione di Siti e Applicazioni Web 2.0:** è resa disponibile una funzione di analisi del contenuto del sito Web che, a front di un download di una pagina Web, effettua un'analisi in tempo reale per verificare che il contenuto corrisponda realmente alla categoria del sito Web (Real Time Classification). Tale funzione è attiva per tutti i siti non categorizzati, per i siti a contenuto dinamico e siti con tecnologia web 2.0

- **Social Web 2.0 Controls:** I Social Web controls permettono all'amministratore di controllare in modo molto granulare alcuni tra i portali Web 2.0 più importanti, tra cui Facebook, Twitter, YouTube e LinkedIn consentendo ad esempio di garantire l'accesso ma bloccando specifiche azioni
- **Data Theft Protection:** Consente di bloccare pattern noti di furto dati da parte di malware, in particolare: custom encrypted upload, file containing password, C&C back channel.

5.3.3 Vincoli e Prerequisiti del Servizio L2.S3.8

Affinché le attività di gestione degli apparati possano essere erogate dal centro servizi del fornitore è necessario instaurare una o più VPN tra i DataCenter di ASL RIETI (o ovunque questi apparati siano attestati) e il centro servizi del fornitore stesso.

5.3.4 Componenti del Servizio L2.S3.8

Si prevede l'avvio dei servizi, fatta salva la messa a disposizione dei locali ASL RIETI e di quanto altro necessario al normale funzionamento degli apparati e delle altre componenti tecnologiche a supporto dell'erogazione del servizio.

5.3.5 Modalità di erogazione del Servizio L2.S3.8

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

5.3.6 Quantità e prezzi del Servizio L2.S3.8

Si veda l'appendice A.3

5.3.7 Attivazione del Servizio L2.S3.8

Si prevede l'estensione del servizio in continuità sino a luglio 2022, come da contratto in essere con l'Amministrazione, la cui fatturazione per quanto riportato nel presente progetto partirà da Settembre 2021.

5.4 Servizio L2.S3.9 - Servizi professionali

I servizi professionali hanno l'obiettivo di supportare ASL RIETI nella realizzazione di attività nell'ambito della sicurezza infrastrutturale, comprensive di quelle relative ai servizi di monitoraggio, attraverso l'utilizzo di specifiche figure professionali messe a disposizione dal Fornitore.

Alcune delle attività che possono essere richieste al Fornitore, a titolo esemplificativo e non esaustivo, sono:

- Assicurare il mantenimento e l'aggiornamento della documentazione di sistemi infrastrutturali e tecnologici gestiti, delle policy di sicurezza stabilite, la produzione della reportistica necessaria.
- Supportare l'Amministrazione nelle attività di individuazione e pianificazione delle evoluzioni finalizzate a mantenere l'infrastruttura costantemente aggiornata rispetto alle evoluzioni del panorama delle minacce informatiche, in costante trasformazione;
- Supportare l'adeguamento alle Misure minime di sicurezza, emanate dall'Agenzia per l'Italia digitale, al Regolamento Europeo per la protezione dei dati personali (GDPR) e nella gestione degli adempimenti al GDPR.

Per l'espletamento di attività del genere, il Fornitore metterà a disposizione di ASL RIETI servizi professionali erogati attraverso l'impiego di figure professionali di comprovata esperienza, maturata nel corso degli anni per le tematiche oggetto del servizio e con riferimento a progetti realizzati presso PA e organizzazioni private, sia nel territorio nazionale sia internazionale.

Il Servizio erogato avrà l'obiettivo di supportare l'Amministrazione nella implementazione di soluzioni tecnologiche e di processo finalizzate di sicurezza, in considerazione di quanto previsto dalle normative vigenti.

Le attività che verranno condotte rientrano nell'ambito dell'adeguamento degli enti pubblici rispetto a quanto previsto dal contesto normativo nazionale: alla luce dei crescenti rischi informatici che minacciano le reti di tutto il Paese, AgID (l'Agenzia per l'Italia digitale) ha pubblicato un documento contenente le Misure minime di sicurezza ICT per le Pubbliche Amministrazioni, le quali costituiscono parte integrante delle Linee Guida per la sicurezza informatica delle Pubbliche Amministrazioni, divenute un bersaglio specifico di alcune tipologie di soggetti particolarmente pericolosi. Le PA dovranno quindi adeguarsi e rispettare queste misure pensate per fornire loro un riferimento pratico per valutare e innalzare il proprio livello di sicurezza informatica.

Profili Professionali adottati

I servizi professionali saranno erogati a ciclo continuo, utilizzando personale altamente specializzato al fine di garantire la copertura dei rischi anche a fronte della naturale evoluzione dell'infrastruttura, delle applicazioni e delle minacce cyber che ASL RIETI deve fronteggiare. Tali servizi avranno come campo di applicazione l'intero perimetro tecnologico specificato da ASL RIETI.

Tali servizi saranno erogati sia nella modalità "on premise", con gli strumenti hardware e software presenti presso ASL RIETI, che nella modalità "as a service".

Di seguito è riportato il dettaglio delle figure professionali previste:

Figura Professionale
Specialista di tecnologia/prodotto Senior
Security Architect
Capo Progetto

Tabella 7: Figure professionali previste

Le attività del servizio saranno coordinate da una figura di Project Manager che sarà impegnata per l'intera durata del contratto in modalità non continuativa.

5.4.1 Modalità di erogazione del Servizio L2.S3.9

Il servizio viene erogato in modalità "on premise".

5.4.2 Quantità e prezzi del Servizio L2.S3.9

Si veda l'appendice A.3.

5.4.3 Attivazione del Servizio L2.S3.9

Si prevede l'estensione del servizio in continuità sino a luglio 2022, come da contratto in essere con l'Amministrazione, la cui fatturazione per quanto riportato nel presente progetto partirà da Settembre 2021.

6 RISERVATEZZA

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

APPENDICE A PROGETTO DI ATTUAZIONE

A.1 Struttura organizzativa

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

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

Tabella 8: Figure professionali.

Ruolo	Caratteristiche e responsabilità
Responsabile Contratto Quadro	È il rappresentante del fornitore verso Agid/Consip, garantisce l'omogeneità e l'uniformità di interfaccia verso le parti interessate a livello di Governo del Contratto Quadro vigilando sull'osservanza di tutte le indicazioni operative, di indirizzo e di controllo, che a tal scopo potranno essere predisposte da Consip e/o da AgID, per quanto di rispettiva competenza. Rappresenta, insieme al Responsabile del Centro Servizi, il RTI nel Comitato di Direzione Tecnica.
Responsabile Contratto Esecutivo	Costituisce l'interfaccia unica verso il Responsabile del Procedimento dell'Amministrazione Beneficiaria. È responsabile dell'erogazione dei servizi acquistati dall'Amministrazione e della rendicontazione e dei meeting di stato avanzamento lavori. Costituisce l'interfaccia unica verso il Responsabile Unico del Procedimento dell'Amministrazione beneficiaria.
Responsabile Tecnico	È il Responsabile unico delle attività tecniche e del raggiungimento degli obiettivi dei servizi oggetto del Contratto. Costituisce l'interfaccia unica verso il Direttore Esecuzione nominato dall'Amministrazione. Ha la visione complessiva e integrata di tutte le attività tecniche legate all'attivazione, all'erogazione e al rilascio dei servizi della fornitura e ne garantisce la qualità.
Responsabile del Centro Servizi	È responsabile del Centro servizi da cui vengono erogati i servizi nella modalità "as a service".
Responsabile Servizi 'on premise'	Coincide con il Responsabile Tecnico
HELP DESK	Primo punto di contatto a disposizione dell'Amministrazione per l'avvio delle attività di acquisizione del servizio. Supporta inoltre i referenti dell'Amministrazione contraente nelle attività di risoluzione di eventuali problematiche di utilizzo del servizio. L'Help Desk è contattabile: - per contatti di natura commerciale e informativa al numero verde **800 894 590**. - per contatti di natura tecnica e di problemi di utilizzo del servizio al seguente indirizzo e-mail **sccd@spc-lotto2-sicurezza.it** Ulteriori informazioni sono reperibili al seguente URL: http://www.spc-lotto2-sicurezza.it presso il quale è presente il Portale di Governo e Gestione della Fornitura.

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

A.2 Specifiche di collaudo

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

A.3 Quantità e costi

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], nella seguente tabella è riportato il riepilogo dei servizi:

Riepilogo Servizi	2021 (4 mesi - 2 rate)	2022 (7 mesi - 4 rate)	Vita Intera
Servizio L2.S3.4 - Vulnerability assessment	€ 0,00	€ 7.705,83	€ 7.705,83
Servizio L2.S3.5 - Data loss/leak prevention	€ 0,00	€ 7.758,33	€ 7.758,33
Servizio L2.S3.8 - Secure Web Gateway	€ 0,00	€ 2.513,58	€ 2.513,58
Servzio L2.S3.9- Servizi professionali	€ 64.145,60	€ 89.898,90	€ 154.044,50
Totale piano dei fabbisogni	**€ 64.145,60**	**€ 107.876,65**	**€ 172.022,25**

Di seguito, il dettaglio delle quantità e dei costi per ciascun servizio previsto.

Servizio L2.S3.9 - Servizi professionali

Totale generale				2021		2022	
Metrica	**Servizio**	**Figura professionale**	**Prezzo unitario**	**Nun.tà**	**Prezzo**	**Nun.tà**	**Prezzo**
giorno/uomo	Normale orario di lavoro (8 ore)	Capo progetto	€ 300,00	32	€ 9.600,00	42	€ 12.600,00
		Security architect	€ 372,90	64	€ 23.865,60	91	€ 33.933,90
		Specialista di tecnologia/prodotto Senior	€ 295,00	104	€ 30.680,00	147	€ 43.365,00
		Specialista di tecnologia/prodotto	€ 235,00	0	€ 0,00	0	€ 0,00
giorno/uomo	Orario continuativo H24	Specialista di tecnologia/prodotto Senior H24	€ 1.180,00	0	€ 0,00	0	€ 0,00
		Specialista di tecnologia/prodotto H24	€ 930,00	0	€ 0,00	0	€ 0,00
					€ 64.145,60		€ 89.898,90

Servizio L2.S3.4 - Vulnerability assessment

Servizio L2.S3.4 - Vulnerability assessment			2021			2022		
Metrica	**Fascia**	**Prezzo unitario**	**Nun.tà**	**Mesi**	**Prezzo**	**Nun.tà**	**Mesi**	**Prezzo**
indirizzo IP/anno	Fascia1: n. 1 indirizzo IP	€ 124,00	0	0	€ 0,00	1	7	€ 72,33
	Fascia 2: da 2 a 15 indirizzi IP	€ 89,00	0	0	€ 0,00	14	7	€ 726,83
	Fascia 3: oltre 15 indirizzi IP	€ 64,00	0	0	€ 0,00	185	7	€ 6.906,67
					€ 0,00			**€ 7.705,83**

Servizio L2.S3.5 - Data loss/leak prevention

Servizio L2.S3.5 - Data loss/leak prevention			2021			2022		
Metrica	Fascia	Prezzo unitario	Nun.tà	Mesi	Prezzo	Nun.tà	Mesi	Prezzo
endpoint/anno	Fascia 1: fino a 500 endpoint	€ 15,00	0	0	€ 0,00	500	7	€ 4.375,00
	Fascia 2: da 501 a 1.000 endpoint	€ 10,00	0	0	€ 0,00	500	7	€ 2.916,67
	Fascia 3: oltre 1.000 endpoint	€ 8,00	0	0	€ 0,00	100	7	€ 466,67
					€ 0,00			**€ 7.758,33**

Servizio L2.S3.8 - Secure Web Gateway

Servizio L2.S3.8 - Secure Web Gateway sedi centrali e periferiche			2021			2022		
Metrica	Fascia	Prezzo unitario	Nun.tà	Mesi	Prezzo	Nun.tà	Mesi	Prezzo
pdli/anno	Fascia 1: fino a 100 pdli	€ 23,09	0	0	€ 0,00	100	7	€ 1.346,92
	Fascia 2: da 101 a 1.000 pdli	€ 10,00	0	0	€ 0,00	200	7	€ 1.166,67
	Fascia 3: da 1.001 a 5.000 pdli	€ 8,00	0	0	€ 0,00	0	7	€ 0,00
	Fascia 4: oltre 5.000 pdli	€ 5,50	0		€ 0,00	0	0	€ 0,00
					€ 0,00			**€ 2.513,58**

A.3.1 Fatturazione servizi

A valle delle verifiche dell'Amministrazione (art 15 dell'Accordo Quadro), i servizi 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. Nella tabella seguente, è riportata la ripartizione dei canoni nei 30 mesi di contratto:

Voce	2021	2022	
	Set-Dic	Gen-Giu	Luglio
Attivazione	€ 0,00	€ 0,00	€ 0,00
Numero di rate bimestrali	2	3	
Numero di rate mensili			1
Mesi fatturazione	Set-Nov	Gen-Mar-Mag	Lug
Canone Bimestrale/Mensile	€ 32.072,80	€ 30.821,90	€ 15.410,95
Canone Annuale/Periodo	€ 64.145,60	€ 92.465,70	€ 15.410,95
Canone Annuale	**€ 64.145,60**	**€ 107.876,65**	
Canone Annuale iva inclusa	**€ 78.257,63**	**€ 131.609,51**	
Totale contratto	**€ 172.022,25**		
Totale contratto (iva inclusa)	**€ 209.867,15**		

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.

B.1 Piano di lavoro

In base a quanto richiesto dall'Amministrazione contraente nel Piano dei fabbisogni [DA-5] la Tabella riporta le attività previste per l'erogazione dei servizi:

Id Servizio	Titolo	Inizio	Fine
L2.S3.4	Vulnerability assessment	Gennaio 2022	Luglio 2022
L2.S3.5	Data loss/leak prevention	Gennaio 2022	Luglio 2022
L2.S3.8	Secure Web Gateway	Gennaio 2022	Luglio 2022
L2.S3.9	Servizi Professionali	Settembre 2021	Luglio 2022