**“Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni – Lotto 1 (ID 2296)”**

**PIANO DEI FABBISOGNI**

**<NOME AMMINISTRAZIONE>**

**Tabella Revisioni**

|  |  |  |
| --- | --- | --- |
| **Revisione** | **Descrizione modifiche** | **Data** |
| 1 | Prima emissione | GG/MM/20AA |

La scrivente Amministrazione:

|  |
| --- |
| **DATI ANAGRAFICI AMMINISTRAZIONE** |
| Ragione sociale Amministrazione |  |
| Tipologia Amministrazione | Pubblica Amministrazione Centrale (cfr. Capitolo 5 del Capitolato Tecnico Generale) |
| Indirizzo Sede Legale (Via, N° civico e CAP) |   |
| Comune (Provincia) |   |
| Codice Fiscale/P.IVA |   |
| Indirizzo mail Amministrazione |   |
| PEC Amministrazione |   |
| **DATI ANAGRAFICI REFERENTE AMMINISTRAZIONE** |
| Nome |   |
| Cognome |   |
| Telefono |   |
| Indirizzo mail Referente Amministrazione |   |

chiede che venga realizzato quanto di seguito indicato (barrare i servizi richiesti con il presente piano dei fabbisogni):

 **L1.S1 - Security Operation Center - SOC** (Compilare sezione A)

 **L1.S2 - Next Generation Firewall - NGFW** (Compilare sezione B)

 **L1.S3 - Web Application Firewall - WAF** (Compilare sezione C)

 **L1.S4 -** **Gestione continua delle vulnerabilità di sicurezza** (Compilare sezione D)

 **L1.S5 - Threat Intelligence & Vulnerability Data Feed - TI & VDF** (Compilare sezione E)

 **L1.S6 - Protezione navigazione Internet e Posta elettronica - SWG e SEG** (Compilare sezione F)

 **L1.S7 - Protezione degli end-point – EPP** (Compilare sezione G)

 **L1.S8 - Certificati SSL** (Compilare sezione H)

 **L1.S9 - Servizio di Formazione e Security awareness** (Compilare sezione I)

 **L1.S10 - Gestione dell’identità e l’accesso utente** (Compilare sezione L)

 **L1.S11 - Firma digitale remota** (Compilare sezione M)

 **L1.S12 - Sigillo elettronico** (Compilare sezione N)

 **L1.S13 - Timbro elettronico** (Compilare sezione O)

 **L1.S14 - Validazione temporale elettronica qualificata** (Compilare sezione P)

 **L1.S15 - Servizi specialistici** (Compilare sezione Q)

FIRMA DEL REFERENTE DELL’AMMINISTRAZIONE

**NOTA**: tale documento deve essere inviato a:

* RTI: TIM quale mandataria del RTI all’indirizzo PEC: *aq.sicurezzadaremoto@pec.telecomitalia.it*
* CONSIP all’indirizzo PEC: *sicurezzaremoto.2296.l1@postacert.consip.it*

**Contratto finanziato dal PNRR**

Il contratto esecutivo è finanziato, in tutto o in parte, con le risorse previste dal Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021 e dal Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, nonché dal PNC.

 **SI** **NO**

**Comunicazione preventiva al CVCN**

 **SI** **NO**

**Categorizzazione degli interventi**

Indicare, nel contesto del Piano Triennale di riferimento per la specifica fornitura di servizi, l’ambito di I livello e uno o più ambiti di II livello, numerandoli in ordine di prevalenza (dove 1= priorità massima)

|  |  |
| --- | --- |
| **Ambito (layer)**  | **Obiettivi Piano Triennale** |
|  Servizi |  Servizi al cittadino |
|  Servizi a imprese e professionisti |
|  Servizi interni alla propria PA |
|  Servizi verso altre PA |
|  Dati |  Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese |
|  Aumentare la qualità dei dati e dei metadati |
|  Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati |
|  Piattaforme |  Favorire l’evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l’azione amministrativa |
|  Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle PA |
|  Incrementare e razionalizzare il numero di piattaforme per le amministrazioni |
|  Infrastrutture |  Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni locali favorendone l’aggregazione e la migrazione sul territorio (Riduzione Data Center sul territorio) |
|  Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni centrali favorendone l’aggregazione e la migrazione su infrastrutture sicure ed affidabili (Migrazione infrastrutture interne verso il paradigma cloud) |
|  Migliorare la fruizione dei servizi digitali per cittadini ed imprese tramite il potenziamento della connettività per le PA |
|  Interoperabilità |  Favorire l’applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API |
|  Adottare API conformi al Modello di Interoperabilità |
|  Sicurezza Informatica |  Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA |
|  Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione |

# SEZIONE A - L1.S1 - Security Operation Center - SOC

**Descrizione del Servizio**

Il servizio di “Security Operation Center” (SOC) è il centro da cui vengono forniti alle Amministrazioni i servizi mirati a garantire la corretta operatività dei sistemi. La sua finalità principale è di gestione e monitoraggio dei servizi di sicurezza oggetto di fornitura e, in aggiunta, ricevere ed analizzare ad esempio la reportistica e i log dando anche la giusta priorità ai processi di risoluzione e/o mitigazione delle minacce.

Il RTI propone per il Servizio SOC una soluzione integrata che consente agli analisti di rilevare rapidamente le anomalie di sicurezza, contestualizzarle e creare le condizioni per porre rapidamente in essere le necessarie azioni di contenimento.

Nella successiva figura sono schematizzate tutte le componenti funzionali che sottendono all’erogazione dei servizi di AQ con particolare riferimento a quelle necessarie per il Servizio SOC.



Componenti funzionali del servizio SOC

La soluzione tecnologica prevista per il Servizio SOC è costituita dalle componenti SIEM e SOAR. Sono inoltre presenti le console di gestione per ciascuna delle tecnologie di erogazione dei servizi che interagiscono con la piattaforma SOC. Completa l’architettura il Portale dei Servizi di Sicurezza che consente alle Amministrazioni di richiedere change alle policy e modifiche alle configurazioni per i servizi proposti.

Ciascun servizio, pur ottimizzato per essere erogato anche singolarmente, esprime la massima potenzialità ed efficacia all’interno della visione integrata con gli altri servizi di sicurezza.

Per l’erogazione del Servizio SOC, il RTI si avvale di una piattaforma tecnologica leader di mercato: Splunk Security Suite.

**Modalità di erogazione:** centralizzata presso il Centro Servizi del RTI.

**Metrica Servizio:** Device Equivalenti

|  |  |
| --- | --- |
|  |  |

*Esempio di calcolo per 4.000 EPS*:

4.000 EPS ricade nella Fascia 4.

Il coefficiente (EPS/Device) è pari a 10.

Il numero di Device Equivalenti è pari a: 4.000/10 = 400

Il Canone annuale verrà calcolato come prodotto tra 400 \* per il prezzo unitario offerto per la fascia di riferimento.

Indicare la fascia di erogazione richiesta:

|  |  |  |
| --- | --- | --- |
| Tipologia di servizio | Fascia di erogazione del servizio(EPS) | Quantità(EPS) |
| L1.S1 - Security Operation Center |  Fascia 1 fino a 300 EPS |  |
|  Fascia 2 fino a 600 EPS |  |
|  Fascia 3 fino a 1.200 EPS |  |
|  Fascia 4 fino a 6.000 EPS |  |
|  Fascia 5 > 6.000 EPS |  |

**Modalità di remunerazione:** Canone Annuo con durata minima 12 mesi.

Durata Contrattuale:\_\_\_\_\_\_\_\_mesi (max 48 mesi decorrenti dalla data di conclusione delle attività di presa in carico)

(NOTA: se la durata richiesta per il contratto è inferiore ai 12 mesi, il Fornitore si riserva la facoltà di accettare tale richiesta)

# SEZIONE B - L1.S2 - Next Generation Firewall (NGFW)

**Descrizione del Servizio**

Il servizio di Next Generation Firewall (NGFW) consente alle Amministrazione di filtrare tutto il traffico che i dispositivi di rete scambiano sia internamente sia esternamente rispetto a un determinato perimetro, limitando o bloccando eventi quali accessi non autorizzati, malware o servizi non consentiti.

Il servizio “Next Generation Firewall”, proposto dal RTI, finalizzato a garantire la protezione di sistemi e rete da minacce esterne, viene fornito attraverso appliance FortiGate (hardware appliance o virtual appliance on premise) di Fortinet, un’avanzata tecnologia firewall con evoluti servizi di sicurezza multi-minaccia, erogati attraverso un’unica piattaforma integrata che consente di contrastare efficacemente attacchi e minacce informatiche, grazie anche alla semplicità di gestione e alla flessibilità di inserimento in una vasta gamma di scenari di implementazione.

La gestione del servizio viene effettuata attraverso il sistema di management centralizzato costituito dalle componenti FortiManager e FortiAnalyzer.



**Modalità di erogazione:** Installazione di appliance dedicate presso le sedi della Pubblica Amministrazione.

**Metrica Servizio:** Throughput/anno

Indicare la fascia di erogazione richiesta:

|  |  |  |
| --- | --- | --- |
| Tipologia di servizio | Fasce di erogazione(Throughput) | Quantità(N. Appliance) |
| L1.S2 - Next Generation Firewall (NGFW) |  Fascia 1: fino a 250 Mbps |  |
|  Fascia 2: fino a 2 Gbps |  |
|  Fascia 3: fino a 4 Gbps |  |
|  Fascia 4: fino a 7 Gbps |  |
|  Fascia 5: fino a 15 Gbps |  |
|  Fascia 6: > 15 Gbps |  |

**Modalità di remunerazione:** Canone Annuo con durata minima 12 mesi

Durata Contrattuale:\_\_\_\_\_\_\_\_mesi (max 48 mesi decorrenti dalla data di conclusione delle attività di presa in carico)

(NOTA: se la durata richiesta per il contratto è inferiore ai 12 mesi, il Fornitore si riserva la facoltà di accettare tale richiesta)

# SEZIONE C - L1.S3 - Web Application Firewall (WAF)

**Descrizione del Servizio**

Il servizio di “Web Application Firewall” consente alle Amministrazioni di filtrare, monitorare e bloccare il traffico HTTP da e verso un servizio Web, esaminando il traffico, utilizzando regole, analisi e firme per rilevare attacchi e quindi proteggendo le stesse Amministrazioni dagli attacchi incorporati nei dati trasmessi dalle applicazioni web.

Il servizio WAF, proposto dal RTI, sarà erogato attraverso il prodotto **FortiWeb** (hardware appliance o virtual appliance on premise) di **Fortinet**. La gestione del servizio viene effettuata mediante la console di management centralizzata **FortiWeb Manager**.



**Modalità di erogazione:** Installazione di appliance dedicate presso le sedi della Pubblica Amministrazione.

**Metrica Servizio:** Throughput/anno

Indicare la fascia di erogazione richiesta:

|  |  |  |
| --- | --- | --- |
| Tipologia di servizio | Fasce di erogazione(Throughput) | Quantità(N. Appliance) |
| L1.S3 - Web Application Firewall (WAF) |  Fascia 1: fino a 500 Mbps |  |
|  Fascia 2: fino a 5 Gbps |  |
|  Fascia 3: fino a 10 Gbps |  |

**Modalità di remunerazione:** Canone Annuo con durata minima 12 mesi

Durata Contrattuale:\_\_\_\_\_\_\_\_mesi (max 48 mesi decorrenti dalla data di conclusione delle attività di presa in carico)

(NOTA: se la durata richiesta per il contratto è inferiore ai 12 mesi, il Fornitore si riserva la facoltà di accettare tale richiesta)

# SEZIONE D - L1.S4 - GESTIONE CONTINUA DELLE VULNERABILITA’ DI SICUREZZA

**Descrizione del Servizio**

Il servizio di “Gestione continua delle vulnerabilità di sicurezza” consente alle Amministrazioni, tramite un processo automatico di assesment delle vulnerabilità, di ottenere una fotografia precisa del livello e gravità del rischio a cui, in quel momento, sono esposti i propri sistemi informatici. Il servizio si avvarrà dell’utilizzo di uno scanner che produrrà un report con le specifiche indicazioni di rischio relative alle vulnerabilità rilevate.

L’aumento degli attacchi informatici e i metodi sempre più sofisticati con cui vengono condotti, ha accresciuto la consapevolezza dei responsabili della sicurezza e della compliance in merito alla necessità di integrare nelle strategie di difesa strumenti e metodologie di verifica continuative. Il servizio proposto dal RTI segue le logiche della **Continuous Adaptive Risk & Trust Assessment** (**CARTA**). L’approccio adottato dal RTI per garantire la sicurezza delle infrastrutture e dei dati delle Amministrazioni promuove una valutazione continua del rischio in modo iterativo. Questa permette di monitorare i cambiamenti di stato e di reagire alla presenza di minacce o pericoli di sicurezza.

Il servizio sarà basato sulla piattaforma Tenable.sc.

L’infrastruttura di erogazione del servizio si avvale delle componenti di seguito descritte:

* **Scanner** – Software reso disponibile su sistema virtuale dell’Amministrazione e presente di default nel Centro Servizi, che esegue le verifiche di sicurezza sui dispositivi raggiungibili ed identificati come target, tramite comunicazioni basate su protocollo IP. La soluzione abilita le Amministrazioni a:
* analizzare sia sistemi esposti su Internet sia sistemi interni;
* eseguire ricerche di vulnerabilità sui propri sistemi senza soluzione di continuità.
* **Console** - Piattaforma centralizzata multi-tenant istanziata presso il Centro Servizi del RTI, utilizzata per la gestione del servizio. Consente la separazione logica delle PA contraenti in domini distinti (Tenant) garantendo la segregazione completa dei dati. È una singola console di management che consente di gestire dispositivi Scanner e fornire funzionalità di settings e update centralizzato per tutti gli apparati gestiti.



**Modalità di erogazione:**

Il modello operativo di erogazione del servizio prevede due possibili scenari architetturali di implementazione:

* installazione di appliance dedicati virtuali on premise presso la sede dell’Amministrazione o presso il cloud dell’Amministrazione, architettura di default proposta dal RTI in caso di IP privati;
* utilizzo di una istanza del servizio installata presso il Centro Servizi del RTI, architettura di default proposta dal RTI in caso di IP pubblici.

**Metrica Servizio:** Numero IP/anno

Indicare la fascia di erogazione richiesta:

|  |  |  |
| --- | --- | --- |
| Tipologia di servizio | Fasce di erogazione(IP) | Quantità(IP) |
| L1.S4 - Gestione continua delle vulnerabilità di sicurezza |  Fascia 1: fino a 50 IP |  |
|  Fascia 2: fino a 200 IP |  |
|  Fascia 3: > 200 IP |  |

**Modalità di remunerazione:** Canone Annuo con durata minima 12 mesi

Durata Contrattuale:\_\_\_\_\_\_\_\_mesi (max 48 mesi decorrenti dalla data di conclusione delle attività di presa in carico)

(NOTA: se la durata richiesta per il contratto è inferiore ai 12 mesi, il Fornitore si riserva la facoltà di accettare tale richiesta)

***SEZIONE E - L1.S5 - Threat Intelligence & Vulnerability Data Feed (TI & VDF)***

**Descrizione del Servizio**

Il servizio di “Threat intelligence e Vulnerability data feed” consente alle Amministrazioni di ricevere un flusso continuo di dati relativi a minacce e vulnerabilità di sicurezza del Sistema informativo permettendo così di prevedere/prevenire le minacce prima che entrino in azione, migliorando gli attuali controlli e le funzionalità forensi.

Il servizio predisposto dal RTI offre alle PA una soluzione end-to-end per definire, monitorare, analizzare e migliorare il proprio livello di sicurezza cyber complessivo secondo un approccio predittivo e di analisi di contesto, seguendo logiche cyber-intelligence driven ad ampio spettro. In aggiunta, sfruttando tecniche e strumenti di automazione, consente di definire un livello di rischio in maniera statica e di studiarne le evoluzioni nel corso del tempo, grazie ad un monitoring costante della security posture di una specifica Amministrazione. Il servizio consente di identificare e definire eventuali minacce esterne, accertare le proprie aree di vulnerabilità e i propri asset a rischio di esposizione e compromissione. Il servizio si basa su una Threat Intelligence Platform consolidata denominata Joshua CybeRisk Vision™.

**Elemento distintivo** del servizio è la possibilità di ottenere, tramite **Joshua**, per ogni Amministrazione, specifici IoC di **Threat Analytics** per il proprio Sistema Informativo esposto su Internet, indicazioni di **Data Breach** presenti su GitHub, Pastebin o servizi FTP e SMB, gli **Info Leak** su Twitter, gli Asset della PA pubblicamente noti mediante **Postural Assessment**, gli account della specifica PA mediante **Theft Accounts**, minacce agli utenti della PA mediante **Web Malware Detection** sui principali siti della PA. Joshua, erogato nella modalità Threat Intelligence Data Feed, coniuga la capacità di ricercare codici di autenticazione, software, e-mail, dati GDPR rilevanti, etc., sui principali siti utilizzati da sviluppatori e Threat Actor, con la capacità di correlare gli elementi con i dati dello specifico Sistema Informativo esposto su Internet di una PA, **contestualizzando il subset informativo delle minacce**. Saranno infine utilizzate **tassonomie e schemi di classificazione** ben noti per supportare la classificazione standard utilizzata da ENISA, Europol, DHS, CSIRT o molte altre organizzazioni.



**Modalità di erogazione:**

Il modello operativo di erogazione del servizio prevede due possibili scenari architetturali di implementazione:

* comunicazione tramite HTTPS API Gateway;
* comunicazione tramite TAXII server.

**Metrica Servizio:** Data-Feed/anno

Indicare la fascia di erogazione richiesta:

|  |  |  |
| --- | --- | --- |
| Tipologia di servizio | Fasce di erogazione(Feed) | Quantità(Feed) |
| L1.S5 - Threat Intelligence & Vulnerability Data Feed (TI & VDF) |  Fascia 1: fino a 10 feed |  |
|  Fascia 2: fino a 50 feed |  |
|  Fascia 3: > 50 feed |  |

**Modalità di remunerazione:** Canone Annuo con durata minima 12 mesi

Durata Contrattuale:\_\_\_\_\_\_\_\_mesi (max 48 mesi decorrenti dalla data di conclusione delle attività di presa in carico)

(NOTA: se la durata richiesta per il contratto è inferiore ai 12 mesi, il Fornitore si riserva la facoltà di accettare tale richiesta)

***SEZIONE F - L1.S6 - Protezione navigazione Internet e Posta elettronica (SWG e SEG)***

**Descrizione del Servizio**

Il servizio di Protezione internet e Posta elettronica consente alle Amministrazioni di proteggersi contro le minacce alla sicurezza online applicando le policy aziendali e filtrando il traffico internet dannoso in tempo reale.

Nel caso della posta elettronica, il servizio consente alle Amministrazioni di proteggersi da contenuti dannosi presenti nelle e-mail impedendo loro di raggiungere il destinatario previsto.

Il servizio di protezione della Navigazione Internet e della Posta Elettronica (di seguito anche SWG&SEG) proposto dal RTI, si avvale di soluzioni best in class basate su tecnologia **Fortinet**. Prevede un modello di erogazione composto da due sotto-servizi, uno dedicato alla protezione della navigazione Internet (SWG) ed uno dedicato alla protezione della posta elettronica (SEG).

Il servizio SWG viene erogato attraverso appliance **FortiGate** (hardware appliance o virtual appliance on premise) mentre il servizio SEG viene erogato in modalità SaaS dal Centro Servizi attraverso la soluzione **FortiMail**.

|  |  |
| --- | --- |
|  |  |

**Modalità di erogazione:**

Il modello operativo di erogazione del servizio prevede il seguente scenario architetturale di implementazione:

* SWG: Installazione di appliance dedicate presso le sedi della Pubblica Amministrazione.
* SEG: Centralizzata presso il Centro Servizi del RTI.

**Metrica Servizio:** Numero utenti/anno

Indicare la fascia di erogazione richiesta:

|  |  |  |
| --- | --- | --- |
| Tipologia di servizio | Fasce di erogazione(Utenti) | Quantità(Utenti) |
| L1.S6 - Protezione navigazione Internet e Posta elettronica (SWG e SEG) |  Fascia 1 - Fino a 1.000 utenti |  |
|  Fascia 2 - Fino a 5.000 utenti |  |
|  Fascia 3 - Fino a 10.000 utenti |  |
|  Fascia 4 - Fino a 20.000 utenti |  |
|  Fascia 5 - > 20.000 utenti |  |

**Modalità di remunerazione:** Canone Annuo con durata minima 12 mesi

Durata Contrattuale:\_\_\_\_\_\_\_\_mesi (max 48 mesi decorrenti dalla data di conclusione delle attività di presa in carico)

(NOTA: se la durata richiesta per il contratto è inferiore ai 12 mesi, il Fornitore si riserva la facoltà di accettare tale richiesta)

# SEZIONE G - L1.S7 - Protezione degli end-point (EPP)

**Descrizione del Servizio**

Il servizio di Protezione endpoint consente alle Amministrazioni di proteggere i dispositivi collegati alla rete aziendale (ad es. pc desktop. laptop, smartphone, tablet) dall’accesso non autorizzato o dall’esecuzione di software dannoso. La protezione degli endpoint garantisce, inoltre, che i dispositivi raggiungano un livello di sicurezza definito e siano conformi ai requisiti di conformità dell’Amministrazione.

Specificatamente, per l’erogazione del servizio di protezione degli endpoint, il RTI adotta la tecnologia Trend Micro Apex One, una soluzione ideata per la protezione degli endpoint da molteplici virus quali ransomware, trojan e altri malware specifici, che consente anche di controllarne ed impedirne la diffusione all’interno della rete.



**Modalità di erogazione:**

L’architettura del servizio proposto dal RTI prevede due componenti principali:

* **Apex Central:** fornisce attraverso una console centralizzata la visibilità ed il controllo per gestire, monitorare e creare policy di sicurezza.
* **Apex One Server**: la componente specifica destinata all’Amministrazione che controlla operativamente i singoli agent installati sui rispettivi endpoint.

**Metrica Servizio:** Numero nodi/anno

Indicare la fascia di erogazione richiesta:

|  |  |  |
| --- | --- | --- |
| Tipologia di servizio | Fasce di erogazione(Nodi) | Quantità(Nodi) |
| L1.S7 - Protezione degli end-point (EPP) |  Fascia 1 - Fino a 500 nodi |  |
|  Fascia 2 - Fino a 1.000 nodi |  |
|  Fascia 3 - Fino a 5.000 nodi |  |
|  Fascia 4 - > 5.000 nodi |  |

**Modalità di remunerazione:** Canone Annuo con durata minima 12 mesi

Durata Contrattuale:\_\_\_\_\_\_\_\_mesi (max 48 mesi decorrenti dalla data di conclusione delle attività di presa in carico)

(NOTA: se la durata richiesta per il contratto è inferiore ai 12 mesi, il Fornitore si riserva la facoltà di accettare tale richiesta)

# SEZIONE H - L1.S8 - Certificati SSL

**Descrizione del Servizio**

Il certificato SSL (Secure Sockets Layer) e il suo successore TLS (Transport Layer Security), sono protocolli standard necessari a garantire affidabilità e sicurezza della comunicazione tra le componenti client e server di un’applicazione internet. Il certificato assicura che le informazioni sensibili fornite dagli utenti sul web rimangano riservate e non vengano in alcun modo intercettate da terze parti (comunicazione criptata tra il client server e il server web).

**Modalità di erogazione:** Centralizzata presso il Centro Servizi del RTI

**Metrica Servizio:** Numero Certificati/anno

Indicare la fascia di erogazione richiesta:

|  |  |  |
| --- | --- | --- |
| Tipologia di servizio | Fasce di erogazione (Certificati) | Quantità(Certificati) |
| L1.S8 - Certificati SSL |  Fascia 1 SSL OV |  |
|  Fascia 2 SSL OV Wildcard |  |
|  Fascia 3 SSL EV |  |
|  Fascia 4 SSL DV |  |
|  Fascia 5 SSL Code Signing |  |
|  Fascia 6 SSL Client Auth |  |

**Modalità di remunerazione:** Canone Annuo

Durata Contrattuale:  12 mesi  36 mesi

# *SEZIONE I - L1.S9 - Servizio di Formazione e Security awareness*

**Descrizione del Servizio**

Il servizio “Formazione e Security awareness” è mirato a sensibilizzare l’Amministrazione su svariati aspetti della sicurezza delle informazioni, incrementando il livello di consapevolezza dei dipendenti, innalzando il livello di sicurezza dell’organizzazione e l’efficacia in termini di protezione dei dati aziendali critici e dei dati personali. Lo scopo è quello di sviluppare negli utenti le competenze essenziali, le tecniche e i metodi fondamentali per prevenire il più possibile gli incidenti di sicurezza e reagire al meglio a fronte di eventuali problemi.

La piattaforma di e-learning utilizzata è **Cyber GURU**, personalizzata per le esigenze della PA con logiche innovative di comunicazione, interazione e ingaggio con un percorso formativo articolato nel tempo che consente di mantenere alta l’attenzione. Grazie alla creazione di un piano editoriale personalizzabile sulla base delle esigenze specifiche e i moduli auto-consistenti, ispirati alla logica del microlearning, l’approccio formativo favorisce una fruizione allineata all’esigenze dell’utente.

Il servizio sarà erogato dalle risorse, facenti parte obbligatoriamente del Team di Servizio Formazione e Security awareness, che dispongono delle competenze, esperienze e capacità richieste ai profili professionali elencati di seguito:

* Security Principal
* Senior Information Security Consultant
* Junior Information Security Consultant

**Modalità di erogazione:** sessioni di formazione on site e/o da remoto, divulgazione del materiale informativo in tema “Security Awareness”, somministrazione dei test di verifica e sessioni di review.

**Metrica Servizio:** Giorni/Persona del Team ottimale (pari a 8 ore lavorative).

**Modalità di remunerazione:** Progettuale (a corpo)

Quantità:\_\_\_\_\_\_\_Giorni/Persona del Team ottimale

Durata Contrattuale:\_\_\_\_\_\_\_\_mesi (min 12 mesi; max 48 mesi)

# *SEZIONE L - L1.S10 - Gestione dell’identità e l’accesso utente*

**Descrizione del Servizio**

Il servizio di Gestione dell’identità e dell’accesso utente (Identity & Access Management) consente all’Amministrazione la completa gestione delle attività di identificazione, autenticazione ed autorizzazione propedeutiche all’accesso da parte di utenti esterni al portale dell’Amministrazione o ai servizi da essa erogati in rete. Per l’autenticazione dei propri utenti il servizio può fare ricorso ad un Identity provider esterno all’Amministrazione.

**Modalità di erogazione:** Installazione di appliance virtuali dedicati presso la PA

**Metrica Servizio:** Numero Utenti/anno

Indicare la fascia di erogazione richiesta:

|  |  |  |
| --- | --- | --- |
| Tipologia di servizio | Fasce di erogazione(Utenti) | Quantità(Utenti) |
| L1.S10 - Gestione dell’identità e l’accesso utente |  Fascia 1: fino a 10.000 utenti |  |
|  Fascia 2: fino a 100.000 utenti |  |
|  Fascia 3: fino a 500.000 utenti |  |
|  Fascia 4: > 500.000 utenti |  |

**Modalità di remunerazione:** Canone Annuo con durata minima 12 mesi

Durata Contrattuale:\_\_\_\_\_\_\_\_mesi (max 48 mesi decorrenti dalla data di conclusione delle attività di presa in carico)

(NOTA: se la durata richiesta per il contratto è inferiore ai 12 mesi, il Fornitore si riserva la facoltà di accettare tale richiesta)

# *SEZIONE M - L1.S11 - Firma digitale remota*

**Descrizione del Servizio**

Il servizio di “Firma digitale” è un tipo di firma elettronica qualificata che consente alle Amministrazioni di dare efficacia probatoria ai documenti informatici firmati digitalmente, favorendo così i processi di dematerializzazione e consentendo l’automazione e l’ottimizzazione dei processi aziendali. La firma digitale è il risultato di una procedura informatica, detta validazione, che garantisce l’autenticità, l’integrità e il non ripudio dei documenti informatici.

**Modalità di erogazione:** Centralizzata presso il Centro Servizi del RTI

**Metrica Servizio:**

1. Numero Utenti/anno (best effort)

Indicare la fascia di erogazione richiesta:

|  |  |  |
| --- | --- | --- |
| Tipologia di servizio | Fasce di erogazione(Utenti) | Quantità(Utenti) |
| L1.S11 - Firma digitale remota |  Fascia 1: > 50 e fino a 200 utenti |  |
|  Fascia 2: > 200 e fino a 500 utenti |  |
|  Fascia 3: > 500 e fino a 1.000 utenti |  |
|  Fascia 4: > 1.000 utenti |  |

1. Numero Firme (SLA Garantito – 1 firma/sec) [Firma Digitale Remota Massiva]

Indicare il numero di pacchetti richiesti:

|  |  |  |
| --- | --- | --- |
| Tipologia di servizio | Fasce di erogazione(Firme) | Quantità(Pacchetti) |
| L1.S11 - Firma digitale remota Massiva (SLA Garantito) |  Garantita - N. 1 firma |  |
|  Garantita - N. 5 firme aggiuntive |  |

**Modalità di remunerazione:** Canone Annuo

Indicare la durata contrattuale richiesta.

Durata Contrattuale:  12 mesi  36 mesi

# *SEZIONE N - L1.S12 – Sigillo Elettronico*

**Descrizione del Servizio**

Il servizio “Sigillo elettronico”, al pari del servizio di “Firma digitale” consente alle Amministrazioni di dare efficacia probatoria ai documenti informatici firmati digitalmente, favorendo così i processi di dematerializzazione e consentendo l’automazione e l’ottimizzazione dei processi aziendali. Beneficiari del servizio sono tutte le persone giuridiche, ovvero società e Pubbliche Amministrazioni.

**Modalità di erogazione:** Centralizzata presso il Centro Servizi del RTI

**Metrica Servizio:** Numero di Sigilli (SLA Garantito – 1 sigillo/sec)

Indicare il numero di pacchetti richiesti:

|  |  |  |
| --- | --- | --- |
| Tipologia di servizio | Fasce di erogazione(Sigilli) | Quantità(Pacchetti) |
| L1.S12 – Sigillo Elettronico |  Garantita - N. 1 sigillo |  |
|  Garantita - N. 5 sigilli aggiuntivi |  |

**Modalità di remunerazione:** Canone Annuo

Durata Contrattuale:  12 mesi  36 mesi

# *SEZIONE O - L1.S13 – Timbro Elettronico*

**Descrizione del Servizio**

Il servizio di “Timbro elettronico” (indicato, anche in relazione alle specificità dello scenario, con termini differenti, quali “Contrassegno elettronico”, “Codice bidimensionale”, “Glifo”) consente alle Amministrazioni la creazione di documenti informatici che possano conservare la medesima validità legale anche dopo essere stati stampati su supporto cartaceo.

In particolare, il servizio in oggetto consente la creazione di un codice grafico bidimensionale posizionato in un punto qualsiasi del documento, a scelta dell’utente, e generato a partire dal contenuto del documento e dalla firma digitale, ove presente. Nell’ambito di tale servizio sono messi a disposizione gli strumenti necessari per la decodifica del timbro e la verifica di conformità rispetto al documento originale.

Il servizio è erogato in modo da garantire la conformità alla normativa vigente in materia di timbro elettronico.

**Modalità di erogazione:** Centralizzata presso il Centro Servizi del RTI

**Metrica Servizio:** Numero di Timbrature

Indicare la fascia di erogazione richiesta:

|  |  |  |
| --- | --- | --- |
| Tipologia di servizio | Fasce di erogazione(Timbrature) | Quantità(Timbrature) |
| L1.S13 – Timbro Elettronico |  Fascia 1: fino a 1.000 timbrature |  |
|  Fascia 2: > 1.000 e fino a 10.000 timbrature |  |
|  Fascia 3: > 10.000 e fino a 100.000 timbrature |  |
|  Fascia 4: > 100.000 e fino a 1.000.000 timbrature |  |
|  Fascia 5: > 1.000.000 e fino a 10.000.000 timbrature |  |
|  Fascia 6: > 10.000.000 timbrature |  |

**Modalità di remunerazione:** A Consumo

Durata Contrattuale:\_\_\_\_\_\_\_\_mesi (min 12 mesi; max 48 mesi)

NOTA BENE: la quantità di timbrature indicata dall’Amministrazione Contraente nella tabella soprariportatata è relativa al consumo stimato per l’intera durata del Contratto Esecutivo; pertanto, qualora a consuntivo finale si verifichi la circostanza per cui il consumo effettivo di timbri sia più basso del limite inferiore della fascia contrattualizzata, sarà effettuato **un conguaglio** dell’importo da corrispondere.

Ad esempio: l’Amministrazione contrattualizza il servizio L1.S13 sottoscrivendo un contratto della durata di 36 mesi per 500.000 timbrature (fascia 4 – da 100.000 fino a 1.000.000 di timbrature). In funzione dei consumi effettuati, il Fornitore fatturerà periodicamente l’importo corrispondente al numero effettivo di timbrature erogate nel periodo, moltiplicato per il prezzo offerto dal Fornitore per la fascia 4. Se al termine dei 36 mesi il consumo totale è pari a 80.000 timbrature (fascia 3 – da 10.000 fino a 100.000 timbrature), il Fornitore effettuerà un conguaglio applicando la differenza di prezzo offerto tra la fascia 3 e la fascia 4 sul totale di 80.000 timbrature.

# *SEZIONE P - L1.S14 - Validazione temporale elettronica qualificata*

**Descrizione del Servizio**

Il servizio di “Validazione temporale elettronica qualificata” (in precedenza qualificato come ““Marca temporale”) consente alle Amministrazioni, mediante un Certificatore accreditato, di associare data e ora, certe e legalmente valide, a un documento informatico, permettendo una validazione temporale del documento opponibile a terzi.

Il servizio permette quindi di garantire l’apposizione di un riferimento temporale certo (legalmente valido) sia a documenti firmati digitalmente sia a documenti non firmati, oltre che l’estensione della validità legale dei propri documenti firmati digitalmente nel tempo.

In definitiva permette di:

* dimostrare che lo specifico documento elettronico esisteva in quella firma alla specifica data;
* estendere la validità di un documento informatico, firmato digitalmente, oltre la data di scadenza del certificato di firma digitale.

**Modalità di erogazione:** Centralizzata presso il Centro Servizi del RTI

**Metrica Servizio:**

1. Numero di marcature (best effort)

Indicare la fascia di erogazione richiesta:

|  |  |  |
| --- | --- | --- |
| Tipologia di servizio | Fasce di erogazione(Marcature) | Quantità(Marcature) |
| L1.S14 - Validazione temporale elettronica qualificata |  Fascia 1: fino a 1.000 marcature |  |
|  Fascia 2: fino a 10.000 marcature |  |
|  Fascia 3: fino a 100.000 marcature |  |
|  Fascia 4: fino a 1.000.000 marcature |  |
|  Fascia 5: fino a 10.000.000 marcature |  |
|  Fascia 6: > 10.000.000 marcature |  |

**Modalità di remunerazione (Numero di marcature (best effort)):** A consumo

Durata Contrattuale:\_\_\_\_\_\_\_\_mesi (min 12 mesi; max 48 mesi)

NOTA BENE: la quantità di marcature indicata dall’Amministrazione Contraente nella tabella soprariportatata è relativa al consumo stimato per l’intera durata del Contratto Esecutivo; pertanto, qualora a consuntivo finale si verifichi la circostanza per cui il consumo effettivo di marcature sia più basso del limite inferiore della fascia contrattualizzata, sarà effettuato **un conguaglio** dell’importo da corrispondere.

Ad esempio: l’Amministrazione contrattualizza il servizio L1.S14 sottoscrivendo un contratto della durata di 36 mesi per 500.000 marcature (fascia 4 – da 100.000 fino a 1.000.000 di marcature). In funzione dei consumi effettuati, il Fornitore fatturerà periodicamente l’importo corrispondente al numero effettivo di marcature erogate nel periodo, moltiplicato per il prezzo offerto dal Fornitore per la fascia 4. Se al termine dei 36 mesi il consumo totale è pari a 80.000 marcature (fascia 3 – da 10.000 fino a 100.000 marcature), il Fornitore effettuerà un conguaglio applicando la differenza di prezzo offerto tra la fascia 3 e la fascia 4 sul totale di 80.000 marcature.

1. Numero di marcature (SLA garantito – 1 marcatura/sec)

Indicare il numero di pacchetti richiesti:

|  |  |  |
| --- | --- | --- |
| Tipologia di servizio | Fasce di erogazione(Marcature) | Quantità (Pacchetti) |
| L1.S14 - Validazione temporale elettronica qualificata (SLA Garantito) |  Garantita - N. 1 marcatura |  |
|  Garantita - N. 1 marcatura aggiuntiva |  |

**Modalità di remunerazione (Numero di marcature/sec (SLA Garantito)):** Canone Annuo

Durata Contrattuale:\_\_\_\_\_\_\_\_mesi (min 12 mesi; max 48 mesi)

# *SEZIONE Q - L1.S15 - Servizi specialistici*

**Descrizione del Servizio**

Il servizio “Servizi specialistici” consente all’Amministrazione di richiedere un supporto tecnico connesso all’attivazione dei servizi da remoto previsti nell’AQ.

Si riportano a titolo esemplificativo e non esaustivo alcune attività che possono essere svolte attraverso il servizio:

* supporto alla migrazione dei servizi di sicurezza dell’Amministrazione di tipo “on premise” verso i servizi oggetto di fornitura, nelle fasi di analisi e configurazione;
* attività di delivery dei servizi oggetto di fornitura durante le operazioni di migrazione;
* supporto nella definizione, configurazione ed erogazione del servizio di monitoraggio continuo delle vulnerabilità di sicurezza con particolare riferimento all’analisi dei deliverable raccolti a seguito dell’esecuzione da parte del fornitore delle sessioni di vulnerability assessment previsto nel servizio di Gestione continua delle vulnerabilita’ di sicurezza.

Descrivere le attività che l’Amministrazione intende svolgere attraverso il servizio di supporto specialistico:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Il servizio sarà erogato dalle risorse, facenti parte obbligatoriamente del Team di Servizio “Servizi Specialistici”, che dispongono delle competenze, esperienze e capacità richieste ai profili professionali elencati di seguito:

* Security Principal
* Security Solution Architect
* Senior Information Security Consultant
* Junior Information Security Consultant

**Modalità di erogazione:** on site e/o da remoto

**Metrica Servizio:** Giorni/Persona del Team ottimale (pari a 8 ore lavorative).

**Modalità di remunerazione:** Progettuale (a corpo)

Quanità:\_\_\_\_\_\_\_Giorni/Persona del Team ottimale

Durata Contrattuale:\_\_\_\_\_\_\_\_mesi (min 12 mesi; max 48 mesi)

# *SEZIONE R – Tabella Riepilogativa*

| Cod. Serv. | Servizio | Fascia di acquisizione | Quantità | Durata Contrattuale (Mesi) | Importo Totale del servizio [€] |
| --- | --- | --- | --- | --- | --- |
| **L1.S1** | Security Operation Center (SOC) | Fascia 1: fino a 300 EPS |  |  |  |
| Fascia 2: fino a 600 EPS |  |  |  |
| Fascia 3: fino a 1200 EPS |  |  |  |
| Fascia 4: fino a 6.000 EPS |  |  |  |
| Fascia 5: >6.000 EPS |  |  |  |
| **L1.S2** | Next Generation Firewall | Fascia 1: fino a 250 Mbps |  |  |  |
| Fascia 2: fino a 2 Gbps |  |  |  |
| Fascia 3: fino a 4 Gbps  |  |  |  |
| Fascia 4: fino a 7 Gbps |  |  |  |
| Fascia 5: fino a 15 Gbps |  |  |  |
| Fascia 6: > 15 Gbps |  |  |  |
| **L1.S3** | Web Application Firewall | Fascia 1: fino a 500 Mbps |  |  |  |
| Fascia 2: fino a 5 Gbps |  |  |  |
| Fascia 3: > 5 Gbps  |  |  |  |
| **L1.S4** | Gestione continua delle vulnerabilità di sicurezza | Fascia 1: fino a 50 IP |  |  |  |
| Fascia 2: fino a 200 IP |  |  |  |
| Fascia 3: > 200 IP  |  |  |  |
| **L1.S5** | Threat Intelligence & Vulnerability Data Feed | Fascia 1: fino a 10 feed |  |  |  |
| Fascia 2: fino a 50 feed |  |  |  |
| Fascia 3: > 50 feed  |  |  |  |
| **L1.S6** | Protezione navigazione Internet e Posta elettronica | Fascia 1: fino a 1.000 Utenti |  |  |  |
| Fascia 2: fino a 5.000 Utenti |  |  |  |
| Fascia 3: fino a 10.000 Utenti |  |  |  |
| Fascia 4: fino a 20.000 Utenti |  |  |  |
| Fascia 5: >20.000 Utenti |  |  |  |
| **L1.S7** | Protezione degli end-point | Fascia 1: fino a 500 Nodi |  |  |  |
| Fascia 2: fino a 1.000 Nodi |  |  |  |
| Fascia 3: fino a 5.000 Nodi |  |  |  |
| Fascia 4: > 5.000 Nodi |  |  |  |
| **L1.S8**  | Certificati SSL | Fascia 1: SSL OV |  |  |  |
| Fascia 2: SSL OV Wildcard |  |  |  |
| Fascia 3: SSL EV |  |  |  |
| Fascia 4: SSL DV |  |  |  |
| Fascia 5: SSL Code Signing |  |  |  |
| Fascia 6: SSL Client Auth |  |  |  |
| **L1.S9**  | Servizio di Formazione e Security awareness | Giorni/persona del Team Ottimale |  |  |  |
| **L1.S10** | Gestione dell’identità e l’accesso utente | Fascia 1: fino a 10.000 Utenti |  |  |  |
| Fascia 2: fino a 100.000 Utenti |  |  |  |
| Fascia 3: fino a 500.000 Utenti |  |  |  |
| Fascia 4: > 500.000 Utenti |  |  |  |
| **L1.S11** | Firma digitale remota | Fascia 1: > 50 e fino a 200 Utenti |  |  |  |
| Fascia 2: > 200 e fino a 500 Utenti |  |  |  |
| Fascia 3: > 500 e fino a 1.000 Utenti |  |  |  |
| Fascia 4: > 1.000 Utenti |  |  |  |
| **L1.S11** | Firma digitale remota massiva [SLA GARANTITO – 1 firma/sec] | Garantita - N. 1 firma |  |  |  |
| Garantita - N. 5 firme aggiuntive |  |  |  |
| **L1.S12** | Sigillo elettronico [SLA GARANTITO – 1 sigillo/sec] | Garantita - N. 1 sigillo |  |  |  |
| Garantita - N. 5 sigilli aggiuntivi |  |  |  |
| **L1.S13** | Timbro elettronico | Fascia 1: fino a 1.000 Timbrature |  |  |  |
| Fascia 2: > 1000 e fino a 1.000 Timbrature |  |  |  |
| Fascia 3: > 10000 e fino a 100.000 Timbrature |  |  |  |
| Fascia 4: > 100.000 e fino a 1.000.000 Timbrature |  |  |  |
| Fascia 5: > 1.000.000 e fino a 10.000.000 Timbrature |  |  |  |
| Fascia 6: > 10.000.000 Timbrature |  |  |  |
| **L1.S14** | Validazione temporale elettronica qualificata | Fascia 1: fino a 1.000 Marcature |  |  |  |
| Fascia 2: > 1.000 e fino a 10.000 Marcature |  |  |  |
| Fascia 3: > 10.000 e fino a 100.000 Marcature |  |  |  |
| Fascia 4: > 100000 e fino a 1.000.000 Marcature |  |  |  |
| Fascia 5: > 1.000.000 e fino a 10.000.000 Marcature |  |  |  |
| Fascia 6: > 10.000.000 Marcature |  |  |  |
| Validazione temporale elettronica qualificata [SLA GARANTITO – 1 marcatura/sec] | Garantita - N. 1 marcatura  |  |  |  |
| Garantita - N. 1 marcatura aggiuntiva |
| **L1.S15** | Servizi specialistici | Giorni/persona del Team Ottimale |  |  |  |
| **IMPORTO TOTALE CONTRATTO =** |  |