ALLEGATO 3 – CAPITOLATO TECNICO DI APPALTO SPECIFICO

AFFIDAMENTO DI "***Cybersecurity – prodotti e servizi connessi***" MEDIANTE APPALTO SPECIFICO NELL'AMBITO DELL'ACCORDO QUADRO STIPULATO DA CONSIP PER LA FORNITURA DI PRODOTTI PER LA GESTIONE DEGLI EVENTI DI SICUREZZA E DEGLI ACCESSI, LA PROTEZIONE DEI CANALI EMAIL, WEB E DATI ED EROGAZIONE DI SERVIZI CONNESSI PER LE PUBBLICHE AMMINISTRAZIONI

ID 2174 – Lotto Unico

Indice

1. APPALTO SPECIFICO "*CYBERSECURITY – PRODOTTI E SERVIZI CONNESSI*"

Il presente Appalto Specifico rientra nell'ambito dell'Accordo Quadro STIPULATO DA CONSIP PER LA FORNITURA DI PRODOTTI PER LA GESTIONE DEGLI EVENTI DI SICUREZZA E DEGLI ACCESSI, LA PROTEZIONE DEI CANALI EMAIL, WEB E DATI ED EROGAZIONE DI SERVIZI CONNESSI PER LE PUBBLICHE AMMINISTRAZIONI

Per tutto quanto non espressamente indicato nel Capitolato Tecnico di Appalto Specifico, dovrà farsi riferimento alle previsioni del Capitolato Tecnico di Accordo Quadro (Generale e Speciale) per le parti di pertinenza, che devono intendersi quindi obbligatorie e vincolanti.

In particolare i requisiti minimi del presente documento sono aggiuntivi ai requisiti minimi espressi in Accordo Quadro così come l'offerta migliorativa di Appalto Specifico deve essere aggiuntiva dell'offerta migliorativa di Accordo Quadro.

1.1 Definizioni

Nel corpo del presente Capitolato Tecnico, con il termine:

- **AQ** si intende l'Accordo Quadro stipulato da Consip;
- **AS** si intende il presente Appalto Specifico;
- **Amministrazione/Amministrazione Contraente**, si intende nel complesso le strutture organizzative facenti capo all'A.O. Ordine Mauriziano di Torino*;*
- **Punto Ordinante o, brevemente, PO** l'Amministrazione richiedente l'AS sul sistema di E-Procurement di Consip;
- **CTAQ** si intende il Capitolato Tecnico Speciale dell'Accordo Quadro;
- **OEAQ** si intende l'offerta economica vincolante del Fornitore Aggiudicatario per l'AQ;
- **OTAQ** si intende l'offerta tecnica vincolante del Fornitore Aggiudicatario per l'AQ;
- **OTAS** si intende l'offerta tecnica vincolante del Fornitore aggiudicatario dell'AS, che integra e migliora l'OTAQ;
- **CTGAQ** si intende il Capitolato Tecnico Generale dell'Accordo Quadro
- **CdO** si intende il Capitolato d'oneri dell'Accordo Quadro
- **Concorrente** o **Offerente**: il RTI che partecipa alla presente gara;
- **Contratto Esecutivo**: il contratto stipulato dall'Amministrazione con il Fornitore, che si perfeziona dopo l'aggiudicazione dell'Appalto Specifico;
- **CV:** centri di valutazione del Ministero dell'interno e del Ministero della difesa;
- **CVCN:** Centro di valutazione e certificazione nazionale istituito presso il Ministero dello sviluppo economico e trasferito dal D.L. 82/2021 presso l'Agenzia per la cybersicurezza nazionale;
- **Giorno lavorativo**: da lunedì a venerdì, esclusi sabato e festivi;
- **Meta-prodotto**: rappresenta l'offerta di riferimento per ogni prodotto richiesto in prima fase. Ogni meta-prodotto è caratterizzato dalla sua descrizione funzionale, da requisiti minimi, dai requisiti migliorativi offerti in prima fase e da un prezzo di riferimento che non potrà essere superato in AS, **ma <u>non</u> da una specifica tecnologia** (marca, modello, release firmware/software);

- **Prodotto**: rappresenta uno specifico prodotto (marca, modello, release firmware/software) offerto in seconda fase come istanza del meta-prodotto offerto in prima fase. Lo specifico prodotto offerto avrà quindi descrizione funzionale, requisiti minimi, requisiti migliorativi del corrispondente meta-prodotto offerto in prima fase ed eventuali ulteriori requisiti migliorativi offerti in base alle richieste dell'Amministrazione Contraente. Il prezzo del prodotto non potrà superare quello del corrispondente meta-prodotto a meno di quanto espressamente previsto nel Capitolato d'Oneri;
- **Portale della fornitura**: il Portale implementato dal Fornitore aggiudicatario secondo le specifiche tecniche descritte nel Capitolato Tecnico parte Generale al paragrafo 4.1
- **Servizi Base**: i servizi, a condizioni non tutte definite, che possono essere richiesti dalle Amministrazioni a completamento della fornitura richiesta in AS, ad eccezione dei servizi inclusi nella fornitura che dovranno essere obbligatoriamente erogati;
- **Servizi Aggiuntivi**: i servizi, a condizioni da definire da parte delle Amministrazioni, che possono essere richiesti a completamento della fornitura prevista in AS. L'Amministrazione potrà valorizzare i servizi accessori secondo le regole riportate nel Capitolato d'Oneri;
- **Sistema telematico (o semplicemente "Sistema")**: indica la piattaforma telematica attraverso cui saranno gestiti gli Appalti Specifici;
- **Responsabile dell'Amministrazione:** la persona indicata dall'Amministrazione nel contratto esecutivo e individuata come interlocutore tecnico con il Fornitore per tutte le attività contrattuali.
- **Responsabile del Fornitore:** la persona indicata dal Fornitore, nell'ambito di ciascun contratto esecutivo, come referente operativo per le attività di fornitura ed erogazione dei relativi servizi connessi, i cui requisiti professionali e compiti sono descritti al par. 2.4.1.2 del Capitolato Tecnico Generale di AQ;
- **RUAC:** responsabile unico delle attività contrattuali, cioè il referente del Fornitore nei confronti di Consip S.p.A. per tutte le attività di gestione relative all'AQ, dotato di appositi poteri di firma tali da impegnare in maniera esecutiva il Fornitore nei confronti delle Amministrazioni, i cui requisiti professionali e compiti sono descritti al par. 2.4.1.1 del Capitolato Tecnico Generale di AQ;
- **Vendor/produttore**: si intende il produttore dello specifico prodotto.
- **SEG:** secure email gateway;

2. CONTESTO DELL'APPALTO SPECIFICO e ELEMENTI TRASVERSALI AI VARI SERVIZI

2.1 Contesto organizzativo, tecnologico e normativo

2.1.1 Contesto Organizzativo

L'Amministrazione Contraente, Azienda Ospedaliera Mauriziano di Torino, è una delle sei Aziende Ospedaliere della Regione Piemonte, classificata come struttura ospedaliera sede di DEA di Livello II.
L'Azienda ospedaliera (AO) Ordine Mauriziano di Torino è stata costituita, ai sensi della Legge regionale n.39 del 24 dicembre 2004, con decreto del Presidente della Giunta regionale n. 5 del 24 gennaio 2005, con decorrenza 1° febbraio 2005. L'AO ha personalità giuridica pubblica ed autonomia imprenditoriale.

Scopo e missione dell'AO Ordine Mauriziano di Torino, nel pieno rispetto della peculiarità storico-sociale dell'Ordine Mauriziano, corrispondono alla presa in carico dei bisogni di salute in fase acuta, in fase cronica nonché delle "patologie inguaribili", delle persone che si rivolgono all'Azienda Ospedaliera, nel rispetto della programmazione sanitaria regionale.

L'AO Ordine Mauriziano di Torino opera pertanto nell'ottica del perseguimento dei seguenti obiettivi:
a) Garantire ai cittadini un'assistenza sanitaria di qualità in continuo miglioramento, curando in particolare lo sviluppo degli interventi finalizzati al contrasto del dolore e delle sofferenze evitabili;
b) Incrementare ed aggiornare la tipologia delle prestazioni adeguandole tempestivamente ai bisogni di salute emergenti;
c) Ottimizzare l'utilizzo delle risorse disponibili, umane, tecniche, strutturali ed economiche;
d) Promuovere la collaborazione ed i collegamenti col territorio;
e) Implementare linee di comportamento condivise e comuni a tutte le strutture;
f) Promuovere la crescita aziendale degli operatori;
g) Soddisfare le aspettative dei cittadini e degli operatori.
h) Rispettare i principi etici ed i valori sociali del contesto ambientale e la normativa.
i) Ridurre le opportunità che si manifestino casi di violazione del quadro di legalità aziendale e creare un contesto sfavorevole alla corruzione, in riferimento a qualsiasi malfunzionamento dell'amministrazione a causa dell'uso a fini privati delle funzioni attribuite al dipendente dell'azienda nonché alle attività provenienti dall'esterno dirette ad inquinare l'azione amministrativa, a prescindere dal fatto che queste attività riescano a realizzare effettivamente il proprio illecito risultato.

I fabbisogni espressi nel presente documento sono coerenti alle esigenze espresse, dall'Amministrazione Contraente, nella scheda di progetto predisposta su indicazioni della Direzione Generale Unità di missione per l'attuazione degli interventi del PNRR del Ministero della Salute nell'ambito della Missione 6 del PNRR - "*M6.C2 – 1.1.1. Ammodernamento del parco tecnologico e digitale ospedaliero (Digitalizzazione delle strutture ospedaliere (DEA Dipartimenti di Emergenza e Accettazione di Livello I e II))*".
I principali dati identificativi della scheda di progetto sopra citata sono i seguenti:

- titolo intervento: Cartella clinica elettronica ospedaliera;
- CUP / codice progetto: G16G22000070005;
- data apertura CUP: 28/02/2022;
- presidio: 010908#Ospedale Mauriziano Umberto I – Torino.

In data 14/06/2022 con DGR numero 25-5186 "*PNRR Missione 6 Salute. Ripartizione, ai sensi dell'art.5, comma 1 del contratto istituzionale dei sviluppo (CIS), delle attività per l'attuazione del PNRR e del Piano nazionale per gli investimenti complementari (PNC), alle Aziende sanitarie regionali, in qualità di soggetti attuatori esterni delegati. Riparto agli Enti del SSR delle risorse del PNRR e PNC per complessivi Euro 524.744.995,00*", ha deliberato l'iniziativa a livello regionale.

La procedura afferisce pertanto agli investimenti pubblici finanziati, 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 o dal PNC

L'Azienda A.O. Mauriziano non è stata al momento individuata tra le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e degli obblighi previsti dal decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133. Tuttavia, a causa della qualità e della quantità di dati sensibili che vi transitano e che ovviamente generano un grande valore economico, il settore sanitario costituisce uno dei principali bersagli dei cyber criminali. In particolare gli ultimi report in materia hanno evidenziato la sanità italiana quale primo settore per numero di attacchi informatici subiti.

In questo contesto l'AO Ordine Mauriziano di Torino ha, in linea anche con gli obiettivi di sicurezza del Piano Triennale, intrapreso diverse misure per rafforzare il lvello di sicurezza ed intende dotarsi di strumenti per la gestione degli eventi di sicurezza e degli accessi, la protezione dei canali email e web ed in particolare - la fornitura dei seguenti prodotti:

- Secure Email Gateway (SEG), per consentire una protezione dalle minacce che provengono dal canale mail attraverso il filtraggio delle mail di spam e dei contenuti dannosi. Il SEG consente l'analisi sia della posta in ingresso sia della posta in uscita consentendo quindi, su quest'ultima, anche di prevenire l'eventuale perdita di dati sensibili contenuti all'interno delle mail.

2.1.2 Contesto Tecnologico

L'Azienda A.O. Ordine Mauriziano di Torino dispone di un propria sala macchine in cui sono ospitati i principali servizi applicativi all'interno di un'infrastruttura virtualizzata basata su VmWare ESXi.
In linea con le indicazioni dell'Agenzia per l'Italia Digitale, ed in particolare con quelle del Piano Triennale per l'Informatica nella Pubblica Amministrazione, ha intrapreso, da alcuni anni, un percorso di migrazione dei servizi applicativi dalla propria infrastruttura verso ambienti cloud che presentino adeguate caratteristiche di sicurezza e affidabilità. In particolare in fase di acquisizione di nuovi software, o di aggiornamento di quelli esistenti è stato applicato il principio "Cloud First" compatibilmente con le esigenze prestazionali e i limiti di continuità. In tale contesto spesso si sono adottati software as a service demandando parte della gestione della sicurezza ai fornitori stessi del servizio.
In generale, per garantire il massimo livello di protezione e resilienza, l'azienda ha adottato misure di sicurezza diversificate, implementando sistemi di sicurezza informatica stratificati, in modo da rispondere a più livelli alle minacce cyber.
Molte delle misure adottate rientrano nel "Sistema di Gestione per la Sicurezza delle Informazioni" aziendale (SGSI) che, attraverso un approccio continuo ed iterativo basato sul modello Plan-Do-Check-Act, si focalizza sull'individuazione, valutazione, trattamento e documentazione dei rischi associati alla gestione dei sistemi e delle infrastrutture informatiche.
A fianco del SGSI, per fornire risposte adeguate alla minaccia cyber, si è ritenuto opportuno selezionare un modello per l'incident response che potesse guidare il processo di risposta alle minacce cibernetiche e agli insider threat.
A tal fine è stato selezionato l'Incident response cycle che, attraverso le fasi di preparazione, identificazione, contenimento, eradicazione, ripristino e lesson learned, si ritiene possa aiutare nelle aree di prevenzione, rilevamento e risposta e per lo sviluppo delle strategie di difesa dagli attacchi.
Molta importanza è stato data proprio allo step di preparazione ed in particolare alla fase di harderning con l'obiettivo di ridurre la superficie di attacco.
Parallelamente, per valutare la completezza degli strumenti messi in campo e identificare eventuali gap da colmare, è stata avviata un'analisi che partendo dalle tecniche del framework "Mitre ATT&CK" (Adversarial Tactics, Techniques & Common Knowledge) ha valutato eventuali strumenti di contrasto e risposta per ciascuna tecnica.
Tale attività ha portato ad identificare alcune necessità tra cui:

- rafforzamento del protezione delle email attraverso un Security Email Gatawey

Tra gli strumenti gli strumenti attualmente in funzione in tema di cybersecurity:

- Protezione degli Endpoint (antivirus, antimalware, protezione da ransoware, web filtering, Botnet blocker) => attraverso la piattaforma F-secure Business Suite Premium

- Endpoint Detection and Response => attraverso la piattaforma F-Secure Elements Endpoint Detection and Response
- Firewall perimetrale => Watchguard Firebox M670
- Application control, Intrusion Prevenction Service (IPS), ATP Blocker, Gateway AntiVirus, WebBlocker (filtro contenuti/url) => attraverso la suite Watchguard Total Security all'interno dei firewall aziendali
- Telemetria attraverso diversi strumenti di monitoring: Cisco Prime per il monitoraggio degli switch e della rete, Check MK per i servizi e gli host, telemetria integrata in VmWare vSphere per le VM: sebbene non siano strumenti di cybersecutirty, aiutano il personale tecnico di rilevare anomalie che potrebbero segnalare un attacco in corso o la presenza di malware.
- Attività trimestrali di vulnerability assessment
- Attività di hardening programmata

In generale la strategia di cyber-sicurezza adottata dall'azienda si basa su alcuni aspetti di rilevo. Tra questi:

- Consapevolezza: la comprensione del rischio effettivo e potenziale è la leva per definire priorità di investimento nella protezione del patrimonio informativo aziendale.
- Pianificazione: una corretta pianificazione deve agire con un approccio di lungo termine e, al contempo, eseguire interventi immediati sugli aspetti più critici. Tutto questo è possibile soltanto quando si è definito un piano strategico, affrontando il problema non solo con la "tattica" giusta, ma con la giusta visione di insieme.
- Visione olistica: la continua evoluzione delle tecniche di attacco fa sì che la sicurezza informatica non debba essere vista come un prodotto, ma come un processo. Per questo occorre avere un approccio basato su una visione olistica, per definire i processi, agire in modo sostenibile, definendo priorità e allocazione degli investimenti.
- Security by design: l'adozione di modelli di security by design è determinante per garantire che il software sviluppato e i sistemi installati siano sicuri, sin dalla progettazione e fino alla fase di messa in produzione.
- Interdisciplinarità. Tutte le figure professionali debbono essere coinvolte nei processi di sicurezza considerando che questa non è solo appannaggio delle figure tecniche. Alcune azioni da introdurre per aumentare la resilienza ai rischi cyber richiedono infatti interdisciplinarità, perché il cybercrime stesso agisce con attacchi che si basano sull'amalgama di molte discipline.
- Elemento umano: l'elemento umano è centrale nell'approccio alla cybersecurity, perché occorre agire su diversi soggetti: su chi può subire un attacco cyber (i dipendenti), chi deve difendere la PA da un attacco (gli addetti alla sicurezza aziendale) e chi deve decidere (direzione e governance) in merito a quali investimenti introdurre per ridurre il rischio cyber e come agire tempestivamente a fronte di attacchi subiti.
- Comunicazione. Uno degli elementi critici nelle organizzazioni complesse è la comunicazione con gli stakeholder interni o esterni. È necessario ottimizzare la comunicazione tra il personale tecnico dei Sistemi Informativi (sviluppatori, sistemisti, dba, tecnici manutentori), il personale tecnico dell'Ingegneria Clinica, il personale amministrativo e sanitario e i gruppi dirigenziali. Una condivisione degli obiettivi in tema di sicurezza cibernetica e delle strategie aiuta nel .
- Aggiornamento delle competenze. Non tutte le professioni evolvono così rapidamente come la sicurezza informatica. In un'ottica di sostenibilità della cybersecurity è importante tenere allineate ed aggiornate le competenze delle figure professionali coinvolte nella cybersecurity.

2.1.3 Contesto Normativo

Attraverso il Piano Triennale per l'Informatica nella Pubblica Amministrazione 2020 – 2022, AgID ha proseguito la propria attività per la regolamentazione della cyber security già avviata negli anni precedenti, evidenziando come l'esigenza per la PA di contrastare le minacce cibernetiche sia divenuta fondamentale in quanto garantisce non solo la disponibilità, l'integrità e la riservatezza delle informazioni proprie del Sistema informativo della Pubblica Amministrazione, ma è il presupposto per la protezione del dato che ha come conseguenza diretta l'aumento della fiducia nei servizi digitali erogati dalla PA .

Nel Piano Triennale AGID fissa pertanto ulteriori obiettivi e relative linee di azione, in capo ad AgID e al Dipartimento per la Trasformazione Digitale, nonché alle **PA**.
In tale contesto, si inserisce anche la pubblicazione, da parte di AgID, delle:

- «Misure minime di sicurezza ICT per le pubbliche amministrazioni (aprile 2017);
- «linee guida di sicurezza nello sviluppo delle applicazioni» (maggio 2020), per lo sviluppo del software sicuro nella PA;
- «linee guida di sicurezza nel procurement ICT» (maggio 2020), che raccolgono indicazioni tecnico amministrative,
- buone prassi e strumenti operativi per garantire all'interno delle procedure di gara per l'approvvigionamento di beni e servizi ICT, la rispondenza di questi ad adeguati livelli di sicurezza.

Le attività di supporto alle PA nella prevenzione e risposta agli incidenti informatici svolte in passato dal CERT –PA, sono invece gestite, come previsto dal DPCM 8 agosto 2019, dallo CSIRT Italia, il nuovo team per la cyberdifesa nazionale dapprima istituito presso il Dipartimento Informazioni per la Sicurezza (DIS) e trasferito, dal DL 82/2021 ("Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale") presso l'Agenzia per la cybersicurezza nazionale .

A ciò si aggiunge l'entrata in vigore (01/06/2021) del D.L. 77/2021 "Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure", che ha l'obiettivo di semplificare e agevolare la realizzazione del Piano Nazionale di Ripresa e Resilienza e che destina 620 milioni di euro alla cyber security delle PP.AA., considerando quindi questo un asset fondamentale a servizio della digitalizzazione del Paese.

Gli ambiti (o layer) – cosiddetti di I livello - e i relativi obiettivi del Piano Triennale che si prevede di mappare mediante le attività che saranno svolte con tale contratto, riguardano:

Ambito (layer) – I livello	**Obiettivi Piano Triennale**
Sicurezza Informatica	Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nell'A.O. Ordine Mauriziano
	Aumentare il livello di sicurezza informatica della posta elettronica

Indicatore Generale: "Obiettivi CAD raggiunti con l'intervento" (art. 51 del CAD, rubricato "*Sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni*")

*Per l'*individuazione delle soluzioni tecnologiche più idonee a garantire la sicurezza dei sistemi, è riportata di seguito in tabella una mappatura tra le tipologie di prodotti acquistabili e le misure minime di sicurezza AGID (*Circolare 18 aprile 2017, n. 2/2017, Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni*" e successive modifiche e integrazioni) ad esse associabili. Tali misure, pertanto, potranno essere implementate, in tutto o in parte, mediante l'adozione della fornitura richiesta.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE					
ABSC_ID			Livello	Descrizione	Ambito
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	SEG
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	SEG
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	SEG

L' Indicatore di Progresso (Ip) , descritto al par. 1.4.2.1 del CTGAQ, potrà essere calcolato relativamente alla classe di controlli ABSC (Agid Basic Security Control) sopra indicate, con l'obiettivo di inserire un sistema che migliori e automatizzi la protezione dalle minacce che provengono dal canale mail attraverso il filtraggio delle mail di spam e dei contenuti dannosi, anche prevenendo l'eventuale perdita di dati sensibili contenuti all'interno delle mail .

3. OGGETTO, DURATA DELL'APPALTO SPECIFICO E LUOGO DI ESECUZIONE

3.1 Oggetto della fornitura

Il presente AS ha ad oggetto i seguenti prodotti/servizi:

Prodotti:

1. *Secure Email Gateway (SEG)*

Funzionalità aggiuntive sui prodotti:

- *Funzionalità aggiuntiva - SEG - Configurazione in alta affidabilità*

Servizi base connessi alla fornitura:

- *installazione e configurazione (inclusi nella fornitura)*
- *formazione e affiancamento*
- *manutenzione profilo LP(comprensiva di help desk)*
- *Contact Center (incluso nella fornitura)*
- *supporto specialistico*

Si rimanda al paragrafo "Descrizione della fornitura" per le caratteristiche specifiche dei prodotti e servizi richiesti.

3.2 Durata del contratto

La durata del contratto è fissata in 24 mesi a decorrere dalla verifica di conformità positiva.

3.3 Luogo di esecuzione ed orario di erogazione dei servizi

- Sede in cui dovranno essere consegnati, installati i prodotti e/o erogati i servizi richiesti : A.O. Ordine Mauriziano – S.C. ICT & Sistemi Informativi – Via Magellano, 1 10128 Torino;
- orari di erogazione dei servizi richiesti: dalle 8,30 alle 16,30

4. DESCRIZIONE DELLA FORNITURA

4.1 Garanzia

Per la garanzia dei prodotti, il Fornitore faccia riferimento al par. 2.1.10 del CTAQ.

4.2 Prodotti

4.2.1 Requisiti del SEG

E' richiesta la fornitura di un sistema di Email SEG che consenta una protezione dalle minacce che provengono dal canale mail attraverso il filtraggio delle mail di spam e dei contenuti dannosi.
Il SEG dovrà consentire non solo l'analisi della posta in ingresso ma anche che di quella in uscita permettendo quindi di prevenire l'eventuale perdita di dati sensibili contenuti all'interno delle mail.

Il sistema proposto dovrà rispettare tutti i requisiti minimi previste dall'accordo quadro e qui di seguito richiamati:

Requisiti minimi

Mail Transfer Agent
Funzionalità di protezione a più livelli per l'individuazione dello SPAM e la rilevazione di minacce attraverso più meccanismi quali l'analisi approfondita del contenuto delle email e il filtraggio delle URL presenti nel corpo del messaggio
Funzionalità di anti-virus, anti-phishing, anti-BEC, anti-spoofing, anti-spam e anti-malware in grado di identificare virus, worms, ransomware attraverso il riconoscimento di signature e analisi euristica dei contenuti
Protezione da email massive e di marketing
Protezione realtime Office 365 attraverso API o SMTP relay
Identificazione di attacchi di tipo zero-day
Blocco email in base alla lingua utilizzata o specifici charset
Rimozione, tramite l'analisi del contenuto dell'email e degli allegati, di file malevoli. Identificazione, tramite analisi di tipo true file type, della tipologia di file e inclusione URLs potenzialmente pericolosi
Trattamento delle email per quali è stato identificato un virus/malware con varie opzioni quali l'invio di una notifica, la quarantena, l'eliminazione del messaggio, l'inserimento in white/black list
Supporto dei filtri basati sulla reputazione dell'indirizzo IP di provenienza e/o URL
Ispezione sulla posta in uscita e in ingresso
Crittografia dei messaggi in uscita con protollo SSL/TLS

Supporto dell'autenticazione tramite LDAP/AD
Aggiornamenti costanti delle signature attraverso feed di threat intelligence
Possibilità di bloccare mail contenenti documenti di Office che utilizzino MACRO. La soluzione deve segnalare all'amministratore/utente l'avvenuto blocco.
La soluzione deve avere funzionalità di reportistica che consentano: - il monitor in real-time attraverso dashboard - la realizzazione di report attraverso template predefiniti - la possibilità di esportare i report
Supporto del protocollo IPv6
Supporto per configurazione in alta affidabilità
Supporto dei protocolli SPF, DKIM o in alternativa del protocollo DMARC

In merito alla verifica degli url presenti nel messaggio, si richiede che sia effettuata in tempo reale al momento del click grazie a meccanismi di sostituzione del url originale con un reindirizzamento ad apposito sistema di sanboxing che provveda ad analizzare la sicurezza della destinazione, non solo attraverso balck list (es. realtime blackhole lists), ma anche grazie a sistemi di intelligenza artificiale e machine learning.

Anche in merito all'analisi degli allegati, si richiede che il SEG disponga di funzionalità atta a rilevare ed eventualmente rimuovere il contenuto attivo presente negli allegati stessi. A titolo esemplificato il sistema dovrà essere in grado di disarmare script powershell contenuto in documenti office o comandi javascript in all'interno di un Pdf.

La soluzione richiesta dall'A.O. Ordine Mauriziano dovrà prevedere quale funzionalità aggiuntiva funzionamento in alta affidabilità e su cloud privato. Come riportato alla risposta 59) dei chiarimenti pubblicati in Accordo Quadro, si precisa che *"la soluzione in fase di Accordo Quadro dovrà essere quotata su appliance fisica Hardware con relativo Software, mentre in fase di Appalto Specifico potrà essere offerta in versione Virtuale, se richiesto dall'Amministrazione"*. Questa Amministrazione ha scelto tale opzione e in particolare è previsto che l'istanza principale del SEG sia fornita in versione virtuale e dovrà essere installata all'interno del private cloud Nivola del CSI Piemonte (nel tenant dell'Amministrazione), mentre la seconda istanza sarà ospitata, sempre nella sua versione virtuale, all'interno dell'infrastruttura VmWare presso la sala Server aziendale.

L'installazione e configurazione del prodotto dovrà avvenire insieme al personale interno in modo da semplificare le operazioni di accesso ai vari sistemi che ospiteranno il SEG. All'interno della configurazione sarà da ricomprendersi le attività di integrazione con l'attuale server email Mdaemon di AltN.

Al momento non sono previste integrazioni con ulteriori sistemi di Cybersecurity, ma il Fornitore indichi e descriva l'eventuale possibilità di integrazione con altre soluzioni di sicurezza (esempio soluzioni Anti APT, NGFW, SIEM, etc).

In sintesi è richiesto il seguente prodotto:

- SEG_3 (fascia 3): fino a 40.000 mail/ora

I requisiti migliorativi oggetto di valutazione di AS e riportati anche nella richiesta d'Offerta sono di seguito elencati:

- Configurazione della soluzione in alta affidabilità. Saranno valutate le modalità implementative proposte per la configurazione in alta affidabilità, in termini di disponibilità della soluzione e delle sue componenti in caso di guasto.

4.3 Servizi

Sono indicati i servizi, base ed aggiuntivi richiesti:

- **servizio di installazione e configurazione** (il relativo costo è da intendersi compreso nei corrispettivi previsti per i prodotti offerti). Il servizio comprende tutto quello che è necessario per le attività di installazione e configurazione degli elementi acquistati dall'Amministrazione Contraente, inclusi eventuali elementi offerti come migliorativi dal Fornitore Aggiudicatario in sede di AQ e in sede di AS. Il servizio dovrà inoltre prevedere :
    - la definizione di processi e modalità operative specifiche del contesto dell'Amministrazione per la realizzazione del servizio
    - il servizio di pre – installazione/configurazione delle soluzioni in ambiente test
    - competenze ed esperienze specifiche del personale addetto al servizio di installazione e configurazione
- ***Servizio di supporto alla verifica di conformità.*** Ai sensi di quanto previsto all'art. 1, comma 6 lett. a) del D.L. 105/2019, la cui efficacia è stata modificata dall'art. 16 comma 9, lett. a) del D.L. n. 82/2021, si precisa innanzitutto che il Fornitore dovrà fornire pieno supporto all' Amministrazione, chiamate a collaborare con il CVCN o con i CV all'effettuazione di verifiche preliminari e condizioni e test hardware e software su forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui all'art 1 comma 2 lett. b della legge 133/2019. In aggiunta, è previsto un servizio di supporto alla verifica di conformità, da intendersi quale assistenza del Fornitore all'Amministrazione nella fase di verifica di quanto fornito e realizzato, obbligatorio ed il cui relativo costo è da intendersi compreso nei corrispettivi previsti per i prodotti offerti. L'Aggiudicatario procederà, con propri mezzi e risorse, alla verifica funzionale di tutti gli elementi oggetto di fornitura; tali prove dovranno consistere in test volti a verificare che quanto installato sia conforme ai requisiti offerti e si intenderà positivamente superata solo se tutti gli elementi installati risultino funzionare correttamente, sia singolarmente che interconnessi tra loro in modo che il complesso dei prodotti implementati operi secondo quanto previsto dai requisiti previsti in AQ ed nell'AS. Al termine di tale verifica, l'Aggiudicatario consegnerà all'Amministrazione Contraente il "*Verbale di Fornitura*" , o il "*Rapporto di Fine Intervento*" nel rispetto dei termini stabiliti nel Capitolato Tecnico, pena l'applicazione delle relative penali. Il Fornitore inoltre, in sede e al termine della verifica, dovrà fornire all'Amministrazione tutte le informazioni di dettaglio necessarie per la presa in carico dei beni da parte della stessa.
- ***Servizio di manutenzione*****.** La manutenzione comprende le attività volte a garantire una pronta correzione dei malfunzionamenti e il ripristino delle funzionalità, anche attraverso attività di supporto on-site. Il servizio di manutenzione deve essere prestato dall'Aggiudicatario nel rispetto degli SLA previsti, con interventi da effettuarsi presso i siti dell'Amministrazione Contraente, pena l'applicazione delle penali previste nell'AQ. **Profilo di qualità richiesto per i servizi erogati, *Low Profile* (*Business Day*) per 24 mesi**. Le attività di manutenzione possono riassumersi in:
    - ricezione della chiamata di assistenza da parte dell'Amministrazione e assegnazione del Severity Code
    - risoluzione del problema tramite supporto telefonico all'utente (ove possibile) e/o eventuale intervento/i remoto/i;
    - risoluzione della causa del guasto tramite, ove necessario intervento presso la sede/luogo interessato, ripristino del servizio/funzionalità sui livelli preesistenti al guasto/anomalia,

anche attraverso sostituzioni di elementi danneggiati, verifica funzionale del sistema per assicurare l'eliminazione della causa del guasto.

Ogni intervento di manutenzione dovrà prevedere la redazione del relativo "*verbale di intervento*" e l'eventuale aggiornamento della documentazione di progetto. Gli interventi dovranno concludersi con l'attività di verifica del corretto funzionamento delle apparecchiature sostituite o riparate e del sistema nella sua globalità. Tutte le attività previste (interventi del Fornitore presso l'Amministrazione, rimozione degli elementi, riparazione degli elementi guasti, successiva installazione) sono da intendersi incluse nel costo del servizio.

Per l'attività di manutenzione sarà richiesto l'accesso da remoto: il Fornitore precisi nell'offerta tecnica l'architettura e la modalità di implementazione del collegamento per l'accesso remoto ai sistemi dell'Amministrazione a supporto delle attività di manutenzione, al fine di garantire l'integrità, la riservatezza e la sicurezza dei dati.

- ***Servizio di supporto specialistico.*** E' richiesto il Servizio di:
  - supporto specialistico - **Senior Security Architect - fascia standard per un totale di 1 giorno.**
  - supporto specialistico - **Senior Security Analist - fascia standard per un totale di 2 giorni.**

Obiettivo dell'Amministrazione è di essere supportata in varie attività inerenti sia la fornitura specifica acquistata in AQ per la propria infrastruttura di sicurezza informatica. Il servizio potrà riguardare le attività di :

- l'effettuazione, nelle fasi successive all'implementazione dei prodotti, di attività di analisi specifiche che consentano di stabilire le policy di sicurezza maggiormente adeguate da implementare nel complesso dei sistemi dell'Amministrazione
- il supporto operativo al personale dell'Amministrazione nella gestione della sua infrastruttura, fornendo competenze specifiche in ambito di sicurezza informatica. Tale supporto potrà essere in modalità "a chiamata"

- ***Servizio di formazione e affiancamento.*** E' richiesto un servizio di formazione presso la sede dell'Azienda per un **totale di 2 giorni** . Il servizio potrà prevedere le seguenti attività:
  - istruire i discenti sulle specifiche tecnologie acquistate nell'AS
  - descrivere i moduli acquistati in termini di caratteristiche, configurazione e funzionalità
  - mettere il personale designato dall'Azienda in grado di provvedere alla gestione delle componenti installate in maniera autonoma ed ottimale con particolare riferimento alla configurazione di regole personalizzate e al troubleshooting e alla risoluzione delle problematiche più comuni.
  - realizzare demo e/o attività di test che consentano ai discenti di apprendere le principali funzionalità dei prodotti attraverso l'esperienza diretta

In seguito alla valutazione positiva effettuata dall'Amministrazione, a conclusione del corso l'Aggiudicatario rilascerà all'Amministrazione un "*Verbale di erogazione del Corso*" attestante la data di effettiva erogazione del servizio, la durata effettiva, il programma effettivamente seguito ed eventuali criticità emerse.

La fatturazione del servizio potrà essere effettuata dall'Aggiudicatario soltanto in seguito all'esito positivo della verifica e valutazione sull'andamento del corso sopra descritta, ossia dalla data riportata nel "*Verbale di erogazione del Corso*".

5. ULTERIORI REQUISITI DI AS

La procedura afferisce agli investimenti pubblici finanziati 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 e pertanto:

- Il Fornitore deve rispettare i requisiti tecnici e ambientali previsti dalla normativa europea e nazionale in ottemperanza al principio di non arrecare un danno significativo all'ambiente "Do No Significant Harm" (DNSH), ivi incluso l'impegno a consegnare all'Amministrazione la documentazione a comprova del rispetto dei suddetti requisiti (sulla base della Circolare RGS n. 32 del 30 dicembre 2021 e dell'art. 17 del Regolamento UE 852/2020)
- Ai sensi dell'art. 47 comma 3, D.l. 77/2021, il Fornitore è tenuto a consegnare una relazione di genere sulla situazione del personale maschile e femminile in ognuna delle professioni ed in relazione allo stato di assunzioni, della formazione, della promozione professionale, dei livelli, dei passaggi di categoria o di qualifica, di altri fenomeni di mobilità, dell'intervento della Cassa integrazione guadagni, dei licenziamenti, dei prepensionamenti e pensionamenti, della retribuzione effettivamente corrisposta. La suddetta relazione dovrà essere tramessa, altresì, alle rappresentanze sindacali aziendali e alla consigliera e al consigliere regionale di parità. La relazione di cui sopra, corredata dall'attestazione dell'avvenuta trasmissione della stessa alle rappresentanze sindacali aziendali e alla consigliera e al consigliere regionale di parità, dovrà essere consegnata , entro 6 mesi dalla stipula dell'Accordo Quadro.
- In riferimento al comma 4 di cui al citato articolo 47, il Fornitore deve assicurare una quota pari almeno al 30 per cento, delle assunzioni necessarie per l'esecuzione del contratto o per la realizzazione di attività ad esso connesse o strumentali, sia all'occupazione giovanile sia all'occupazione femminile (come meglio specificato nel Contratto Esecutivo).

6. LIVELLI DI SERVIZIO E PENALI

- I livelli di servizio e qualità sono da intendersi quelli previsti nell'Accordo Quadro.
- L'Amministrazione potrà applicare al Fornitore le penali dettagliatamente descritte e regolate nell'Accordo Quadro , qui da intendersi integralmente trascritte.
- L'Amministrazione potrà applicare altresì le seguenti penali: in relazione alle procedure afferenti gli investimenti pubblici finanziati, 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, inserire penali di cui all'art. 47 comma 6 D.L. 31 maggio 2021 n. 77, convertito con mod. in l. 108/2021, con riguardo al mancato rispetto dei requisiti necessari e ulteriori requisiti premiali dell'offerta come previsto dall'art. 47, comma 4 e 5, D.L. n. 77/2021. L'operatore economico, entro 6 (sei) mesi dalla conclusione del contratto, è tenuto a consegnare alla stazione appaltante una relazione relativa all'assolvimento degli obblighi volti a favorire la pari opportunità di genere e generazionali, nonché l'inclusione lavorativa delle persone con disabilità nei contratti pubblici finanziati con le risorse del PNRR e del PNC, come da Decreto della Presidenza del Consiglio dei Ministri Dipartimento per le Pari Opportunità, pubblicato in data 30/12/2021, di cui al suddetto articolo: per ogni giorno lavorativo di ritardo sarà calcolata una penale di € 100,00.
- Per le modalità di contestazione ed applicazione delle penali vale tra le Parti quanto stabilito all'articolo 11 dell'Accordo Quadro.

7. PIANO OPERATIVO DELL'AS

Il Fornitore dovrà presentare entro 15 giorni lavorativi dalla data di stipula del Contratto e pena l'applicazione delle penali di cui al CTAQ, un "*Piano Operativo*" che riporti almeno i contenuti di cui al par. 3.2.1 del CTAQ.