SISTEMA SANITARIO REGIONALE
ASL ROMA 5

REGIONE LAZIO

REGIONE LAZIO
AZIENDA SANITARIA LOCALE ROMA 5

DELIBERAZIONE DIRETTORE GENERALE N° 001277 DEL 29 GIU. 2023

STRUTTURA PROPONENTE: DIPARTIMENTO TECNICO

Oggetto: Adesione Accordo Quadro Consip per i servizi si sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni (ID 2296) per un periodo di 48 mesi - CIG derivato 98493260F1

PARERE DEL DIRETTORE AMMINISTRATIVO Dott. Filippo Coiro

☒ Favorevole ☐ Non favorevole (vedi motivazioni allegate)

data 29 GIU. 2023

PARERE DEL DIRETTORE SANITARIO F.F. Dr. Franco Cortellessa

☒ Favorevole ☐ Non favorevole (vedi motivazioni allegate)

data 29 GIU. 2023

Atto trasmesso al Collegio Sindacale

☐ Senza osservazioni ☐ Con osservazioni (vedi allegato)

Il Presidente _____ data _____

Il Dirigente addetto al controllo del budget, con la sottoscrizione del presente atto, attesta che lo stesso non comporta scostamenti sfavorevoli rispetto al budget economico.

Voce del conto economico su cui si imputa la spesa: 502020106-

Registrazione n. 2023/1582- del 12-06-2023

Il Direttore ad interim UOC Bilancio e Contabilità
(Dott. Fabio Filippi) _____

Il Dirigente e/o il responsabile del procedimento proponente, con la sottoscrizione del presente atto a seguito dell'istruttoria effettuata attesta che l'atto è legittimo nella forma e nella sostanza ed è utile per il servizio pubblico

Il Resp.le F.O. Gestione Amm.va e di Progetto Dr.ssa M. Fatima Pellegrino _____

Il RUP Dott. Luca Centurelli _____

Il Direttore Dipartimento Tecnico Dott. Mario Petrucci _____

La presente deliberazione è costituita da n. 4 pagine

Da n. 1 allegati per un totale di n. 28 pagine

Il Direttore del Dipartimento Tecnico relaziona al Direttore Generale quanto segue e sottopone il seguente schema di deliberazione:

ai sensi e per gli effetti della Deliberazione n. 933 del 19/07/2019, parzialmente modificata con Deliberazione n. 1126 del 10/09/2019, con la quale è stato adottato l'Atto Aziendale pubblicato sul B.U.R.L. n. 84 del 17/10/2019 e della deliberazione n. 993 del 07/06/2022, con la quale sono state proposte modifiche all'Atto Aziendale approvate con determina regionale G07864 del 16/06/2022 e pubblicate sul B.U.R.L. n. 56, suppl. I, del 05/07/2022,

PREMESSO

che con D.M. del 24 febbraio 2000 pubblicato sulla G.U. della Repubblica Italiana - Serie Generale n. 58 del 10 marzo 2000, il Ministero ha affidato alla Consip S.p.A. tra l'altro l'assistenza nella pianificazione e nel monitoraggio dei fabbisogni di beni e servizi delle Pubbliche Amministrazioni;

che l'Agenzia per l'Italia Digitale prevede espressamente, fra gli strumenti e le risorse per l'attuazione del Piano Triennale per l'informatica nella Pubblica Amministrazione, la realizzazione degli acquisti utilizzando le iniziative Consip e, nello specifico, "Tra le iniziative Consip, quelle che da una prima analisi possono trovare applicazione nella realizzazione delle linee di azione del Piano da parte delle PA, sono gli Accordi quadro e le Convenzioni/Contratti quadro", come indicato nel Piano Triennale 2017-2019, Allegato 2, punto 4 "Iniziative Consip";

che Consip S.p.A., in esito ad apposita procedura ristretta per l'affidamento dei "Servizi di Identità Digitale e Sicurezza Applicativa", Lotto 2 (ID SIGEF 1403), aveva stipulato un Contratto Quadro con il RTI Aggiudicatario, composto dalle aziende Leonardo-Finmeccanica S.p.A, IBM Italia S.p.A. , FASTWEB S.p.A. e Sistemi Informativi S.r.l.;

che questa Azienda, con deliberazioni n. 856 del 04/07/2019 e n. 335 del 01/03/2022 aveva aderito alla citata procedura ristretta ((ID SIGEF 1403) per l'affidamento dei "Servizi di Identità Digitale e Sicurezza Applicativa", Lotto 2, prevedendo servizi di fornitura firma digitale, vulnerability assessment, secure web gateway, servizi professionali e di monitoraggio;

ATTESO

che, ai sensi di quanto previsto nella direttiva del 1° agosto 2015 del Presidente del Consiglio dei Ministri relativa alle misure minime di sicurezza ICT per le Pubbliche Amministrazioni, questa Azienda aveva prodotto, entro il 31 dicembre 2017, "La Relazione sullo studio preliminare sugli interventi da effettuare nell'ASL ROMA 5 per l'adeguamento obbligatorio delle misure minime di sicurezza ICT per le Pubbliche Amministrazioni", così come indicato nella Circolare AgID n. 2/2017 pubblicata in Gazzetta Ufficiale il 5 maggio 2017;

che, anche a seguito delle attività di assessment sull'infrastruttura e i sistemi informatici aziendali svolte nel corso del 2022 attraverso l'erogazione dei servizi di cui alla citata Deliberazione n. 335 del 01/03/2022, la UOC IT ha prodotto un piano di mappatura dei rischi e degli interventi valutati come necessari per ridurre l'impatto di minacce in ambito di sicurezza informatica;

che il piano di mappatura dei rischi e degli interventi necessari per ridurre l'impatto di minacce in ambito di sicurezza informatica è stato adottato con deliberazione n. 2254 del 29 dicembre 2022;

PRESO ATTO

che in data 24/05/2022 è stato aggiudicato da CONSIP al RTI Accenture S.p.A., Fastweb S.p.A., Fincantieri NexTech S.p.A., Difesa e Analisi Sistemi S.p.A. l'Accordo Quadro per i servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni (ID 2296);

che a partire dal mese di Novembre 2022 il nuovo Accordo Quadro è stato reso attivo per le pubbliche amministrazioni interessate;

ATTESO

che, secondo quanto previsto nella Guida al contratto quadro per "servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni (ID 2296)", la UOC IT ha redatto un "Piano dei Fabbisogni" contenente la descrizione delle esigenze aziendali e le indicazioni di tipo quantitativo dei servizi ritenuti necessari, inoltrandolo successivamente al RTI aggiudicatario, tramite PEC, in data 7 aprile 2023;

che il RTI Accenture S.p.A., Fastweb S.p.A., Fincantieri NexTech S.p.A., Difesa e Analisi Sistemi S.p.A, aggiudicatario del citato Accordo Quadro ha trasmesso in data 08/05/2023 il "Piano Operativo" identificato come AQSEC-2296L1-PO Rev. 01, acquisito al protocollo ASL Roma 5 con n. 19147 del 08/05/2023, che forma parte integrante e sostanziale del presente provvedimento come Allegato n. 1;

PRESO ATTO

che secondo quanto previsto dalla citata Guida al contratto quadro per "servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni (ID 2296)", "L'Amministrazione, entro 30 giorni solari dalla relativa ricezione, ha la facoltà di approvare il Piano Operativo", e che "Il Contratto si perfeziona in seguito della decorrenza del termine di 4 giorni lavorativi dalla ricezione del Piano operativo da parte dell'operatore economico sulla base dell'apposito schema allegato alla documentazione di gara";

che, a seguire, le PP.AA. aderenti procedono a stipulare il conseguente "Contratto Esecutivo" approvando il "Progetto dei Fabbisogni", che insieme al "Piano operativo" ne costituisce parte integrante (cfr. Guida all'AQ LOTTO 1 – Servizi di sicurezza da remoto, paragrafo 4.2.4: "Con l'approvazione del Piano Operativo, si stipulerà con il Fornitore il Contratto Esecutivo, sulla base dell'apposito schema di contratto esecutivo che conterrà quali allegati il Piano dei Fabbisogni e il Piano Operativo");

VISTO

il piano aziendale di mappatura dei rischi e degli interventi necessari per ridurre l'impatto di minacce in ambito di sicurezza informatica, approvato con Deliberazione n. 2254 del 29 dicembre 2022;

ACCERTATO

che il Piano Operativo AQSEC-2296L1-PO Rev. 01, trasmesso in data 08/05/2023 dal RTI Accenture S.p.A., Fastweb S.p.A., Fincantieri NexTech S.p.A., Difesa e Analisi Sistemi S.p.A., e acquisito al protocollo ASL Roma 5 con n. 19147 del 08/05/2023, che forma parte integrante e sostanziale del presente provvedimento come Allegato n. 1 risponde alle esigenze della ASL Roma 5;

RITENUTO

opportuno approvare il sopra citato Piano Operativo AQSEC-2296L1 Rev. 01, redatto dall'RTI aggiudicatario, procedendo alla successiva sottoscrizione del Contratto esecutivo, sulla base dell'apposito schema di contratto esecutivo che conterrà quali allegati il "Piano dei Fabbisogni" e il "Piano Operativo";

DATO ATTO

che la spesa complessiva derivante dall'adesione all'Accordo Quadro risulta pari ad € 1.399.425,48 IVA esclusa, per una durata di 48 mesi a partire dal 01 giugno 2023;

che la ripartizione annuale dei costi derivanti, sulla base della priorità delle azioni necessarie a elevare i livelli di sicurezza sui sistemi aziendali, viene stimata come segue:

- anno 2023, costo di €675.596,37 IVA esclusa;
- anno 2024, costo di €241.276,37 IVA esclusa;
- anno 2025, costo di €241.276,37 IVA esclusa;
- anno 2026, costo di €241.276,37 IVA esclusa;

che, per il relativo affidamento è stato acquisito dal sito dell'Autorità di Vigilanza sui Contratti Pubblici il CIG 98493260F1, derivato dal CIG 88846293CA;

PROPONE

Per le motivazioni espresse in premessa che si intendono qui riportate:

1. di aderire all' Accordo Quadro Consip per i servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni (ID 2296) per un periodo di 48 mesi a partire dal 01/06/2023, in favore del RTI aggiudicatario Accenture S.p.A., Fastweb S.p.A., Fincantieri NexTech S.p.A., Difesa e Analisi Sistemi S.p.A., per un importo complessivo pari ad € 1.707.299,09 Iva inclusa – CIG derivato 98493260F1;
2. di approvare il Piano Operativo trasmesso in data 08/05/2023 al prot. generale n. 19147 ASL Roma 5 dal RTI Accenture S.p.A., Fastweb S.p.A., Fincantieri NexTech S.p.A., Difesa e Analisi Sistemi S.p.A., e identificato con AQSEC-2296L1-PO Rev. 01, che forma parte integrante e sostanziale del presente provvedimento come Allegato n. 1 e di procedere successivamente alla sottoscrizione del Contratto Esecutivo dell'Accordo Quadro Consip per i servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni (ID 2296);
3. di trasmettere il presente atto alla UOC Bilancio e Contabilità per l'imputazione dei relativi costi sul conto 502020106 "servizi di assistenza informatica" sui rispettivi anni di competenza, secondo lo schema seguente:
   - anno 2023, per un costo di €675.596,37 IVA esclusa, per un importo totale di €824.227,57;
   - anno 2024, per un costo di €241.276,37 IVA esclusa, per un importo totale di €294.357,17;
   - anno 2025, per un costo di €241.276,37 IVA esclusa, per un importo totale di €294.357,17;
   - anno 2026 per un costo di €241.276,37 IVA esclusa, per un importo totale di €294.357,17;
4. di nominare, quale Responsabile unico del procedimento, ai sensi dell'art. 31 del D. Lgs. n. 50/2016 il Dott. Luca Centurelli e Direttore dell'esecuzione ai sensi dell'art. 101 del D. Lgs. n. 50/2016 la Dott.ssa Maria Fatima Pellegrino;
5. di dare mandato alla UOC IT di provvedere, per quanto di competenza, alla gestione del rapporto contrattuale, all'emissione del relativo ordine elettronico e alla liquidazione delle competenze effettivamente spettanti per il periodo di vigenza contrattuale;
6. di disporre che il presente atto venga pubblicato nell'Albo Pretorio on-line aziendale ai sensi dell'Art. 32 comma 1 della Legge n. 69 del 18 giugno 2009;

Attesta, altresì, che la presente proposta, a seguito dell'istruttoria effettuata, nella forma e nella sostanza, è legittima e pienamente conforme alla normativa che disciplina la fattispecie trattata.

Il Responsabile UOS Flussi Informativi e CUP
Dott. Luca Centurelli

Il Direttore Dipartimento Tecnico
Dott. Mario Petrucci

SULLA SUPERIORE PROPOSTA VENGONO ESPRESSI

Parere Favorevole
Data 29 GIU. 2023

Il Direttore Amministrativo
Dott. Filippo Coiro

Parere Favorevole
Data 29 GIU. 2023

Il Direttore Sanitario f.f.
Dr. Franco Cortellessa

IL DIRETTORE GENERALE

Dott. Giorgio Giulio Santonocito, nominato con Decreto del Presidente della Regione Lazio n. T00262 del 22 ottobre 2019
Vista la superiore proposta di deliberazione, formulata dal Direttore del Dipartimento Tecnico dott. Mario Petrucci, che, a seguito dell'istruttoria effettuata, nella forma e nella sostanza, ne ha attestato la legittimità e la piena conformità alla normativa che disciplina la fattispecie trattata;
Ritenuto di condividere il contenuto della medesima proposta;

D E L I B E R A

Di approvare la superiore proposta, che qui si intende integralmente riportata e trascritta, per come sopra formulata e sottoscritta dal Direttore del Dipartimento Tecnico dott. Mario Petrucci.
di disporre che il presente atto **venga pubblicato** nell'Albo Pretorio on-line aziendale ai sensi dell'art. 32 comma 1 della Legge n. 69 del 18 giugno 2009;

Il Direttore Amministrativo
Dott. Filippo Coiro

Il Direttore Sanitario f.f.
Dr. Franco Cortellessa

Il Direttore Generale
Dott. Giorgio Giulio Santonocito

PUBBLICAZIONE

Copia della presente deliberazione è stata affissa all'Albo delle Pubblicazioni presso la Sede Legale dell'Azienda Sanitaria Locale Roma 5 in data: 29 GIU. 2023

Il Direttore f.f. U.O.C. Affari Generali e Legali
Avv. Enzo Fasani

_____

L'addetto alla Pubblicazione

_____

Per copia conforme all'originale, per uso amministrativo

Il Direttore f.f. U.O.C. Affari Generali e Legali
Avv. Enzo Fasani

_____

Tivoli, _____

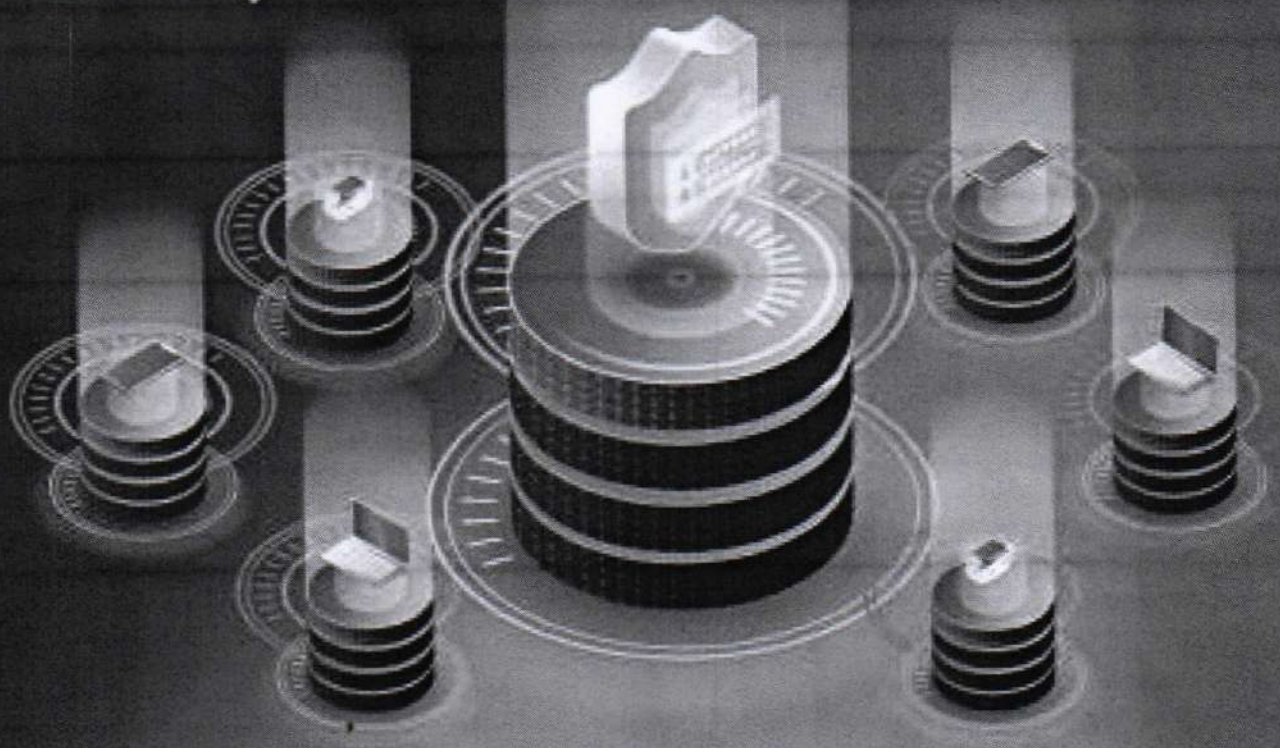
ALL. 1

Accordo quadro avente ad oggetto l'affidamento
di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni

ID 2296 - **LOTTO** 1

Piano Operativo

AQ SICUREZZA



accenture | FASTWEB | FINCANTIERI | D E A S

Rev.	Data	Descrizione delle modifiche	Autore
01	3/05/2023	Prima emissione	RTI

Le informazioni contenute nel presente documento sono di proprietà di Accenture S.p.A., Fastweb S.p.A., Fincantieri NexTech S.p.A., Difesa e Analisi Sistemi S.p.A. e non possono, al pari di tale documento, essere riprodotte, utilizzate o divulgate in tutto o in parte a terzi senza preventiva autorizzazione scritta delle citate aziende.

Sommario

1 INTRODUZIONE 5
1.1 Scopo 5
1.2 Ambito di Applicabilità 5
1.3 Assunzioni 8
2 RIFERIMENTI 9
2.1 Normativa di riferimento 9
2.2 Documenti Applicabili 9
3 DEFINIZIONI E ACRONIMI 10
3.1 Acronimi 10
4 ORGANIZZAZIONE DEL CONTRATTO ESECUTIVO 12
4.1 Attività in carico alle aziende del RTI 13
4.2 Organizzazione e figure di riferimento del Fornitore 14
4.3 Luogo di erogazione e di esecuzione della Fornitura 15
5 AMBITI E SERVIZI 16
5.1 Ambiti di intervento 16
5.2 Servizi 17
5.3 Indicatore di progresso 18
6 SOLUZIONE PROPOSTA 19
6.1 Descrizione dei servizi richiesti 19
6.1.1 L1.S1 - Security Operation Center 19
6.1.2 L1.S2 – Next Generation Firewall 19
6.1.3 L1-S4 - Gestione continua delle vulnerabilità di sicurezza 20
6.1.4 L1.S6 – Protezione Navigazione Internet e Posta Elettronica 20
6.1.5 L1.S11 – Firma digitale remota 21
6.1.6 L1.S12 – Sigillo elettronico 21
6.1.7 L1.S15 – Servizi Specialistici 21
6.1.7.1 L1.S15 Servizi Specialistici ad integrazione servizi di sicurezza per L1.S1 - Security Operation Center 22
6.1.7.2 L1.S15 Servizi Specialistici ad integrazione servizi di sicurezza per L1.S2 - Next Generation Firewall 22
6.1.7.3 L1.S15 Servizi Specialistici ad integrazione servizi di sicurezza per L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza 22
6.1.7.4 L1.S15 Servizi Specialistici ad integrazione servizi di sicurezza per L1.S6– Protezione Navigazione Internet e Posta Elettronica 22
6.2 Utenza interessata / coinvolta 23
6.3 Eventuali riferimenti / vincoli normativi 23
7 PIANO DI PROGETTO 24
7.1 Cronoprogramma 24
7.2 Data di Attivazione e Durata del Servizio 24
7.3 Gruppo di Lavoro 24
7.4 Modalità di esecuzione dei Servizi 25
7.5 Modalità di ricorso al Subappalto da parte del Fornitore 25
8 DIMENSIONAMENTO ECONOMICO 27
8.1 Modalità di erogazione dei Servizi 27
8.2 Indicazioni in ordine alla fatturazione ed ai termini di pagamento 27
9 ALLEGATI 28
9.1 Piano di Lavoro Generale 28
9.2 Piano di Presa in Carico 28
9.3 Piano della Qualità Specifico 28
9.4 Curriculum Vitae dei Referenti 28
9.5 Misure di Sicurezza poste in essere 28

9.6 Documentazione relativa al principio "Do No Significant Harm" (DNSH) 28

Indice delle tabelle

Tabella 1 - Assunzioni 8
Tabella 2 - Documenti Applicabili 9
Tabella 3 - Definizioni 10
Tabella 4 - Acronimi 11
Tabella 5 - Ripartizione attività in carico 14
Tabella 6 - Figure di riferimento e referenti del Fornitore 14
Tabella 7 - Servizi richiesti 18
Tabella 8 - Schema definizione Indicatore di Progresso 18
Tabella 9 – Cronoprogramma 24
Tabella 10 - Descrizione milestone per obiettivo 25
Tabella 11 - Modalità di ricorso al Subappalto da parte del Fornitore 26
Tabella 12 - Quadro economico di riferimento 27

Indice delle figure

Figura 1 – Mappatura Servizi di Sicurezza e Framework NIST 6
Figura 2 - Organizzazione dell'AQ proposta dal RTI 12

1 INTRODUZIONE

L'Azienda Sanitaria Locale Roma 5 (nel seguito anche "Azienda" o "Amministrazione") insiste su un territorio di 70 Comuni nella provincia est di Roma cui fa riferimento una popolazione di circa 502.000 abitanti.
In tale contesto sono presenti 5 Presidi Ospedalieri, di cui una sede di DEA di I livello, e 6 Distretti Sanitari, articolati sul territorio attraverso ulteriori sedi di erogazione dei servizi.
Presso la sede legale dell'Azienda, sita in Via Acquaregna - Tivoli, è presente il data center aziendale, dove sono attestati gli accessi internet e la connessione alla rete regionale messi a disposizione dell'intera rete aziendale tramite apparati di sicurezza perimetrale.

1.1 Scopo

L'Azienda Sanitaria Locale Roma 5 necessita dei servizi riportati nel presente Piano Operativo coerentemente a quanto indicato nel Piano dei Fabbisogni, al fine di assicurare, mediante l'utilizzo di risorse, strumenti e figure professionali in logica di servizio, la protezione e la difesa del sistema informativo dell'Amministrazione.

I servizi di sicurezza di seguito descrittiti, erogati da remoto e in logica continuativa, si pongono come obiettivo sia la protezione delle infrastrutture, delle applicazioni e dei dati che l'ampliamento e la fortificazione del livello generale di sicurezza del sistema informativo dell'Azienda.

Inoltre,, in caso di riscontro di eventi anomali, vulnerabilità critiche e altri eventi di sicurezza degni di nota, l'Azienda necessita di un'analisi approfondita degli eventi occorsi, dell'attuale livello di sicurezza dell'intera infrastruttura monitorata e di allertare di conseguenza i corretti riferimenti aziendali indicati dall'Azienda stessa.

In tal modo, le strutture interne dell'Amministrazione preposte potranno di conseguenza intervenire con azioni correttive su indicazione dello stesso sistema di monitoraggio.

1.2 Ambito di Applicabilità

Il **Piano Triennale per l'informatica della Pubblica Amministrazione** è uno strumento essenziale per promuovere la trasformazione digitale dell'amministrazione italiana e del Paese e, in particolare quella della Pubblica Amministrazione (PA) italiana. Tale trasformazione dovrà avvenire nel contesto del mercato unico europeo di beni e servizi digitali, secondo una strategia che in tutta la UE si propone di migliorare l'accesso online ai beni e servizi per i consumatori e le imprese e creare un contesto favorevole affinché le reti e i servizi digitali possano svilupparsi per massimizzare il potenziale di crescita dell'economia digitale europea. In tale contesto dove quindi i servizi digitali rappresentano un elemento indispensabile per il funzionamento di un Paese, la PA ne è parte fondamentale e indispensabile.

È ampiamente noto che la minaccia cibernetica è sempre più attiva e cresce continuamente in qualità e quantità minacciando infrastrutture critiche, processi digitali e rappresentando anche un elevato rischio di natura militare visto l'utilizzo che è sempre più diffuso verso quello che chiamiamo il perimetro di sicurezza cibernetico. In questo scenario di notevole fermento, il Piano delle Gare Strategiche ICT, concordato tra Consip e AgID, ha l'obiettivo, tra le altre cose, di mettere a disposizione delle Pubbliche Amministrazioni delle specifiche iniziative finalizzate all'acquisizione di prodotti e di servizi nell'ambito della sicurezza informatica, facilitando l'attuazione del Piano Triennale e degli obiettivi del PNRR in ambito, restando in linea con le disposizioni normative relative al settore della cybersicurezza. Il Piano mantiene l'attenzione rispetto al passato ponendosi anche il cruciale problema della protezione del dato. Questo elemento è fondamentale perché tale protezione è strettamente connessa alla sua qualità e agire correttamente consente di attuare anche gli obblighi normativi europei in materia di protezione dei dati personali (GDPR).

Il Piano si focalizza sulla **Cyber Security Awareness**, poiché tale consapevolezza fa scaturire azioni organizzative indispensabili per mitigare il rischio connesso alle potenziali minacce informatiche. Nella PA ci sono frequenti attacchi a portali che bloccano i servizi erogati e costituiscono danno di immagine. È in crescita anche il fenomeno denominato data breach (violazione dei dati) che rappresenta anche una grave violazione del GDPR. Le azioni stabilite nel Piano sono tutte indispensabili rispetto allo scenario possibile. Oltre agli attori coinvolti nel Piano resta indispensabile e cruciale il supporto del Garante per la protezione dei dati

personali quantomeno per verificare se la PA ha nominato un adeguato DPO (figura obbligatoria per il GDPR) ed è organizzata, almeno ai minimi termini, in linea con le regole del GDPR (Regolamento europeo 679/2016). Il Piano affida a Linee guida e regole specifiche ma anche alle strutture specifiche di AgID il supporto alle Pubbliche Amministrazioni.

In particolare, AgID ha concordato l'indirizzo strategico per la progettazione della presente iniziativa con particolare riferimento sui contenuti tecnici e sui meccanismi di coordinamento e controllo dell'utilizzo dello strumento di acquisizione; Consip S.p.A., in qualità di soggetto Stazione Appaltante, ha aggregato i fabbisogni e predisposto la procedura di gara e gestirà la stipula dei contratti per le amministrazioni centrali e locali. Le PA devono intraprendere misure ed azioni per l'avvio di progetti finalizzati alla trasformazione digitale dei propri servizi in base al Modello strategico evolutivo dell'informatica della PA e ai principi definiti nel Piano Triennale.

In capo ai Fornitori è la responsabilità di supportare le Amministrazioni mediante i servizi resi disponibili dalla presente iniziativa e supportare i soggetti deputati al coordinamento e controllo, secondo quanto previsto dalla documentazione di gara.

L'RTI ha basato il modello di tali servizi sul National Institute of Standards and Technology (NIST) Cyber Security Framework (principale standard di sicurezza in ambito cyber, anche il framework nazionale si basa su di esso), arricchito dai principali standard e best practice di settore (ISO 27001, NERC-CIP, MITRE ATT&CK, ISF, SANS, ITIL e COBIT), integrando i requisiti normativi cogenti (es. GDPR/Privacy, NIS) e, come fattore abilitante nel contesto della PA, è allineato al Framework Nazionale per la Cybersecurity e la Data Protection.

In particolare, nella figura sottostante è riportata la mappatura dei servizi offerti al Framework, al fine di illustrare come tali servizi siano funzionali a ciascuna area del Framework.

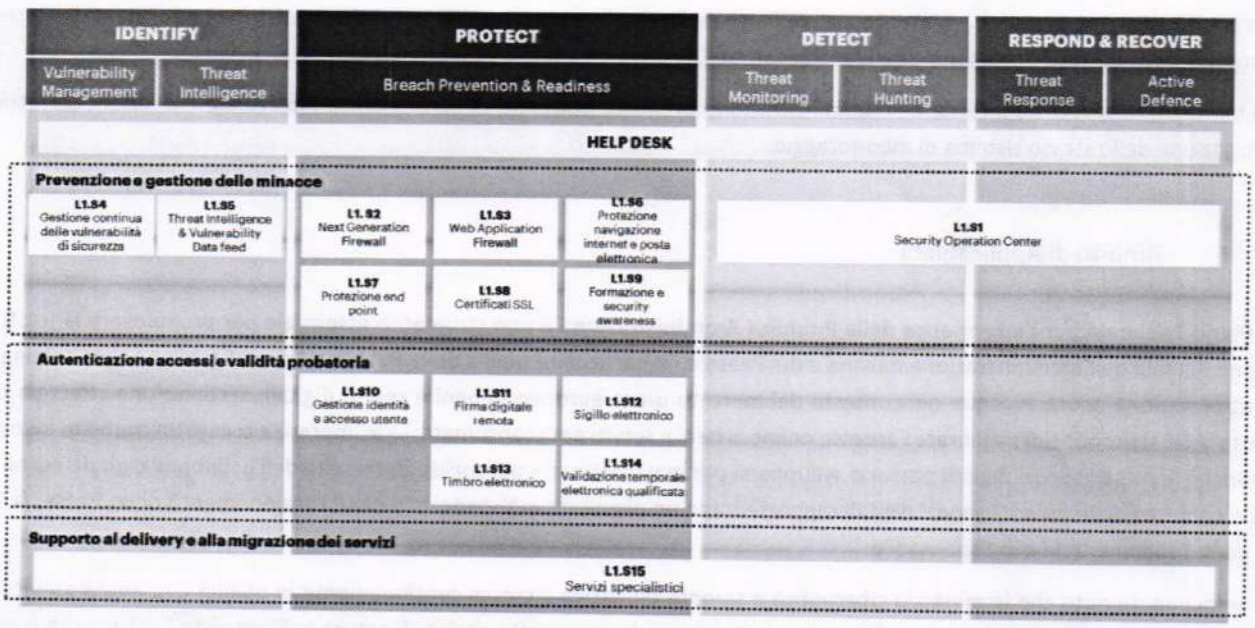


Figura 1 – Mappatura Servizi di Sicurezza e Framework NIST

In linea con le previsioni del Piano Triennale e al fine di indirizzare e governare la trasformazione digitale della PA italiana, sono previste la definizione e l'implementazione di misure di governance centralizzata, anche mediante la costituzione di **Organismi di coordinamento e controllo**, finalizzati alla direzione strategica e alla direzione tecnica della stessa. In particolare, le attività di direzione strategica prevedono il coinvolgimento di soggetti istituzionali, mentre nell'ambito delle attività di direzione tecnica saranno coinvolti anche soggetti non istituzionali, individuati nei Fornitori Aggiudicatari della presente acquisizione. Si precisa che per "Organismi di coordinamento e controllo", si intendono i soggetti facenti capo alla Presidenza del Consiglio e/o al Ministero per l'Innovazione tecnologica e la Digitalizzazione (es: Agid, Team Digitale), che, in base alle funzioni attribuite ex lege, sono ad oggi deputati, per quanto di rispettiva competenza, al monitoraggio e al controllo delle iniziative rientranti nel Piano Triennale per l'informatica nella Pubblica Amministrazione. Nell'ambito di tali Organismi è ricompresa altresì Consip S.p.A., per i compiti di propria competenza. Rimangono salve eventuali modifiche organizzative che interverranno a livello istituzionale nel corso della durata del presente Accordo Quadro.

Gli Organismi di coordinamento e controllo saranno normati da appositi Regolamenti che, resi disponibili alla stipula dei contratti relativi alla presente iniziativa o appena possibile, definiranno gli aspetti operativi delle attività di coordinamento e controllo, sia tecnico che strategico.

I meccanismi di governance sopra introdotti e applicati anche a tutte le iniziative afferenti al Piano Triennale riguarderanno:

- i processi di procurement, veicolati attraverso gli strumenti di acquisizione messi a disposizione da Consip;
- l'inquadramento o categorizzazione degli interventi delle Amministrazioni, realizzati mediante la sottoscrizione di uno o più contratti esecutivi afferenti alle iniziative del Piano Strategico, nel framework del Piano Triennale;
- l'individuazione, da parte delle Amministrazioni beneficiarie, secondo quanto fornito in documentazione di gara, degli indicatori di digitalizzazione coi quali gli Organismi di coordinamento e controllo analizzeranno e valuteranno gli interventi realizzati dalle Amministrazioni con i contratti afferenti alle Gare strategiche;
- la valutazione e l'attuazione della revisione dei servizi previsti dagli Accordi Quadro e/o dei relativi prezzi, per le Gare Strategiche che lo prevedono in documentazione di gara e in funzione dell'evoluzione tecnologica del mercato e/o della normativa applicabile;
- l'analisi e la verifica di coerenza, rispetto al perimetro di ogni Gara Strategica, degli interventi delle Amministrazioni realizzati mediante contratti attuativi afferenti alle Gare Strategiche;
- le modalità e le tempistiche con cui i fornitori dovranno consegnare i dati relativi ai contratti esecutivi, con particolare riferimento alla fase di chiusura degli Accordi Quadro.

L'iniziativa in oggetto si affianca alle gare strategiche previste da AgID ai fini dell'attuazione del Piano Triennale per l'informatica nella Pubblica Amministrazione nelle versioni 2018-2020 e successive, nell'attuazione del processo di trasformazione digitale del Paese. Storicamente, il Sistema Pubblico di Connettività (SPC) ha seguito la rete unitaria della pubblica amministrazione (RUPA), nata con l'intento di connettere le pubbliche amministrazioni, almeno quelle centrali. Il Sistema Pubblico di Connettività (SPC), è posto alla base delle infrastrutture materiali dell'architettura disegnata nel Piano Triennale l'informatica nella Pubblica Amministrazione 2017-2019 di AgID, il cosiddetto Modello Strategico. È un sistema composto da molti servizi stratificati, dalla connettività ai servizi Cloud, ed è stato aggiornato nel 2016 con nuove gare Consip SPC2, SPC Cloud ampliando il portafoglio dei servizi e delle infrastrutture.

L'iniziativa Sicurezza da remoto si pone un **duplice obiettivo**:

- quello di garantire la continuità e l'evoluzione dei servizi già previsti nella precedente iniziativa SPC Cloud – Lotto 2 avente ad oggetto servizi di sicurezza volti alla protezione dei sistemi informativi in favore delle Pubbliche Amministrazioni, nell'ambito del Sistema pubblico di connettività;
- quello di rendere disponibili alle Amministrazioni servizi con carattere di innovazione tecnologica per l'attuazione del Codice dell'Amministrazione Digitale, nonché del Piano Triennale ICT della PA.

Lo scenario è contestualmente caratterizzato dalla presenza di due Lotti dedicati ai servizi di Sicurezza da remoto e servizi di Compliance e controllo. Tale specializzazione si innesta in considerazione dei diversi obiettivi a cui i due Lotti rispondono.
In particolare:

- il **Lotto di servizi di Sicurezza da remoto (Lotto 1)** ha l'obiettivo di mettere a disposizione delle Amministrazioni un insieme di servizi di sicurezza - erogati da remoto e in logica continuativa - per la protezione delle infrastrutture, delle applicazioni e dei dati;
- il **Lotto di servizi di Compliance e controllo (Lotto 2)** ha l'obiettivo di mettere a disposizione delle Amministrazioni servizi - erogati "on-site" in logica di progetto – finalizzati alla elaborazione di un "progetto di sicurezza" che identifica lo stato di salute della sicurezza del sistema informativo dell'Amministrazione e nel controllo imparziale sulla corretta esecuzione dei servizi di sicurezza del Lotto 1 nonché sulla efficacia delle misure di sicurezza attuate, a partire dalla fase di acquisizione degli stessi sino alla loro esecuzione a regime.

In riferimento a quanto sopra riportato, l'**Azienda Sanitaria Locale Roma 5**, intende avvalersi dei **servizi di Sicurezza da Remoto** previsti per il **Lotto 1**, secondo i termini e le condizioni dell'**Accordo Quadro per l'Affidamento di Servizi da Remoto, di Compliance e Controllo per le Pubbliche Amministrazioni – Lotto 1 ID2296 –** (Accordo Quadro o AQ), senza riaprire il confronto competitivo tra gli operatori economici parti dell'Accordo Quadro ("AQ a condizioni tutte fissate").

Nell'ambito di tale lotto, si riportano di seguito i **servizi fruibili**, così come previsto dall'Accordo Quadro:

- L1.S1 - Security Operation Center (SOC)
- L1.S2 - Next Generation Firewall
- L1.S3 - Web Application Firewall
- L1.S4 - Gestione continua delle vulnerabilità di sicurezza
- L1.S5 - Threat Intelligence & Vulnerability Data Feed
- L1.S6 - Protezione navigazione Internet e Posta elettronica
- L1.S7 - Protezione degli endpoint
- L1.S8 - Certificati SSL
- L1.S9 - Servizio di Formazione e Security awareness
- L1.S10 - Gestione dell'identità e l'accesso utente
- L1.S11 - Firma digitale remota
- L1.S12 - Sigillo elettronico
- L1.S13 - Timbro elettronico
- L1.S14 - Validazione temporale elettronica qualificata
- L1.S15 - Servizi specialistici

A tal fine, **Azienda Sanitaria Locale Roma 5**, ha individuato il Raggruppamento Temporaneo di Imprese (RTI) composto da Accenture S.p.A. (Accenture, impresa mandataria), Fastweb S.p.A. (Fastweb), Fincantieri NexTech S.p.A. (Fincantieri), e Difesa e Analisi Sistemi S.p.A. (DEAS) , quale aggiudicatario dell'Accordo Quadro che effettuerà la prestazione, sulla base di decisione motivata in relazione alle specifiche esigenze dell'amministrazione e in relazione a quanto stipulato nell'Accordo Quadro di riferimento.

1.3 Assunzioni

ID	AMBITO	ASSUNZIONE
1	Adeguamenti Normativi	A fronte di eventuali novità di carattere normativo che riguardano i processi e i sistemi oggetto della presente fornitura, dovranno essere valutati e condivisi tra **Azienda Sanitaria Locale Roma 5** e fornitore gli eventuali interventi progettuali da attivare/modificare nonché gli impatti in termini di Piano di Lavoro Generale

hTabella 1 - Assunzioni

2 RIFERIMENTI

2.1 Normativa di riferimento

Trovano applicazione le normative e gli standard internazionali riportate al "Capitolato Tecnico Generale" (§ 4.6) [DA-1].

2.2 Documenti Applicabili

Rif.	Titolo
DA-1.	ALLEGATO 1 - CAPITOLATO TECNICO GENERALE - Gara a procedura aperta per la conclusione di un accordo quadro, ai sensi del d.lgs. 50/2016 e s.m.i., suddivisa in 2 lotti e avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni.
DA-2.	ALLEGATO 2A - CAPITOLATO TECNICO SPECIALE SERVIZI DI SICUREZZA DA REMOTO
DA-3.	Accordo Quadro
DA-4.	Offerta Tecnica – Lotto 1 GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI
DA-5.	Appendice 1 al CTS Lotto 1_Indicatori di qualità - ID 2296 - Gara Sicurezza da remoto
DA-6.	Piano dei Fabbisogni - PEC del 7/04/2023

Tabella 2 - Documenti Applicabili

3 DEFINIZIONI E ACRONIMI

3.1 Acronimi

Definizione	Descrizione
Accordo Quadro (AQ)	L'Accordo Quadro stipulato tra il/i Fornitore/i aggiudicatario/i e Consip S.p.A. all'esito della procedura di gara di prima fase
Aggiudicatario / Fornitore	Se non diversamente indicato vanno intesi gli aggiudicatari previsti per ciascun AQ per ciascuno dei Lotti della fornitura
Amministrazioni	Pubbliche Amministrazioni
Amministrazione Aggiudicatrice	Consip S.p.A.
Amministrazione/i Contraente/i	Pubbliche Amministrazioni che hanno siglato o intendono affidare un contratto esecutivo con il Fornitore per l'erogazione di uno dei servizi oggetto dell'Accordo Quadro
Capitolato Tecnico Generale	Documento che definisce il funzionamento e i requisiti comuni ai lotti oggetto della presente iniziativa
Capitolati Tecnici Speciali	Integrano il Capitolato Tecnico Generale e definiscono i contenuti di dettaglio e i requisiti minimi in termini di quantità, qualità e livelli di servizio, relativamente al Lotto 1 avente ad oggetto i Servizi di Sicurezza da remoto e al Lotto 2 avente ad oggetto i Servizi di Compliance e controllo
Collaudo e verifica di Conformità	Effettuati dall'Amministrazione e corrispondenti alla valutazione con verifica di merito dei prodotti consegnati
Componente	Il singolo elemento della configurazione di un sistema sottoposto a monitoraggio
Contratto Esecutivo	Il Contratto avente ad oggetto Servizi di Sicurezza da remoto, di Compliance e di Controllo per le Pubbliche Amministrazioni (Lotto 1)
Piano dei Fabbisogni	Il documento inviato dall'Amministrazione al Fornitore, al quale l'Amministrazione medesima affida il singolo Contratto Esecutivo e nel quale dovranno essere riportate, tra l'altro, le specifiche esigenze dell'Amministrazione che hanno portato alla scelta del fornitore
Piano Operativo	Il documento, inviato dal Fornitore all'Amministrazione, contenente la traduzione operativa dei fabbisogni espressi dall'Amministrazione con le modalità indicate nel presente documento
Prodotto della Fornitura	Tutto ciò che viene realizzato dal fornitore. Comprende tutta la documentazione contrattuale e gli artefatti come definiti nell'appendice Livelli di servizio
Modalità di erogazione da remoto	Servizio erogato - in modalità *managed* - attraverso i Centri Servizi del Fornitore
Modalità di lavoro *On-site*	Servizio erogato presso le strutture dell'Amministrazione contraente o altre strutture indicate dalla stessa o in alternativa presso la sede del Fornitore
Milestone	In ingegneria del software e Project Management indica ciascun traguardo intermedio e il traguardo finale dello svolgimento del progetto. Sono i punti di controllo all'interno di ciascuna fase oppure di consegna di specifici deliverable o raggruppamenti di deliverable. Sono normalmente attività considerate convenzionalmente a durata zero che servono per isolare nella schedulazione i principali momenti di verifica e validazione. Di fatto ciascun punto di controllo serve per approvare quanto fatto a monte della milestone ed abilitare le attività previste a valle della milestone
Sistema	Per Sistema si intende la singola immagine del sistema operativo, comprensiva di tutte le periferiche fisiche e/o logiche e di tutti i prodotti e/o servizi necessari al corretto funzionamento delle applicazioni, oppure l'insieme delle componenti HW e SW inserite in un unico chassis atto alla interconnessione e l'estensione di reti TLC (ad esempio apparati che gestiscono i primi quattro livelli della pila ISO-OSI)
Centro Servizi (CS)	La/e sede/i da cui l'Aggiudicatario eroga i servizi in modalità "da remoto" di cui al presente Capitolato per lo specifico Lotto di fornitura
Perimetro di Sicurezza Nazionale Cibernetica	Ai sensi del DL. Del 21 settembre 2002 n.105, il Perimetro è composto dai sistemi informativi e dai servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali

Tabella 3 - Definizioni

Vocabolo	Titolo
AgID	Agenzia per l'Italia Digitale
AQ	Accordo Quadro
BC	Business Continuity
CE	Contratto Esecutivo
CS	Centro Servizi
CTS	Capitolato Tecnico Speciale
DA	Documenti Applicabili
DDoS	Distributed Denial-of-Service
DR	Disaster Recovery
HVAC	Heating, Ventilation and Air Conditioning
HW	Hardware
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
LRP	Livello di Rischio Previsto
LRR	Livello di Rischio Residuo
MGMT	Management
MPLS	MultiProtocol Label Switching
NDA	Non-Disclosure Agreement
OLO	Other Licensed Operators
PA	Pubblica Amministrazione
PEC	Posta Elettronica Certificata
PMO	Project Management Office
RPO	Recovery Point Objective
RTI	Raggruppamento Temporaneo di Impresa
RTO	Recovery Time Objective
SAN	Storage Area Network
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni
SIEM	Security Information and Event Management
SOC	Security Operation Center
SPC	Sistema Pubblico di Connettività
SSL	Secure Sockets Layer
SW	Software
UPS	Uninterruptible Power Supply
UTP	Unified Threat Protection
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network

Tabella 4 - Acronimi

4 ORGANIZZAZIONE DEL CONTRATTO ESECUTIVO

L'approccio organizzativo che il RTI propone è volto a garantire:

- la gestione dell'Accordo Quadro (AQ) nel suo complesso, con ruoli di organizzazione, indirizzo e controllo dei diversi Contratti Esecutivi (CE) attivati (Governo dell'AQ);
- il coordinamento dei singoli CE e l'erogazione dei servizi richiesti per ciascuno di essi (Gestione dei CE);
- la capacità di adattarsi dinamicamente alle necessità della singola PA in base, ad esempio, alla maturità della stessa in ambito Cybersecurity, alle dimensioni, al contesto tecnologico, alla tipologia di dati trattati, alla distribuzione geografica e all'appartenenza del Perimetro di Sicurezza Cibernetico Nazionale.

L'organizzazione del RTI proposta per la conduzione dell'Accordo Quadro è mostrata nella figura di seguito riportata:

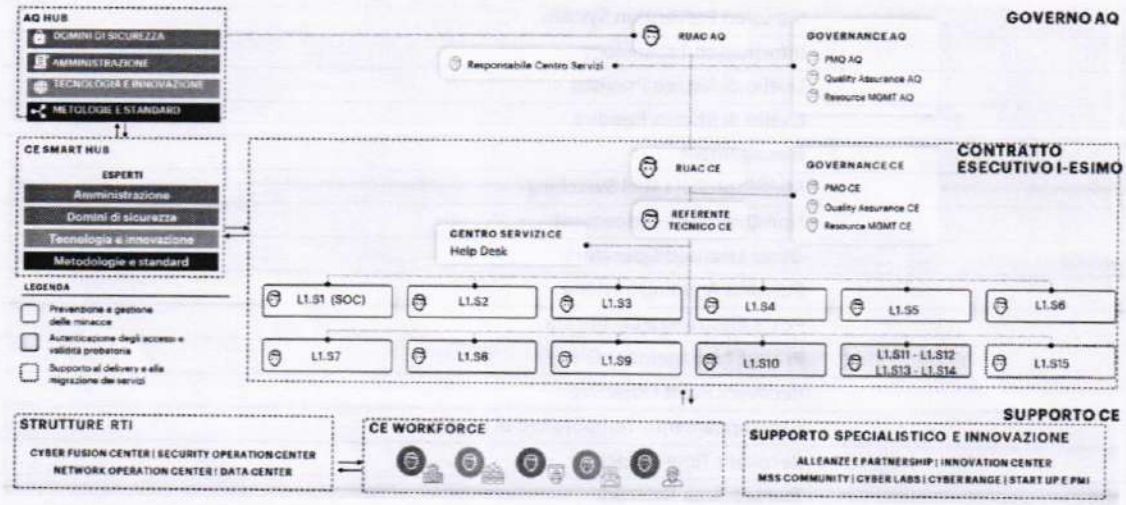


Figura 2 - Organizzazione dell'AQ proposta dal RTI

L'organigramma proposto prevede che il coordinamento delle attività del presente Accordo Quadro venga svolto dal Responsabile Unico della Attività Contrattuali dell'Accordo Quadro.

Il modello proposto si articola sui tre livelli di seguito illustrati:

- **Livello di Governo dell'AQ** - rappresenta il livello organizzativo più elevato per la gestione e il coordinamento dell'intera Fornitura. È presieduto dal Responsabile Unico delle Attività Contrattuali dell'AQ (RUAC AQ), che svolge un'azione di indirizzo e controllo strategico in ottica di gestione unitaria dei CE. Il RUAC AQ è designato dalla mandataria, presiede il Comitato di Coordinamento del RTI composto da figure manageriali delle aziende in esso contenute e dal Responsabile del Centro Servizi, che insieme definiscono la strategia di AQ e assicurano una visione unica e integrata dell'andamento dei servizi oggetto di gara, garantendo al tempo stesso la qualità complessiva dei CE per conseguire la piena soddisfazione delle PA.
  Il RUAC AQ è il principale riferimento del RTI per Consip, rappresenta inoltre il RTI all'interno dell'Organismo Tecnico di Coordinamento e Controllo ed è quindi la principale interfaccia verso i soggetti istituzionali su tutte le tematiche contrattuali. È supportato dal team di Governance AQ che include strutture/ruoli aggiuntivi (offerti senza oneri aggiuntivi) quali: Project Management Office, Quality Assurance e Resource Management.
- **Livello dei Contratti Esecutivi** - è progettato per adattarsi alle diverse tipologie di PA che aderiranno, garantendo la qualità e fornendo la maggiore flessibilità possibile per l'erogazione dei servizi. A tale livello sono coordinati ed erogati i servizi previsti per ogni CE ed è prevista la presenza di:
  - ❖ un Responsabile unico delle attività contrattuali del CE (RUAC CE);
  - ❖ un Referente Tecnico CE;
  - ❖ un team di Governance CE;
  - ❖ un Help Desk dedicato all'assistenza dei Referenti identificati dall'Amministrazione,

- ❖ team responsabili dell'erogazione dei servizi previsti.

Il RUAC CE ha una responsabilità speculare a quella del RUAC AQ e rappresenta la principale interfaccia verso le singole PA per tutte le tematiche contrattuali, avendo allo stesso tempo compiti di raccordo tra i due livelli.
Il Referente Tecnico CE è responsabile del corretto svolgimento delle attività e dei servizi e il relativo livello di qualità di erogazione per il singolo CE ed è supportato dal team di Governance CE (PMO CE, Quality Assurance CE e Resource Management CE).
I Team responsabili dell'erogazione dei servizi, composti da professionisti di settore, hanno l'ulteriore supporto dei maggiori esperti di tematica del RTI (Subject Matter Expert) per assicurare omogeneità di metodologie e innovazione continua in base all'evoluzione del contesto.

- **Livello Supporto CE** - garantisce due tipi di supporto:
  - ❖ *Scalabilità* - La CE Workforce comprende le strutture di appartenenza delle risorse assegnate ai CE, quali Cyber Fusion Center/Security Operation Center/Network Operation Center/Data Center, la cui dimensione garantisce flessibilità e scalabilità adeguata alle esigenze (es. aumento della domanda, complessità progettuale, contesto tecnologico, sensibilità dei dati);
  - ❖ *Supporto specialistico e innovazione* - Garantito da:
    - ✓ i CdC tecnologici (es. infrastruttura, rete, applicazioni, DB, S.O., sistemi di virtualizzazione e HW);
    - ✓ i Cyber Labs di Accenture, operanti a livello globale per introdurre nuove tecnologie di sicurezza tramite prove di laboratorio che ne facilitano l'integrazione sui sistemi cliente, e i centri di ricerca e sviluppo in ambito cyber di Fastweb (FDA-Fastweb Digital Academy), Fincantieri e DEAS;
    - ✓ il network di start-up e PMI innovative;
    - ✓ le partnership con i principali vendor in materia sicurezza;
    - ✓ le MSS COMMUNITY, specializzate per ambito (es. Application Security, Digital Identity, Threat Operations, Cloud Security, Continuous Risk Management), tecnologia delle soluzioni offerte e/o presenti presso le PA richiedenti, tematica (es. ambiti Difesa, Sanità);
    - ✓ i Cyber Range (Poligoni Cibernetici) di Accenture e DEAS;
    - ✓ i laboratori di test plant di Fastweb utilizzati per testare gli apparati di sicurezza, così come nella verifica della conformità dei prodotti effettuata dai CVCN (Centro di Valutazione e Certificazione Nazionale) e CV. In particolare, per la capacità del RTI di supportare Consip, le PA e gli organismi istituzionali (es. AgID, Agenzia per la Cyber Sicurezza Nazionale) in materia di Innovazione.
- **AQ HUB e CE SMART HUB** - Strutture aggiuntive composte da esperti di diversi ambiti, con il compito di stimolare e promuovere, rispettivamente a livello di AQ e di CE, l'innovazione e le competenze tecnologiche nell'erogazione dei servizi, rafforzare il livello di conoscenze nei vari domini di sicurezza e di awareness verso le PA anche rispetto alle opportunità offerte dal contratto, garantire la conformità a standard e best practice di settore.

Per quanto concerne invece i **Centri Servizi**, questi vengono coordinati da uno specifico Responsabile che opera a livello "Governo AQ" e in accordo ai seguenti criteri:

- struttura organizzativa unica che assume la responsabilità dell'erogazione del servizio per tutte le sedi operative;
- assegnazione di responsabilità specifiche centralizzate, a livello di CS e a diretto riporto del responsabile del CS, in merito alla gestione della sicurezza informatica e della continuità operativa;
- assegnazione di responsabilità specifiche distribuite, a livello di sede operativa, in merito alla sicurezza fisica e alla gestione ambientale ed energetica.

4.1 Attività in carico alle aziende del RTI

Nell'ambito della specifica fornitura le attività saranno svolte dalle aziende secondo la ripartizione seguente:

SERVIZIO	ACCENTURE	FASTWEB	FINCANTIERI	DEAS
L1.S1 – Security Operation Center		X		

SERVIZIO	ACCENTURE	FASTWEB	FINCANTIERI	DEAS
L1.S2 – Next Generation Firewall		X		
L1.S3 – Web Application Firewall				
L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza	X			
L1.S5 – Threat Intelligence & Vulnerability Data Feed				
L1.S6 – Protezione Navigazione Internet e Posta Elettronica		X		
L1.S7 – Protezione degli endpoint				
L1.S8 – Certificati SSL				
L1.S9 – Formazione e Security Awareness				
L1.S10 – Gestione dell'Identità e dell'accesso dell'utente				
L1.S11 – Firma digitale remota		X		
L1.S12 – Sigillo Elettronico		X		
L1.S13 – Timbro Elettronico				
L1.S14 – Validazione temporale elettronica qualificata				
L1.S15 – Servizi Specialistici	X	X	X	X
TOTALE (%)	3,601%	96,189%	0,105%	0,105%
TOTALE (€)	50.400,00 €	1.346.097,48 €	1.464,00 €	1.464,00 €

Tabella 5 - Ripartizione attività in carico

4.2 Organizzazione e figure di riferimento del Fornitore

Nella tabella che segue sono riportate le principali figure di riferimento del Fornitore, cui ruoli e responsabilità sono stati illustrati nella parte introduttiva del Capitolo:

FIGURE DI RIFERIMENTO E REFERENTI DEL FORNITORE
RUAC AQ
GOVERNANCE AQ (PROJECT MANAGEMENT OFFICE, QUALITY ASSURANCE, RESOURCE MANAGEMENT)
RESPONSABILE CENTRO SERVIZI
RESPONSABILE DI SICUREZZA INFORMATICA E CONTINUITÀ OPERATIVA
RESPONSABILE DI SEDE OPERATIVA
RUAC CE
GOVERNANCE CE (PROJECT MANAGEMENT OFFICE, QUALITY ASSURANCE, RESOURCE MANAGEMENT)
REFERENTE TECNICO CE
RESPONSABILI DELL'EROGAZIONE DEI SERVIZI

Tabella 6 - Figure di riferimento e referenti del Fornitore

4.3 Luogo di erogazione e di esecuzione della Fornitura

In base alla modalità di esecuzione dei servizi le prestazioni contrattuali dovranno essere svolte come di seguito indicato:

- per i servizi erogati da remoto, attraverso i Centri Servizi del Fornitore;
- per i servizi on-site, - ove necessario ed opportuno in relazione all'attività, presso le sedi principali di interesse dell'Amministrazione.

5 AMBITI E SERVIZI

5.1 Ambiti di intervento

Di seguito vengono descritti gli ambiti di intervento per i servizi richiesti nel Piano dei Fabbisogni:

L1.S1 – Security Operation Center: attraverso adeguati strumenti tecnologici di back-end, il servizio di monitoraggio e alerting degli eventi/minacce di sicurezza questo servizio consente una gestione degli incidenti di sicurezza dalla fase di identificazione e notifica dell'evento, fino alle azioni di contenimento, ripristino e prevenzione futura possibile anche grazie ad in stretta collaborazione tra il RTIr e le strutture dell'Amministrazione preposte alla gestione sistemistica. Tra le funzioni proposte ci sono: raccolta centralizzata dei log e degli eventi; correlazione tra eventi diversi raccolti; disponibilità di un cruscotto (dashboard) che fornisca agli analisti, in tempo reale, una rappresentazione della situazione in essere; capacità di identificazione, gestione, mitigazione e risoluzione degli attacchi; produzione di report periodici di sintesi, di incident report di dettaglio ed istruzioni operative. E' prevista , infine, analisi della reportistica e dei log tale da dare la giusta priorità ai processi di risoluzione e/o mitigazione delle minacce. In linea con quanto indicato nel Piano dei Fabbisogni, il piano di lavoro prevede una durata complessiva del servizio di 48 mesi con volumi di riferimento pari a 220 device equivalent /annui equivalenti a 2200 EPS/annui in Fascia 4.

L1.S2 - Next Generation Firewall: il servizio permette di filtrare tutto il traffico che i dispositivi di rete selezionati scambiano internamente 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. In linea con quanto indicato nel Piano dei Fabbisogni, il piano di lavoro prevede una durata complessiva del servizio di 48 mesi con volumi di riferimento pari a 3 device /annui in Fascia 3.

L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza: tale servizio consente, 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 sistemi informatici. Il servizio si avvarrà dell'utilizzo di uno o più scanner che produrrà un report con le specifiche indicazioni di rischio relative alle vulnerabilità rilevate. Il servizio prevede: la scansione dell'infrastruttura dell'Amministrazione; l'individuazione dei livelli di gravità e classificazione CVSS; la possibilità di disporre di un report; attività a supporto per la risoluzione o mitigazione di quanto rilevato. Nell'ambito delle attività sopra riportate, ed in particolare per la verifica delle vulnerabilità attive eseguita in ambiente di produzione, l'Amministrazione approverà formalmente l'esecuzione di questi test e verifiche di sicurezza, manlevando il Fornitore nel caso in cui detta esecuzione provochi degli impatti e/o danni.
Resta inteso che il Fornitore e l'Amministrazione condivideranno, tramite comunicazione formale, il perimetro che sarà interessato dall'attività di analisi e di test, la tipologia e la descrizione dei controlli da effettuare e la valutazione dell'impatto potenziale.
In ogni caso, prima di eseguire test che richiedano l'accesso ai sistemi, l'Amministrazione dovrà fornire specifica autorizzazione in tal senso; pertanto, qualora detta autorizzazione non fosse fornita, il Fornitore non potrà procedere.

In linea con quanto indicato nel Piano dei Fabbisogni, il piano di lavoro prevede una durata complessiva del servizio di 48 mesi con volumi di riferimento pari a 250 asset/annui in Fascia 3.

L1.S6 – Protezione Navigazione Internet e Posta Elettronica: il servizio di protezione della Navigazione in internet consente di bloccare l'accesso a siti potenzialmente dannosi, filtrare il codice dannoso e controllare le applicazioni Web rilevando e preservando affidabilità, disponibilità, riservatezza e integrità della comunicazione tra le componenti client e server.
Benché non esplicitato dal PDF il RTI propone il servizio L1S6 completo, come previsto dall'Accordo Quadro, e quindi inclusivo del servizio di protezione di posta elettronica. Tale servizio a
contempla il tracciamento delle relazioni mittenti-destinatari e il monitoraggio transazioni/interazioni per misurare le reti di fiducia e migliorare il rilevamento delle minacce, unitamente alla protezione delle email in uscita (funzionalità aggiuntive: attachment e URL analysis, recipient verification, impostor detection e account compromission detection).

In linea con quanto indicato nel Piano dei Fabbisogni, il piano di lavoro prevede una durata complessiva del servizio di 48 mesi con volumi di riferimento pari a 4000 utenti/annui in Fascia 2.

L1.S11 – Firma digitale remota: il servizio attraverso strumenti di autenticazione (tipicamente user id+ password +OTP o telefono cellulare) consente la generazione della firma su un dispositivo (HSM) custodito dal prestatore del servizio fiduciario qualificato.
In linea con quanto indicato nel Piano dei Fabbisogni, il piano di lavoro prevede una durata complessiva del servizio di 48 mesi con volumi di riferimento pari a 200 utenti/annui in Fascia 1.

L1.S12 – Sigillo elettronico: il servizio consente all'Amministrazione di dare efficacia probatoria ai documenti informatici firmati digitalmente.
In linea con quanto indicato nel Piano dei Fabbisogni, il piano di lavoro prevede una durata complessiva del servizio di 48 mesi con volumi di riferimento pari a 1 sigillo/secondo in Fascia 1.

L1.S15 – Servizi Specialistici: il RTI sulla base della richiesta inserita nel Piano dei Fabbisogni come servizi L1.S15, propone un supporto specialistico integrativo per molti degli altri servizi di cui al presente Piano Operativo e quindi per la stessa durata pari a 48 mesi, con una stima complessiva di gg/p team ottimale pari a 2391 per Anno 1 e 611/anni per gli anni successivi calcolata dal RTI tenendo conto dell'iniziale periodo di set up e sulla base del dimensionamento degli altri servizi cosi come proposto dalla Amministrazione stessa.

5.2 Servizi

In tabella sono riportati i servizi offerti e le relative quantità. In relazione al dimensionamento si specifica quanto segue:
- Per i servizi **L1.S1, L1.S2, L1.S4, L1.S6, L1.S11, L1S12** il dimensionamento riportato è equivalente a quanto indicato nel PDF;
- Per i servizi **L1.S15** il dimensionamento, non essendo esplicitato nel PDF; è proposto dal RTI sulla base delle necessità espresse dall'Amministrazione nel Piano dei Fabbisogni stesso nel paragrafo SINTESI DEI SERVIZI RICHIESTI punto 7, e tenendo conto delle necessità di set up iniziale e del dimensionamento degli altri servizi previsti nel presente Piano Operativo.

SERVIZIO	FASCIA	IMPORTO / QUANTITA' I ANNO	IMPORTO / QUANTITA' II ANNO	IMPORTO / QUANTITA' III ANNO	IMPORTO / QUANTITA' V ANNO
L1.S1 – Security Operation Center	Fascia 4 - Fino a 6.000 Eps	48.048,00 € / 220 (device equivalent)	48.048,00 € / 220 (device equivalent)	48.048,00 € / 220 (device equivalent)	48.048,00 € / 220(device equivalent)
L1.S2 – Next Generation Firewall	Fascia 3 - Fino a 4 Gbps	19.427,52 € / 3 (device)	19.427,52 € / 3 (device)	19.427,52 € / 3 (device)	19.427,52 € / 3 (device)
L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza	Fascia 3 - > 200 IP	3.450,00 € / 250 (IP)	3.450,00 € / 250 (IP)	3.450,00 € / 250 (IP)	3.450,00 € / 250 (IP)
L1.S6 – Protezione Navigazione Internet e Posta Elettronica	Fascia 2 - Fino a 5.000 utenti	16.148,00 € / 4000 (utenti)	16.148,00 € / 4000 (utenti)	16.148,00 € / 4000 (utenti)	16.148,00 € / 4000 (utenti)

SERVIZIO	FASCIA	IMPORTO / QUANTITA' I ANNO	IMPORTO / QUANTITA' II ANNO	IMPORTO / QUANTITA' III ANNO	IMPORTO / QUANTITA' V ANNO
L1.S11 - Firma Elettronica	Fascia 1 - 50 e fino a 200 utenti	1.228,60 € / 200 (utenti)	1.228,60 € / 200 (utenti)	1.228,60 € / 200 (utenti)	1.228,60 € / 200 (utenti)
L1.S12 – Sigillo Elettronico	Fascia 1 - Garantita - N. 1 firma	3.890,25 € / 1 (sigillo)	3.890,25 € / 1 (sigillo)	3.890,25 € / 1 (sigillo)	3.890,25 € / 1(sigillo)
L1.S15 – Servizi Specialistici	GG/P Team Ottimale	583.404,00 € / 2391 (gg/p team ottimale)	149.084,00 € / 611 (gg/p team ottimale)	149.084,00 € / 611 (gg/p team ottimale)	149.084,00 € / 611 (gg/p team ottimale)

Tabella 7 - Servizi richiesti

5.3 Indicatore di progresso

Di seguito l'indicatore di progresso identificato in questa fase per l'erogazione della fornitura.

Denominazione	Indicatore di progresso		
Aspetto da valutare	Grado di mappatura di ciascuna classe di controlli ABSC delle misure minime di sicurezza AGID		
Unità di misura	Numero di Controlli	**Fonte dati**	Piano dei Fabbisogni o Piano di lavoro Generale
Periodo di riferimento	Momento di Pianificazione dell'intervento	**Frequenza di misurazione**	Per ogni intervento pianificato
Dati da rilevare	*N1: numero di controlli relativi alla specifica classe ABSC soddisfatti attraverso l'intervento* *NT: numero totale di controlli relativi alla specifica classe previsti dalle misure minime di sicurezza AGID*		
Regole di campionamento	Nessuna		
Formula	$Ip = (N_1 - N_0)/N_T$		
Regole di arrotondamento	Nessuna		
Valore di soglia	*N0: numero di controlli relativi alla specifica classe soddisfatti prima dell'intervento;*		
Applicazione	Amministrazione Contraente		

Tabella 8 - Schema definizione Indicatore di Progresso

Tale indicatore sarà oggetto di revisione con l'Amministrazione a valle della fase di presa in carico. In particolare, sarà attivato uno specifico tavolo di lavoro mirato a:

- valutare il grado di maturità digitale dei servizi offerti e il grado di maturità atteso;
- consolidare l'indicatore;
- definire le misure iniziali dell'indicatore;
- stabilire i target e cioè le misure attese alla fine del contratto.

6 SOLUZIONE PROPOSTA

Si riportano di seguito i servizi proposti in linea con le esigenze espresse dall'Azienda Sanitaria Locale Roma 5.

6.1 Descrizione dei servizi richiesti

6.1.1 L1.S1 - Security Operation Center

Il servizio prevede di implementare, attraverso adeguati strumenti tecnologici, un servizio di monitoraggio e alerting degli eventi/minacce di sicurezza al fine di consentire una gestione degli incidenti di sicurezza dalla fase di identificazione e notifica dell'evento, fino alle raccomandazioni relative alle azioni di contenimento e ripristino e prevenzione futura.

Il servizio SOC si basa sui dati raccolti e correlati dal SIEM (tecnologia IBM QRadar) e sarà gestito anche attraverso un "Security Orchestration, Automation & Response (SOAR)". E' pertanto effettuata una ottimizzazione degli eventi raccolti dai sistemi ed inviati al SIEM, selezionando solo quelli significativi in termini di sicurezza e scartando tutte le righe di log non utili al sistema SIEM ed al servizio SOC, al fine di attuare i servizi previsti nell'offerta tecnica del RTI, tra cui il servizio che prevede la gestione degli incidenti di sicurezza generati, arricchimento automatico di incidenti con informazioni di interesse, correlazione tra incidenti diversi e coordinamento delle azioni di risposta tra team distribuiti.

Il servizio SOC è erogato in modalità remota dal Centro Servizi preposto del RTI e agisce in modalità strettamente coordinata con gli altri servizi oggetto della presente fornitura, beneficiando delle informazioni da essi raccolte, contribuendo in modalità proattiva al miglioramento continuo delle policy e intervenendo con azioni di inibizione/mitigazione a fronte di evidenze di incidenti o potenziali rischi in essere.

6.1.2 L1.S2 – Next Generation Firewall

Il servizio di Next-Generation Firewall (NGFW) che rappresenta uno dei servizi offerto dal Centro servizi, prevede l'implementazione di controlli di sicurezza essenziali alla protezione di rete, applicando restrizioni alle comunicazioni esterne o interne alla Amministrazione, limitando gli accessi delle singole risorse ai soli flussi di traffico definiti come leciti. Ciò viene abilitato utilizzando policy basate non solo sui meccanismi classici di segregazione di rete L3 (network) e L4 (trasporto), ma anche su capacità di analisi del layer applicativo, ispezionando il contenuto dei messaggi scambiati con protocolli quali HTTP, FTP, SIP, ecc. che consentono di implementare filtri molto più dettagliati rispetto alle funzionalità base dei firewall standard. Ulteriori elementi di valore sono rappresentati dalla possibilità di definire regole basate sull'identità dell'utente, abilitando l'infrastruttura ad ammettere flussi di traffico in base al principio least-privilege e di procedere all'ispezione di traffico TLS/SSL necessaria per controllare efficacemente il traffico cifrato che costituisce gran parte del traffico interno ed esterno all'Amministrazione.

Il servizio prevede un livello di interfaccia utile all'interazione con il servizio stesso, un livello di erogazione in cui sono espletate le funzioni principali del servizio, un livello di automazione (intelligent layer) che aggiunge funzioni avanzate, un livello interazioni per le relazioni con gli altri servizi. I livelli comprendono tutte le funzionalità richieste dal capitolato tecnico dell'AQ e ne aggiungono alcune migliorative, descritte di seguito:

- Gestione politiche e configurazioni: funzioni di "Geo-IP filtering e Geo-Blocking" per consentire la creazione di regole di policy da applicare a specifici paesi e/o regioni geografiche;
- Stima degli impatti e misura del rischio: la funzione esegue le stime di impatti e rischio sulle configurazioni implementate o che si prevede di implementare fornendo all'utente e all'operatore una vista chiara delle modifiche necessarie per una configurazione sicura. Tali valutazioni sono effettuate tenendo in considerazione:
  - ✓ la classificazione delle informazioni trattate,
  - ✓ la criticità del servizio abilitato per l'Amministrazione,
  - ✓ le dipendenze e interazioni con altri servizi, funzioni e sistemi;
- Rilevamento avanzato del malware: la funzione prevede metodi avanzati di 'malware detection' fortemente potenziate dall'integrazione con il SOC e prevedono azioni automatizzate per isolare comportamenti di rete anomali che possono segnalare la presenza di malware noto o di possibili varianti.

6.1.3 L1-S4 - Gestione continua delle vulnerabilità di sicurezza

Il servizio proposto utilizza la piattaforma TVMP (Threat and Vulnerability Management Platform), locata nel Centro Servizi, alla quale accede esclusivamente personale altamente qualificato e certificato (SANS, GEVA/GXPN, OSCP, OSCE, CEH, OPST, etc.). Il servizio prevede:

- Rilevazione delle vulnerabilità presenti in sistemi, apparati di rete, applicazioni (web, mobile, client-server, etc.), dispositivi ad uso professionale, con rendicontazione delle tecniche, dirette od articolate (OWASP, MITRE kill-chain, etc.) capaci di sfruttarle; la fase di ricerca delle vulnerabilità agevola peraltro la ricostruzione (ove non presente) di un 'Asset Inventory' (con CCE e CPE) del patrimonio informativo dell'Amministrazione ai fini della successiva misura del livello di esposizione alla minaccia cyber associato ai singoli cespiti IT;
- Categorizzazione, classificazione e misura del potenziale impatto delle vulnerabilità rilevate, sulla base della misura del rischio ponderato con il livello di criticità associato all'asset e derivante dalla rilevanza dei processi dell'Amministrazione che l'asset abilita, dalla sensibilità dei dati trattati e delle interdipendenze (con altre funzioni e/o sistemi), unitamente alle indicazioni sulle modalità tecniche, organizzative e procedurali di risoluzione (o mitigazione) delle problematiche riscontrate;
- Supporto per la oianificazione, su base priorità (stante la misura del rischio residuo corrente), delle azioni di risoluzione o mitigazione delle problematiche di sicurezza individuate e delle fasi di controllo orientate al rientro dalle non conformità e al miglioramento continuo;
- Supporto tecnico-organizzativo e tecnico-funzionale;
- Reportistica relativa alle scansioni con un alto grado di personalizzazione di elementi quali la superficie d'attacco esposta, livelli di rischio residuo, vulnerabilità associate agli asset (pregresse ed attuali) e stato d'avanzamento dei piani di rientro.

L'architettura della piattaforma TVMP che abilita il servizio è composta dalle seguenti componenti principali:

- Sonda fisica o virtuale, da installare da parte dell'Amministrazione nella propria infrastruttura qualora necessaria per raggiungere gli asset target, per l'esecuzione delle scansioni verso gli apparati di rete, gli host, i server, le applicazioni web, i database e tutti i dispositivi dotati di un indirizzo IP presenti nelle reti in perimetro; se necessario il RTI connetterà la sonda alla rete dell'Amministrazione e quest'ultimo abiliterà la comunicazione verso tutte le porte TCP e UDP dei i sistemi informativi presenti nelle reti in perimetro per eseguire le scansioni.
- Una console di gestione, installata presso il Centro Servizi, da cui è possibile pianificare le analisi infrastrutturali e applicative, visualizzare i risultati e gestire la reportistica per mantenere una visione complessiva dello stato di esposizione del contraente; la console di gestione comunica con le sonde tramite una connessione VPN.
- Una console per il dashboarding avanzato e l'automazione, installata presso il Centro Servizi, per la configurazione e la gestione remota delle sonde; la console di gestione comunica con le sonde tramite una connessione VPN.
- Un modulo di supporto con acceleratori e strumenti di diagnostica per l'esecuzione delle scansioni manuali, le analisi delle evidenze e la rappresentazione dei risultati.
- Un modulo di monitoraggio del rischio calcolato sui processi.
- Una knowledge base contestualizzata e aperta all'information sharing.

6.1.4 L1.S6 – Protezione Navigazione Internet e Posta Elettronica

Il servizio si compone delle seguenti funzionalità:

- Analisi del traffico per bloccare malware, botnet, spyware e furto dei dati;
- Identificazione dei comportamenti potenzialmente pericolosi o non aderenti alle politiche aziendali. Blocco dei siti potenzialmente malevoli, consentendo o negando l'accesso ad un elenco di URL classificati;
- Ispezione del traffico internet per vietare l'accesso ad un sito sulla base di una valutazione "risk based scoring" calcolata mediante informazioni di threat intelligence;
- Aggiornamento automatico delle liste di siti malevoli;
- Produzione di report di sintesi (executive summary) e di dettaglio (technical report);
- Gestione della navigazione tramite utilizzo di categorie di siti web e protocolli;

Data la sua criticità, il servizio utilizza un framework di comunicazione che prevede allineamenti a differenti livelli, da quello operativo fino a quello Direzionale/Leadership. Infatti, il servizio è erogato da un unico gruppo di lavoro denominato Web Navigation and Email Protection (WNEP) Team, che risponde a un responsabile del servizio, il quale rappresenta il punto di contatto tra il WNEP Team e l'Amministrazione.
Il servizio sarà abilitato secondo due fasi, prevedendo l'attivazione della componente proxy nella prima fase e solo successivamente la messa in opera della componente di email security, secondo le indicazioni e le tempistiche concordate con l'Amministrazione.

6.1.5 L1.S11 – Firma digitale remota

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.
Il servizio prevede la modalità di utilizzo "da remoto": si intende la firma digitale generata usando strumenti di autenticazione (tipicamente user id+ password +OTP o telefono cellulare) che consentono la generazione della firma su un dispositivo (HSM) custodito dal prestatore del servizio fiduciario qualificato.
Il servizio è configurato come un servizio online nel quale la chiave privata del firmatario viene generata e conservata assieme al certificato di firma rilasciato da parte di un Certificatore accreditato, all'interno di un server remoto sicuro (basato su un HSM conforme alla normativa vigente in materia).
È utilizzato un sistema di autenticazione forte che prevede l'uso, oltre alla conoscenza di un codice segreto (es. PIN), di sistemi OTP fisici o logici (USB, telefono cellulare, token), eliminando in tal modo i problemi e i rischi relativi all'utilizzo delle sole password statiche.
L'attività di verifica dell'identità dei titolari dei certificati di firma digitali, propedeutica al loro rilascio, è effettuata a cura e sotto la responsabilità dell'Amministrazione.
Il servizio garantisce la conformità alla normativa vigente in materia di firme digitali (CAD d.lgs. 82 del 7 marzo 2005 e successive modifiche) e la Determinazione Commissariale n. 63/2014 dell'Agenzia per l'Italia Digitale.
È inclusa la fornitura dei certificati digitali rilasciati da un Ente Certificatore accreditato a norma e delle relative coppie di chiavi pubblica/privata con lunghezza minima di 2048 bit, necessarie alla generazione delle firme.

6.1.6 L1.S12 – Sigillo elettronico

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.
Il Sigillo elettronico si riferisce a una persona giuridica (un organismo unitario composto da una pluralità di individui o un complesso di beni, al quale vengono riconosciuti diritti e doveri).

6.1.7 L1.S15 – Servizi Specialistici

Il servizio prevede il coinvolgimento di figure professionali con determinate competenze rispetto all'esigenza espressa dall'Amministrazione all'interno dei Piano dei Fabbisogni. Si specifica che sebbene i servizi specialistici non siano esplicitamente dimensionati nel Piano dei Fabbisogni, il RTI propone un dimensionamento a corpo, posto che quest'ultimo è indispensabile per l'erogazione dei servizi di cui al Piano dei Fabbisogni stesso, e sul quale il RTI pone la massima disponibilità al contraddittorio con l'Amministrazione stessa su quanto dimensionato. A tal proposito è stato previsto un adeguato dimensionamento dei Servizi Specialistici per far fronte alle seguenti attività:

- supporto alla migrazione dei servizi di sicurezza dell'Amministrazione verso nuovi servizi e soluzioni, in particolare nelle fasi di analisi e configurazione;
- attività di delivery dei servizi di cyber security, in particolare durante le operazioni di migrazione;
- supporto nella definizione, configurazione ed erogazione dei servizi di monitoraggio degli eventi di sicurezza e di monitoraggio continuo delle vulnerabilità di sicurezza.

Nei paragrafi che seguono viene fornito con maggior dettaglio il tipo di supporto proposto ad integrazione dei principali servizi previsti nel presente Piano Operativo.

6.1.7.1 L1.S15 Servizi Specialistici ad integrazione servizi di sicurezza per L1.S1 - Security Operation Center

I Servizi Specialistici a supporto del servizio SOC, prevedono l'utilizzo di personale specializzato in logica di progetto, finalizzato a supportare l'evoluzione del processo di monitoraggio e di gestione degli incidenti di sicurezza. Gli obiettivi indicati per tale servizio specialistico sono i seguenti e saranno oggetto di pianificazione puntuale durante il periodo contrattuale:

- Supporto nella "remediation" degli incidenti di sicurezza;
- Supporto alla identificazione e realizzazione di nuovi Use Case a supporto del processo di detection al fine di migliorare continuamente la libreria di casi dedicati;
- Supporto alla identificazione e realizzazione di nuovi playbook dedicati, con lo scopo di contestualizzare il monitoraggio e la risposta alla violazione;
- Supporto alla investigazione di possibili attacchi informatici o "data breach".

6.1.7.2 L1.S15 Servizi Specialistici ad integrazione servizi di sicurezza per L1.S2 - Next Generation Firewall

I Servizi Specialistici a supporto del servizio di sicurezza perimetrale sono relativi alle attività di: raccolta dei dati nei sistemi di esercizio, individuazione dettagliata delle soluzioni personalizzate per l'Amministrazione, pianificazione delle strategie di migrazione, controllo della corretta esecuzione del servizio.

6.1.7.3 L1.S15 Servizi Specialistici ad integrazione servizi di sicurezza per L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza

I Servizi Specialistici a supporto della Gestione Continua delle vulnerabilità prevedono il coinvolgimento di figure professionali con competenze adeguate rispetto all'esigenza espressa dall'Amministrazione all'interno dei Piano dei Fabbisogni. A tal proposito è stato previsto un adeguato dimensionamento dei Servizi Specialistici per far fronte all'integrazione del servizio in oggetto prevedendo, alla consegna del report delle vulnerabilità periodico sui sistemi, una assistenza all'Amministrazione nella valutazione delle vulnerabilità al fine di identificare un piano di rientro in base alle priorità dettate dalla ASL ROMA 5 stessa e dai suoi team tecnici/operativi, che avranno l'onere di valutare la fattibilità e i tempi per loro competenza.

6.1.7.4 L1.S15 Servizi Specialistici ad integrazione servizi di sicurezza per L1.S6– Protezione Navigazione Internet e Posta Elettronica

Nell'ambito dei Servizi Specialisti connessi al servizio remoto di Protezione Navigazione Internet e Posta Elettronica rientrano tutte le attività di setup necessarie all'erogazione del servizio stesso. Vengono, inoltre, svolte attività di supporto anche durante l'esecuzione del servizio finalizzate alla individuazione di eventuali compromissioni preesistenti sull'infrastruttura dell'Amministrazione che possano compromettere lo scopo del progetto.

6.2 Utenza interessata / coinvolta

Personale dell'Azienda Sanitaria Locale Roma 5.

6.3 Eventuali riferimenti / vincoli normativi

N.A.

7 PIANO DI PROGETTO

7.1 Cronoprogramma

L'erogazione dei servizi avrà durata **48 mesi**, a decorrere dalla data di conclusione delle attività di presa in carico T0 (data di firma del contratto esecutivo + periodo di presa in carico), come indicato nella seguente tabella:

	ANNO I												ANNO II												ANNO III												ANNO IV											
	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
L1.S1 SOC																																															
L1.S2 – Next Generation Firewall																																															
L1.S4 Gest. Continua Vulnerabilità																																															
L1.S6 – Protezione Navigazione Internet e Posta Elettronica																																															
L1.S11 - Firma Elettronica																																															
L1.S12 – Sigillo Elettronico																																															
L1.S15 Servizi Specialistici																																															

Tabella 9 – Cronoprogramma

7.2 Data di Attivazione e Durata del Servizio

Il contratto esecutivo produrrà i suoi effetti dalla data di stipula e avrà una durata di 48 mesi a decorrere dalla data di conclusione delle attività di presa in carico.

7.3 Gruppo di Lavoro

L'approccio organizzativo individuato e descritto all'interno del Capitolo 4 consente di predisporre team e organizzazioni del lavoro secondo condizioni ad hoc per ogni progetto, secondo i carichi di lavoro previsti nella progettualità condivisa ma facilmente scalabili, qualora in corso d'opera maturassero condizioni tali da richiedere una modifica al numero dei team, delle risorse o del perimetro d'intervento. Una volta individuate le peculiarità dell'Amministrazione contraente, la selezione del gruppo di lavoro avviene analizzando il contesto della stessa sia dal punto di vista tecnologico, individuando il personale maggiormente qualificato sulle tecnologie e sui prodotti già in uso o attese, che tematico, andando ad identificare le figure professionali con esperienze e competenze nel settore pubblico.

7.4 Modalità di esecuzione dei Servizi

Per la modalità di esecuzione dei servizi è possibile far riferimento al Capitolo 8 del Capitolato Tecnico Speciale. In generale, a partire dal Piano di Lavoro Generale, l'Amministrazione richiederà la stima ed il Piano di Lavoro del singolo stream progettuale (obiettivo), fornendo la documentazione di supporto ed i macro-requisiti per poter effettuare una stima dell'obiettivo.
Di seguito si riporta una tabella di sintesi con le principali milestone per ogni servizio:

MILESTONE	DESCRIZIONE	ATTORE
Richiesta stima e Piano di Lavoro	Richiesta al fornitore di procedere alla stima dei tempi e costi del servizio	Amministrazione
Stima (pre-dimensionamento)	Comunicazione dei tempi e dei costi previsti per servizio	RTI
Collaudo	Esecuzione del collaudo dei servizi per cui è stato richiesto	RTI
Attivazione	Individuazione del ciclo di vita ed avvio del fornitore a procedere con le attività sul servizio. Al momento dell'attivazione saranno noti elementi caratteristici ai quali si associa una valutazione di complessità	Amministrazione
Consegna	Rilascio degli artefatti previsti dal piano di lavoro, sia intermedi che finali	RTI
Approvazione e Verifica di Conformità	Riscontro degli artefatti consegnati in quantità e tipologia (ricevuta), senza valutazione di contenuto	Amministrazione
Accettazione e Verifica di Conformità	Verifica e validazione dei prodotti intermedi di servizio, previa verifica di merito. Certificazione della corretta esecuzione del servizio relativamente ai prodotti oggetto di approvazione	Amministrazione
Valutazione difettosità all'avvio e Verifica di Conformità	Verifica della piena fruizione delle funzionalità e dei servizi da parte dell'utente (cittadino/ impresa/ operatore amministrativo/ decisore/ fruitore) tramite l'esame della quantità e della tipologia di malfunzionamenti e non conformità rilevati durante il periodo di avvio in esercizio. Certificazione della corretta esecuzione del servizio	Amministrazione

Tabella 10 - Descrizione milestone per obiettivo

Per il Governo della Fornitura, si propone l'adozione delle pratiche di seguito descritte:

- **Stato avanzamenti lavori – tecnico.** Con cadenza mensile (o su richiesta dell'Amministrazione) per le attività progettuali e mensile (o su richiesta dell'Amministrazione) per quelle continuative, verrà prodotto un report di sintesi che sarà discusso nel corso di un meeting ad hoc con l'Amministrazione. Il report riporterà, a livello di progetto e a livello di obiettivo: i) avanzamento e scostamenti rispetto al piano di lavoro; ii) attività svolte e attività previste; iii) rischi e problematiche operative; iv) punti aperti; v) azioni da intraprendere per il corretto svolgimento delle attività.

7.5 Modalità di ricorso al Subappalto da parte del Fornitore

La quota massima di attività subappaltabile – o concedibile in cottimo – **da parte del RTI è pari al 50% dell'importo complessivo** previsto dal contratto. Di seguito è riportato l'elenco delle attività / prestazioni per parti delle quali il RTI intende ricorrere al subappalto:

SERVIZIO	AZIENDA	QUOTA MASSIMA SUBAPPALTABILE
L1.S1 – Security Operation Center, L1.S2 – Next Generation Firewall, L1.S6 – Protezione Navigazione Internet e Posta Elettronica, L1.S11 – Firma Elettronica, L1.S12 – Sigillo Elettronico, L1.S15 – Servizi Specialistici	Fastweb	50%
L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza, L1.S15 – Servizi Specialistici	Accenture	50%
L1.S15 – Servizi Specialistici	Fincantieri	50%
L1.S15 – Servizi Specialistici	Deas	50%

Tabella 11 - Modalità di ricorso al Subappalto da parte del Fornitore

8 DIMENSIONAMENTO ECONOMICO

8.1 Modalità di erogazione dei Servizi

Di seguito è riportato per ogni servizio le metriche di misura e le modalità di erogazione e consuntivazione.

ID SERVIZIO	METRICA	MODALITÀ EROGAZIONE	MODALITÀ CONSUNTIVAZIONE	PERIODICITÀ CONSUNTIVAZIONE	PREZZO UNITARIO OFFERTO	QUANTITÀ/ANNO	VALORE ECONOMICO (Per 48 mesi)
L1.S1 – Security Operation Center	Device Eq./anno	Da remoto	Canone	Mensile	€218,40	220 Device Equivalent/Anno	€192.192,00
L1.S2 – Next Generation Firewall	**Ngfw Throughput/anno**	Da remoto	Canone	Mensile	€6.475,84	3 Ngfw Throughput/anno	€77.710,08
L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza	IP/anno	Da remoto	Canone	Mensile	€13,80	250 IP/Anno	€13.800,00
L1.S6 – Protezione Navigazione Internet e Posta Elettronica	Utenti/anno	Da remoto	Canone	Mensile	€4,037	4.000 Utenti/Anno	€64.592,00
L1.S11 - Firma Elettronica	Utenti/anno	Da remoto	Canone	Mensile	€6,143	200 Utenti/Anno	€4.914,40
L1.S12 – Sigillo Elettronico	N. Sigilli/secondo	Da remoto	Canone	Mensile	€3.890,25	1 Sigillo/secondo per ciascun anno	€15.561,00
L1.S15 – Servizi Specialistici	GG/P	Da remoto / On Site	Progettuale - A corpo	Mensile	€244,00	4224 GG/P Team Ottimale/TOTALI	€1.030.656,00

Tabella 12 - Quadro economico di riferimento

L'importo complessivo dell'ordinativo di fornitura ammonta a **1.399.425,48 €.**

8.2 Indicazioni in ordine alla fatturazione ed ai termini di pagamento

La fatturazione sarà eseguita in accordo con quanto previsto nello Schema di Contratto Esecutivo. Per quanto concerne i termini di pagamento si fa riferimento a quanto previsto nell'Accordo Quadro.

9 ALLEGATI

9.1 Piano di Lavoro Generale

Per il piano di lavoro generale si rimanda all'allegato Piano di Lavoro Generale.

9.2 Piano di Presa in Carico

Come riportato nel Piano dei Fabbisogni, una prima pianificazione di queste attività, è riportato nell'allegato Piano di Presa in Carico. Il RTI si impegna a garantire l'esecuzione dei collaudi nelle modalità e con riferimento ai servizi per i quali è richiesto come sarà concordato con l'Amministrazione durante il periodo di presa in carico.

9.3 Piano della Qualità Specifico

Per il piano di qualità specifico si rimanda al documento denominato Piano della Qualità Specifico.

9.4 Curriculum Vitae dei Referenti

Si allega, nel Piano di Lavoro Generale, il CV del RUAC di CE. Per quanto concerne il Referente Tecnico di CE, il relativo nominativo sarà fornito per la stipula del CE ed il relativo CV sarà fornito entro 5 giorni dalla stipula.

9.5 Misure di Sicurezza poste in essere

Per le misure di sicurezza poste in essere si rimanda al Piano di Sicurezza del Centro Servizi.

9.6 Documentazione relativa al principio "Do No Significant Harm" (DNSH)

Si allega la documentazione trasmessa a Consip tramite pec in data 11/11/2022, relativa al principio "Do No Significant Harm" (DNSH).