REGIONE CAMPANIA
AZIENDA SANITARIA NAPOLI 3 SUD
Via Marconi n. 66
80059 - Torre del Greco (Na)
C.F. e Partita I.V.A. 06322711216

DELIBERAZIONE N. 923 DEL 31/07/2023

OGGETTO:	**ADESIONE ALL'ACCORDO QUADRO CONSIP, PER L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI ID 2296 LOTTO 1. PRESA D'ATTO E APPROVAZIONE PIANO OPERATIVO DEI SERVIZI INVIATO DALLA ACCENTURE SPA, MANDATARIA DEL R.T.I. ACCENTURE SPA. FASTWEB SPA, FINCANTIERI NEXTECH SPA, DEAS SPA, CON PEC DEL 27/07/2023 - CIG MASTER 88846293CA; CIG DERIVATO 99970545FO**

STRUTTURA PROPONENTE:	**U.O.C. ACQUISIZIONE BENI E SERVIZI**

PROVVEDIMENTO:	**Immediatamente Esecutivo**

IL DIRETTORE GENERALE

dr. Giuseppe Russo, nominato con Delibera della Giunta Regionale della Campania n. 321 del 21 Giugno 2022 e con D.P.G.R.C. n. 111 del 4 Agosto 2022, con l'assistenza del Segretario verbalizzante, previa acquisizione del parere del Direttore Amministrativo Aziendale, ha adottato la deliberazione in oggetto di cui al testo che segue:

Azienda Sanitaria Locale Napoli 3 Sud
Sede Legale Via Marconi n. 66 – 80059 Torre del Greco
U.O.C. ACQUISIZIONE BENI E SERVIZI
C.F. e Partita I.V.A. 06322711216

OGGETTO: ADESIONE ALL'ACCORDO QUADRO CONSIP, PER L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI ID 2296 LOTTO 1. PRESA D'ATTO E APPROVAZIONE PIANO OPERATIVO DEI SERVIZI INVIATO DALLA ACCENTURE SPA, MANDATARIA DEL R.T.I. ACCENTURE SPA. FASTWEB SPA, FINCANTIERI NEXTECH SPA, DEAS SPA, CON PEC DEL 27/07/2023 - CIG MASTER 88846293CA; CIG DERIVATO 99970545FO

IL DIRETTORE DEL **U.O.C. ACQUISIZIONE BENI E SERVIZI**

Alla stregua dell'istruttoria compiuta dal Direttore **U.O.C. ACQUISIZIONE BENI E SERVIZI** delle risultanze degli atti tutti richiamati nelle premesse che seguono, costituenti istruttoria a tutti gli effetti di legge, nonché dell'espressa dichiarazione di regolarità tecnica e amministrativa della stessa, resa dallo stesso Dirigente responsabile proponente a mezzo della sottoscrizione della presente;

dichiarata, altresì, espressamente con la sottoscrizione, nella qualità di Responsabile del trattamento anche nella fase di pubblicazione, la conformità del presente atto ai princìpi di cui al Regolamento europeo n. 679 del 27 aprile 2016 ed al D.Lgs. 10 agosto 2018, n. 101 in materia di protezione dei dati personali;

dichiarata, allo stato ed in relazione al procedimento di cui al presente atto, l'insussistenza del conflitto di interessi ai sensi dell'art. 6 bis della Legge n. 241/1990, delle disposizioni di cui al vigente Codice di Comportamento Aziendale e delle misure previste dal vigente Piano Triennale della Prevenzione della corruzione e della Trasparenza;

dichiarata, infine, la conformità del presente atto ai princìpi di cui alla legge 6 novembre 2012, n. 190.

Premesso che:

- che la Consip, società interamente partecipata dal Ministero dell'economia e delle finanze, ai sensi dell'articolo 26, Legge 23 dicembre 1999, n. 488, dell'articolo 58, Legge 23 dicembre 2000, n. 388, nonché dei relativi decreti attuativi, DD.MM. del 24 febbraio 2000 e del 2 maggio 2001, ha, tra l'altro, il compito di attuare lo sviluppo e la gestione operativa del Programma di razionalizzazione della spesa di beni e servizi per la pubblica amministrazione;
- che l'art.1, comma 548, della Legge 28 dicembre 2015, n. 208 prevede che "*Al fine di garantire la effettiva realizzazione degli interventi di razionalizzazione della spesa mediante aggregazione degli acquisti di beni e servizi, gli enti del Servizio sanitario nazionale sono tenuti ad approvvigionarsi, relativamente alle categorie merceologiche del settore sanitario, come individuate dal decreto del Presidente del Consiglio dei ministri di cui all'articolo 9, comma 3, del decreto-legge 24 aprile 2014, n.*

66, convertito, con modificazioni, dalla legge 23 giugno 2014, n. 89, avvalendosi, in via esclusiva, delle centrali regionali di committenza di riferimento, ovvero della Consip SpA";

- che sul portale CONSIP è attivo l'Accordo Quadro Sicurezza da Remoto Lotto 1 con cui si mette 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;
- che l'iniziativa *Sicurezza da remoto* è stata bandita ai sensi dell'art. 4, comma 3 quater del d.l. 95/2012, ove Consip S.p.A. svolge altresì le attività di centrale di committenza relative alle Reti telematiche delle pubbliche amministrazioni, al Sistema pubblico di connettività ai sensi del decreto legislativo 7 marzo 2005, n. 82, e alla Rete internazionale delle pubbliche amministrazioni ai sensi del decreto medesimo nonché ai contratti-quadro ai sensi dell'articolo 1, comma 192, della legge 30 dicembre 2004, n. 311;
- che l'obiettivo, dell'A.Q., è duplice e consiste in particolare nel:

a 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;

b 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.

Preso atto che:

- con nota prot.150223 del 28/07/2023, la U.O.C. Sistemi Informativi ha trasmesso alla UOC ABS il Piano dei fabbisogni relativo all'A.Q. avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni, ad essa inviato dalla società Accenture S.p.A.in qualità di mandataria del RTI costituito Accenture S.p.A., Fincantieri Nextech S.p.A., Fasteweb S.p.A., Deas, Difesa e Analisi Sistemi S.p.A., per un importo complessivo di € 1.506.986,92 iva esclusa;
- che, altresì, con detta nota la U.O.C. Sistemi Informativi ha chiesto alla UOC Acquisizione Beni e Servizi di provvedere agli adempimenti amministrativi di competenza ai fini della adesione al già menzionato A.Q.;

Visti:

- Il Capitolato Tecnico di gara;
- Il D.Lgs. 50/2016 e ss.mm.ii.
- l'articolo 26, Legge 23 dicembre 1999, n. 488;
- l'articolo 58, Legge 23 dicembre 2000, n. 388;
- nonché i relativi decreti attuativi, DD.MM. del 24 febbraio 2000 e del 2 maggio 2001;

Dato atto che alla presente procedura, in forza del combinato disposto degli artt. nn. 226, c.2 lett. b), e 229, c.2, del D.lgs.36/2023, si applicano le disposizioni di cui al D.lgs.50/2016 ss.mm.ii;

Ritenuto, pertanto, necessario:

- **prendere atto ed approvare** tutta la documentazione oggetto del presente provvedimento, agli atti della U.O.C. A.B.S, e tutte le attività regolarmente avviate dallo stesso Servizio, per l'affidamento della fornitura de qua, nel rispetto di quanto previsto dalle normative vigenti;
- per l'effetto **di aderire** all'accordo quadro stipulato da Consip per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni id 2296 lotto 1, alle condizioni tecniche ed economiche riportate nell'allegato Piano Operativo inviato dalla Accenture spa, mandataria del R.T.I. Accenture spa, Fastweb spa, Fincantieri Nextech spa, Deas spa;
- **autorizzare** il Direttore della U.O.C. A.B.S. Direttore della U.O.C. A.B.S., individuato quale punto Ordinante, ad emettere l'Ordinativo di Fornitura (ODF), attraverso il Sistema di e-Procurement MePa;

PROPONE AL DIRETTORE GENERALE di

- **DI PRENDERE ATTO ED APPROVARE** il Piano Operativo ***(all.1)*** trasmesso dalla Accenture spa, mandataria del R.T.I. Accenture spa, Fastweb spa, Fincantieri Nextech spa, Deas spa con pec del 27/07/2023 contenente la proposta tecnica ed economica, sulla base delle richieste contenute nel Piano dei Fabbisogni dal quale si rileva la quantificazione dell'importo per i servizi richiesti secondo la tabella riepilogativa di seguito riportata:

SERVIZIO	ACCENTURE	FASTWEB	FINCANTIERI	DEAS
L1.S1 – Security Operation Center	X			
L1.S4 – Gestione continua delle vulnerabilità	X			
L1.S5 – Threat Intelligence	X			
L1.S7 – Protezione End Point		X		
L1.S9 – Formazione e security awareness	X			
L1.S15 – Servizi Specialistici	X	X	X	X
TOTALE (%)	48,63%	51,15%	0,11%	0,11%
TOTALE (€)	€ 732.769,92	€ 770.801,00	€ 1.708,00	€ 1.708,00
TOTALE COMPLESSIVO IVA ESCLUSA	€ 1.506.986,92			
TOTALE COMPLESSIVO IVA INCLUSA	€ 1.838.524,04			

- **DI ADERIRE** all'Accordo Quadro avente ad oggetto l'affidamento per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni id 2296 lotto 1;
- **DI AUTORIZZARE** il Direttore della U.O.C. A.B.S., individuato quale punto Ordinante, ad emettere l'Ordinativo di Fornitura (ODF), attraverso il Sistema di e-Procurement MePa, al quale dovrà allegare il Contratto Esecutivo sottoscritto da questa Amministrazione;
- **DI PRENDERE ATTO** che la spesa complessiva massima, per un periodo di 24 mesi, è di **€ 1.506.986,92** Iva esclusa trova copertura sul conto 5020201150 – Centro di responsabilità QC01103, Bilancio 2013;

- **DI PRENDERE ATTO** che i corrispettivi dovuti al fornitore per i servizi prestati in esecuzione del contratto matureranno in ragione delle attività effettivamente erogate nel rispetto del Piano Operativo (Allegato 1);
- **DI NOMINARE** quale Responsabile Unico del Procedimento il dott. Ulderico Izzo, Dirigente Amministrativo in forza alla UOC Acquisizione Beni e Servizi;
- **DI NOMINARE** quale responsabile della fase di esecuzione del contratto l'ing. Andrea Vitolo, Dirigente in forza alla UOC Sistemi Informatici.
- **DI PRENDERE ATTO** che tutti gli stati di avanzamento sono soggetti ad approvazione da parte dell'Asl Napoli 3 Sud;
- **DI TRASMETTERE** copia del presente provvedimento al Direttore dell'U.O.C. G.E.F; Direttore della UOC Controlli Integrati Interni ed Esterni, nonché alla Consip ed alla società Fastweb;

Il Direttore U.O.C. ACQUISIZIONE BENI E SERVIZI

TOMO DOMENICO
(Firmato digitalmente ai sensi del D. Lgs. 7.3.2005 n. 82 s.m.i. e norme collegate – Sostituisce la firma autografa)

Il Direttore Generale

In forza della Delibera della Giunta Regionale della Campania n. 321 del 21 Giugno 2022 e con D.P.G.R.C. n. 111 del 4 Agosto 2022

Preso atto della dichiarazione resa dal dirigente proponente con la sottoscrizione, in ordine alla regolarità tecnica ed amministrativa del presente atto, nonché relativa alla conformità dello stesso atto alle disposizioni vigenti in materia di tutela della privacy;

Sentito il parere favorevole espresso dal Direttore Amministrativo aziendale

Il Direttore Amministrativo aziendale
dr. Michelangelo Chiacchio

(Firmato digitalmente ai sensi del D. Lgs. 7.3.2005 n. 82 s.m.i. e norme collegate – Sostituisce la firma autografa)

DELIBERA

- **DI PRENDERE ATTO ED APPROVARE** il Piano Operativo ***(all.1)*** trasmesso dalla Accenture spa, mandataria del R.T.I. Accenture spa, Fastweb spa, Fincantieri Nextech spa, Deas spa con pec del 27/07/2023 contenente la proposta tecnica ed economica, sulla base delle richieste contenute nel Piano dei Fabbisogni dal quale si rileva la quantificazione dell'importo per i servizi richiesti secondo la tabella riepilogativa di seguito riportata:

SERVIZIO	ACCENTURE	FASTWEB	FINCANTIERI	DEAS
L1.S1 – Security Operation Center	X			
L1.S4 – Gestione continua delle vulnerabilità	X			
L1.S5 – Threat Intelligence	X			
L1.S7 – Protezione End Point		X		
L1.S9 – Formazione e security awareness	X			
L1.S15 – Servizi Specialistici	X	X	X	X
TOTALE (%)	48,63%	51,15%	0,11%	0,11%
TOTALE (€)	€ 732.769,92	€ 770.801,00	€ 1.708,00	€ 1.708,00
TOTALE COMPLESSIVO IVA ESCLUSA	€ 1.506.986,92			
TOTALE COMPLESSIVO IVA INCLUSA	€ 1.838.524,04			

- **DI ADERIRE** all'Accordo Quadro avente ad oggetto l'affidamento per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni id 2296 lotto 1;
- **DI AUTORIZZARE** il Direttore della U.O.C. A.B.S., individuato quale punto Ordinante, ad emettere l'Ordinativo di Fornitura (ODF), attraverso il Sistema di e-Procurement MePa, al quale dovrà allegare il Contratto Esecutivo sottoscritto da questa Amministrazione;
- **DI PRENDERE ATTO** che la spesa complessiva massima, per un periodo di 24 mesi, è di **€ 1.506.986,92** Iva esclusa trova copertura sul conto 5020201150 – Centro di responsabilità QC01103, Bilancio 2013;
- **DI PRENDERE ATTO** che i corrispettivi dovuti al fornitore per i servizi prestati in esecuzione del contratto matureranno in ragione delle attività effettivamente erogate nel rispetto del Piano Operativo (Allegato 1);
- **DI NOMINARE** quale Responsabile Unico del Procedimento il dott. Ulderico Izzo, Dirigente Amministrativo in forza alla UOC Acquisizione Beni e Servizi;
- **DI NOMINARE** quale responsabile della fase di esecuzione del contratto l'ing. Andrea Vitolo, Dirigente in forza alla UOC Sistemi Informatici.
- **DI PRENDERE ATTO** che tutti gli stati di avanzamento sono soggetti ad approvazione da parte dell'Asl Napoli 3 Sud;
- **DI TRASMETTERE** copia del presente provvedimento al Direttore dell'U.O.C. G.E.F; Direttore della UOC Controlli Integrati Interni ed Esterni, nonché alla Consip ed alla società Fastweb;

Il Dirigente proponente sarà responsabile in via esclusiva, dell'esecuzione della presente deliberazione, che viene resa immediatamente esecutiva, data l'urgenza, curandone tutti i consequenziali adempimenti, nonché quelli di pubblicità e di trasparenza previsti dal D.L.gs 14 marzo 2013 n° 33 e s.m.i.

Il Direttore Generale
Dr. Giuseppe Russo
(Firmato digitalmente ai sensi del D. Lgs. 7.3.2005 n. 82 s.m.i. e norme collegate.
– Sostituisce la firma autografa)

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 | DEAS

Rev.	Data	Descrizione delle modifiche	Autore
01	27/07/2023	Prima emissione	RTI

Tabella 1 - Registro delle versioni

Sommario

Indice delle tabelle

Indice delle figure

1 INTRODUZIONE

L'Azienda Sanitaria Locale Napoli 3 Sud (nel seguito anche l'"Amministrazione" o l'"ASL NA3 SUD") si avvale di un'infrastruttura digitale complessa attraverso la quale eroga servizi ad un'ampia area metropolitana. In tale contesto, l'adozione di nuovi paradigmi di costruzione ed erogazione dei servizi digitali (cloud computing, mobile workplace), la crescita costante di attacchi cyber sempre più sofisticati, l'adeguamento del quadro normativo alle nuove esigenze di privacy e protezione delle infrastrutture critiche, rendono necessaria una profonda rivalutazione degli aspetti concettuali, tecnici e organizzativi legati alla cybersicurezza, soprattutto in relazione alla estrema dinamicità e complessità delle sue manifestazioni.

1.1 Scopo

L'ASL NA3 SUD necessita dei servizi di seguito indicati, al fine di mettere in atto una serie di contromisure per la mitigazione del rischio cyber e migliorare la consapevolezza delle persone.

- L1.S1 – Security Operation Center
- L1.S4 – Gestione continua delle vulnerabilità
- L1.S5 – Threat Intelligence
- L1.S7 – Protezione End Point
- L1.S9 – Formazione e security awareness
- L1.S15 – Servizi Specialistici

L'esigenza inoltre è quella di assicurare, in caso di riscontro di eventi anomali, vulnerabilità critiche e altri eventi di sicurezza degni di nota, un'analisi approfondita degli eventi occorsi, dell'attuale livello di sicurezza dell'intera infrastruttura monitorata e allertare di conseguenza i corretti riferimenti aziendali indicati dall'Amministrazione stessa..

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 co-genti (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.

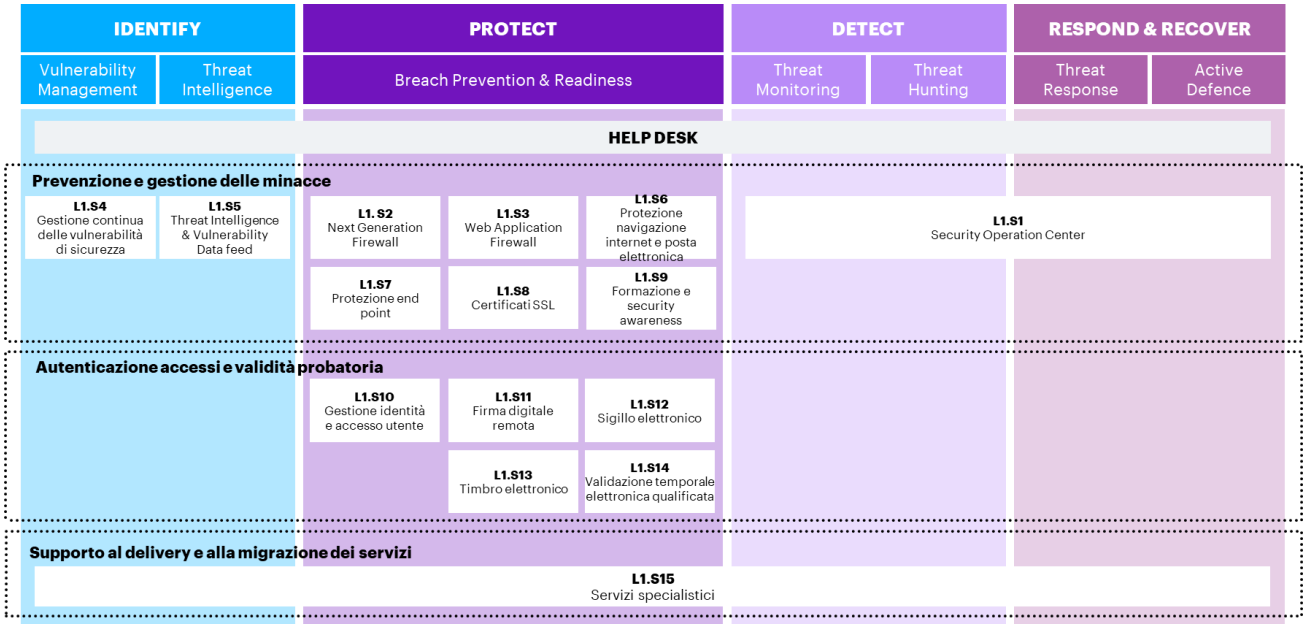

Figura 1-Mappatura Servizi di Sicurezza e Framework NIST

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, **Azienda Sanitaria Locale Napoli 3 Sud,** 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 di 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 Napoli 3 Sud,** 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 l'Azienda Sanitaria Locale Napoli 3 Sud e Fornitore gli eventuali interventi progettuali da attivare/modificare nonché gli impatti in termini di Piano di Lavoro Generale

Tabella 2 - Assunzioni

2 RIFERIMENTI

2.1 Normativa di riferimento

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

2.2 Documenti Applicabili

Rif.	Titolo
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.
2	ALLEGATO 2A - CAPITOLATO TECNICO SPECIALE SERVIZI DI SICUREZZA DA REMOTO
3	Accordo Quadro
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
5	Appendice 1 al CTS Lotto 1_Indicatori di qualità - ID 2296 - Gara Sicurezza da remoto
6	Piano dei Fabbisogni nominato: “20230705_2296_Lotto 1_Sicurezza da Remoto_Piano dei fabbisogni_ASL NA3 SUD-signed.pdf”- PEC 06/07/2023

Tabella 3 - Documenti Applicabili

3 DEFINIZIONI E 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 4 - Definizioni

Vocabolo	Titolo
AgID	Agenzia per l'Italia Digitale
AQ	Accordo Quadro
BC	Business Continuity
CE	Contratto Esecutivo

Vocabolo	Titolo
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 5 - 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:

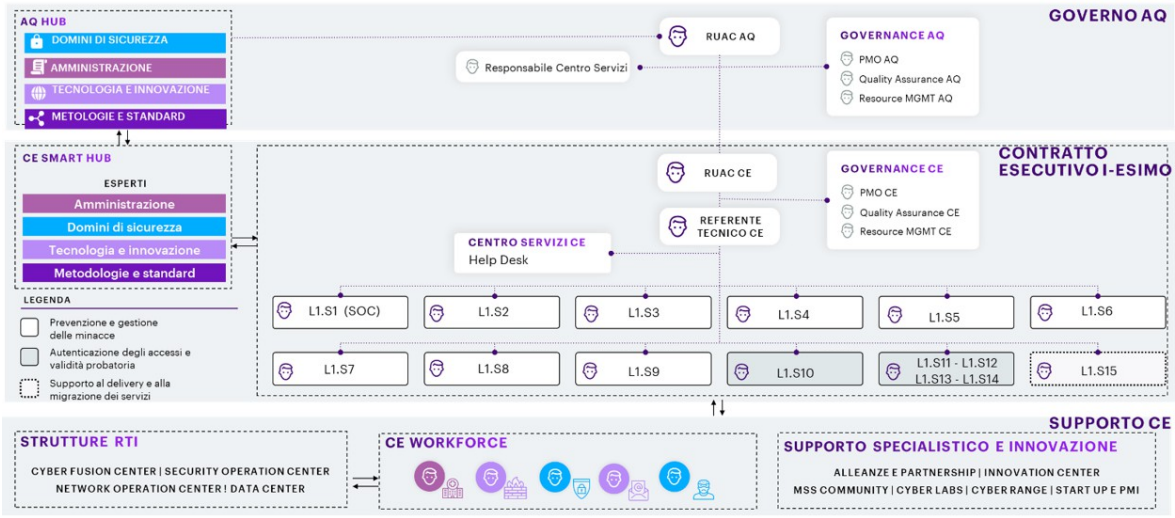

Figura 2-Organizzazione dell'AQ proposta dal RTI

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 del RTI secondo la ripartizione seguente:

SERVIZIO	ACCENTURE	FASTWEB	FINCANTIERI	DEAS
L1.S1 – Security Operation Center	X			
L1.S4 – Gestione continua delle vulnerabilità	X			
L1.S5 – Threat Intelligence	X			
L1.S7 – Protezione End Point		X		
L1.S9 – Formazione e security awareness	X			
L1.S15 – Servizi Specialistici	X	X	X	X
TOTALE (%)	48,63 %	51,15 %	0,11 %	0,11 %
TOTALE (€)	€732.769,92	€ 770.801,00	€ 1.708,00	€ 1.708,00

Tabella 6 - Ripartizioni 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 7 - 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 di interesse dell'Amministrazione.

5 AMBITI E SERVIZI

5.1 Ambiti di intervento

Gli ambiti d'intervento oggetto di fornitura come di seguito elencati hanno l'obiettivo di soddisfare i requisiti dell'**Azienda Sanitaria Locale Napoli 3 Sud** così come riportati nel Piano dei Fabbisogni:

- L1.S1: Security Operation Center
- L1.S4: Gestione Continua delle vulnerabilità
- L1.S5: Threat Intelligence
- L1.S7: Protezione degli end point
- L1.S9: Formazione e security awareness
- L1.S15: Servizi Specialistici

5.2 Servizi

In tabella sono riportati i servizi offerti e le relative quantità.

SERVIZIO	FASCIA	IMPORTO I ANNO/Quantità	IMPORTO II ANNO/Quantità
L1.S1 – Security Operation Center	Fino a 6.000 Eps- Fascia 4	€ 109.200,00/500 (device equivalent)	€ 109.200,00/500 (device equivalent)
L1.S4 – Gestione Continua delle vulnerabilità	> 200 IP-Fascia 3	€ 6.900,00 /500	€ 6.900,00 /500
L1.S5 – Threat Intelligence	> 50 datafeed-Fascia 3	€14.000,00 /70	€ 14.000,00/70
L1.S7 – Protezione degli end point	> 5.000 nodi-Facia 4	€ 45.020,5 /3.500	€ 45.020,5 /3.500
L1.S9 – Formazione e security awareness	gg/p Team ottimale	€92.324,96 /373	€ 92.324,96 /373
L1.S15 – Servizi Specialistici	gg/p Team ottimale	€633.424,00 /2.596	€ 338.672,00/ 1.388

Tabella 8- 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 9 - 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

6.1 Descrizione dei servizi

Di seguito i servizi proposti in linea con le esigenze espresse dall'Azienda Sanitaria Locale Napoli 3 Sud.

6.1.1 L1.S1 - Security Operation Center

La ventennale esperienza di Accenture, unitamente a quella di Fastweb nell'ambito della pubblica amministrazione, ha permesso di consolidare e far evolvere un modello di servizio ponendo a fattor comune esperienze analoghe nella realizzazione ed erogazione di servizi di Security Operation Center per istituzioni governative nazionali ed internazionali. Si è giunti alla definizione ed ingegnerizzazione di un modello di "**Next Generation Security Operation Center (NG-SOC)**" basato su tecnologia **Splunk** per la parte di "Security Information & Event Management (SIEM)" e **Palo Alto Cortex XSOAR** per la parte di "Security Orchestration, Automation & Response (SOAR)", entrambi leader di mercato secondo fonti affermate di analisti di settore quali Gartner e Forrester e partner decennali a livello globale delle aziende del RTI.
Il servizio proposto di SOC ha l'obiettivo di individuare nel minor tempo possibile potenziali incidenti di sicurezza, supportato dalle informazioni di dettaglio fornite dalle sorgenti di eventi di sicurezza dell'Amministrazione.
Il servizio SOC è erogato da un unico gruppo di lavoro (Accenture Cyber Fusion Center Napoli) che risponde a un Responsabile del Servizio SOC (RSOC, vale a dire il Service Manager) il quale rappresenterà il punto di contatto con il Referente tecnico dell'Amministrazione.

6.1.1.1 Team di servizio

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.

Il team per il SOC del RTI è composto da:

- **un RSOC** in qualità di referente tecnico del RTI SOC;
- **un SOC team** con SME (Subject Matter Expert) esperti verticali nelle varie aree di Cyber Security.

Il RSOC rappresenta il punto di contatto tra il Referente Tecnico dell' Azienda Sanitaria Locale Napoli 3 Sud e il SOC Team ed ha le seguenti responsabilità:

- stilare e condividere il Questionario di Preinstallazione (QPI) adattato al contesto e perimetro dell' Azienda Sanitaria Locale Napoli 3 Sud contenente le informazioni necessarie al processo di onboarding, i contatti dei referenti operativi dell' Azienda Sanitaria Locale Napoli 3 Sud e i processi di escalation;
- valutare e convalidare il perimetro di monitoraggio, inteso come l'insieme di sorgenti di log (eventi di sicurezza) dell'Azienda Sanitaria Locale Napoli 3 Sud, identificati come fondamentali per la valutazione e la copertura del monitoraggio e, quindi, potenziali incidenti di sicurezza;
- valutare e convalidare la configurazione delle varie sorgenti di log di cui il punto precedente e, quindi, i collector/agent da utilizzare, aree geografiche coinvolte, canale di comunicazione protetto per il trasferimento di tali eventi di sicurezza dall'IT dell'Azienda Sanitaria Locale Napoli 3 Sud verso il Centro Servizi, informazioni sugli use case e modello di automatizzazione e quanto altro al fine di definire al meglio il perimetro di lavoro;
- condividere e confermare le aspettative dell'Azienda Sanitaria Locale Napoli 3 Sud ed evidenziare/indirizzare potenziali disallineamenti;
- creare i collegamenti tra i vari referenti dei team coinvolti;
- raccogliere le procedure di escalation e di incident management per individuare i punti di aggiornamento;
- lavorare a contatto con i referenti dell'Azienda Sanitaria Locale Napoli 3 Sud per recepire i riscontri operativi e tradurli in attività di miglioramento continuo;

- mantenere contatti regolari con eventuali altri team, esterni all'ambito sicurezza, per condividere informazioni rilevanti che possano aiutare/migliorare l'integrazione e la collaborazione;
- identificare i processi di automazione che facilitino la condivisione delle informazioni e la risposta alle minacce per guidare una reazione più rapida e accurata.

Il SOC Team è composto da SME (Subject Matter Expert) esperti verticali nelle varie aree di Cyber Security e, si presenta suddiviso in tre gruppi di analisti incaricati dell'analisi e gestione degli incidenti a complessità crescente: L1, L2 ed L3.

Gli SME sono esperti di sicurezza certificati che operano all'interno di gruppi di lavoro ben definiti con chiara responsabilità e interagiscono tra loro e con l'Azienda Sanitaria Locale Napoli 3 Sud attraverso canali di comunicazione con **massimi livelli di confidenzialità** in base alla natura delle informazioni scambiate. Di seguito si riporta una vista sintetica delle figure che compongono il 'SOC Team' adattato secondo le esigenze dell'Azienda Sanitaria Locale Napoli 3 Sud:

FUNZIONE-TEAM	RUOLO / PROFILO	COMPITI E RESPONSABILITÀ
Responsabile del servizio	RSOC / SP	Punto di contatto tra l'Azienda Sanitaria Locale Napoli 3 Sud e il SOC team con le responsabilità riportate precedentemente. Possiede certificazioni quali: ISO 27001, CISSP, ITIL, CISM.
Supporto di sicurezza Livello 1	Team L1 / Jr-ISC	Effettua il monitoraggio 24x7 degli allarmi di sicurezza, verifica la priorità degli allarmi, effettua l'analisi degli eventi e la verifica degli stessi, notifica gli eventi attraverso la piattaforma di ITSM del Centro Servizi ed attraverso mail o chiamate al reperibile dell' Azienda Sanitaria Locale Napoli 3 Sud. Possiede certificazioni quali: SSCP, CEH.
Supporto di sicurezza Livello 2	Team L2 / Sr-ISC	Fornisce report SIEM predefiniti, revisiona e analizza i report, effettua l'analisi degli allarmi e la verifica dei falsi positivi, fornisce supporto per la prima investigazione di breve periodo, effettua la qualifica di un evento in incidente di sicurezza, crea e traccia gli incidenti, monitora le performance, identifica le azioni di contenimento di breve periodo. Inoltre, interagisce con il team operativo dell'Azienda Sanitaria Locale Napoli 3 Sud a supporto dell'attività di risoluzione e successivamente di chiusura del caso, che è comunque a carico dell'Azienda Sanitaria Locale Napoli 3 Sud ed in particolare del suo team operativo di competenza.
Supporto di sicurezza Livello 3	Team L3 / Sr-ISC	Supporta la risoluzione in caso di interruzione della raccolta dei log, supporta il tuning delle regole (casi d'uso), raccoglie e trasmette evidenze, valuta il post incidente per miglioramento continuo.
Legenda: SP Security Principal, Sr-ISC Senior Information Sec. Consultant, Jr-ISC Junior Information Sec.		

Tabella 10 - Figure del SOC team

Di seguito si elencano quelli che sono i prerequisiti al servizio in carico all'Azienda Sanitaria Locale Napoli 3 Sud:

- Configurazione delle sorgenti di log (eventi di sicurezza) e di rete, per la lettura e/o invio degli eventi utili al completamento del servizio;
- Procedure di security incident management, escalation, Crisis Management.

6.1.1.2 Modello Operativo

Il modello operativo del servizio SOC proposto prevede il monitoraggio continuo delle informazioni prodotte dalle sorgenti di log (eventi di sicurezza) identificati come perimetro di monitoraggio dall'Azienda Sanitaria Locale Napoli 3 Sud.

In sintesi, il servizio consentirà di:

- Controllare in maniera attiva il perimetro infrastrutturale soggetto al servizio di monitoraggio, attraverso attività di "monitoring real-time" così da anticipare per quanto possibile eventuali incidenti di sicurezza;
- Produrre specifici allarmi e reportistica sugli eventi raccolti;
- Identificazione e comunicazione verso l'Azienda Sanitaria Locale Napoli 3 Sud, delle possibili azioni correttive da intraprendere nell'immediato per contenere l'attacco e prevenirne la propagazione;
- Acquisizione di eventuali evidenze digitali da utilizzare nella ricostruzione di quanto accaduto in seguito all'incidente. Le evidenze digitali raccolte sono poi trasmesse al referente tecnico dell'Azienda Sanitaria Locale Napoli 3 Sud;
- Valutazione post incidente, in modo da individuare possibili azioni migliorative da implementare sui sistemi di sicurezza dell'Azienda Sanitaria Locale Napoli 3 Sud aumentando l'efficacia del SOC team.

6.1.1.3 Modalità di erogazione

Il modello di erogazione del servizio SOC si basa sulla logica che prevede la raccolta degli allarmi generati dal sistema di monitoraggio del Centro Servizi che, in seguito ad incidenti di sicurezza, apre il ticket verso il team "L1 SOC" sul sistema ITSM. Il team "L1 SOC" controllerà le informazioni evidenziate dall'allarme, ed eseguirà le prime verifiche per una eventuale escalation verso il team "L2 SOC" o/e il reperibile dell'Azienda Sanitaria Locale Napoli 3 Sud, nel caso di un fuori orario di servizio.

Successivamente alla conferma di un possibile incidente, il SOC Team procederà con le necessarie azioni, elencate di seguito solo a scopo esemplificativo:

- drill down sugli eventi aggregati che hanno generato l'evidenza/alert;
- verifica dei falsi positivi;
- investigazione/deep analysis del caso;
- escalation verso team di sicurezza ed il team operativo di pertinenza dell'Azienda Sanitaria Locale Napoli 3 Sud per segnalare/supportare azioni di remediation;
- verifica di chiusura del caso segnalato, da parte del team operativo dell'Azienda Sanitaria Locale Napoli 3 Sud.

6.1.2 L1.S4 – Gestione Continua delle vulnerabilità

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 del RTI (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 pianificazione, 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.

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.

6.1.3 L1.S5 – Threat Intelligence

Il servizio in oggetto è erogato dal Centro Servizi avvalendosi della piattaforma Threat Intelligence Service (TIS), sviluppata e gestita da Accenture che, a sua volta integra il servizio specialistico iDefense di Accenture che prevede l'accesso tramite interfaccia e API alle informazioni di intelligence che coprono le vulnerabilità di oltre 1.000 vendor, strumenti e tecniche malware, Indicatori di Compromissione, organizzazioni target, threat actor e loro motivazioni, campagne di phishing e minacce pertinenti l'organizzazione aziendale.
Il servizio sarà reso disponibile tramite una interfaccia web e accesso API.
Per l'utilizzo di tale piattaforma l'Amministrazione dovrà siglarne le relative condizioni di uso.

Funzioni offerte

Il servizio TI&VDF consente di elaborare ed estrarre le informazioni necessarie attraverso le funzionalità offerte, articolate nei livelli riportati nella seguente figura:

Figura 3-Livelli Funzionalità

Tali livelli comprendono tutte le funzionalità previste nel capitolato dell'AQ Sicurezza e ne aggiungono alcune migliorative, come di seguito descritto:

- **Accesso web** - la piattaforma integra l'interfaccia che si basa su un modello di rappresentazione dei dati che consente agli analisti di mettere in relazione nodi di informazioni su threat actor, malware, vulnerabilità, campagne, target, domini, e-mail di phishing, ecc. Tale struttura di dati consente un accesso più rapido ai dati rilevanti e la capacità di visualizzare le relazioni tra i diversi dati;

- **Personalizzazione delle informazioni -** la piattaforma consente di personalizzare le informazioni richieste dalla Amministrazione in funzione dei sistemi adottati. Tramite l'interfaccia è possibile consultare i bollettini predisposti dal team di Threat Intelligence (TI) e generare report personalizzati; nello specifico saranno predisposti report contenenti:
  - IOCs, specifici per i sistemi gestiti dall'ASLNapoli 3 Sud ;
  - notizie di interesse per l'Amministrazione e con lo scopo di mantenere, l'Amministrazione allineata su possibili eventi di interesse, fintanto che questi non si traducano in una minaccia fattuale;
  - sintesi delle segnalazioni effettuate nel periodo di riferimento e la loro classificazione sia per tipologia che per serverity (mensile).
- **Intelligence -** la piattaforma è gestita da un team specialistico di intelligence che ha l'obiettivo di arricchire le informazioni e contestualizzarle rispetto al contesto operativo della Amministrazione;
- **Analisi / Prioritizzazione -** la piattaforma dispone di funzionalità atte a filtrare le informazioni in funzione delle necessità dell'ASL Napoli 3 Sud secondo meccanismi dinamici e continuativi che consentono di focalizzare l'attenzione sui fenomeni più rilevanti.

Feed di Threat Intelligence

I feed utilizzati per l'erogazione del servizio TI&VDF saranno gli outcome:

- di prodotti di Vendor di riferimento;
- di programmi di Bug Bounty;
- di analisi effettuate da ricercatori di sicurezza;
- del network Accenture costituito da tutti Centri di Competenza a livello Globale progressivamente acquisiti negli anni.

Tali Feed, contengono **informazioni affidabili, aggiornate e dettagliate** sulle vulnerabilità di sicurezza. Ove possibile, i feed provengono dalle **fonti primarie** dei dati di intelligence in modo da **ridurre la ridondanza** delle informazioni raccolte e **ottimizzarne l'utilizzo**.
Di seguito vengono rappresentate le **caratteristiche**, in termini di descrizione e informazioni fornite, dei **71 feed** utilizzati raggruppati per **Tipologia** provenienti anche dai Centri di Competenza delle società acquisite quali **Symantec e Context-IS**.

TIPOLOGIA - Vulnerability data feed	
Descrizione	Feed costituiti da informazioni sulle vulnerabi
Informazioni	Descrizione della vulnerabilità, CPE impattate,

Tabella 11- Vulnerability data feed

TIPOLOGIA - Vulnerability Intelligence Data Feed	
Descrizione	Feed costituiti da informazioni sulle vulnerabi
Informazioni	Descrizione della vulnerabilità, CPE impattate,

Tabella 12- Vulnerability Intelligence data feed

TIPOLOGIA - Threat Advisory Data Feed	
Descrizione	Bollettini riguardanti le minacce che impattan
Informazioni	Descrizione di minacce, informazioni di contes

Tabella 13- Threat Advisory data feed

TIPOLOGIA - Threat Intelligence Data Feed	
Descrizione	Feed riguardanti il panorama globale delle mi
Informazioni	Informazioni sulle minacce esistenti a livello g

Tabella 14- Threat Intelligence data feed

TIPOLOGIA - Threat Indicators Data Feed	
Descrizione	Feed costituiti da Indicatori di Compromission

Informazioni	IoC aggiornati relativi alle minacce di interesse

Tabella 15- Threat Indicators data feed

6.1.4 L1.S7 – Protezione degli end point

Il servizio di Protezione degli Endpoint rappresenta uno degli elementi chiave forniti dal Centro Servizi per garantire la sicurezza delle infrastrutture secondo quanto concordato l'ASL NA3 SUD, operando direttamente sui dispositivi in uso agli utenti e abilitando sia l'identificazione di anomalie di processo che le azioni di contenimento e reazione da implementare in caso di violazione.
Il servizio si potrà avvalere anche di strumenti tecnologici disponibili presso l'Amministrazione e di proprietà/licenza della stessa, messi a disposizione dall'Amministrazione al personale del RTI. Nello specifico, il servizio consente almeno di:

1. effettuare l'ispezione del traffico generato dalla postazione di lavoro;
2. effettuare un analisi real-time dei vari file presenti sulla postazione di lavoro;
3. controllare lo stato di compliance dei dispositivi rispetto a policy di sicurezza dell'Amministrazione dalla stessa ben definite.

6.1.5 L1.S9 – Formazione e Security Awareness

Il servizio "Formazione e Security awareness" è mirato a sensibilizzare il personale dell'Amministrazione, su svariati aspetti della sicurezza delle informazioni, incrementando il livello di consapevolezza dei dipendenti, innalzando il livello di sicurezza dell'organizzazione e l'efficacia in termini di protezione dei dati aziendali critici e dei dati personali. Lo scopo è quello di sviluppare negli utenti le competenze essenziali, le tecniche e i metodi fondamentali per prevenire il più possibile gli incidenti di sicurezza e reagire al meglio a fronte di eventuali problemi.
Il servizio verrà erogato mediante la messa a disposizione di figure professionali da parte del Fornitore coadiuvate dall'utilizzo della piattaforma Cyberguru. Il percorso include un subset di contenuti per ciascun modulo ed è destinato agli utenti che hanno necessità formative in ambito cyber security.
Nello specifico il percorso include
i seguenti contenuti : 36 contenuti del modulo di "Awareness" (erogati agli intervalli che le Parti concorderanno all'avvio delle attività) e 6 del modulo "Informativo". Non è previsto un limite di attacchi simulati, così da garantire un percorso modulare basato sul profilo comportamentale del singolo utente.

6.1.6 L1.S15 - Servizi Specialistici

Tale servizio prevede un supporto specialistico con l'obiettivo di fornire all'Azienda Sanitaria Locale Napoli 3 Sud supporto tecnico connesso al servizio di Security Operation Center, come di seguito descritto.

6.1.6.1 Servizi Specialistici a supporto dei servizi di sicurezza L1.S1 - Security Operation Center

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

- Supporto nell'integrazione con le log source identificate
- Supporto all'identificazione e realizzazione di nuovi Use Case a supporto del processo di detection al fine di migliorare continuamente la libreria di casi dedicati
- Supporto nell'integrazione di playbook per l'ottimizzazione dei processi di risposta ad eventi di sicurezza
- Supporto alla investigazione di possibili attacchi informatici o "data breach".

6.1.6.2 Servizi Specialistici a supporto dei servizi di sicurezza L1.S4 – Gestione Continua delle vulnerabilità

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 dall'ASL Napoli 3 Sud stesso e dai suoi team tecnici/operativi, che avranno l'onere di valutare la fattibilità e i tempi per loro competenza.

6.1.6.3 Servizi Specialistici a supporto dei servizi di sicurezza L1.S5 – Threat Intelligence

I Servizi saranno forniti all'Amministrazione per un supporto tecnico connesso all'attivazione e alla delivery dei servizi da remoto oggetto di fornitura.

6.1.6.4 Servizi Specialistici a supporto dei servizi di sicurezza L1.S7 – Protezione degli end point

Nell'ambito dei Servizi Specialistici a supporto dei servizi di Protezione degli End Point il RTI, nel rispetto della totalità delle giornate l'anno indicate nel Piano dei Fabbisogni ed in considerazione degli altri servizi specialistici richiesti, supporterà l'Amministrazione in fase di avvio per le attività di setup, e durante tutto il periodo contrattuale, nel mantenimento del livello e delle policy di sicurezza stabilite dall'Amministrazione stessa, anche attraverso il supporto nell'individuazione e pianificazione delle attività necessarie per fronteggiare le evoluzioni del panorama delle minacce informatiche e nella produzione della reportistica necessaria alla gestione della protezione degli endpoint.

6.2 Utenza interessata / coinvolta

Personale dell'Azienda Sanitaria Locale Napoli 3 Sud.

6.3 Eventuali riferimenti / vincoli normativi

N.A.

7 PIANO DI PROGETTO

7.1 Cronoprogramma

L'erogazione dei servizi avrà durata **24 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:

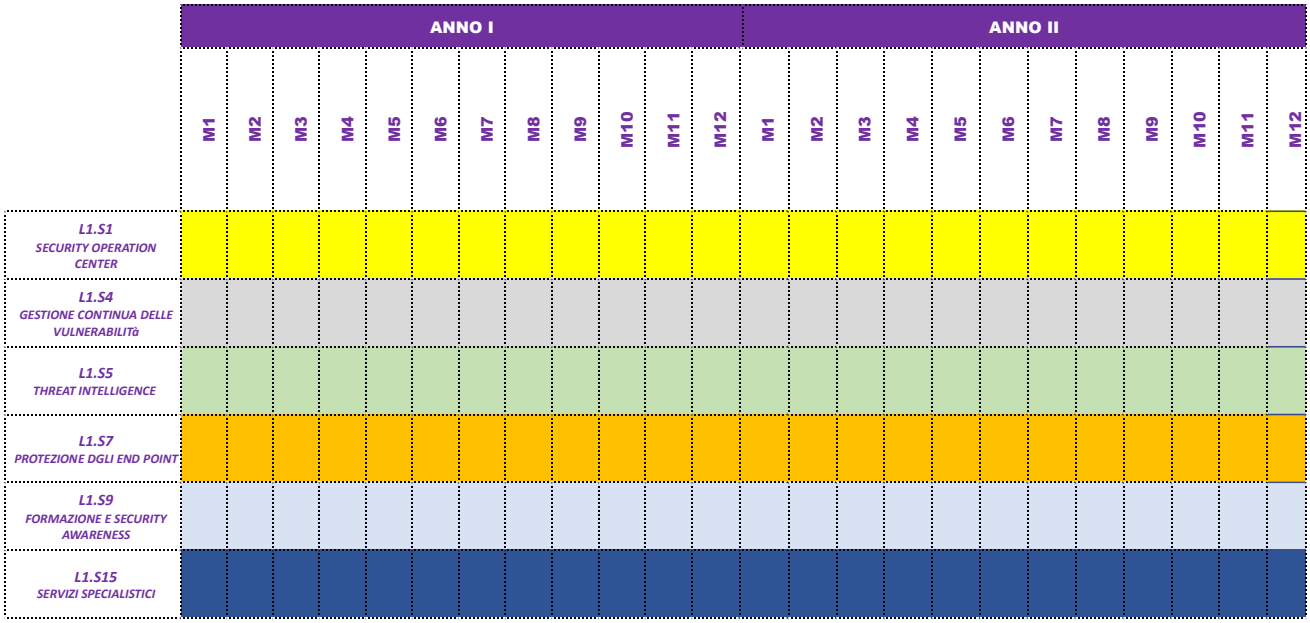

Tabella 16- Cronoprogramma

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 24 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 17- 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.S4 – Gestione Continua delle vulnerabilità, L1.S5 – Threat Intelligence, L1.S9 – Formazione e security awareness, L1.S15 – Servizi Specialistici	**Accenture**	**50%**
L1.S7– Protezione degli end point, L1.S15 – Servizi Specialistici	**Fastweb**	**50%**
L1.S15 – Servizi Specialistici	**Fincantieri**	**50%**
L1.S15 – Servizi Specialistici	**Deas**	**50%**

Tabella 18- Modalità di ricorso al Subappalto da parte del Fornitore

8 DIMENSIONAMENTO ECONOMICO

8.1 Modalità di erogazione dei Servizi

Di seguito sono riportate 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 TOTALE
L1.S1	Device Equivalent/ anno	Da remoto	Canone	Mensile	€ 218,4	500/Anno	€ 218.400,00
L1.S4	IP/anno	Da remoto	Canone	Mensile	€ 13,8	500/Anno	€ 13.800,00
L1.S5	NumeroData feed/anno	Da remoto	Canone	Mensile	€ 200,00	70/Anno	€ 28.000,00
L1.S7	Nodi/anno	Da remoto	Canone	Mensile	€ 12,863	3.500/Anno	€ 90.041,00
L1.S9	Giorni persona del team ottimale /anno	Da remote/on site	Progettuale – a corpo	Mensile	€ 247,52	373/Anno	€ 184.649,92
L1.S15 per L1.S1	Giorni persona del team ottimale	Da remoto /on site	Progettuale a corpo	Mensile	244,00 €	174/Anno	€ 84.912,00
L1.S15 per L1.S4	Giorni persona del team ottimale	Da remoto /on site	Progettuale a corpo	Mensile	244,00 €	209/Anno	€ 101.992,00
L1.S15 per L1.S5	Giorni persona del team ottimale	Da remoto /on site	Progettuale a corpo	Mensile	244,00 €	210/Anno	€ 102.480,00
L1.S15 per L1.S7	Giorni persona del team ottimale	Da remoto /on site	Progettuale a corpo	Mensile	244,00 €	2.003 1° Anno/795 2° Anno	€ 682.712,00

Tabella 19- Quadro economico di riferimento

L'importo complessivo dell'ordinativo di fornitura ammonta a **€ 1.506.986,92 iva esclusa.**

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

Per il piano di presa in carico si rimanda all'allegato Piano 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).