ARNAS G.Brotzu
Azienda di Rilievo Nazionale
ed Alta Specializzazione

D eliberazione n. 1670

Adottata dal Direttore Generale in data 18.12.2023

Oggetto: Adesione "Accordo Quadro per l'affidamento di servizi di sicurezza da remoto e controllo per le pubbliche amministrazioni - Lotto 1", stipulato da Consip S.p.A., da destinare alla SC Servizio Informatico e Tecnologie Sanitarie. Ditta Accenture S.p.A. Spesa complessiva annuale € 124.437,00 oltre Iva di Legge. Codice Cig A03DC883D7.

PDEL/2023/1803 MP

Pubblicata all'Albo Pretorio dell'Azienda a partire da 18.12.2023 per 15 giorni consecutivi e posta a disposizione per la consultazione.

Il Direttore Generale Dott.ssa Agnese Foddis

Coadiuvato
dal Direttore Amministrativo Dott. Ennio Filigheddu
dal Direttore Sanitario Dott. Raimondo Pinna

S.C. Affari Generali
Firmato digitalmente da PERRA LUISANNA

La presente Deliberazione prevede un impegno di spesa a carico dell'ARNAS

SI □ NO□

Su proposta della SC Acquisizione Beni, Servizi ed Economato;

Vista la deliberazione n. 1500 del 12.12.2022, con la quale è stata conferita delega di funzioni in favore del Dott. Davide Massacci, Responsabile del Settore "Area acquisti di beni sanitari e servizi/liquidazione fatture";

Atteso che con nota, agli atti del Servizio, il Direttore della SC Servizio Informatico e Tecnologie Sanitarie ha richiesto l'attivazione dell'Accordo Quadro per l'affidamento di servizi di sicurezza da remoto e controllo per le pubbliche amministrazioni - Lotto 1, stipulato da Consip S.p.A.;

Preso atto che Consip S.p.A, 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;

Considerato che in data 24.05.2022 Consip S.p.A. ha aggiudicato, in favore di varie Ditte, l'Accordo Quadro per l'affidamento di servizi di sicurezza da remoto e controllo per le pubbliche amministrazioni;

Dato atto che in data 07.12.2023 il Direttore della SC Servizio Informatico e Tecnologie Sanitarie ha trasmesso, a mezzo pec, al fornitore aggiudicatario dell'accordo quadro, e contestualmente alla Consip S.p.A., il "Piano dei Fabbisogni" contenente i requisiti, i servizi, le caratteristiche qualitative, i dimensionamenti, la descrizione del contesto tecnologico ed applicativo e la descrizione delle attività dimensionate;

Segue delibera n. 1670 del 18.12.2023

Preso atto del contenuto “Piano Operativo” trasmesso, a mezzo pec, dall’Operatore Economico Accenture S.p.A. sulla base del “Piano dei Fabbisogni”, dal quale si evince che il valore complessivo annuale della fornitura ammonta ad € 124.437,00 oltre Iva di Legge (All. “A” fg. 24);

Ritenuto pertanto di dover aderire, all’Accordo Quadro per l'affidamento di servizi di sicurezza da remoto e controllo per le pubbliche amministrazioni - Lotto 1", stipulato da Consip S.p.A. con l'Operatore Economico Accenture S.p.A., per una spesa complessiva annuale pari a € 124.437,00 oltre Iva di Legge, come di seguito indicato:

Descrizione/ ID SERVIZIO	Quantità annuale	Importo Unitario Iva esclusa	Importo Complessivo Iva esclusa	Piano dei Conti	Centro di Costo
L1.S1 – Security Operation Center	150	€ 218,40	€ 32.760,00	A506010108	100031
L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza	225	€ 13,80	€ 3.105,00		
L1.S15 – Servizi Professionali	363	€ 244,00	€ 88.572,00		

Atteso che ai sensi dell'art. n. 4 della Legge n. 241/90 le pubbliche amministrazioni sono tenute a determinare per ciascun tipo di procedimento relativo ad atti di loro competenza l'unità organizzativa responsabile dell'istruttoria e di ogni altro adempimento procedimentale, nonché dell'adozione del provvedimento finale;

Atteso altresì che ai sensi dell’art. n. 5 della Legge n. 241/90 e dell’art. n. 31 del D. Lgs. n. 50/2016 si deve procedere alla nomina del Responsabile del Procedimento;

Ritenuto altresì di dover individuare quale Direttore dell’esecuzione del contratto la Sig.ra Margherita Ruiu che possiede i requisiti per svolgere tale incarico;

Dato atto che non sussistono conflitti di interesse con la Ditta assegnataria della fornitura;

Visto il D. Lgs. n. 50/16;

Con il parere favorevole del Direttore Amministrativo e del Direttore Sanitario;

D E L I B E R A

1. di aderire, all’Accordo Quadro per l'affidamento di servizi di sicurezza da remoto e controllo per le pubbliche amministrazioni - Lotto 1", stipulato da Consip S.p.A. con l'Operatore Economico Accenture S.p.A., per una spesa complessiva annuale pari a € 124.437,00 oltre Iva di Legge, come di seguito indicato:

ARNAS G.Brotzu
Azienda di Rilievo Nazionale
ed Alta Specializzazione

Segue delibera n. 1670 del 18.12.2023

Descrizione/ ID SERVIZIO	Quantità annuale	Importo Unitario Iva esclusa	Importo Complessivo Iva esclusa	Piano dei Conti	Centro di Costo
L1.S1 – Security Operation Center	150	€ 218,40	€ 32.760,00	A506010108	100031
L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza	225	€ 13,80	€ 3.105,00		
L1.S15 – Servizi Professionali	363	€ 244,00	€ 88.572,00		

2. di individuare l'Unità Organizzativa responsabile della istruttoria e di ogni altro adempimento procedimentale, nonché dell'adozione del provvedimento finale, nella S.C. Acquisizione Beni, Servizi ed Economato;
3. di nominare, ai sensi dell'art. 31 del D. Lgs. 50/2016, quale Responsabile del Procedimento, il Dott. Davide Massacci titolare della Posizione Organizzativa presso la S.C. A.B.S.E. relativa al Settore di Acquisizione Beni Sanitari e Servizi/Liquidazione Fatture, in possesso di specifiche competenze;
4. di individuare quale Direttore dell'esecuzione del contratto la Sig.ra Margherita Ruiu, che possiede i requisiti per svolgere tale incarico;
5. di dare atto che l'esecuzione del relativo contratto avrà inizio contestualmente alla pubblicazione del presente atto, ai sensi dell'art. 32, comma 13 del D. Lgs. n. 50/2016;
6. di autorizzare la S.C. Economico Finanziario all'emissione dei relativi ordini di pagamento, a seguito di presentazione dei giustificativi recanti l'attestazione di regolarità della fornitura da parte degli Uffici competenti.

Il Direttore Generale
Dott.ssa Agnese Foddis
FODDIS AGNESE Firmato digitalmente da FODDIS AGNESE

Il Direttore Amministrativo
Dott. Ennio Filigheddu

FILIGHEDDU ENNIO Firmato digitalmente da FILIGHEDDU ENNIO
Data: 2023.12.15 13:54:52 +01'00'

Il Direttore Sanitario
Dott. Raimondo Pinna

PINNA RAIMONDO Firmato digitalmente da PINNA RAIMONDO
Data: 2023.12.15 18:21:22 +01'00'

SC Acquisizione Beni, Servizi ed Economato
Il Delegato Responsabile SC Acquisizione Beni, Servizi ed Economato Dott. D. Massacci
Ass. Amm.vo Sig.ra Pisu Monica

MONICA PISU Firmato digitalmente da MONICA PISU
Data: 2023.12.14 15:17:09 +01'00'

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	13/12/2023	Prima emissione	RTI

Tabella 1 - Registro delle versioni

Sommario

Indice delle tabelle

Indice delle figure

1 INTRODUZIONE

L'ARNAS (Azienda di Rilievo Nazionale ed Alta Specializzazione) "G. Brotzu" (di seguito anche "Amministrazione") con l'obiettivo di andare in continuità con la gara SPC Cloud (ID SIGEF 1403) e rafforzare la propria postura di sicurezza, intende avvalersi del presente Accordo Quadro bandito da Consip, ***AQ2296 per l'affidamento di servizi di sicurezza da remoto e controllo per le pubbliche amministrazioni – Lotto 1***, per acquisire i servizi a catalogo messi a disposizione che verranno elencati e dettagliati nei paragrafi seguenti.

1.1 Scopo

L'intervento si propone di consolidare la strategia di cybersecurity finora attuata dall'Amministrazione con l'obiettivo di porre le basi per una governance della sicurezza allargata e rafforzare la resilienza al rischio cyber sul perimetro dell'Amministrazione

I servizi di seguito elencati, come descritti all'interno dei paragrafi successivi, costituiscono l'oggetto del presente Piano Operativo

- **L1.S1 SECURITY OPERATION CENTER**
- **L1.S4 GESTIONE CONTINUA DELLE VULNERABILITA' DI SICUREZZA**
- **L1.S15 SERVIZI SPECIALISTICI**

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.

Il 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 dal Framework, al fine di illustrare come tali servizi siano funzionali a ciascuna area del Framework.

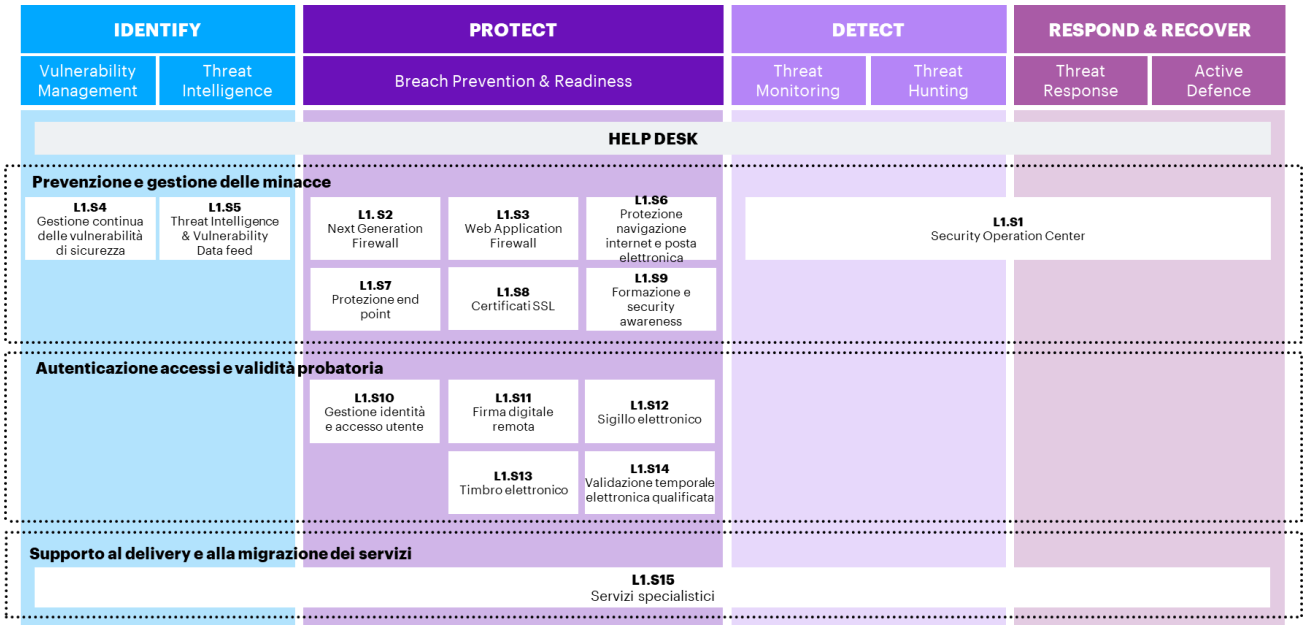

Figura 1 – Mappatura Servizi di Sicurezza e Framework NIST

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 con i 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, la **ARNAS G. Brotzu**, 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, **l'Amministrazione**, ha individuato il Raggruppamento Temporaneo di Imprese (RTI o Fornitore) 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'Amministrazione 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) [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 "2296_Lotto 1_Sicurezza da Remoto_AO BROTZU Piano dei fabbisogni_v.1.1_" inviato in data 07/12/2023 (inoltrato a Consip nella stessa data)

Tabella 3 - 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 4 - 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
CVSS	Common Vulnerability Scoring System
DA	Documenti Applicabili
DDoS	Distributed Denial-of-Service
DR	Disaster Recovery
DSI	Direzione Sistemi Informativi
HSM	Hardware Security Module
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
PIN	Personal Identification Number
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
WNEP	Web Navigation and Email Protection

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:

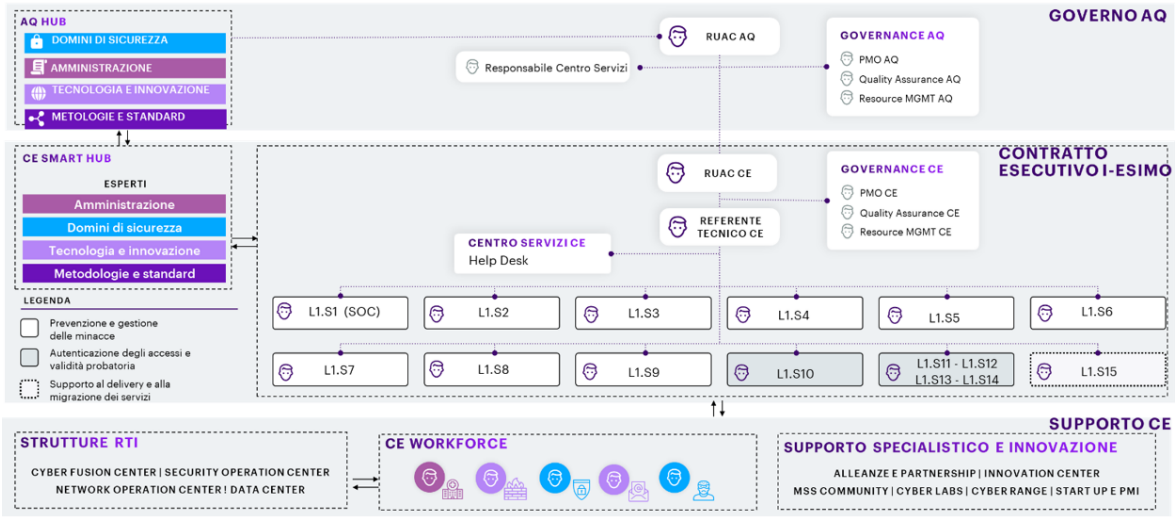

Figura 2 - Organizzazione dell'AQ proposta dal RTI

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 secondo la ripartizione seguente:

SERVIZIO	ACCENTURE	FASTWEB	FINCANTIERI	DEAS
L1.S1 – Security Operation Center		X		
L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza		X		
L1.S15 – Servizi Specialistici	X	X	X	X
TOTALE (%)	0,20%	99,41%	0,20%	0,20%
TOTALE (€)	244,00 €	123.705,00 €	244,00 €	244,00 €

Tabella 6 - 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 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 saranno erogate come di seguito indicato:

- per i servizi erogati da remoto: attraverso i Centri Servizi del Fornitore;
- per i servizi on-site (in special modo per parte dei servizi specialistici e di formazione): presso le sedi dell'Amministrazione ove specificato dall'Amministrazione stessa. In alternativa, presso la Sede del Fornitore.

5 AMBITI E SERVIZI

5.1 Ambiti di intervento

Di seguito viene fornito un dettaglio degli ambiti di intervento per i servizi richiesti tra quelli elencati al par. 1.2.

Servizio di Security Operation Center L1.S1

Il RTI garantisce 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.

Servizio di Gestione Continua delle Vulnerabilità di Sicurezza L1.S4

Questo servizio consentirà, al personale della Amministrazione, tramite un processo automatico di assesment delle vulnerabilità, di ottenere una fotografia precisa del livello e gravità del rischio a cui, in quel momento, sono esposti i propri sistemi informatici. Il servizio si avvarrà dell'utilizzo di uno scanner che produrrà un report con le specifiche indicazioni di rischio relative alle vulnerabilità rilevate. Tra le funzioni del servizio si prevede: la capacità di scansione nella complessa infrastruttura dell'Amministrazione (come descritta nel PDF); la capacità di individuare i livelli di gravità e classificazione CVSS; la possibilità per l'Amministrazione di disporre di un report relativo alla valutazione delle vulnerabilità riscontrate; un'attività a supporto per la risoluzione o mitigazione di quanto rilevato.

Servizi Specialistici L1.S15

I servizi di Supporto Specialistico hanno l'obiettivo di fornire all'Ammnistrazione il supporto tecnico specializzato per un miglioramento della sicurezza in ambito infrastrutturale connesso ai servizi oggetto del presente Piano Operativo, attraverso l'utilizzo di specifiche figure professionali messe a disposizione dal Fornitore, come meglio dettagliato in seguito.

5.2 Servizi richiesti

SERVIZIO	FASCIA	IMPORTO I ANNO	IMPORTO II ANNO	IMPORTO III ANNO	IMPORTO IV ANNO
L1.S1 – Security Operation Center	Fino a 6000 EPS	32.760,00 €/150 (device equivalenti)	-	-	-
L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza	Maggiore di 200 IP	3.105,00 €/225 (IP)	-	-	-
L1.S15 – Servizi Specialistici a supporto di L1.S1 – Security Operation Center	gg/p Team ottimale	86.376,00 €/354 (gg/p Team ottimale)	-	-	-
L1.S15 – Servizi Specialistici a supporto di L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza	gg/p Team ottimale	2.196,00 €/9 (gg/p Team ottimale)	-	-	-

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		

W

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

Di seguito i servizi proposti in linea con le esigenze espresse dalla **ARNAS G. Brotzu**.

6.1 Descrizione dei servizi richiesti

6.1.1 L1.S1 – Security Operation Center

Il servizio prevede di implementare, attraverso gli 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 baserà sui dati raccolti e correlati dal SIEM basato su tecnologia IBM QRadar. Sarà 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 Case Management assistito (raccolta degli incidenti sulla base di filtri rilevanti, gestione assistita degli incidenti, arricchimento automatico di incidenti con informazioni di interesse, correlazione tra incidenti diversi e coordinamento delle azioni di risposta tra team distribuiti).

Il servizio SOC verrà erogato in modalità remota dal Centro Servizi (di seguito "CS") preposto dal RTI e agirà 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.

Il servizio sarà configurato in modo tale che anche il personale autorizzato dal Committente possa avere accesso alle informazioni ed agli alert prodotti dal SOC e dal SIEM, secondo le modalità previste dalla Capitolato Tecnico e dalla risposta tecnica di AQ.

Di seguito si elencano quelli che saranno i prerequisiti al servizio:

- Configurazione delle sorgenti di log (eventi di sicurezza) e di rete a carico del team di competenza dell'Amministrazione, per la lettura e/o invio degli eventi utili al completamento del servizio, verso il Centro Servizi che costituisce la struttura unica abilitante per l'erogazione;
- Procedure di security incident management, escalation, Crisis Management.

Modello Operativo

Il modello operativo prevede il monitoraggio continuo delle informazioni prodotte dalle sorgenti di log (eventi di sicurezza) identificati come perimetro di monitoraggio ed in uso presso il data center dell'Amministrazione.

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 per l'auditing sugli eventi raccolti;
- Identificazione e comunicazione verso l'Amministrazione 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'Amministrazione ed archiviate;
- Valutazione post incidente, in modo da individuare possibili azioni migliorative da implementare sui sistemi di sicurezza dell'Amministrazione aumentando l'efficacia del SOC team.

Modalità di erogazione

Il modello di erogazione si baserà 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 previsto per tale Convenzione. 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'Amministrazione, 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'Amministrazione per segnalare/supportare azioni di remediation;
- verifica di chiusura del caso segnalato, da parte del team operativo dell'Amministrazione.

6.1.2 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 e personale, con rendicontazione delle tecniche, dirette od articolate (OWASP, MI-TRE 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; inoltre, l'integrazione con le piattaforme di Cyber Threat Intelligence (es. TIS e iDefense) rende più profonda la ricerca di nuove vulnerabilità sulla base delle evidenze predittive prodotte degli analisti (artifact, IoC, IoA, etc.) anche se non note alla community (es. CVE);
- 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'Amministrazioneche 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:

- Una 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.

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, manlevando il Fornitore nel caso in cui l'esecuzione dei test approvati provochi degli impatti e/o danni, eccetto nei casi di negligenza o dolo. Resta inteso che il Fornitore segnalerà all'Amministrazione, 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 tale autorizzazione non venga fornita il Fornitore non potrà procedere. Fermo restando quanto sopra, l'Amministrazione si impegna a verificare che siano resi al Fornitore tutti i consensi, le autorizzazioni e le manleve suddette e necessarie.

6.1.3 L1.S15 – Servizi Specialistici

Di seguito si riportano i progetti a corpo, identificati come Servizi Specialistici, ad integrazione di ciascuno dei servizi selezionati dalla **ARNAS G. Brotzu**, tra quelli previsti dall'Accordo Quadro.

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, finalizzati al controllo imparziale della corretta esecuzione del servizio, nel supportare ed evolvere il processo di monitoraggio e gestione degli incidenti di sicurezza. Gli obiettivi indicati per tale servizio specialistico aggiuntivo sono i seguenti e saranno oggetto di pianificazione:

- Supporto nell'integrazione con la piattaforma di log collection in essere presso l'Amministrazione;
- Supporto nella "remediation" degli incidenti di sicurezza;
- Identificazione e realizzazione di nuovi Use Case a supporto del processo di detection al fine di migliorare continuamente la libreria di casi dedicati;
- 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".

Il servizio sarà erogato sia in modalità da remoto che on-site.

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 coinvolte principalmente nell'integrazione del servizio e nell'assistenza all'Amministrazione nella valutazione delle vulnerabilità al fine di identificare un piano di rientro in base alle priorità dettate dalla PA stessa e dai suoi team tecnici/operativi, che avranno l'onere di valutare la fattibilità e i tempi per loro competenza.

6.2 Utenza interessata / coinvolta

Referenti dell'Amministrazione della **ARNAS G. Brotzu**.

6.3 Eventuali riferimenti / vincoli normativi

N.A.

7 PIANO DI PROGETTO

7.1 Cronoprogramma

L'erogazione dei servizi avrà durata 12 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											
	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
Servizio L1.S1												
Servizio L1.S4												
Servizio L1.S9												
Servizio L1.S15												

Tabella 10 – Cronoprogramma

7.2 Data di Attivazione e Durata del Servizio

La durata del servizio è pari a 12 mesi, come meglio dettagliato di seguito.
Il contratto esecutivo dispiegherà i suoi effetti dalla data di stipula e avrà una durata di 12 mesi decorrenti 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 11 - 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.S15 – Servizi Specialistici	**Accenture**	**50 %**
L1.S1 – Security Operation Center **L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza** **L1.S9 – Formazione e Security Awareness** **L1.S15 – Servizi Specialistici**	**Fastweb**	**50 %**
L1.S15 – Servizi Specialistici	**Fincantieri**	**50 %**
L1.S15 – Servizi Specialistici	**Deas**	**50 %**

Tabella 12 - 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	VALORE ECONOMICO (totale su 12 mesi)
L1.S1 – Security Operation Center	Device Equivalente/anno	Da remoto	Canone	Mensile	218,400 €	150	32.760,00 €
L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza	Numero IP/anno	Da remoto	Canone	Mensile	13,80 €	225	3.105,00 €
L1.S15 – Servizi Specialistici per L1.S1	Giorni persona del team ottimale	Da remoto /on site	Progettuale a corpo	Mensile	244,00 €	354	69.052,00 €
L1.S15 – Servizi Specialistici per L1.S4	Giorni persona del team ottimale	Da remoto /on site	Progettuale a corpo	Mensile	244,00 €	9	2.196,00 €

Tabella 13 - Quadro economico di riferimento

L'importo complessivo dell'ordinativo di fornitura ammonta a **124.437,00 € (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

Una prima pianificazione delle attività di presa in carico è riportata nell'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 del CE. Per quanto concerne il Responsabile del CE, il 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).