REGIONE CAMPANIA
AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE E DI ALTA SPECIALIZZAZIONE
"SANT'ANNA E SAN SEBASTIANO"
CASERTA

Deliberazione del Direttore Generale N. 22 del 26/08/2025

Proponente: Il Direttore UOC SERVIZI INFORMATICI AZIENDALI

Oggetto: FONDI PNRR – M6.C2 - INVESTIMENTO 1.1.1 - DIGITALIZZAZIONE DEA I E II LIVELLO: ACCORDO QUADRO PER L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI – ID 2296 – LOTTO 1

PUBBLICAZIONE
In pubblicazione dal 27/08/2025 e per il periodo prescritto dalla vigente normativa in materia (art.8 D.Lgs 14/2013, n.33 e smi)

ESECUTIVITA'
Atto immediatamente esecutivo

TRASMISSIONE
La trasmissione di copia della presente Deliberazione è effettuata al Collegio Sindacale e ai destinatari indicati nell'atto nelle modalità previste dalla normativa vigente. L'inoltro alle UU. OO. aziendali avverrà in forma digitale ai sensi degli artt. 22 e 45 D.gs. n° 82/2005 e s.m.i. e secondo il regolamento aziendale in materia.

UOC AFFARI GENERALI
Direttore Eduardo Chianese

ELENCO FIRMATARI

Gennaro Volpe - DIREZIONE GENERALE

Eduardo Chianese - UOC GESTIONE ECONOMICO FINANZIARIA

Giovanni Sferragatta - UOC SERVIZI INFORMATICI AZIENDALI

Vincenzo Giordano - DIREZIONE SANITARIA

Chiara Di Biase - DIREZIONE AMMINISTRATIVA

Per delega del Direttore della UOC AFFARI GENERALI, Dr. Mauro Ottaiano

Oggetto: FONDI PNRR – M6.C2 - INVESTIMENTO 1.1.1 - DIGITALIZZAZIONE DEA I E II LIVELLO: ACCORDO QUADRO PER L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI – ID 2296 – LOTTO 1

Direttore UOC SERVIZI INFORMATICI AZIENDALI

A conclusione di specifica istruttoria, descritta nella narrazione che segue e i cui atti sono custoditi presso la struttura proponente, rappresenta che ricorrono le condizioni e i presupposti giuridico-amministrativi per l'adozione del presente provvedimento, ai sensi dell'art. 2 della Legge n. 241/1990 e s.m.i. e, in qualità di responsabile del procedimento, dichiara l'insussistenza del conflitto di interessi, allo stato attuale, ai sensi dell'art. 6 bis della legge 241/90;

Premesso

- che il Piano Nazionale di Ripresa e Resilienza prevede fondi per l'ammodernamento tecnologico delle Aziende Sanitarie;
- che con nota prot. n. 4262/u del 07/02/2022 quest'Azienda ha trasmesso, tra l'altro, alla Giunta Regionale della Campania Direzione Generale per la Tutela della Salute e Coordinamento del Sistema Sanitario Regionale, il nominativo del Direttore U.O.C. Servizi Informatici Aziendali, Dr. Giovanni Sferragatta, quale referente aziendale e compilatore delle schede sulla piattaforma AGENAS, relativamente all'ammodernamento parco tecnologico da finanziare con il PNRR;
- che con nota prot. n. 86579 del 16/02/2022, la Giunta Regionale della Campania Direzione Generale per la Tutela della Salute e Coordinamento del Sistema Sanitario Regionale ha comunicato a quest'Azienda che le apparecchiature dovranno essere acquistate con gare centralizzate Consip e non sarà possibile avviare alcuna procedura aziendale, neanche di adesione ad Accordi Quadro Consip già attivi, se non preventivamente autorizzate dalla Direzione Regionale;

Rilevato

- che con DGRC n. 195 del 26/04/2022 è stato preso atto del D.M. 20/01/2022 relativo alla ripartizione programmatica delle risorse alle Regioni per i progetti del PNRR e del piano degli investimenti complementari previsti dalla misura M6C2 I1.1.1;
- che con DGRC n. 249 del 24/05/2022 è stato approvato il Piano Operativo Regionale definitivo di ciascun investimento e le schede dei singoli interventi dei fondi PNRR, confermando per l'AORN Caserta interventi di ammodernamento del parco tecnologico Aziendale e digitalizzazione DEA tra i cui interventi è previsto:
    - 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 azioni di contenimento, ripristino e prevenzione futura.

Considerato

- che in merito agli interventi a valere su Fondi PNRR, la centrale di committenza Consip ha provveduto a stipulare gli Accordi Quadro, tra cui, l'iniziativa *"ID 2296 - "Cybersecurity 2" - Fornitura di servizi di sicurezza da remoto, di compliance e controllo per le PA"* così suddivisa:
  - Lotto 1 - Servizi di Sicurezza da Remoto
  - Lotto 2 - Servizi di Compliance e Controllo
- che i servizi in argomento sono finanziati con contributo di cui alla DGR 249/2022 del 24 maggio 2022 recante ad oggetto DGR 195/2022 "Piano Nazionale di Ripresa e Resilienza PNRR - missione 6 Salute – Presa d'atto del Contratto istituzionale di sviluppo ai sensi del DM 20 gennaio 2022;
- che per supportare tale percorso, l'AORN Sant'Anna e San Sebastiano intende avvalersi dell'Accordo Quadro *"ID 2296 - "Cybersecurity 2" - Fornitura di servizi di sicurezza da remoto, di compliance e controllo per le PA"* Lotto 1 assegnato alla RTI costituito da:
  - Accenture S.p.A.;
  - Fincantieri Nextech S.p.A.;
  - Fasteweb S.p.A.;
  - Deas, Difesa e Analisi Sistemi S.p.A.;

  così come indicato nel piano dei fabbisogni predisposto dal Direttore della UOC Servizi Informatici Aziendali, in copia allegato;

Visto

- che il Direttore della U.O.C. Servizi Informatici Aziendali, nominato RUP con nota prot. 31631 del 26/10/2024, ha dato parere favorevole al Piano Operativo, in copia allegato;
- che la spesa così come derivante dal Piano Operativo è di € 968.061,60 oltre IVA a valere sulle risorse del PNRR;

Ritenuto

- di procedere alla formalizzazione dell'adesione relativa al *Piano Nazionale di Ripresa e Resilienza - missione 6 - componente 2 investimento 1.1 sub-investimento 1.1 "Ammodernamento del parco tecnologico e digitale ospedaliero (Digitalizzazione DEA I e II)"* mediante la sottoscrizione dei documenti contrattuali e la contestuale adozione del presente provvedimento

Attestata

la conformità del presente atto alle norme sul trattamento dei dati di cui al D.lgs. 196/2003, così come integrato con le modifiche prodotte dal D.lgs. 101/2018 per l'adeguamento della normativa nazionale al Regolamento UE 2016/679 (GDPR) e dalle successive introduzioni previste dalla legge 27 dicembre 2019 n. 160, che contiene principi e prescrizioni per il trattamento dei dati personali, anche con riferimento alla loro "diffusione", e dichiarato di aver valutato la rispondenza del testo, compreso gli eventuali allegati, destinato alla diffusione per il mezzo dell'Albo Pretorio alle suddette prescrizioni e ne dispone la pubblicazione nei modi di legge;

PROPONE

1. di procedere alla formalizzazione dell'adesione relativa al *Piano Nazionale di Ripresa e Resilienza - missione 6 - componente 2 investimento 1.1 sub-investimento 1.1 "Ammodernamento del parco tecnologico e digitale ospedaliero (Digitalizzazione DEA I e II)"* mediante l'adozione del presente provvedimento;
2. di aderire all'Accordo Quadro Consip "*ID 2296 - "Cybersecurity 2" - Fornitura di servizi di sicurezza da remoto, di compliance e controllo per le PA - Lotto 1"* e, per gli effetti, di procedere all'affidamento definitivo della fornitura di servizi di monitoraggio e alerting degli eventi/minacce di sicurezza;
3. di imputare il costo complessivo di € 1.181.035,15, iva inclusa al 22%, sul C.E. 1010103010 – "Software proprietà licenza d'uso tempo indeterminato" del corrente bilancio 2025;
4. di ascrivere la spesa complessiva pari ad € 1.181.035,15, iva inclusa al 22%, sui fondi PNRR previsti dalla misura M6C2 I1.1.1 – assegnati a quest'Azienda;
5. di precisare che al finanziamento di cui trattasi è stato assegnato il CUP n. C29E22000000006;
6. di dare atto che il RUP è il Dr. Giovanni Sferragatta, Direttore U.O.C. Servizi Informatici Aziendali di questa A.O.R.N.;
7. di nominare DEC l'Ing. Roberto Villani, collaboratore tecnico professionale informatico presso la UOC Servizi Informatici Aziendali di questa A.O.R.N.;
8. di trasmettere copia del presente atto al Collegio Sindacale, ai sensi di legge, nonché alle UU.OO.CC. Gestione Economico–Finanziaria, Provveditorato ed Economato e Programmazione e Controllo di Gestione ed alla Direzione Generale per la Tutela della Salute ed il Coordinamento del Sistema Sanitario Regionale della Regione Campania;
9. di rendere lo stesso immediatamente eseguibile, al fine di porre in essere le attività delineate nel progetto di cui trattasi.

IL DIRETTORE U.O.C. S.I.A.
Dr. Giovanni Sferragatta

(f.to Digitalmente)

IL DIRETTORE GENERALE
Dr. Gennaro Volpe
individuato con D.G.R.C. n. 591 del 06/08/2025
immesso nelle funzioni con D.P.G.R.C. n. 109 del 08/08/2025

Vista la proposta di deliberazione che precede, a firma del Direttore UOC Servizi Informatici Aziendali Dr. Giovanni Sferragatta;

Acquisiti i pareri favorevoli del Direttore Sanitario e del Direttore Amministrativo sotto riportati:
Il Direttore Sanitario Dr. Vincenzo Giordano (f.to digitalmente)

Il Direttore Amministrativo Avv. Chiara Di Biase (f.to digitalmente)

DELIBERA

per le causali in premessa, che qui si intendono integralmente richiamate e trascritte, di prendere atto della proposta di deliberazione che precede e, per l'effetto:

di procedere alla formalizzazione dell'adesione relativa al *Piano Nazionale di Ripresa e Resilienza - missione 6 - componente 2 investimento 1.1 sub-investimento 1.1 "Ammodernamento del parco tecnologico e digitale ospedaliero (Digitalizzazione DEA I e II)"* mediante l'adozione del presente provvedimento;

di aderire all'Accordo Quadro Consip *"ID 2296 - "Cybersecurity 2" - Fornitura di servizi di sicurezza da remoto, di compliance e controllo per le PA - Lotto 1"* e, per gli effetti, di procedere all'affidamento definitivo della fornitura di servizi di monitoraggio e alerting degli eventi/minacce di sicurezza;

di imputare il costo complessivo di € 1.181.035,15, iva inclusa al 22%, sul C.E. 1010103010 – "Software proprietà licenza d'uso tempo indeterminato" del corrente bilancio 2025;

di ascrivere la spesa complessiva pari ad € 1.181.035,15, iva inclusa al 22%, sui fondi PNRR previsti dalla misura M6C2 I1.1.1 – assegnati a quest'Azienda;

di precisare che al finanziamento di cui trattasi è stato assegnato il CUP n. C29E22000000006;

di dare atto che il RUP è il Dr. Giovanni Sferragatta, Direttore U.O.C. Servizi Informatici Aziendali di questa A.O.R.N.;

di nominare DEC l'Ing. Roberto Villani, collaboratore tecnico professionale informatico presso la UOC Servizi Informatici Aziendali di questa A.O.R.N.;

di trasmettere copia del presente atto al Collegio Sindacale, ai sensi di legge, nonché alle UU.OO.CC. Gestione Economico–Finanziaria, Provveditorato ed Economato e Programmazione e Controllo di Gestione ed alla Direzione Generale per la Tutela della Salute ed il Coordinamento del Sistema Sanitario Regionale della Regione Campania;

di rendere lo stesso immediatamente eseguibile, al fine di porre in essere le attività delineate nel progetto di cui trattasi.

Il Direttore Generale
Dr. Gennaro Volpe
(f.to digitalmente)

ATTESTAZIONE DI VERIFICA E REGISTRAZIONE CONTABILE
(per le proposte che determinano un costo per l'AORN – VEDI ALLEGATO)

ACCORDO QUADRO PER L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI – ID 2296 – **LOTTO 1**

PIANO DEI FABBISOGNI

INDICE

1. DATI ANAGRAFICI DELL'AMMINISTRAZIONE

Ragione sociale Amministrazione:	Azienda Ospedaliera Sant'Anna e San Sebastiano di Caserta
Indirizzo	Via Ferdinando Palasciano
CAP	81100
Comune	CASERTA
Provincia	CE
Regione	CAMPANIA
Codice Fiscale	2201130610
Codice IPA	2201130610
Indirizzo mail	direzionegenerale@ospedale.caserta.it
PEC	direzionegenerale@ospedalecasertapec.it

Referente Amministrazione	Giovanni Sferragatta
Ruolo	Responsabile Unico Progetto
Telefono	0823-232699
Indirizzo mail	sia@ospedale.caserta.it
PEC	sia@ospedalecasertapec.it

2. CONTESTO

- ***DESCRIZIONE DELL'AMMINISTRAZIONE CONTRAENTE***

L'Azienda Ospedaliera Sant'Anna e San Sebastiano di Caserta si avvale di un'infrastruttura digitale complessa attraverso la quale eroga servizi ad un'ampia area metropolitana.

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.

- ***DESCRIZIONE DEL CONTESTO TECNOLOGICO, APPLICATIVO E PROCEDURALE***

La transizione digitale gioca un ruolo chiave nell'evoluzione dei modelli organizzativi della PA, soprattutto in un contesto come quello odierno che necessita di un'intensa collaborazione tra gli attori della pubblica amministrazione per offrire servizi utili, efficienti e innovativi ai cittadini. La necessità di garantire la collaborazione tra diversi attori istituzionali e la spinta normativa del GDPR che sancisce l'obbligo di attuare le misure tecniche e organizzative per mitigare il rischio connesso ai trattamenti dei dati privati, attribuiscono alla cyber sicurezza un ruolo cruciale per la realizzazione di nuovi servizi digitali.

Le pratiche del lavoro agile e il cloud computing nelle diverse declinazioni adottato dall'Amministrazione hanno determinato il superamento del tradizionale modello di difesa basato sul presidio di un perimetro aziendale definito entro il quale contenere risorse e utenze aziendali e attraverso il quale relazionarsi al mondo esterno. L'Amministrazione è quindi nella condizione di dover adottare un modello di borderless security focalizzata sulle entità che erogano, abilitano o fruiscono i servizi digitali, sulla verifica delle identità che le qualificano, sul monitoraggio pervasivo di eventi e comportamenti.

▪ DESCRIZIONE DELL'ESIGENZA

Il presente capitolo ha lo scopo di descrivere le esigenze dell'Azienda Ospedaliera Sant'Anna e San Sebastiano di Caserta nell'ambito dei servizi offerti dall'Accordo quadro AQ 2296 – Lotto 1 per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni, stipulato da Consip S.p.A. (Consip) e dal Raggruppamento Temporaneo di Imprese (RTI) composto da:

- Accenture S.p.A.
- Fastweb S.p.A.
- Fincantieri NexTech S.p.A.
- Difesa e Analisi Sistemi S.p.A.

L'Amministrazione rileva un forte deficit di competenze e strumenti per la gestione efficace del rischio cyber determinato da minacce sofisticate e in continua evoluzione. La casistica recente degli incidenti relativa ad amministrazioni pubbliche che attuano una gestione della sicurezza digitale analoga a quella dell'Amministrazione, evidenzia la necessità di dotarsi quanto prima possibile delle competenze e degli strumenti necessari a riportare il rischio cyber a un livello accettabile e compatibile con la missione dell'Amministrazione. Le criticità rilevate riguardano i seguenti aspetti:

- monitoraggio delle vulnerabilità e delle minacce

Gli interventi previsti indirizzano in maniera diretta le criticità elencate, e si calano in un contesto organizzativo che prevede un deciso potenziamento delle Security Operation con l'obiettivo di conseguire una gestione efficace del rischio cyber in tutti i suoi aspetti.

L'Azienda Ospedaliera Sant'Anna e San Sebastiano di Caserta si impegna ad effettuare l'opportuna segnalazione al Centro di Valutazione e Certificazione Nazionale (CVCN) qualora i servizi richiesti siano inseriti nel Perimetro di sicurezza nazionale cibernetica.

- ***SINTESI DEI SERVIZI RICHIESTI***

Le richieste del presente Piano dei Fabbisogni riguardano l'erogazione dei seguenti servizi:

- **L1.S1. Servizio SOC Security Operation Center**

Si richiede di implementare, 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 azioni di contenimento, ripristino e prevenzione futura in stretta collaborazione tra l'outsourcer e le strutture dell'Amministrazione preposte alla gestione sistemistica. Tra le funzioni richieste ci si aspetta quindi raccolta centralizzata dei log e degli eventi; correlazione tra eventi diversi raccolti; disponibilità di un cruscotto (dashboard) che fornisca agli analisti, in tempo reale, una rappresentazione della situazione in essere; capacità di identificazione, gestione, mitigazione e risoluzione degli attacchi; produzione di report periodici di sintesi, di incident report di dettaglio ed istruzioni operative. Si richiede, infine, di ricevere ed analizzare la reportistica e i log dando anche la giusta priorità ai processi di risoluzione e/o mitigazione delle minacce.

- **L1.S15. Servizi Specialistici**

Si richiede di prevedere un'adeguata quantità di giornate di servizi specialistici e team di cybersecurity per dare supporto, gestire, trattare o comunque coprire quanto già dettagliato nei precedenti servizi e nei paragrafi di descrizione del contesto di interesse.

Tali servizi sono riassunti nella seguente tabella che descrive le numerosità richieste per la loro erogazione. Si richiede, altresì che il piano di lavoro abbia una durata complessiva di 12 mesi.

L1.S1 – SECURITY OPERATION CENTER								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S1	Security Operation Center	As a service (Device equivalenti)	A canone (annuale)	Fino a 300 Eps	-	-	-	-
				Fino a 600 Eps	-	-	-	-
				Fino a 1.200 Eps	-	-	-	-
				Fino a 6.000 Eps	129	-	-	-
				> 6.000 Eps	-	-	-	-

L1.S2 – NEXT GENERATION FIREWALL

Codice	Descrizione	Tipologia d'erogazione	Valutazione economica	Fasce	Q.tà I Anno	Q.tà II Anno	Q.tà III Anno	Q.tà IV Anno
L1.S2	Next Generation Firewall	As a service	A canone (annuale)	Fino a 250 Mbps				
				Fino a 2 Gbps				
				Fino a 4 Gbps				
				Fino a 7 Gbps				
				Fino a 15 Gbps				
				> 15 Gbps				

L1.S3 – WEB APPLICATION FIREWALL								
Codice	Descrizione	Tipologia d'erogazione	Valutazione economica	Fasce	Q.tà I Anno	Q.tà II Anno	Q.tà III Anno	Q.tà IV Anno
L1.S3	Web Application Firewall	As a service	A canone (annuale)	Fino a 500 Mbps				
				Fino a 5 Gbps				
				> 5 Gbps				

L1.S4 – GESTIONE CONTINUA DELLE VULNERABILITÀ								
Codice	Descrizione	Tipologia d'erogazione	Valutazione economica	Fasce	Q.tà I Anno	Q.tà II Anno	Q.tà III Anno	Q.tà IV Anno
L1.S4	Gestione continua delle vulnerabilità	As a service	A canone (canone annuale per indirizzo IP)	Fino a 50 IP	-	-	-	-
				Fino a 200 IP	-	-	-	-
				> 200 IP	-	-	-	-

L1.S5 – THREAT INTELLIGENCE & VULNERABILITY DATA FEED								
Codice	Descrizione	Tipologia d'erogazione	Valutazione economica	Fasce	Q.tà I Anno	Q.tà II Anno	Q.tà III Anno	Q.tà IV Anno
L1.S5	Threat intelligence & Vulnerability data feed	As a service	A canone (canone annuale per datafeed)	Fino a 10 datafeed	-	-	-	-
				Fino a 50 datafeed	-	-	-	-
				> 50 datafeed	-	-	-	-

L1.S6 – PROTEZIONE NAV. INTERNET E POSTA ELETTRONICA								
Codice	Descrizione	Tipologia d'erogazione	Valutazione economica	Fasce	Q.tà I Anno	Q.tà II Anno	Q.tà III Anno	Q.tà IV Anno

L1.S6	Protezione navigazione internet e posta elettronica	As a service	A canone (canone annuale per utente)	Fino a 1.000 utenti				
				Fino a 5.000 utenti				
				Fino a 10.000 utenti				
				Fino a 20.000 utenti				
				> 20.000 utenti				

L1.S7 – PROTEZIONE END POINT								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S7	Protezione End Point	As a service	A canone (canone annuale per numero di nodi)	Fino a 500 nodi	-	-	-	-
				Fino a 1.000 nodi	-	-	-	-
				Fino a 5.000 nodi	-	-	-	-
				> 5.000 nodi	-	-	-	-

L1.S8 – CERTIFICATI SSL								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S8	Certificati SSL	As a service	A corpo (costo per certificato)	SSL OV				
				SSL OV Wildcard				
				SSL EV				
				SSL DV				
				SSL Code signing				
				SSL Client Auth				

L1.S9 – FORMAZIONE E SECURITY AWARENESS								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S9	Formazione e Security Awareness	A task	A corpo	gg/p Team ottimale	-	-	-	-

L1.S10 – GESTIONE IDENTITÀ E ACCESSO UTENTE								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S10		As a service		Fino a 10.000 utenti				

	Gestione identità e accesso utente		A canone (canone annuale per utente)	Fino a 100.000 utenti				
				Fino a 500.000 utenti				
				> 500.000 utenti				

L1.S11 – FIRMA DIGITALE REMOTA								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S11	Firma digitale remota	As a service	A canone (canone annuale per utente)	50 e fino a 200 utenti				
				200 e fino a 500 utenti				
				500 e fino a 1.000 utenti				
				> 1.000 utenti				
				Garantita - N. 1 firma				
				Garantita - N. 5 firme aggiuntive				

L1.S12 – SIGILLO ELETTRONICO								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S12	Sigillo elettronico	As a service	A canone (canone annuale per numero di firma)	Garantita - N. 1 firma				
				Garantita - N. 5 firme aggiuntive				

L1.S13 – TIMBRO ELETTRONICO								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S13	Timbro elettronico	As a service	A consumo (costo per timbratura)	Fino a 1.000 timbrature				
				Fino a 10.000 timbrature				
				Fino a 100.000 timbrature				
				Fino a 1.000.000 timbrature				
				Fino a 10.000.000 timbrature				
				> 10.000.000 timbrature				

L1.S14 – VALIDAZIONE TEMPORALE ELETTRONICA QUALIFICATA								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**Q.tà IV Anno**

L1.S14	Validazione temporale elettronica qualificata	As a service	A canone (canone annuale per marca)	Fino a 1.000 Marcature				
				Fino a 10.000 Marcature				
				Fino a 100.000 Marcature				
				Fino a 1.000.000 Marcature				
				Fino a 10.000.000 Marcature				
				> 10.000.000 Marcature				
				Garantita - N. 1 marcatura				
				Garantita - N. 1 marcatura aggiuntiva				

L1.S15 – SERVIZI SPECIALISTICI								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S15	Servizi specialistici	A task	A corpo	gg/p Team ottimale	3.852	-	-	-

- ***LUOGO DI EROGAZIONE***

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

- per i servizi erogati *da remoto*: presso i Centri Servizi del Fornitore;
- per i servizi on-site: presso la sede dell'Amministrazione.

INDICATORE DI PROGRESSO

Per ogni classe di controlli ABSC (Agid Basic Security Control) previsti dalle misure minime di sicurezza AGID, ove successivamente modificate ed integrate, sarà calcolato il valore del relativo Indicatore di Progresso (Ip) dell'intervento ottenuto attraverso la realizzazione dell'Ordinativo di Fornitura (acquisto di servizi previsti nell'Ordinativo), che sarà determinato come da schema seguente:

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		

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	30/07/2025	Prima emissione	RTI

Tabella 1 – Registro delle versioni

Sommario

Indice delle tabelle

Indice delle figure

1 INTRODUZIONE

L'**Azienda Ospedaliera Sant'Anna e San Sebastiano di Caserta** (nel seguito anche "Amministrazione") si avvale di un'infrastruttura digitale complessa attraverso la quale eroga servizi ad un'ampia area metropolitana.
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'Ente, si trova nella condizione di dover adottare un nuovo modello organizzativo e tecnico focalizzato sulla sicurezza informatica "moderna" ovvero dover adottare un modello di borderless security focalizzato sulle entità che erogano, abilitano o fruiscono i servizi digitali (applicazioni, dispositivi, utenti), sulla verifica delle identità che le qualificano e sul monitoraggio pervasivo di eventi e comportamenti.

L'esigenza è quella di adottare un insieme di soluzioni tecnologiche e di servizi che, nell'ambito del Framework Nazionale per la Cybersecurity e la Data Protection, consentano all'Amministrazione di migliorare la propria postura cyber e indirizzino l'Ente verso i seguenti obiettivi di carattere generale: accrescere la protezione degli asset informatici e degli utenti che li utilizzano, rilevare vulnerabilità presenti all'interno del perimetro aziendale, effettuare analisi/scouting di potenziali attacchi provenienti dall'esterno, creare una sinergia costante tra strutture cyber esterne e strutture interne all'ente preposte alla gestione dei sistemi informativi al fine di intervenire con azioni correttive tempestive ed efficaci preservando la coerenza dei dati e garantendo la protezione dell'intero patrimonio informativo dell'Amministrazione.

1.2 Ambito di Applicabilità

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

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

Il Piano si focalizza sulla **Cyber Security Awareness**, poiché tale consapevolezza fa scaturire azioni organizzative indispensabili per mitigare il rischio connesso alle potenziali minacce informatiche. Nella PA ci sono frequenti attacchi a portali che bloccano i servizi erogati e costituiscono danno di immagine. È in crescita anche il fenomeno denominato data breach (violazione dei dati) che rappresenta anche una grave violazione del GDPR. Le azioni stabilite nel Piano sono tutte indispensabili rispetto allo scenario possibile. Oltre agli attori coinvolti nel Piano resta indispensabile e cruciale il supporto del Garante per la protezione dei dati personali quantomeno per verificare se la PA ha nominato un adeguato DPO (figura obbligatoria per il GDPR) ed è organizzata, almeno ai minimi termini, in linea con le regole del GDPR (Regolamento europeo 679/2016). Il Piano affida a Linee guida e regole specifiche ma anche alle strutture specifiche di AgID il supporto alle Pubbliche Amministrazioni.

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

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

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

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

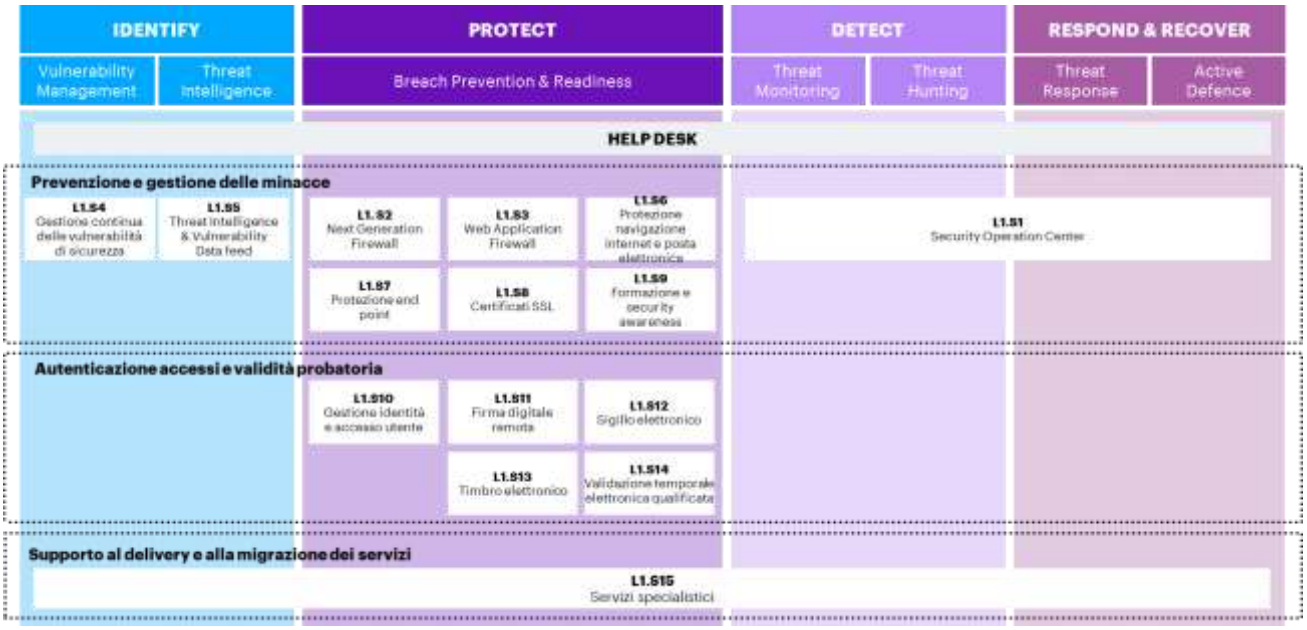

Figura 1 – Mappatura Servizi di Sicurezza e Framework NIST

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

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

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

- i processi di procurement, veicolati attraverso gli strumenti di acquisizione messi a disposizione da Consip;

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

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

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

Lo scenario è contestualmente caratterizzato dalla presenza di due Lotti dedicati ai servizi di Sicurezza da remoto e servizi di Compliance e controllo. Tale specializzazione si innesta in considerazione dei diversi obiettivi a cui i due Lotti rispondono.
In particolare:
- il **Lotto di servizi di Sicurezza da remoto (Lotto 1)** ha l'obiettivo di mettere a disposizione delle Amministrazioni un insieme di servizi di sicurezza - erogati da remoto e in logica continuativa - per la protezione delle infrastrutture, delle applicazioni e dei dati;
- il **Lotto di servizi di Compliance e controllo (Lotto 2)** ha l'obiettivo di mettere a disposizione delle Amministrazioni servizi - erogati "on-site" in logica di progetto – finalizzati alla elaborazione di un "progetto di sicurezza" che identifica lo stato di salute della sicurezza del sistema informativo dell'Amministrazione e nel controllo imparziale sulla corretta esecuzione dei servizi di sicurezza del Lotto 1 nonché sulla efficacia delle misure di sicurezza attuate, a partire dalla fase di acquisizione degli stessi sino alla loro esecuzione a regime.

In riferimento a quanto sopra riportato, l'Azienda Ospedaliera Sant'Anna e San Sebastiano di Caserta, 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'Azienda Ospedaliera Sant'Anna e San Sebastiano di Caserta, 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 Ospedaliera Sant'Anna e San Sebastiano di Caserta e fornitore gli eventuali interventi progettuali da attivare/modificare nonché gli impatti in termini di Piano di Lavoro Generale

Tabella 1 - Assunzioni

2 RIFERIMENTI

2.1 Normativa di riferimento

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

2.2 Documenti Applicabili

Rif.	Titolo
DA-1.	ALLEGATO 1 - CAPITOLATO TECNICO GENERALE - Gara a procedura aperta per la conclusione di un accordo quadro, ai sensi del d.lgs. 50/2016 e s.m.i., suddivisa in 2 lotti e avente ad oggetto l’affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni.
DA-2.	ALLEGATO 2A - CAPITOLATO TECNICO SPECIALE SERVIZI DI SICUREZZA DA REMOTO
DA-3.	Accordo Quadro
DA-4.	Offerta Tecnica – Lotto 1 GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L’AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI
DA-5.	Appendice 1 al CTS Lotto 1_Indicatori di qualità - ID 2296 - Gara Sicurezza da remoto
DA-6.	Piano dei Fabbisogni nominato: “20250707_2296_Lotto 1_Sicurezza da Remoto_Piano dei fabbisogni_AO Caserta_review.pdf” PEC del 09/07/2025

Tabella 2 - Documenti Applicabili

3 DEFINIZIONI E ACRONIMI

3.1 Acronimi

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

Tabella 3 - Definizioni

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

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 4 - Acronimi

4 ORGANIZZAZIONE DEL CONTRATTO ESECUTIVO

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

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

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

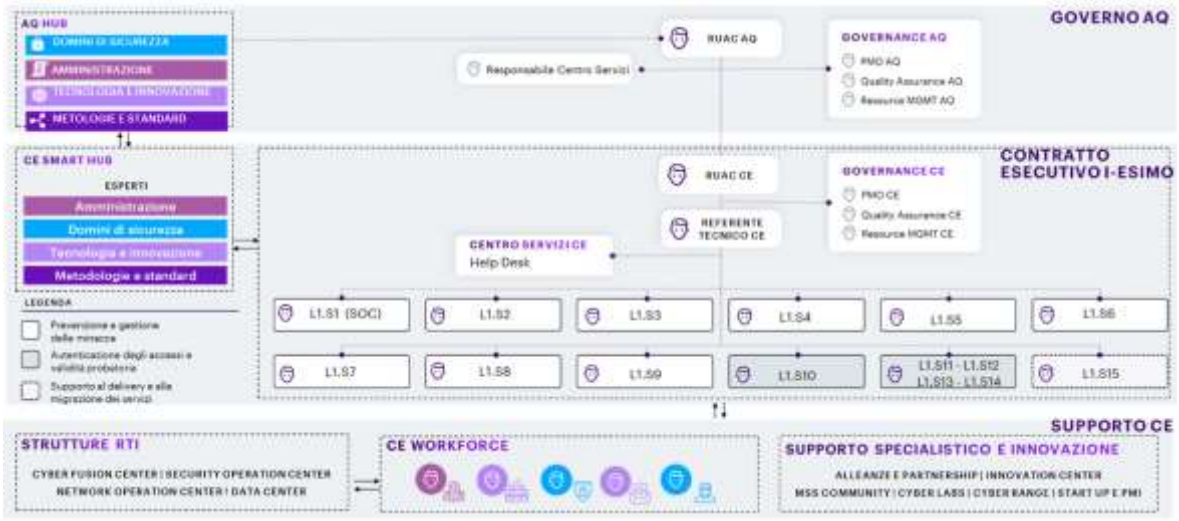

Figura 2 - Organizzazione dell'AQ proposta dal RTI

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

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

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

  Il RUAC CE ha una responsabilità speculare a quella del RUAC AQ e rappresenta la principale interfaccia verso le singole PA

per tutte le tematiche contrattuali, avendo allo stesso tempo compiti di raccordo tra i due livelli.

Il Referente Tecnico CE è responsabile del corretto svolgimento delle attività e dei servizi e il relativo livello di qualità di erogazione per il singolo CE ed è supportato dal team di Governance CE (PMO CE, Quality Assurance CE e Resource Management CE).

I Team responsabili dell'erogazione dei servizi, composti da professionisti di settore, hanno l'ulteriore supporto dei maggiori esperti di tematica del RTI (Subject Matter Expert) per assicurare omogeneità di metodologie e innovazione continua in base all'evoluzione del contesto.

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

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

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

4.1 Attività in carico alle aziende del RTI

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

SERVIZIO	ACCENTURE	FASTWEB	FINCANTIERI	DEAS
L1.S1 – Security Operation Center				
L1.S15 – Servizi Specialistici				
TOTALE (%)				
TOTALE (€)				

Tabella 5 - Ripartizione attività in carico

4.2 Organizzazione e figure di riferimento del Fornitore

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

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

Tabella 6 - Figure di riferimento e referenti del Fornitore

4.3 Luogo di erogazione e di esecuzione della Fornitura

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

- per i servizi erogati da remoto: attraverso i Centri Servizi del Fornitore;
- per i servizi on-site: presso le sedi dell'Amministrazione ove specificato dall'Amministrazione stessa.

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'Amministrazione così come riportati nel Piano dei Fabbisogni:

- L1.S1 – Security Operation Center
- L1.S15 – Servizi Specialistici

5.2 Servizi richiesti

SERVIZIO	FASCIA	IMPORTO / QUANTITA' I ANNO	IMPORTO / QUANTITA' II ANNO	IMPORTO / QUANTITA' III ANNO	IMPORTO / QUANTITA' IV ANNO
L1.S1 – Security Operation Center	Fascia 4 – Fino a 6000 EPS	28.173,60€ / Q.TA 129			
L1.S15 – Servizi Specialistici	GG/p team ottimale	939.888,00€ / Q.TA 3.852			

Tabella 7 - Servizi richiesti

5.3 Indicatore di progresso

Di seguito l'indicatore di progresso (IP) identificato in questa fase per l'erogazione della fornitura, che sarà determinato come da schema seguente:

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

Tabella 8 - Schema definizione Indicatore di Progresso

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

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

6 SOLUZIONE PROPOSTA

6.1 Descrizione dei servizi richiesti

Di seguito i servizi proposti in linea con le esigenze espresse da **Azienda Ospedaliera Sant'Anna e San Sebastiano di Caserta.**

6.1.1 L1.S1 – Security Operation Center

Il servizio prevede di implementare, attraverso adeguati strumenti tecnologici, un servizio di monitoraggio e alerting degli eventi/minacce di sicurezza al fine di consentire una gestione degli incidenti di sicurezza dalla fase di identificazione e notifica dell'evento, fino alle raccomandazioni relative alle azioni di contenimento e ripristino/prevenzione futura.
Il servizio SOC si baserà sui dati raccolti e correlati dal SIEM. 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 dall'Amministrazione 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 i prerequisiti al servizio, in carico all'Amministrazione:

- Configurazione delle sorgenti di log (eventi di sicurezza) e di rete, per la lettura e/o invio degli eventi utili al Centro Servizi;
- 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 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;
- Valutazione post incidente, in modo da individuare possibili azioni migliorative da implementare sui sistemi di sicurezza dell'Amministrazione.

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 del RTI "L1 SOC" sul sistema ITSM del RTI previsto per tale AQ. Il team "L1 SOC" controllerà le informazioni evidenziate dall'allarme ed eseguirà le prime verifiche per una eventuale escalation verso il team del RTI "L2 SOC" e/o il reperibile dell'Amministrazione, nel caso di un fuori orario di servizio.
Successivamente alla conferma di un possibile incidente, il team preposto del RTI procederà con le necessarie azioni. Di seguito un elenco a scopo esemplificativo e non esaustivo delle possibili azioni:

- drill down sugli eventi aggregati che hanno generato l'evidenza/alert;
- verifica dei falsi positivi;
- investigazione/deep analysis del caso;
- escalation verso i team di sicurezza e operativo 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.S15-Servizi Specialistici a supporto di L1.S1

I Servizi Specialistici a supporto del Servizio SOC prevedono l'utilizzo di personale specializzato in logica di progetto e sono finalizzati al supporto, alla realizzazione e all' evoluzione del processo di monitoraggio e gestione degli incidenti di sicurezza.
Gli obiettivi di tale servizio specialistico sono i seguenti e saranno oggetto di puntale pianificazione durante il periodo contrattuale:

- Supporto nella integrazione del SOC con i sistemi in uso presso l'Amministrazione;
- Supporto nella "mitigazione" 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".

6.2 Utenza interessata / coinvolta

Personale dell'**Azienda Ospedaliera Sant'Anna e San Sebastiano di Caserta**

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 e periodo di presa in carico), come indicato nella seguente tabella:

	ANNO I												ANNO II												ANNO III												ANNO IV											
	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
L1.S1																																															
L1.S15																																																

Tabella 9 – Cronoprogramma

7.2 Data di Attivazione e Durata del Servizio

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**

MILESTONE	DESCRIZIONE	ATTORE
Approvazione e Verifica di Conformità	Riscontro degli artefatti consegnati in quantità e tipologia (ricevuta), senza valutazione di contenuto	**Amministrazione**
Accettazione e Verifica di Conformità	Verifica e validazione dei prodotti intermedi di servizio, previa verifica di merito. Certificazione della corretta esecuzione del servizio relativamente ai prodotti oggetto di approvazione	**Amministrazione**
Valutazione difettosità all'avvio e Verifica di Conformità	Verifica della piena fruizione delle funzionalità e dei servizi da parte dell'utente (cittadino/ impresa/ operatore amministrativo/ decisore/ fruitore) tramite l'esame della quantità e della tipologia di malfunzionamenti e non conformità rilevati durante il periodo di avvio in esercizio. Certificazione della corretta esecuzione del servizio	**Amministrazione**

Tabella 10 - Descrizione milestone per obiettivo

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

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

7.5 Modalità di ricorso al Subappalto da parte del Fornitore

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

SERVIZIO	AZIENDA	QUOTA MASSIMA SUBAPPALTABILE
L1.S1 – Security Operation Center, L1.S15 – Servizi Specialistici	**RTI**	**50%**

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

8 DIMENSIONAMENTO ECONOMICO

8.1 Modalità di erogazione dei Servizi

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

ID SERVIZIO	METRICA	MODALITA' EROGAZIONE	MODALITA' CONSUNTIVAZIONE	PERIODICITA' CONSUNTIVAZIONE	PREZZO UN OFFERTO	QUANTITA' TOTALE	VALORE ECONOMICO TOTALE
L1.S1	Device equivalenti /anno	Da remoto	Canone	Mensile	218,40 €	129	28.173,60 €
L1.S15	GG/P- team ottimale	Da remoto / On Site	Progettuale – A corpo	Mensile	244,00 €	3.852	939.888,00 €

Tabella 12 - Quadro economico di riferimento

L'importo complessivo dell'ordinativo di fornitura ammonta a **968.061,60 €** (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

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

9.3 Piano della Qualità Specifico

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

9.4 Curriculum Vitae dei Referenti

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

9.5 Misure di Sicurezza poste in essere

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

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

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

REGIONE CAMPANIA
AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE E DI ALTA SPECIALIZZAZIONE
"SANT'ANNA E SAN SEBASTIANO"
CASERTA

ATTESTAZIONE DI VERIFICA E REGISTRAZIONE CONTABILE
relativa alla DELIBERAZIONE DEL DIRETTORE GENERALE con oggetto:
FONDI PNRR – M6.C2 - INVESTIMENTO 1.1.1 - DIGITALIZZAZIONE DEA I E II LIVELLO: ACCORDO QUADRO PER L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI – ID 2296 – LOTTO 1

ATTESTAZIONE DI VERIFICA E REGISTRAZIONE CONTABILE 1 (per le proposte che determinano un costo per l'AORN)
Il costo derivante dal presente atto : €1.181.035,15

- è di competenza dell'esercizio 2025 , imputabile al conto economico 1010103010 - Software proprietà licenza d'uso tempo
  da scomputare dal preventivo di spesa che presenta la necessaria disponibilità
- è relativo ad acquisizione cespiti di cui alla Fonte di Finanziamento

---

Caserta li, 25/08/2025

il Direttore
UOC GESTIONE ECONOMICO FINANZIARIA
Eduardo Chianese