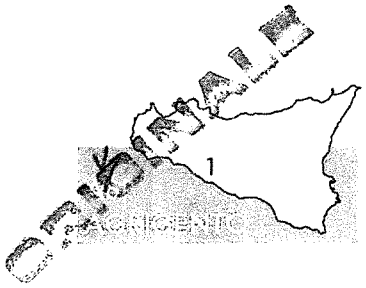


Regione Siciliana

Azienda Sanitaria Provinciale di

AGRIGENTO

DELIBERAZIONE COMMISSARIO STRAORDINARIO N. 691 **DEL** 14 APR 2023

OGGETTO: Adesione accordo quadro per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni – id 2296 – LOTTO 1 Approvazione Piani Operativi ed Autorizzazione Adesione Accordo Quadro anche *per la realizzazione degli interventi finanziati nell'ambito del Piano* Nazionale di Ripresa e Resilienza (PNRR) — Missione 6 Salute, - CUP: C46G22002010006, C86G22001320006 e C96G22002340006, - Innovazione, ricerca e digitalizzazione del servizio sanitario - 1.1: Ammodernamento del parco tecnologico e digitale ospedaliero.

STRUTTURA PROPONENTE: **U.O.C. PROVVEDITORATO**

PROPOSTA N. 830 DEL 07/04/2023

IL FUNZIONARIO ISTRUTTORE	IL DIRIGENTE AMMINISTRATIVO	IL DIRETTORE U.O.C. SERVIZIO PROVVEDITORATO
(Dott. Pietro Vitellaro)	*(Dott.ssa Rosalia Calà)*	*(Dott. Oreste Falco)*

VISTO CONTABILE

Si attesta la copertura finanziaria:
( ) come da prospetto allegato (ALL. N. _____) che è parte integrante della presente delibera.
P.N. 44378/23 ex art. 113.

( ) Autorizzazione n. REG del 11/04/2023 C.E. / C.P. C5020201116

Il RESPONSABILE DEL PROCEDIMENTO
S.E.F. Faneli
L'ADDETTO RESPONSABILE
Sig. Giovanni Faneli

IL DIRETTORE UOC SEF e P.
IL DIRETTORE U.O.C. SERVIZIO ECONOMICO FINANZIARIO E PATRIMONIALE
Dr. Beatrice Salvago

RICEVUTA DALL'UFFICIO ATTI DELIBERATIVI IN DATA 12 APR. 2023

L'anno duemilaventitre il giorno QUATTORDICI del mese di APRILE nella sede dell'Azienda Sanitaria Provinciale di Agrigento

IL COMMISSARIO STRAORDINARIO

Dott. Mario Zappia, nominato con Decreto Assessoriale n. 696/2020 del 31/07/2020, come modificato con D.A. 3/2023/GAB del 10/01/2023, coadiuvato dal Direttore Amministrativo, dott. Alessandro Mazzara, nominato con delibera n. 414 del 17/06/2019 e dal Direttore Sanitario, dott. Emanuele Cassarà, nominato con delibera n. 376 del 22/02/2023, con l'assistenza del Segretario verbalizzante DOTT.SSA TERESA CINQUE adotta la presente delibera sulla base della proposta di seguito riportata.

PROPOSTA

Il Direttore U.O.C. Provveditorato, dott. Oreste Falco

VISTO:

- l'Atto Aziendale di questa ASP, adottato con delibera n. 265 del 23/12/2019 ed approvato con D.A. n. 478 del 04/06/2020, di cui si è preso atto con Delibera n. 880 del 10/06/2020;
- il Regolamento (UE) 2021/241 del Parlamento Europeo e del Consiglio del 12 febbraio 2021, nel con il quale viene istituito il Dispositivo per la Ripresa e la Resilienza (Recovery and Resilience Facility, RRF), della durata di sei anni, dal 2021 al 2026, che costituisce la principale componente del programma Next Generation EU (NGEU) con l'obiettivo specifico di fornire agli Stati Membri il sostegno finanziario al fine di conseguire le tappe intermedie e gli obiettivi delle riforme e degli investimenti stabiliti nel PNRR;
- i contenuti del superiore Programma riguardanti la Missione 6 "Salute" (di seguito, per brevità, anche M6) che ha l'obiettivo di rafforzare la prevenzione e i servizi sanitari sul territorio, modernizzare e digitalizzare il sistema sanitario e garantire equità di accesso alle cure ed è composta da due Componenti che comprendono le seguenti otto Linee di investimento: Componente 1 (Cl) - Reti di prossimità, strutture intermedie e telemedicina per l'assistenza sanitaria territoriale 1.1 Case della comunità e presa in carico della persona; 1.2 Casa come primo luogo di cura, assistenza domiciliare e telemedicina: 1.3 Rafforzamento dell'assistenza sanitaria intermedia e delle sue strutture (Ospedali di Comunità); Componente 2 (C2) - Innovazione, ricerca e digitalizzazione del servizio sanitario nazionale 1.1 Ammodernamento del parco tecnologico e digitale ospedaliero. 1.2 Verso un nuovo ospedale sicuro e sostenibile; 1.3 Rafforzamento dell'infrastruttura tecnologica e degli strumenti per la raccolta, l'elaborazione, l'analisi dei dati e la simulazione; 2.1 Valorizzazione e potenziamento della ricerca biomedica del SSN; 2.2 Sviluppo delle competenze tecnico-professionali, digitali e manageriali del personale del sistema sanitario;
- il D.L. 31 maggio 2021 n. 77, convertito con modificazioni dalla Legge 29 luglio 2021 n. 108, concernente la governance del PNRR, che prevede misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle relative procedure;
- il Decreto 15 settembre 2021 con cui il Ministro della salute, di concerto con il Ministro dell'economia e delle finanze, istituisce l'Unità di Missione del Ministero della salute titolare di interventi PNRR;
- il Decreto 20 gennaio 2022 del Ministero della salute, pubblicato sulla GURI n. 57 del 09/03/2022, recante "Ripartizione programmatica delle risorse alle regioni e alle province autonome per i progetti del Piano nazionale di ripresa e resilienza (PNRR) e del Piano per gli investimenti complementari (PNC) " con il quale sono state determinate le risorse a valere sul PNRR e a valere sul PNC e ripartite a favore dei Soggetti Attuatori Regioni e Province Autonome;
- il D.A. n. 406 del 26/05/2022, con cui l'Assessore regionale della Salute, in aderenza ai contenuti dello Statuto della Regione Siciliana, con particolare riferimento agli articoli 9 e 20, ha approvato il Piano Operativo Regionale (POR) della Regione Siciliana, che, tra l'altro, comprende le 59 Schede territorialmente di competenza dell'Azienda Sanitaria Provinciale di Agrigento, Ì cui interventi possono sinteticamente riassumersi nel modo seguente: n. 19 "Case della Comunità e presa in carico della persona"; n. 4 "Centrali Operative Territoriali (COT)"; n. 3 "Ospedali di Comunità"; n. 21 di "Digitalizzazione DEA di I e II livello"; n. 7 "Grandi apparecchiature"; n. 5 "Verso un nuovo ospedale sicuro e sostenibile, di cui n. 2 a valere sul PNRR e n. 3 a valere sul PNC;

- il Contratto Istituzionale di Sviluppo (CIS), sottoscritto in data 30/05/2022 dal Ministro della Salute e dal Presidente della Regione Siciliana, nella qualità di Soggetto Attuatore, concernente la realizzazione degli interventi finanziati nell'ambito del PNRR Missione 6 - Componenti 1 e 2 - e dal PNC, sulla scorta del POR allegato al CIS, nonché l'impegno a rispettare tutti gli obblighi previsti nel citato CIS, che costituiranno elementi prioritari ed essenziali per l'attuazione dei singoli interventi e per la verifica del relativo stato di avanzamento, secondo gli standard contenuti nel Decreto 23 maggio 2022, n. 77;
- il Decreto n. 664 del 29/07/2022 dell'Assessorato della Salute, con il quale la Regione siciliana, al fine di dare esecuzione agli interventi relativi ai progetti finanziati dal PNRR e dal PNC degli Enti del Servizio sanitario regionale in base alla competenza territoriale, ha delegato l'Azienda Sanitaria Provinciale di Agrigento a svolgere, quale Soggetto Attuatore Esterno, specifiche attività finalizzate alla realizzazione dei 59 interventi ad essa attribuiti sulla base del citato criterio di competenza territoriale;

CONSIDERATO:

- che nell'ambito del citato D.M. 20 gennaio 2022 è stata disposta l'assegnazione in favore della Regione Siciliana (Soggetto Attuatore) della somma complessiva di € 796.573.463,33;
- che l'art. 1 del D.A. n. 664/22 delega l'Azienda Sanitaria Provinciale di Agrigento, in qualità di "Soggetto Attuatore esterno", a svolgere specifiche attività relativamente ai 59 interventi di propria competenza territoriale inseriti nel POR e, cioè: n. 19 "Case della comunità e presa in carico della persona"-, n. 4 "Centrali Operative Territoriali (COT)"-, n. 3 "Ospedali di Comunità"-, n. 21 di "Digitalizzazione DEA di I e II livello"-, n. 7 "Grandi apparecchiature"-, n. 5 "Verso un nuovo ospedale sicuro e sostenibile, di cui n. 2 a valere sul PNRR e n. 3 a valere sul PNC, secondo gli standard contenuti nel Decreto 23 maggio 2022, n. 77;
- che nell'elenco degli interventi per i quali, con D.A. n. 664/22, sono state conferite specifiche deleghe all'Azienda Sanitaria Provinciale di Agrigento, sono inclusi i seguenti progetti concernenti la linea M6C2 - Innovazione, ricerca e digitalizzazione del servizio sanitario - 1.1: Ammodernamento del parco tecnologico e digitale ospedaliero e dove nello specifico sono stati assegnati i seguenti CUP:
    - CUP C46G22002010006: OSPEDALE SAN GIOVANNI DI DIO DI AGRIGENTO*CONTRADA CONSOLIDA* MISURE DI INFORMATIZZAZIONE PNRR;
    - CUP C86G22001320006: OSPEDALE DI SCIACCA *VIA POMPEI*MISURE DI INFORMATIZZAZIONE PNRR;
    - CUP C96G22002340006: PRESIDIO OSPEDALIERO DI RIBERA* VIA CIRCONVALLAZIONE, 1* MISURE DI INFORMATIZZAZIONE PNRR;

CONSIDERATO CHE:

- con atto deliberativo n. 488 del 18/03/2022 questa Azienda ha individuato quale RUP della linea di intervento del PNRR la Missione 6.C2 - 1.1.1. Ammodernamento del parco tecnologico e digitale ospedaliero (Digitalizzazione delle strutture ospedaliere (DEA Dipartimenti di Emergenza e Accettazione di Livello I e II) il Dirigente Analista Aziendale Dott. Riccardo Insalaco;
- con successivo atto deliberativo n. 319 del 21/02/2023, per la linea di intervento in commento sono stati individuati i due nuovi RUP : Dott. Pietro Vitellaro e Dott. Maurizio Arena;
- che a seguito di due diverse richieste dell'Assessorato alla Salute sono state approvate da questa azienda due rimodulazioni della programmazione della linea di intervento Missione 6.C2 - 1.1.1 (Digitalizzazione DEA) con deliberazioni n. 379 del 24/02/2023 e n. 610 del 05/04/2023;

- che nella deliberazione citata n. 610 del 05/04/2023 è stato individuato quale referente tecnico dell'intera linea di intervento il Dirigente Analista dei Sistemi Informativi Aziendali Dott. Riccardo Insalaco;
- la fase di attuazione e di rendicontazione delle Linee di intervento del PNRR sopramenzionate segue specifiche e separate direttive nazionali e regionali tramite apposite piattaforme;

ATTESO CHE

- Il Dirigente Analista Aziendale con nota prot. n. 32444 del 24/02/2023, allegata al presente provvedimento quale parte integrante e sostanziale dello stesso **(ALLEGATO 1)**, ha predisposto i piani dei fabbisogni propedeutici accordo quadro per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni – id 2296 – LOTTO 1 i quali rientrano tra le linee di attuazione della Missione 6.C2 - 1.1.1. Ammodernamento del parco tecnologico e digitale ospedaliero (Digitalizzazione delle strutture ospedaliere (DEA Dipartimenti di Emergenza e Accettazione di Livello I e II)) distinguendo le attività sui tre diversi PP.OO. oggetto degli interventi PNRR;
- Nella medesima nota Allegato 1 il Dirigente Analista Aziendale ha predisposto un piano dei fabbisogni, propedeutico all'Adesione dell'Accordo quadro in commento, che non rientra nelle attività finanziate dal PNRR, ma che tuttavia si rendono comunque necessarie per colmare le esigenze aziendali di cybersicurezza;
- questo servizio, nel pieno rispetto delle modalità di adesione indicate negli atti dell'Accordo quadro, con PEC del 27/02/2023 allegata al presente provvedimento quale parte integrante e sostanziale dello stesso **(ALLEGATO 2)**, ha trasmesso i quattro Piani dei Fabbisogni Allegati **(ALLEGATO 3)** quali parte integrante e sostanziale dello stesso, al fornitore Aggiudicatario il RTI costituito Accenture S.p.A.,Fincantieri Nextech S.p.A., Fastweb S.p.A., Deas, Difesa e Analisi Sistemi S.p.A e nello specifico:
    - Piano dei fabbisogni nell'ambito dell'Intera ASP di Agrigento;
    - Piano dei fabbisogni nell'ambito della PNRR MISSIONE 6 SALUTE - M6.C2 1.1.1.1 AMMODERNAMENTO DEL PARCO TECNOLOGICO E DIGITALE OSPEDALIERO (DIGITALIZZAZIONE DEA I E II)presso il P.O. di Agrigento;
    - Piano dei fabbisogni nell'ambito della PNRR MISSIONE 6 SALUTE - M6.C2 1.1.1.1 AMMODERNAMENTO DEL PARCO TECNOLOGICO E DIGITALE OSPEDALIERO (DIGITALIZZAZIONE DEA I E II)presso il P.O. di Sciacca;
    - Piano dei fabbisogni nell'ambito della PNRR MISSIONE 6 SALUTE - M6.C2 1.1.1.1 AMMODERNAMENTO DEL PARCO TECNOLOGICO E DIGITALE OSPEDALIERO (DIGITALIZZAZIONE DEA I E II)presso il P.O. di Ribera;
- il fornitore aggiudicatario dell'Accordo Quadro, con PEC del 20/03/2023, ha trasmesso quattro piani operativi, allegati al presente provvedimento **(ALLEGATO 4)** quali parte integrante e sostanziale dello stesso rispondenti ai quattro piani dei fabbisogni sopra menzionati;
- il dirigente Analista Aziendale con nota prot. n. 49544 del 24/03/2023, allegata al presente provvedimento quale parte integrante e sostanziale dello stesso **(ALLEGATO 5)**, ha valutato i quattro piani operativi affermando che: *" lo scrivente, ha operato la verifica di congruità e corrispondenza tra la richiesta preliminare di fornitura ed i piani operativi, accertandone la correttezza formale delle quantità e qualità dei servizi offerti rispetto ai fabbisogni rilevati da questa Azienda e tecnicamente rivalutato dal RTI Aggiudicatario dell'AQ Consip ID 2296"* ed ancora, sempre il dirigente analista aziendale ha asserito: *"si suggerisce di procedere rapidamente all'adozione degli atti necessari all'adesione all'AQ in esame che peraltro consentirebbe all'Azeidna di dotarsi di sistemi di firma remota la cui necessità è ampiamente conosciuta dalla Direzione Strategica Aziendale";*

RICHIAMATO l'art. 1, c. 512 della L. 208/2015, così come modificato dall'art. 1, c. 419 della L. 232/2016, il quale dispone che, al fine di garantire l'ottimizzazione e la razionalizzazione degli acquisti di beni e servizi informatici e di connettività, le P.A. provvedono ai propri approvvigionamenti esclusivamente tramite gli strumenti di acquisto e di negoziazione di Consip Spa;

RITENUTO:

- di approvare i Piani Operativi ALLEGATO 4 proposti dal fornitore aggiudicatario dell'accordo quadro sopramenzionato in riferimento alla linea PNRR (PP.OO. di Agrigento, Sciacca e Ribera) ed in riferimento ai fabbisogni aziendali, verificato dal dirigente analista aziendale di cui alla nota prot. n. 49544 del 24/03/2023 (ALLEGATO 5) ;
- di dover definire la procedura di adesione all'Accordo Quadro per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni – id 2296 – LOTTO 1 secondo le modalità di cui all'Accordo Quadro ed ai piani operativi ALLEGATO 4;

RILEVATO

- che l'onere economico complessivo presunto del servizio della durata massima di 36 mesi, è pari ad € 643.182,52 Iva esclusa, e quindi 784.682,67 IVA Inclusa specificato come di seguito esposto:
    - a valere sui fondi del PNRR (programma di spesa n. 1127) relativamente ai Piani Operativi del:
        - P.O. di Agrigento: € 135.682,73 Iva Esclusa e € 165.532,93 Iva Inclusa;
        - P.O. di Sciacca: € 125.746,52 Iva Esclusa e € 153.410,75 Iva Inclusa;
        - P.O. di Ribera: € 52.902,56 Iva Esclusa e € 64.541,12 Iva Inclusa;
    - a valere sui fondi del bilancio aziendale per € 328.850,71 Iva Esclusa e € 401.197,87 Iva Inclusa;
- che l'onere economico complessivo presunto del presente provvedimento della durata massima di 36 mesi, è pari ad € 647.684,80 Iva esclusa, e quindi 789.184,67 IVA Inclusa che saranno inputati sui conti del bilancio d'esercizio come di seguito esposto
    - € 643.182,52 Iva esclusa, e quindi 784.682,67 IVA Inclusa costituisce l'importo del contratto di adesione all'Accordo Quadro, secondo le modalità disciplinate nel Piano Operativo Allegato 4 da imputare al conto n. C502020116 del bilancio d'esercizio come segue:
        - € 160.795,63, Iva esclusa, quindi € 196.170,67 Iva Inclusa nel Bilancio Aziendale 2023;
        - € 214.394,17, Iva Esclusa, quindi € 261.560,89 Iva Inclusa nel Bilancio Aziendale anno 2024 e anno 2025;
        - € 53.598,54, Iva Esclusa, quindi € 65.390,22 Iva Inclusa nel Bilancio d'esercizio anno 2026;
    - € 4.502,28 per competenze per incentivi per funzioni tecniche di cui all'art.113 del D.Lgs. n.50 del 2016 secondo le modalità di cui allo specifico Regolamento Aziendale, sui relativi conti aziendali n. C516040605 "Fondo Incentivi per funzioni tecniche ex art. 113 del D.Lgs. n. 50/2016 e sul conto P202050601 "Fondo per l'innovazione tecnologica" nel Bilancio Aziendale 2023;

PROPONE

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

1. **APPROVARE** i Piani Operativi (ALLEGATO 4) proposti dal fornitore aggiudicatario dell'accordo quadro sopramenzionato in riferimento alla linea PNRR (PP.OO. di Agrigento, Sciacca e Ribera) ed in riferimento ai fabbisogni aziendali, verificato dal dirigente analista aziendale di cui alla nota prot. n. 49544 del 24/03/2023 (ALLEGATO 5);

2. **AUTORIZZARE** il Servizio Provveditorato ad emettere i relativi ordinativi di fornitura al fine di definire l'adesione all'Accordo Quadro per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni – id 2296 – LOTTO 1 per la durata di 36 mesi secondo le modalità di cui ai Piani Operativi (allegato 5) *per la realizzazione, tra l'altro, degli interventi finanziati nell'ambito del Piano* Nazionale di Ripresa e Resilienza (PNRR) — Missione 6 Salute, - CUP: C46G22002010006, C86G22001320006 e C96G22002340006, - Innovazione, ricerca e digitalizzazione del servizio sanitario - 1.1: Ammodernamento del parco tecnologico e digitale ospedaliero;

3. **DARE ATTO** che l'onere economico complessivo presunto del presente provvedimento della durata massima di 36 mesi, è pari ad € 647.684,80 Iva esclusa, e quindi 789.184,67 IVA Inclusa che sarà inputato sui conti del bilancio d'esercizio come di seguito esposto:
    - € 643.182,52 Iva esclusa, e quindi 784.682,67 IVA Inclusa costituisce l'importo del contratto di adesione all'Accordo Quadro, secondo le modalità disciplinate nel Piano Operativo Allegato 4 da imputare al conto n. C502020116 del bilancio d'esercizio come segue:
        - € 160.795,63, Iva esclusa, quindi € 196.170,67 Iva Inclusa nel Bilancio Aziendale 2023;
        - € 214.394,17, Iva Esclusa, quindi € 261.560,89 Iva Inclusa nel Bilancio Aziendale anno 2024 e anno 2025;
        - € 53.598,54, Iva Esclusa, quindi € 65.390,22 Iva Inclusa nel Bilancio d'esercizio anno 2026;
    - € 4.502,28 per competenze per incentivi per funzioni tecniche di cui all'art.113 del D.Lgs. n.50 del 2016 secondo le modalità di cui allo specifico Regolamento Aziendale, sui relativi conti aziendali n. C516040605 "Fondo Incentivi per funzioni tecniche ex art. 113 del D.Lgs. n. 50/2016 e sul conto P202050601 "Fondo per l'innovazione tecnologica" nel Bilancio Aziendale 2023;
4. **DARE ATTO**
    - che i relativi CIG verranno generati a seguito dell'adozione del presente provvedimento;
    - che con separato provvedimento si procederà alla determinazione e liquidazione degli incentivi, ex art. 113 del D.Lgs 50/2016, al personale costituente con la disposizione di servizio prot. n. 57146 del 07/04/2023;
5. **NOMINARE**, ai sensi dell'art. 31 del D.Lgs. 50/2016, in relazione all'intervento oggetto del presente provvedimento, il Responsabile Unico del Procedimento (RUP), il Dott. Pietro Vitellaro, in qualità di Collaboratore Amministrativo Professionale in servizio presso l'U.O.C. Servizio Provveditorato, che sarà coadiuvato nell'esercizio dei compiti, previsti negli atti di gara e dalla vigente normativa, anche dalle altre strutture aziendali in base alla relativa competenza;
6. **NOMINARE**, Direttore dell'Esecuzione del Contratto, il Dirigente Analista Aziendale, Dott. Riccardo Insalaco;

7. **DICHIARARE** il presente provvedimento immediatamente esecutivo, ai sensi dell'art. 65 della L.R. 25/1993, come modificato dall'art. 53 della L.R. 30/1993 al fine di porre in essere tutti gli atti consequenziali nel più breve tempo possibile;
8. **ATTESTA**, altresì, che la presente proposta, a seguito dell'istruttoria effettuata, nella forma e nella sostanza, è legittima e pienamente conforme alla normativa che disciplina la fattispecie trattata.

Il Direttore della UOC Provveditorato
(Dott. Oreste Falco)

SULLA SUPERIORE PROPOSTA VENGONO ESPRESSI

Parere favorevole
Data 13/04/2023

Il Direttore Amministrativo
Dott. Alessandro Mazzara

Parere favorevole
Data 13/04/2023

Il Direttore Sanitario
Dott. Emanuele Cassarà

IL COMMISSARIO STRAORDINARIO

Vista la superiore proposta di deliberazione, formulata dal Dott. Oreste Falco Direttore della U.O.C. Provveditorato, che, a seguito dell'istruttoria effettuata, nella forma e nella sostanza, ne ha attestato la legittimità e la piena conformità alla normativa che disciplina la fattispecie trattata;
Ritenuto di condividere il contenuto della medesima proposta;
Tenuto conto dei pareri espressi dal Direttore Amministrativo e dal Direttore Sanitario;

DELIBERA

di approvare la superiore proposta, che qui si intende integralmente riportata e trascritta, per come sopra formulata e sottoscritta dal Dott. Oreste Falco, Direttore della U.O.C. Provveditorato.

IL COMMISSARIO STRAORDINARIO
Dott. Mario Zappia

Il Segretario verbalizzante
IL COLLABORATORE AMM.VO TPO
"Ufficio Staff e Controllo di Gestione"
Dott.ssa Teresa Cinque


SERVIZIO SANITARIO NAZIONALE REGIONE SICILIA - S
Azienda
Sanitaria
Provinciale
Agrigento

ASP AGRIGENTO
Viale della Vittoria, 321 - 92100 AGRIGENTO (AG)
TEL:0922407111 FAX:0922407230

11/04/2023

Contabilita': Tutte
Classe : Tutte
Distretto : Tutti
Per l'anno : 2023
Dal Conto :
Al Conto : zzzzzzzzzzzzzzz
Dalla data : 11/04/2023
Alla data : 11/04/2023
Dalla P.Nota: 44378
Alla P.Nota : 44378
Causale Mov.: Tutte

P. Nota	Dt.Reg.	Data Doc.	Sezion.	Conto	Cli/For.	Descrizione	Cont.	D A R E	A V E R E
	N. Reg.	Num. Doc		Protoc.		Causale Movimento			
44378	11/04/23	07/04/23		P202050601		ALTRI FONDI INCENTIVI FUNZIONI IS/GE		0,00	4.502,28
	1	P.N.830/23 PROVV.				P.N.830/23 PROVV.INNOVAZ.RIC. E.DIGIT. SSN.AMMOD.-INCENTIVI			
	2			C516040605		ACCANTONAMENTI INCENTIVI FUNZI IS/GE		4.502,28	0,00
						T O T A L E M O V I M E N T I ---->		4.502,28	4.502,28

ALL. 1

SERVIZIO SANITARIO NAZIONALE - REGIONE SICILIANA
Azienda Sanitaria Provinciale di Agrigento
Sede legale : Viale della Vittoria n.321 92100 Agrigento
Partita IVA – Codice Fiscale : 02570930848
Sistemi Informatici Aziendali

Tel. 0922407111
cell: 3388002237
EMail : riccardo.insalaco@aspag.it

Prot.n. *00 32444 del 24/02/2023*

Al Direttore U.O.C. Servizio Provveditorato

e.p.c. Al Commissario Straordinario
Al Direttore Amministrativo

SEDE

Oggetto: *Missione 6 PNRR - Ammodernamento tecnologico Digitalizzazione DEA – Trasmissione Piano dei Fabbisogni adesione A.Q. Consip* ***Sicurezza "da remoto"*** *– ID 2296.*

Con riferimento al procedimento di cui in oggetto, nel mese dicembre u.s., questa Amministrazione ha richiesto all'RTI aggiudicataria dell'A.Q. ID 2296 la redazione dei Piani Operativi, ID: AQSEC-2296L1- Versione: 1.0 Data: 30/12/2022, conseguenti all'invio di due distinti piani dei fabbisogni redatti sulla scorta delle valutazioni tecniche responsabilmente operate dallo scrivente.
Tuttavia, i Piani Operativi prodotti dall'aggiudicatario sono risultati non in linea con il reale fabbisogno aziendale e, quindi, ritenuti non idoneo.
Conseguentemente, stante l'immutata necessità di acquisire servizi in ambito di Cyber Security, si è reso necessario procedere con la revisione dei PdF precedente sviluppati con un maggiore grado di dettaglio delle richieste operative e con suddivisione dei progetti tra PNRR e parte da finanziare con il bilancio aziendale.
In particolare, i progetti PNRR sono stati distinti con riguardo a ciascun DEA e con indicazione della previsione di spesa massima finanziabile.
Per quanto sopra ed al fine di potere riattivare la procedura di adesione all'A.Q. "Sicurezza da remoto", con la presente, si trasmettono quattro distinti PdF, di cui tre orientati all'approvvigionamento di servizi costituenti l'intervento PNRR - Missione 6 Salute - M6.C2 – 1.1.1. Ammodernamento del parco tecnologico e digitale ospedaliero (Digitalizzazione delle strutture ospedaliere (DEA Dipartimenti di Emergenza e Accettazione di Livello I e II)).
I predetti PdF, inoltre, risultano specificamente afferenti alle attività progettuali PNRR di seguito elencate:

Presidio	***Intervento***	***Importo***
PO Ribera	parte del 5	64.556,62 €
PO Sciacca	parte del 13	153.416,58 €
PO Agrigento	parte del 21	165.547,10 €
		383.520,31 €

Il prefato quadro economico è stato elaborato tenuto conto delle attività e servizi che il fornitore dell'A.Q. per le Pubbliche Amministrazioni Locali (PAL) - RTI costituito Accenture S.p.A., Fincantieri Nextech S.p.A., Fasteweb S.p.A., Deas, Difesa e Analisi Sistemi S.p.A. deve eseguire

tenuto conto del Piano dei Fabbisogni che lo scrivente ha redatto per la realizzazione degli obiettivi PNRR.

Oltre, però, rilevano tutte le esigenze aziendali che, in ambito di cyber security, discendono dallo specifico e stringente dettato normativo dispiegato con la circolare dell'Agenzia per la Cybersicurezza Nazionale n. 4336 del 21 aprile 2022.

Quindi, gli obiettivi finalizzati dal PNRR rappresentano soltanto una parte delle esigenze di adeguamento tecnologico dell'ASP di Agrigento e richiedono un'integrazione con servizi da declinare in un ulteriore PdF da sottoporre al medesimo aggiudicatario dell'A.Q. "Sicurezza da remoto".

Peraltro, le predette decisioni operative risultano in linea con le indicazioni fornite, in tal senso, dal Dipartimento Regionale per la Pianificazione Strategica con nota prot. n. 42762 del 21.09.2022.

Indicazioni, quest'ultime, che impongono di avvalersi delle iniziative che Consip S.p.A. ha reso disponibili per soddisfare le esigenze delle Pubbliche Amministrazioni per la cybersicurezza e, quindi, con adesione all'accordo Quadro "Servizi di sicurezza da remoto" – ID SIGEF 2296.

Il piano dei fabbisogni riporta una elencazione di attività e servizi che lo stesso richiamato fornitore aggiudicatario dell'AQ Consip dovrà esplicitare con il progetto da sottoporre all'approvazione dell'Amministrazione con quantificazione dei costi che in atto non è possibile preventivare.

Per tutto quanto sopra, codesto Servizio è invitato ad attivare le procedure indicate da Consip al punto 2 "Emissione del Piano dei Fabbisogni" della Guida all'AQ LOTTO 1 – Servizi di sicurezza da remoto - ID 2296 - per l'acquisizione di quattro distinti progetti esecutivi che lo scrivente si riserva, fin da subito, di compulsare per verificarne l'aderenza al complessivo bisogno manifestato con i rispettivi PdF.

Sicché, dovrà trasmettere gli allegati Piani dei Fabbisogni che lo scrivente ha redatto per consentire a questa Amministrazione di potere soddisfare il fabbisogno aziendale in termini di "cyber security" con costi che trovano copertura nelle risorse PNRR, fatta eccezione per il quarto PdF da finanziare con fondi del bilancio aziendale.

Peraltro, chiarisce che l'adesione all'AQ. "Sicurezza da remoto" rappresenta una parte del fabbisogno complessivo di ammodernamento tecnologico dei sistemi ICT che verrà a completarsi con le adesioni successive in quanto già previste nel report Age.na.s.

Il Referente Sistemi Informatici Aziendali
Dott. Riccardo Insalaco

ALL. 2

Servizio Sanitario Nazionale Regione Siciliana
Azienda Sanitaria Provinciale di Agrigento
Tel. 0922 407111 * Fax 0922 401229
P.Iva e C.F. 02570930848
Web: www.aspag.it

UFFICIO
U.O.C. SERVIZIO PROVVEDITORATO
VIALE DELLA VITTORIA N. 321
CAP. 92100 CITTA' AGRIGENTO
Telefono 0922-407408

FAX 0922-407408
Pec: forniture@pec.aspag.it
Mail: forniture@aspag.it

DATA 27/02/2023

PROT. 33276

Alla RTI costituito Accenture S.p.A.,
Fincantieri Nextech S.p.A., Fastweb S.p.A.,
Deas, Difesa e Analisi Sistemi S.p.A.

Tramite PEC: sicurezza.remotolotto1.pec@legalmail.it

Oggetto: Procedura di Adesione ACCORDO QUADRO PER L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI – ID 2296 – LOTTO 1. Trasmissione Piani dei Fabbisogni.

In ottemperanza delle modalità di adesione indicate negli atti dell'Accordo quadro per i servizi di cui all'oggetto, si trasmettono in allegato i quattro piani dei fabbisogni di seguito elencati:

- Piano dei fabbisogni nell'ambito dell'Intera ASP di Agrigento;
- Piano dei fabbisogni nell'ambito della PNRR MISSIONE 6 SALUTE - M6.C2 1.1.1.1 AMMODERNAMENTO DEL PARCO TECNOLOGICO E DIGITALE OSPEDALIERO (DIGITALIZZAZIONE DEA I E II)presso il P.O. di Agrigento;
- Piano dei fabbisogni nell'ambito della PNRR MISSIONE 6 SALUTE - M6.C2 1.1.1.1 AMMODERNAMENTO DEL PARCO TECNOLOGICO E DIGITALE OSPEDALIERO (DIGITALIZZAZIONE DEA I E II)presso il P.O. di Sciacca;
- Piano dei fabbisogni nell'ambito della PNRR MISSIONE 6 SALUTE - M6.C2 1.1.1.1 AMMODERNAMENTO DEL PARCO TECNOLOGICO E DIGITALE OSPEDALIERO (DIGITALIZZAZIONE DEA I E II)presso il P.O. di Ribera;

Si resta in attesa di ricevere i quattro rispettivi piani operativi
Distinti Saluti

Il Coll. Amministrativo
Dott. Pietro Vitellaro

Il Direttore UOC Servizio
Provveditorato
Dott. Oreste Falco

U.O.C. PROVVEDITORATO
Il Dirigente Amministrativo
Dr.ssa Rosalia Cala'

PROCEDURA DI ADESIONE ACCORDO QUADRO PER L`AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI - ID 2296 - LOTTO 1 - TRASMISSIONE PIANI DEI FABBISOGNI

Da **Posta Certificata Legalmail** <posta-certificata@legalmail.it>
A **forniture@pec.aspag.it** <forniture@pec.aspag.it>
Data lunedì 27 febbraio 2023 - 12:44

Ricevuta di avvenuta consegna

Il giorno 27/02/2023 alle ore 12:44:36 (+0100) il messaggio "PROCEDURA DI ADESIONE ACCORDO QUADRO PER L`AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI - ID 2296 - LOTTO 1 - TRASMISSIONE PIANI DEI FABBISOGNI" proveniente da "forniture@pec.aspag.it" ed indirizzato a "sicurezza.remotolotto1.pec@legalmail.it" è stato consegnato nella casella di destinazione.

Questa ricevuta, per Sua garanzia, è firmata digitalmente e la preghiamo di conservarla come attestato della consegna del messaggio alla casella destinataria.

Identificativo messaggio: opec21004.20230227124429.139413.844.1.54@pec.aruba.it

Delivery receipt

The message "PROCEDURA DI ADESIONE ACCORDO QUADRO PER L`AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI - ID 2296 - LOTTO 1 - TRASMISSIONE PIANI DEI FABBISOGNI" sent by "forniture@pec.aspag.it", on 27/02/2023 at 12:44:36 (+0100) and addressed to "sicurezza.remotolotto1.pec@legalmail.it", was delivered by the certified email system.

As a guarantee to you, this receipt is digitally signed. Please keep it as certificate of delivery to the specified mailbox.

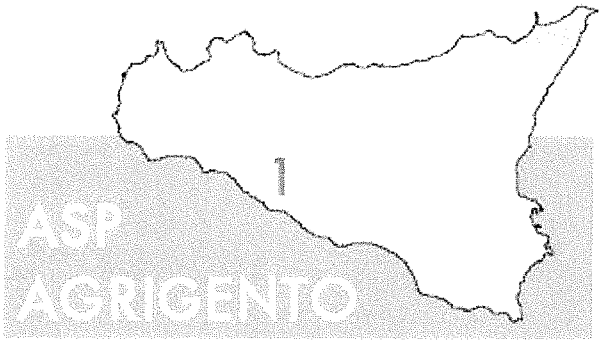
Message ID: opec21004.20230227124429.139413.844.1.54@pec.aruba.it

postacert.eml
daticert.xml
smime.p7s

ALL. 3

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

Azienda Sanitaria Provinciale di Agrigento



PIANO DEI FABBISOGNI

AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO

(CIG_____)

NOTA BENE:

Durante l'esecuzione contrattuale è possibile che il progresso tecnologico innovi i servizi di base con l'introduzione di nuove funzionalità e/o nuovi servizi in ogni caso complementari/supplementari ai servizi previsti in gara mediante procedura negoziata ai sensi dell'art. 63 co. 3 lett b), d.lgs. n. 50/2016 oppure mediante una modifica ai sensi dell'art. 106 co.1 lett. b) d lgs. n. 50/2016.

L'organismo tecnico di Coordinamento e Controllo, raccolta la necessità di introduzione di un nuovo servizio, esclusivamente se lo stesso risulta nella disponibilità dell'aggiudicatario dell'Accordo Quadro, richiederà allo stesso, sulla base di un apposito documento di "specifiche tecniche" (con annessi i requisiti da garantire), la quotazione di un servizio da inserire nei servizi oggetto di fornitura. Tale nuovo servizio sarà dunque inserito in perimetro tra i servizi acquistabili.

INDICE

1. DATI ANAGRAFICI DELL'AMMINISTRAZIONE

Ragione sociale Amministrazione:	Azienda Sanitaria Provinciale di Agrigento
Indirizzo	Viale Della Vittoria, 321
CAP	92100
Comune	Agrigento
Provincia	AG
Regione	Sicilia
Codice Fiscale	02570930848
Codice IPA	asp_ag
Indirizzo mail	servizi.informatici@aspag.it
PEC	protocollo@pec.aspag.it

Referente Amministrazione	DOTT. RICCARDO INSALACO
Ruolo	Referente Informatico Aziendale
Telefono	3388002237
Indirizzo mail	riccardo.insalaco@aspag.it
PEC	servizi.informatici@pec.aspag.it

2. CONTESTO

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

L'Azienda Sanitaria, con sede legale in Viale della Vittoria 321 – 92100 Agrigento, è stata istituita con la Legge regionale 14 aprile 2009 N. 5 ed è divenuta operativa a partire dal 1° settembre 2009. L'organizzazione ed il funzionamento dell'azienda, disciplinati con atto aziendale di diritto privato, mirano ad assicurare l'erogazione delle prestazioni essenziali ed appropriate, lo sviluppo dei sistemi di qualità, la massima accessibilità ai servizi dei cittadini, l'equità delle prestazioni erogate, il raccordo istituzionale con gli Enti Locali, il collegamento con le altre organizzazioni sanitarie e di volontariato, nonché l'ottimalizzazione e l'integrazione delle risorse e delle risposte assistenziali.

Fine istituzionale dell' "Azienda Sanitaria Provinciale di Agrigento " è l'erogazione, sia in regime di ricovero che in forma ambulatoriale, di servizi e prestazioni di diagnosi e cura delle malattie acute e di quelle che richiedono interventi di urgenza.

Le prestazioni erogate dall'Azienda ospedaliera comprendono le visite mediche, l'assistenza infermieristica, e ogni atto e procedura diagnostica e terapeutica necessari per risolvere i problemi di salute di adulti e bambini, degenti e non degenti, compatibili con il livello di dotazione tecnologica delle singole strutture.

L'Azienda, dotata di oltre 500 posti letto, partecipa ai programmi nazionali e regionali nei settori dell'emergenza, dei trapianti, della prevenzione, della tutela materno-infantile e delle patologie oncologiche, e svolge attività didattiche e di ricerca.

L'attività ospedaliera, coordinata dalla direzione aziendale, è erogata attraverso due Distretti Ospedalieri dell'Azienda Sanitaria Provinciale (denominati AG1 e AG2) che operano mediante un'organizzazione in rete anche al fine di assicurare all'utente l'appropriatezza del percorso di accoglienza, presa in carico, cura e dimissione.

Del distretto AG1 fanno parte i seguenti Presidi Ospedalieri:

- S. Giovanni di Dio (Agrigento)
- Barone Lombardo (Canicattì)
- S. Giacomo D'Altopasso (Licata)

Del distretto AG2 fanno parte i seguenti Presidi Ospedalieri:

- Fratelli Parlapiano (Ribera)
- Giovanni Paolo II (Sciacca)

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

Di seguito si riporta una descrizione semplificata, relativa allo stato di fatto inerente vari aspetti di cybersecurity gestiti oggi presso l'Amministrazione ed in generale dell'architettura di rete dell'Azienda Sanitaria Provinciale di Agrigento.

L'Amministrazione si è dotata di una coppia di accessi dati alle reti INTERNET/INTRANET, in convenzione Consip SPC CONN. Tali collegamenti dati si trovano presso il CED di Viale Della Vittoria – Agrigento e sono in alta affidabilità con banda pari ad 600 Mbps. Le sedi periferiche dell'Amministrazione sono collegate al centro stella attraverso dei collegamenti VPN MPLS ed accedono alla rete INTERNET attraverso i firewall di centro stella.

Attualmente i servizi di sicurezza perimetrale, per tutti i server/Virtual Machine, vengono gestiti dall'Amministrazione attraverso dei firewall, brand Watchguard, attivi su appliance fisiche. Tutti i servizi vengono esposti alla rete pubblica attraverso questa appliance.

I server/VM sono collegati, attraverso l'infrastruttura LAN cliente, alla subnet *private* dei firewall perimetrali. La gestione della virtualizzazione viene garantita dal VMware Cluster Datastore. Tutti i server, su cui sono attive circa N.135 VM, e le

storage aziendali sono installati, quasi, nella loro totalità nel CED di Viale della Vittoria. Circa 10 VM risiedono invece tra i Presidi ospedalieri di Sciacca e Canicattì (i server totali tra fisici e virtuali sono circa 200). Non esiste un sito di Disaster-Recovery esterno al campus ed i backup vengono effettuati mediante il software VEEAM Backup, mentre i backup dei DB vengono effettuati su nastri esterni.

I PC dei dipendenti navigano protetti dai Watchguard, dove vengono applicate policy di navigazione, content-filtering, IDS, ecc..

La gestione da remoto sulle singole PDL (circa 2500) viene effettuata grazie al software di *remote control* Rustdesk.

La rete interna dell'Azienda dispone di N.2 core-switch, presso il CED di Viale della Vittoria, in alta affidabilità. Tali core-switch sono interconnessi ai router spc2. Gli switch che servono i padiglioni amministrativi e sanitari della sede di Viale della Vittoria vengono interconnessi con dorsali, sempre in F.O. ed a questi si attestano gli apparati Layer2 posti nei vari piani/reparti: il totale degli apparati per questo sito, al netto dei core-switch, è pari a N.35. Gli altri Presidi Ospedalieri contano una totalità di circa 154 *device*. La rete LAN è segmentata logicamente attraverso l'uso di VLAN dedicate e di access-list per consentire/negare (secondo necessità) la comunicazione tra le subnet all'interno del campus. Il numero complessivo degli apparati di rete è pari a 300.

La maggior parte degli apparati di rete sono managed ma esistono, pochissimi, apparati unmanaged nella rete cliente. Tutti gli switch, Access-Point ed UPS vengono monitorati attraverso il software Zabbix, gestito dal presidio tecnico.

Non esistono server syslog su cui si dovrebbero conservare, quantomeno, i log del Domain Controller, del server di posta elettronica e dell'antispam né tantomeno software per interpolare gli eventi tracciati.

Per ciò che riguarda l'accesso esterno, nella rete dell'Amministrazione, di fornitori/dipendenti sono state create, in un VPN Concentrator, delle utenze ad hoc. L'accesso avviene attraverso il solo inserimento della doppietta username/password.

La protezione delle macchine dell'Amministrazione è garantita ad oggi da un sistema antivirus di brand Kaspersky.

▪ DESCRIZIONE DELL'ESIGENZA

La trasformazione digitale nell'ambito sanitario gioca un ruolo chiave nell'evoluzione dei modelli assistenziali e organizzativi, soprattutto in un contesto come quello odierno che necessita di un'intensa collaborazione tra gli attori del Servizio Sanitario con lo scopo di offrire i servizi più idonei per la salvaguardia della salute e del benessere dei cittadini. La necessità di garantire i processi collaborativi tra diversi attori istituzionali e la spinta normativa del GDPR che sancisce l'obbligo di attuare le misure tecniche e organizzative atte a mitigare il rischio connesso ai trattamenti dei dati privati, attribuiscono alla sicurezza digitale un ruolo cruciale per la realizzazione di nuovi servizi che rispondano alla crescente domanda di efficacia, tempestività, sicurezza e appropriatezza delle prestazioni. La natura dei dati trattati da aziende sanitarie caratterizzate da un elevato grado di complessità organizzativa, richiede un focus specifico rispetto ai temi della cybersicurezza anche in relazione alla potenziale attribuzione dello status di infrastruttura critica di interesse nazionale (Commissione Europea - Council Directive 2008/114/EC of 8 December 2008, Ministero dell'Interno – Decreto del 9 gennaio 2008 "Individuazione delle infrastrutture critiche informatiche di interesse nazionale").

L' Azienda Sanitaria Provinciale di Agrigento è un'organizzazione al servizio del cittadino e detiene informazioni pubblicamente accessibili e informazioni riservate ai fini della privacy. La modifica non autorizzata delle informazioni pubblicate o la diffusione di quelle riservate possono avere un impatto rilevante sull'operatività aziendale:

- compromissione della mission aziendale
- danni a terzi con potenziali rischi di rivalsa
- sanzioni per violazione degli obblighi normativi
- danno alla reputazione e crollo della fiducia

In relazione alla protezione dei dati personali, il "Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016... (GDPR – General Data Protection Regulation)" sancisce l'obbligo di attuare le misure tecniche e organizzative atte a mitigare il rischio connesso ai trattamenti dei dati privati e a conseguire un adeguato livello di sicurezza, limitando, per quanto possibile, la distruzione accidentale o illecita, la perdita, la modifica, la rivelazione, l'accesso non autorizzato ai dati detenuti da un'organizzazione o ente titolare. L'individuazione e l'attuazione delle misure secondo un principio di proporzionalità tra mezzi e fini, rientra tra compiti dell'organizzazione attuatrice che, a tale fine, potrà avvalersi di codici di condotta o pratiche dettate da organismi accreditati o autorevoli nel campo della sicurezza delle informazioni.

Il presente capitolo ha lo scopo di descrivere le esigenze di Azienda Sanitaria Provinciale di Agrigento 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'Azienda Sanitaria Provinciale di Agrigento necessita dei servizi di seguito indicati, mirati a garantire la corretta operatività dei sistemi attraverso la prevenzione, gestione, risoluzione di qualsiasi criticità di sicurezza che possa degradare il servizio all'utenza. La finalità principale è la gestione ed il monitoraggio dei servizi di sicurezza ed, in aggiunta, la ricezione e l'analisi di reportistica (log) dando priorità ai processi di risoluzione e/o mitigazione delle minacce.

Si necessita inoltre dei servizi di seguito indicati, al fine di assicurare, in caso di riscontro di eventi anomali nelle workstation o server aziendali e altri eventi di sicurezza degni di nota, un'analisi approfondita degli eventi occorsi, dell'attuale livello di sicurezza dell'intera infrastruttura monitorata e allertare di conseguenza i corretti riferimenti aziendali indicati dall'Amministrazione. In tal modo, le strutture interne preposte potranno di conseguenza intervenire con azioni correttive su indicazione dello stesso sistema di monitoraggio. L'ASP intende sostituire i sistemi di End Point Protection ad oggi in uso con quelli offerti dal RTI nel presente accordo quadro.

Azienda Sanitaria Provinciale di Agrigento 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 per l'Ente coinvolto:

Servizi di Security Operation Center L1.S1

Si richiede l'erogazione di un servizio da remoto che, attraverso gli adeguati strumenti tecnologici di back-end, garantisca un servizio di monitoraggio ed *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 ai suggerimenti di azioni di contenimento, ripristino e prevenzione futura in stretta collaborazione con le strutture dell'Ente preposte alla gestione sistemistica. Tra le funzioni richieste si richiede, quindi, la raccolta centralizzata dei log e degli eventi di sicurezza; la correlazione di più eventi che caratterizzano il potenziale incidente; la capacità di identificazione, gestione, mitigazione e risoluzione degli attacchi; la produzione di report periodici di sintesi. 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.

Servizi di protezione degli End-point L1.S7

Si richiede l'erogazione di un servizio remoto che, dovrà consentire la protezione dei dispositivi collegati alla rete (PC e Server) dall'accesso non autorizzato o dall'esecuzione di software dannoso. La protezione degli endpoint deve garantire, inoltre, che i dispositivi (es. pc desktop, laptop, ecc.) raggiungano un livello di sicurezza definito e siano conformi alle policy e ai requisiti di conformità e sicurezza stabiliti dall'Ente. Nel dettaglio devono essere fornite le funzioni di: protezione con sistemi antimalware; ispezione localmente anche del traffico HTTPS; controllo dell'uso o anche blocco dei dispositivi USB; trasmissione degli eventi alle piattaforme di correlazione; monitoraggio continuo delle minacce avanzate e protezione da malware basati su file e senza file; protezione e prevenzione dalla perdita di dati.

Servizi Specialistici L1.S15

Si richiede l'erogazione di tali servizi finalizzati:

- alle attività d'analisi, raccolta informazioni, meeting tecnici, configurazioni personalizzate e migrazione relative ai servizi SIEM e SOAR dell'Amministrazione verso gli analoghi servizi proposti all'interno del centro servizi del RTI;
- alla migrazione dai sistemi di end-point protection attuali (Kaspersky) a quelli previsti dalla convenzione, comprese tutte le attività di analisi e configurazione per l'attivazione di configurazioni ad hoc, raccolta informazioni, meeting tecnici, ecc.; supporto nell'analisi dei deliverable raccolti a seguito di rilevazioni di violazioni.

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 36 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	200	200	200	0
				> 6.000 Eps				

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	1699	1699	1699	0
				> 5.000 nodi				

- ***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 le sedi dell'Amministrazione ove specificato dall'Amministrazione stessa; in alternativa presso la Sede del Fornitore.

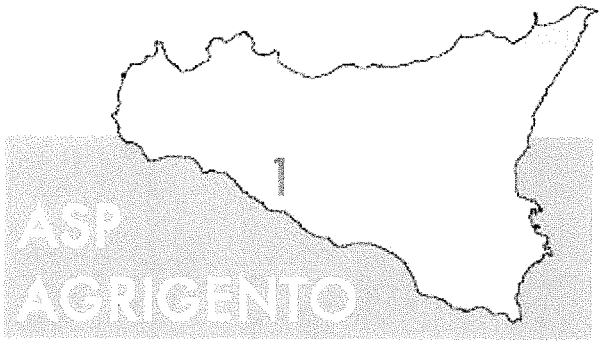
INDICATORE DI PROGRESSO

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

Azienda Sanitaria Provinciale di Agrigento



PIANO DEI FABBISOGNI

P.O. Fratelli Parlapiano Ribera

(CUP C96G22002340006**, CIG_____)**

NOTA BENE:

Durante l'esecuzione contrattuale è possibile che il progresso tecnologico innovi i servizi di base con l'introduzione di nuove funzionalità e/o nuovi servizi in ogni caso complementari/supplementari ai servizi previsti in gara mediante procedura negoziata ai sensi dell'art. 63 co. 3 lett b), d.lgs. n. 50/2016 oppure mediante una modifica ai sensi dell'art. 106 co.1 lett. b) d.lgs. n. 50/2016.

L'organismo tecnico di Coordinamento e Controllo, raccolta la necessità di introduzione di un nuovo servizio, esclusivamente se lo stesso risulta nella disponibilità dell'aggiudicatario dell'Accordo Quadro, richiederà allo stesso, sulla base di un apposito documento di "specifiche tecniche" (con annessi i requisiti da garantire), la quotazione di un servizio da inserire nei servizi oggetto di fornitura. Tale nuovo servizio sarà dunque inserito in perimetro tra i servizi acquistabili.

INDICE

1. DATI ANAGRAFICI DELL'AMMINISTRAZIONE

Ragione sociale Amministrazione:	Azienda Sanitaria Provinciale di Agrigento
Indirizzo	Viale Della Vittoria, 321
CAP	92100
Comune	Agrigento
Provincia	AG
Regione	Sicilia
Codice Fiscale	02570930848
Codice IPA	asp_ag
Indirizzo mail	servizi.informatici@aspag.it
PEC	protocollo@pec.aspag.it

Referente Amministrazione	DOTT. RICCARDO INSALACO
Ruolo	Referente Informatico Aziendale
Telefono	3388002237
Indirizzo mail	riccardo.insalaco@aspag.it
PEC	servizi.informatici@pec.aspag.it

2. CONTESTO

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

L'Azienda Sanitaria, con sede legale in Viale della Vittoria 321 – 92100 Agrigento, è stata istituita con la Legge regionale 14 aprile 2009 N. 5 ed è divenuta operativa a partire dal 1° settembre 2009. L'organizzazione ed il funzionamento dell'azienda, disciplinati con atto aziendale di diritto privato, mirano ad assicurare l'erogazione delle prestazioni essenziali ed appropriate, lo sviluppo dei sistemi di qualità, la massima accessibilità ai servizi dei cittadini, l'equità delle prestazioni erogate, il raccordo istituzionale con gli Enti Locali, il collegamento con le altre organizzazioni sanitarie e di volontariato, nonché l'ottimalizzazione e l'integrazione delle risorse e delle risposte assistenziali.

Fine istituzionale dell' "Azienda Sanitaria Provinciale di Agrigento " è l'erogazione, sia in regime di ricovero che in forma ambulatoriale, di servizi e prestazioni di diagnosi e cura delle malattie acute e di quelle che richiedono interventi di urgenza.

Le prestazioni erogate dall'Azienda ospedaliera comprendono le visite mediche, l'assistenza infermieristica, e ogni atto e procedura diagnostica e terapeutica necessari per risolvere i problemi di salute di adulti e bambini, degenti e non degenti, compatibili con il livello di dotazione tecnologica delle singole strutture.

L'Azienda, dotata di oltre 500 posti letto, partecipa ai programmi nazionali e regionali nei settori dell'emergenza, dei trapianti, della prevenzione, della tutela materno-infantile e delle patologie oncologiche, e svolge attività didattiche e di ricerca.

L'attività ospedaliera, coordinata dalla direzione aziendale, è erogata attraverso due Distretti Ospedalieri dell'Azienda Sanitaria Provinciale (denominati AG1 e AG2) che operano mediante un'organizzazione in rete anche al fine di assicurare all'utente l'appropriatezza del percorso di accoglienza, presa in carico, cura e dimissione.

Del distretto AG1 fanno parte i seguenti Presidi Ospedalieri:

- S. Giovanni di Dio (Agrigento)
- Barone Lombardo (Canicattì)
- S. Giacomo D'Altopasso (Licata)

Del distretto AG2 fanno parte i seguenti Presidi Ospedalieri:

- Fratelli Parlapiano (Ribera)
- Giovanni Paolo II (Sciacca)

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

Di seguito si riporta una descrizione semplificata, relativa allo stato di fatto inerente vari aspetti di cybersecurity gestiti oggi presso l'Amministrazione ed in generale dell'architettura di rete dell'Azienda Sanitaria Provinciale di Agrigento.

L'Amministrazione si è dotata di una coppia di accessi dati alle reti INTERNET/INTRANET, in convenzione Consip SPC CONN. Tali collegamenti dati si trovano presso il CED di Viale Della Vittoria – Agrigento e sono in alta affidabilità con banda pari ad 600 Mbps. Le sedi periferiche dell'Amministrazione sono collegate al centro stella attraverso dei collegamenti VPN MPLS ed accedono alla rete INTERNET attraverso i firewall di centro stella.

Attualmente i servizi di sicurezza perimetrale, per tutti i server/Virtual Machine, vengono gestiti dall'Amministrazione attraverso dei firewall, brand Watchguard, attivi su appliance fisiche. Tutti i servizi vengono esposti alla rete pubblica attraverso questa appliance.

I server/VM sono collegati, attraverso l'infrastruttura LAN cliente, alla subnet *private* dei firewall perimetrali. La gestione della virtualizzazione viene garantita dal VMware Cluster Datastore. Tutti i server, su cui sono attive circa N.135 VM, e le

storage aziendali sono installati, quasi, nella loro totalità nel CED di Viale della Vittoria. Circa 10 VM risiedono invece tra i Presidi ospedalieri di Sciacca e Canicattì (i server totali tra fisici e virtuali sono circa 200). Non esiste un sito di Disaster-Recovery esterno al campus ed i backup vengono effettuati mediante il software VEEAM Backup, mentre i backup dei DB vengono effettuati su nastri esterni.

I PC dei dipendenti navigano protetti dai Watchguard, dove vengono applicate policy di navigazione, content-filtering, IDS, ecc..

La gestione da remoto sulle singole PDL (circa 2500) viene effettuata grazie al software di *remote control* Rustdesk.

La rete interna dell'Azienda dispone di N.2 core-switch, presso il CED di Viale della Vittoria, in alta affidabilità. Tali core-switch sono interconnessi ai router spc2. Gli switch che servono i padiglioni amministrativi e sanitari della sede di Viale della Vittoria vengono interconnessi con dorsali, sempre in F.O. ed a questi si attestano gli apparati Layer2 posti nei vari piani/reparti: il totale degli apparati per questo sito, al netto dei core-switch, è pari a N.35. Gli altri Presidi Ospedalieri contano una totalità di circa 154 *device*. La rete LAN è segmentata logicamente attraverso l'uso di VLAN dedicate e di access-list per consentire/negare (secondo necessità) la comunicazione tra le subnet all'interno del campus. Il numero complessivo degli apparati di rete è pari a 300.

La maggior parte degli apparati di rete sono managed ma esistono, pochissimi, apparati unmanaged nella rete cliente. Tutti gli switch, Access-Point ed UPS vengono monitorati attraverso il software Zabbix, gestito dal presidio tecnico.

Non esistono server syslog su cui si dovrebbero conservare, quantomeno, i log del Domain Controller, del server di posta elettronica e dell'antispam né tantomeno software per interpolare gli eventi tracciati.

Per ciò che riguarda l'accesso esterno, nella rete dell'Amministrazione, di fornitori/dipendenti sono state create, in un VPN Concentrator, delle utenze ad hoc. L'accesso avviene attraverso il solo inserimento della doppietta username/password.

La protezione delle macchine dell'Amministrazione è garantita ad oggi da un sistema antivirus di brand Kaspersky.

▪ DESCRIZIONE DELL'ESIGENZA

La trasformazione digitale nell'ambito sanitario gioca un ruolo chiave nell'evoluzione dei modelli assistenziali e organizzativi, soprattutto in un contesto come quello odierno che necessita di un'intensa collaborazione tra gli attori del Servizio Sanitario con lo scopo di offrire i servizi più idonei per la salvaguardia della salute e del benessere dei cittadini. La necessità di garantire i processi collaborativi tra diversi attori istituzionali e la spinta normativa del GDPR che sancisce l'obbligo di attuare le misure tecniche e organizzative atte a mitigare il rischio connesso ai trattamenti dei dati privati, attribuiscono alla sicurezza digitale un ruolo cruciale per la realizzazione di nuovi servizi che rispondano alla crescente domanda di efficacia, tempestività, sicurezza e appropriatezza delle prestazioni. La natura dei dati trattati da aziende sanitarie caratterizzate da un elevato grado di complessità organizzativa, richiede un focus specifico rispetto ai temi della cybersicurezza anche in relazione alla potenziale attribuzione dello status di infrastruttura critica di interesse nazionale (Commissione Europea - Council Directive 2008/114/EC of 8 December 2008, Ministero dell'Interno – Decreto del 9 gennaio 2008 "Individuazione delle infrastrutture critiche informatiche di interesse nazionale").

L' Azienda Sanitaria Provinciale di Agrigento è un'organizzazione al servizio del cittadino e detiene informazioni pubblicamente accessibili e informazioni riservate ai fini della privacy. La modifica non autorizzata delle informazioni pubblicate o la diffusione di quelle riservate possono avere un impatto rilevante sull'operatività aziendale:

- compromissione della mission aziendale
- danni a terzi con potenziali rischi di rivalsa
- sanzioni per violazione degli obblighi normativi
- danno alla reputazione e crollo della fiducia

In relazione alla protezione dei dati personali, il "Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016... (GDPR – General Data Protection Regulation)" sancisce l'obbligo di attuare le misure tecniche e organizzative atte a mitigare il rischio connesso ai trattamenti dei dati privati e a conseguire un adeguato livello di sicurezza, limitando, per quanto possibile, la distruzione accidentale o illecita, la perdita, la modifica, la rivelazione, l'accesso non autorizzato ai dati detenuti da un'organizzazione o ente titolare. L'individuazione e l'attuazione delle misure secondo un principio di proporzionalità tra mezzi e fini, rientra tra compiti dell'organizzazione attuatrice che, a tale fine, potrà avvalersi di codici di condotta o pratiche dettate da organismi accreditati o autorevoli nel campo della sicurezza delle informazioni.

La presente richiesta rientra nell'ambito delle misure e azioni intraprese per l'attuazione del PNRR MISSIONE 6 SALUTE - M6.C2 1.1.1.1 AMMODERNAMENTO DEL PARCO TECNOLOGICO E DIGITALE OSPEDALIERO (DIGITALIZZAZIONE DEA I E II) – Linea d'intervento Fabbisogni Ulteriori Tecnologie – "***Altro***" per:

- Il P.O. FRATELLI PARLAPIANO – Via Circonvallazione - Ribera.

Riguarda inoltre l'avvio di progetti finalizzati alla trasformazione digitale dei propri servizi in base al Modello strategico evolutivo dell'informatica della PA e ai principi afferenti al Piano Triennale per l'informatica della Pubblica Amministrazione.

Il presente capitolo ha lo scopo di descrivere le esigenze di Azienda Sanitaria Provinciale di Agrigento 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..

Azienda Sanitaria Provinciale di Agrigento necessita dei servizi di seguito indicati, al fine di assicurare, in caso di riscontro di eventi anomali, vulnerabilità critiche e altri eventi di sicurezza degni di nota, un'analisi approfondita degli eventi occorsi, dell'attuale livello di sicurezza dell'intera infrastruttura monitorata e allertare di conseguenza i corretti riferimenti aziendali indicati da Azienda Sanitaria Provinciale di Agrigento. In tal modo, le strutture interne preposte potranno di conseguenza intervenire con azioni correttive su indicazione dello stesso sistema di monitoraggio.

Il rilevamento delle vulnerabilità presenti all'interno del perimetro aziendale e la dotazione degli strumenti di efficacia probatoria e validità legale (Firme digitali remote) sono ulteriori obbiettivi che si pone questa azione.

Azienda Sanitaria Provinciale di Agrigento 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 per l'Ente coinvolto:

Servizi di gestione continua delle Vulnerabilità di Sicurezza L1.S4

Tale servizio dovrà consentire all'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.

Servizi di certificati SSL L1.S8

L'amministrazione necessita di N.2 certificati SSL. Il certificato SSL (*Secure Sockets Layer*) e il suo successore TLS (*Transport Layer Security*), sono protocolli standard necessari a garantire affidabilità e sicurezza della comunicazione tra le componenti client e server di un'applicazione internet. Il certificato assicura che le informazioni sensibili fornite dagli utenti sul web rimangano riservate e non vengano in alcun modo intercettate da terze parti (comunicazione criptata tra il client server e il server web).

Servizi di firma digitale remota L1.S11

Tale servizio richiesto dovrà consentire all'Amministrazione di dare efficacia probatoria ai documenti informatici firmati digitalmente, favorendo così i processi di dematerializzazione e consentendo l'automazione e l'ottimizzazione dei processi aziendali.

Servizi Specialistici L1.S15

Si richiede l'erogazione di tali servizi finalizzati:

- raccolta informazioni, meeting tecnici e analisi per l'*assesment* di vulnerabilità prodotto e conseguenti attività propedeutiche;
- ad attività di delivery dei servizi oggetto di fornitura durante le operazioni di migrazione;
- al supporto nella definizione, configurazione ed erogazione del servizio di monitoraggio continuo delle vulnerabilità di sicurezza con particolare riferimento all'analisi dei deliverable raccolti a seguito dell'esecuzione da parte del fornitore delle sessioni di vulnerability assessment previsti nell'accordo quadro 2296.
- alle attività d'analisi, raccolta informazioni, meeting tecnici, configurazioni personalizzate, predisposizione connettori ed integrazione dei sistemi di firma digitale con gli applicativi aziendali.

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 36 mesi.

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	250	250	250	0

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	1	0	0	0
				SSL OV Wildcard	1	0	0	0
				SSL EV				
				SSL DV				
				SSL Code signing				
				SSL Client Auth				

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	201	201	201	0
				500 e fino a 1.000 utenti				
				> 1.000 utenti				
				Garantita - N. 1 firma				
				Garantita - N. 5 firme aggiuntive				

- ***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 le sedi dell'Amministrazione ove specificato dall'Amministrazione stessa; in alternativa presso la Sede del Fornitore.

▪ 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		

SERVIZIO SANITARIO NAZIONALE - REGIONE SICILIANA
Azienda Sanitaria Provinciale di Agrigento
Sede legale : Viale della Vittoria n.321 92100 Agrigento
Partita IVA - Codice Fiscale : 02570930848
Sistemi Informatici Aziendali

Tel. 0922407111
cell: 3388002237
EMail : riccardo.insalaco@aspag.it

Prot.n. 00 32444 *del* 24/02/2023

Al **Direttore U.O.C. Servizio Provveditorato**

e.p.c. Al **Commissario Straordinario**
Al **Direttore Amministrativo**

SEDE

Oggetto: *Missione 6 PNRR - Ammodernamento tecnologico Digitalizzazione DEA - Trasmissione Piano dei Fabbisogni adesione A.Q. Consip* ***Sicurezza "da remoto"*** *- ID 2296.*

Con riferimento al procedimento di cui in oggetto, nel mese dicembre u.s., questa Amministrazione ha richiesto all'RTI aggiudicataria dell'A.Q. ID 2296 la redazione dei Piani Operativi, ID: AQSEC-2296L1- Versione: 1.0 Data: 30/12/2022, conseguenti all'invio di due distinti piani dei fabbisogni redatti sulla scorta delle valutazioni tecniche responsabilmente operate dallo scrivente.
Tuttavia, i Piani Operativi prodotti dall'aggiudicatario sono risultati non in linea con il reale fabbisogno aziendale e, quindi, ritenuti non idoneo.
Conseguentemente, stante l'immutata necessità di acquisire servizi in ambito di Cyber Security, si è reso necessario procedere con la revisione dei PdF precedente sviluppati con un maggiore grado di dettaglio delle richieste operative e con suddivisione dei progetti tra PNRR e parte da finanziare con il bilancio aziendale.
In particolare, i progetti PNRR sono stati distinti con riguardo a ciascun DEA e con indicazione della previsione di spesa massima finanziabile.
Per quanto sopra ed al fine di potere riattivare la procedura di adesione all'A.Q. "Sicurezza da remoto", con la presente, si trasmettono quattro distinti PdF, di cui tre orientati all'approvvigionamento di servizi costituenti l'intervento PNRR - Missione 6 Salute - M6.C2 – 1.1.1. Ammodernamento del parco tecnologico e digitale ospedaliero (Digitalizzazione delle strutture ospedaliere (DEA Dipartimenti di Emergenza e Accettazione di Livello I e II)).
I predetti PdF, inoltre, risultano specificamente afferenti alle attività progettuali PNRR di seguito elencate:

Presidio	***Intervento***	***Importo***
PO Ribera	parte del 5	64.556,62 €
PO Sciacca	parte del 13	153.416,58 €
PO Agrigento	parte del 21	165.547,10 €
		383.520,31 €

Il prefato quadro economico è stato elaborato tenuto conto delle attività e servizi che il fornitore dell'A.Q. per le Pubbliche Amministrazioni Locali (PAL) - RTI costituito Accenture S.p.A., Fincantieri Nextech S.p.A., Fasteweb S.p.A., Deas, Difesa e Analisi Sistemi S.p.A. deve eseguire

tenuto conto del Piano dei Fabbisogni che lo scrivente ha redatto per la realizzazione degli obiettivi PNRR.

Oltre, però, rilevano tutte le esigenze aziendali che, in ambito di cyber security, discendono dallo specifico e stringente dettato normativo dispiegato con la circolare dell'Agenzia per la Cybersicurezza Nazionale n. 4336 del 21 aprile 2022.

Quindi, gli obiettivi finalizzati dal PNRR rappresentano soltanto una parte delle esigenze di adeguamento tecnologico dell'ASP di Agrigento e richiedono un'integrazione con servizi da declinare in un ulteriore PdF da sottoporre al medesimo aggiudicatario dell'A.Q. "Sicurezza da remoto".

Peraltro, le predette decisioni operative risultano in linea con le indicazioni fornite, in tal senso, dal Dipartimento Regionale per la Pianificazione Strategica con nota prot. n. 42762 del 21.09.2022.

Indicazioni, quest'ultime, che impongono di avvalersi delle iniziative che Consip S.p.A. ha reso disponibili per soddisfare le esigenze delle Pubbliche Amministrazioni per la cybersicurezza e, quindi, con adesione all'accordo Quadro "Servizi di sicurezza da remoto" - ID SIGEF 2296.

Il piano dei fabbisogni riporta una elencazione di attività e servizi che lo stesso richiamato fornitore aggiudicatario dell'AQ Consip dovrà esplicitare con il progetto da sottoporre all'approvazione dell'Amministrazione con quantificazione dei costi che in atto non è possibile preventivare.

Per tutto quanto sopra, codesto Servizio è invitato ad attivare le procedure indicate da Consip al punto 2 "Emissione del Piano dei Fabbisogni" della Guida all'AQ LOTTO 1 - Servizi di sicurezza da remoto - ID 2296 - per l'acquisizione di quattro distinti progetti esecutivi che lo scrivente si riserva, fin da subito, di compulsare per verificarne l'aderenza al complessivo bisogno manifestato con i rispettivi PdF.

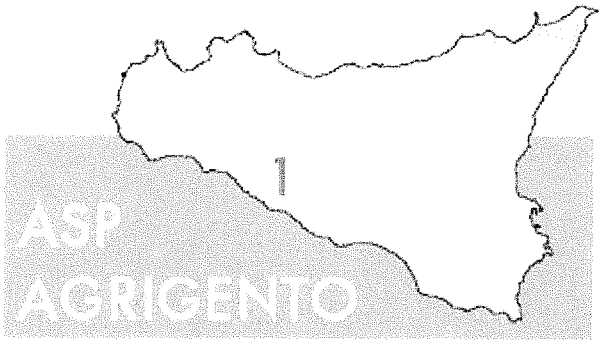
Sicché, dovrà trasmettere gli allegati Piani dei Fabbisogni che lo scrivente ha redatto per consentire a questa Amministrazione di potere soddisfare il fabbisogno aziendale in termini di "cyber security" con costi che trovano copertura nelle risorse PNRR, fatta eccezione per il quarto PdF da finanziare con fondi del bilancio aziendale.

Peraltro, chiarisce che l'adesione all'AQ. "Sicurezza da remoto" rappresenta una parte del fabbisogno complessivo di ammodernamento tecnologico dei sistemi ICT che verrà a completarsi con le adesioni successive in quanto già previste nel report Age.na.s.

Il Referente Sistemi Informatici Aziendali
Dott. Riccardo Insalaco

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

Azienda Sanitaria Provinciale di Agrigento



PIANO DEI FABBISOGNI

P.O. S. GIOVANNI DI DIO AGRIGENTO

(CUP C46G22002010006**, CIG_____)**

NOTA BENE:

Durante l'esecuzione contrattuale è possibile che il progresso tecnologico innovi i servizi di base con l'introduzione di nuove funzionalità e/o nuovi servizi in ogni caso complementari/supplementari ai servizi previsti in gara mediante procedura negoziata ai sensi dell'art. 63 co. 3 lett b), d.lgs. n. 50/2016 oppure mediante una modifica ai sensi dell'art. 106 co.1 lett. b) d.lgs. n. 50/2016.

L'organismo tecnico di Coordinamento e Controllo, raccolta la necessità di introduzione di un nuovo servizio, esclusivamente se lo stesso risulta nella disponibilità dell'aggiudicatario dell'Accordo Quadro, richiederà allo stesso, sulla base di un apposito documento di "specifiche tecniche" (con annessi i requisiti da garantire), la quotazione di un servizio da inserire nei servizi oggetto di fornitura. Tale nuovo servizio sarà dunque inserito in perimetro tra i servizi acquistabili.

INDICE

1. DATI ANAGRAFICI DELL'AMMINISTRAZIONE

Ragione sociale Amministrazione:	Azienda Sanitaria Provinciale di Agrigento
Indirizzo	Viale Della Vittoria, 321
CAP	92100
Comune	Agrigento
Provincia	AG
Regione	Sicilia
Codice Fiscale	02570930848
Codice IPA	asp_ag
Indirizzo mail	servizi.informatici@aspag.it
PEC	protocollo@pec.aspag.it

Referente Amministrazione	DOTT. RICCARDO INSALACO
Ruolo	Referente Informatico Aziendale
Telefono	3388002237
Indirizzo mail	riccardo.insalaco@aspag.it
PEC	servizi.informatici@pec.aspag.it

2. CONTESTO

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

L'Azienda Sanitaria, con sede legale in Viale della Vittoria 321 – 92100 Agrigento, è stata istituita con la Legge regionale 14 aprile 2009 N. 5 ed è divenuta operativa a partire dal 1° settembre 2009. L'organizzazione ed il funzionamento dell'azienda, disciplinati con atto aziendale di diritto privato, mirano ad assicurare l'erogazione delle prestazioni essenziali ed appropriate, lo sviluppo dei sistemi di qualità, la massima accessibilità ai servizi dei cittadini, l'equità delle prestazioni erogate, il raccordo istituzionale con gli Enti Locali, il collegamento con le altre organizzazioni sanitarie e di volontariato, nonché l'ottimalizzazione e l'integrazione delle risorse e delle risposte assistenziali.

Fine istituzionale dell' "Azienda Sanitaria Provinciale di Agrigento " è l'erogazione, sia in regime di ricovero che in forma ambulatoriale, di servizi e prestazioni di diagnosi e cura delle malattie acute e di quelle che richiedono interventi di urgenza.

Le prestazioni erogate dall'Azienda ospedaliera comprendono le visite mediche, l'assistenza infermieristica, e ogni atto e procedura diagnostica e terapeutica necessari per risolvere i problemi di salute di adulti e bambini, degenti e non degenti, compatibili con il livello di dotazione tecnologica delle singole strutture.

L'Azienda, dotata di oltre 500 posti letto, partecipa ai programmi nazionali e regionali nei settori dell'emergenza, dei trapianti, della prevenzione, della tutela materno-infantile e delle patologie oncologiche, e svolge attività didattiche e di ricerca.

L'attività ospedaliera, coordinata dalla direzione aziendale, è erogata attraverso due Distretti Ospedalieri dell'Azienda Sanitaria Provinciale (denominati AG1 e AG2) che operano mediante un'organizzazione in rete anche al fine di assicurare all'utente l'appropriatezza del percorso di accoglienza, presa in carico, cura e dimissione.

Del distretto AG1 fanno parte i seguenti Presidi Ospedalieri:

- S. Giovanni di Dio (Agrigento)
- Barone Lombardo (Canicattì)
- S. Giacomo D'Altopasso (Licata)

Del distretto AG2 fanno parte i seguenti Presidi Ospedalieri:

- Fratelli Parlapiano (Ribera)
- Giovanni Paolo II (Sciacca)

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

Di seguito si riporta una descrizione semplificata, relativa allo stato di fatto inerente vari aspetti di cybersecurity gestiti oggi presso l'Amministrazione ed in generale dell'architettura di rete dell'Azienda Sanitaria Provinciale di Agrigento.

L'Amministrazione si è dotata di una coppia di accessi dati alle reti INTERNET/INTRANET, in convenzione Consip SPC CONN. Tali collegamenti dati si trovano presso il CED di Viale Della Vittoria – Agrigento e sono in alta affidabilità con banda pari ad 600 Mbps. Le sedi periferiche dell'Amministrazione sono collegate al centro stella attraverso dei collegamenti VPN MPLS ed accedono alla rete INTERNET attraverso i firewall di centro stella.

Attualmente i servizi di sicurezza perimetrale, per tutti i server/Virtual Machine, vengono gestiti dall'Amministrazione attraverso dei firewall, brand Watchguard, attivi su appliance fisiche. Tutti i servizi vengono esposti alla rete pubblica attraverso questa appliance.

I server/VM sono collegati, attraverso l'infrastruttura LAN cliente, alla subnet *private* dei firewall perimetrali. La gestione della virtualizzazione viene garantita dal VMware Cluster Datastore. Tutti i server, su cui sono attive circa N.135 VM, e le

storage aziendali sono installati, quasi, nella loro totalità nel CED di Viale della Vittoria. Circa 10 VM risiedono invece tra i Presidi ospedalieri di Sciacca e Canicattì (i server totali tra fisici e virtuali sono circa 200). Non esiste un sito di Disaster-Recovery esterno al campus ed i backup vengono effettuati mediante il software VEEAM Backup, mentre i backup dei DB vengono effettuati su nastri esterni.

I PC dei dipendenti navigano protetti dai Watchguard, dove vengono applicate policy di navigazione, content-filtering, IDS, ecc..

La gestione da remoto sulle singole PDL (circa 2500) viene effettuata grazie al software di *remote control* Rustdesk.

La rete interna dell'Azienda dispone di N.2 core-switch, presso il CED di Viale della Vittoria, in alta affidabilità. Tali core-switch sono interconnessi ai router spc2. Gli switch che servono i padiglioni amministrativi e sanitari della sede di Viale della Vittoria vengono interconnessi con dorsali, sempre in F.O. ed a questi si attestano gli apparati Layer2 posti nei vari piani/reparti: il totale degli apparati per questo sito, al netto dei core-switch, è pari a N.35. Gli altri Presidi Ospedalieri contano una totalità di circa 154 *device*. La rete LAN è segmentata logicamente attraverso l'uso di VLAN dedicate e di access-list per consentire/negare (secondo necessità) la comunicazione tra le subnet all'interno del campus. Il numero complessivo degli apparati di rete è pari a 300.

La maggior parte degli apparati di rete sono managed ma esistono, pochissimi, apparati unmanaged nella rete cliente. Tutti gli switch, Access-Point ed UPS vengono monitorati attraverso il software Zabbix, gestito dal presidio tecnico.

Non esistono server syslog su cui si dovrebbero conservare, quantomeno, i log del Domain Controller, del server di posta elettronica e dell'antispam né tantomeno software per interpolare gli eventi tracciati.

Per ciò che riguarda l'accesso esterno, nella rete dell'Amministrazione, di fornitori/dipendenti sono state create, in un VPN Concentrator, delle utenze ad hoc. L'accesso avviene attraverso il solo inserimento della doppietta username/password.

La protezione delle macchine dell'Amministrazione è garantita ad oggi da un sistema antivirus di brand Kaspersky.

▪ DESCRIZIONE DELL'ESIGENZA

La trasformazione digitale nell'ambito sanitario gioca un ruolo chiave nell'evoluzione dei modelli assistenziali e organizzativi, soprattutto in un contesto come quello odierno che necessita di un'intensa collaborazione tra gli attori del Servizio Sanitario con lo scopo di offrire i servizi più idonei per la salvaguardia della salute e del benessere dei cittadini. La necessità di garantire i processi collaborativi tra diversi attori istituzionali e la spinta normativa del GDPR che sancisce l'obbligo di attuare le misure tecniche e organizzative atte a mitigare il rischio connesso ai trattamenti dei dati privati, attribuiscono alla sicurezza digitale un ruolo cruciale per la realizzazione di nuovi servizi che rispondano alla crescente domanda di efficacia, tempestività, sicurezza e appropriatezza delle prestazioni. La natura dei dati trattati da aziende sanitarie, caratterizzate da un elevato grado di complessità organizzativa, richiede un focus specifico rispetto ai temi della cybersicurezza anche in relazione alla potenziale attribuzione dello status di infrastruttura critica di interesse nazionale (Commissione Europea - Council Directive 2008/114/EC of 8 December 2008, Ministero dell'Interno – Decreto del 9 gennaio 2008 "Individuazione delle infrastrutture critiche informatiche di interesse nazionale").

L' Azienda Sanitaria Provinciale di Agrigento è un'organizzazione al servizio del cittadino e detiene informazioni pubblicamente accessibili e informazioni riservate ai fini della privacy. La modifica non autorizzata delle informazioni pubblicate o la diffusione di quelle riservate possono avere un impatto rilevante sull'operatività aziendale:

- compromissione della mission aziendale
- danni a terzi con potenziali rischi di rivalsa
- sanzioni per violazione degli obblighi normativi
- danno alla reputazione e crollo della fiducia

In relazione alla protezione dei dati personali, il "Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016... (GDPR – General Data Protection Regulation)" sancisce l'obbligo di attuare le misure tecniche e organizzative atte a mitigare il rischio connesso ai trattamenti dei dati privati e a conseguire un adeguato livello di sicurezza, limitando, per quanto possibile, la distruzione accidentale o illecita, la perdita, la modifica, la rivelazione, l'accesso non autorizzato ai dati detenuti da un'organizzazione o ente titolare. L'individuazione e l'attuazione delle misure secondo un principio di proporzionalità tra mezzi e fini, rientra tra compiti dell'organizzazione attuatrice che, a tale fine, potrà avvalersi di codici di condotta o pratiche dettate da organismi accreditati o autorevoli nel campo della sicurezza delle informazioni.

La presente richiesta rientra nell'ambito delle misure e azioni intraprese per l'attuazione del PNRR MISSIONE 6 SALUTE - M6.C2 1.1.1.1 AMMODERNAMENTO DEL PARCO TECNOLOGICO E DIGITALE OSPEDALIERO (DIGITALIZZAZIONE DEA I E II) – Linea d'intervento Fabbisogni Ulteriori Tecnologie – "***Altro***" per:

- Il P.O. S. GIOVANNI DI DIO - Contrada Consolida - Agrigento.

Riguarda inoltre l'avvio di progetti finalizzati alla trasformazione digitale dei propri servizi in base al Modello strategico evolutivo dell'informatica della PA e ai principi afferenti al Piano Triennale per l'informatica della Pubblica Amministrazione.

Il presente capitolo ha lo scopo di descrivere le esigenze di Azienda Sanitaria Provinciale di Agrigento 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..

Azienda Sanitaria Provinciale di Agrigento necessita dei servizi di seguito indicati, al fine di assicurare, in caso di riscontro di eventi anomali nelle workstation o server aziendali e altri eventi di sicurezza degni di nota, un'analisi approfondita degli eventi occorsi, dell'attuale livello di sicurezza dell'intera infrastruttura monitorata e allertare di conseguenza i corretti riferimenti aziendali indicati da Azienda Sanitaria Provinciale di Agrigento. In tal modo, le strutture interne preposte potranno di conseguenza intervenire con azioni correttive su indicazione dello stesso sistema di monitoraggio. L'ASP intende sostituire i sistemi di End Point Protection ad oggi in uso con quelli offerti dal RTI nel presente accordo quadro.

E' un ulteriore obbiettivo di questa azione la dotazione degli strumenti di efficacia probatoria e validità legale (Firme digitali remote), per i dipendenti aziendali.

Azienda Sanitaria Provinciale di Agrigento 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 per l'Ente coinvolto:

Servizi di protezione degli End-point L1.S7

Si richiede l'erogazione di un servizio remoto che, dovrà consentire la protezione dei dispositivi collegati alla rete (PC e Server) dall'accesso non autorizzato o dall'esecuzione di software dannoso. La protezione degli endpoint deve garantire, inoltre, che i dispositivi (es. pc desktop, laptop, ecc.) raggiungano un livello di sicurezza definito e siano conformi alle policy

e ai requisiti di conformità e sicurezza stabiliti dall'Ente. Nel dettaglio devono essere fornite le funzioni di: protezione con sistemi antimalware; ispezione localmente anche del traffico HTTPS; controllo dell'uso o anche blocco dei dispositivi USB; trasmissione degli eventi alle piattaforme di correlazione; monitoraggio continuo delle minacce avanzate e protezione da malware basati su file e senza file; protezione e prevenzione dalla perdita di dati.

Servizi di certificati SSL L1.S8

L'amministrazione necessita di un certificato SSL. Il certificato SSL (Secure Sockets Layer) e il suo successore TLS (Transport Layer Security), sono protocolli standard necessari a garantire affidabilità e sicurezza della comunicazione tra le componenti client e server di un'applicazione internet. Il certificato assicura che le informazioni sensibili fornite dagli utenti sul web rimangano riservate e non vengano in alcun modo intercettate da terze parti (comunicazione criptata tra il client server e il server web).

Servizi di firma digitale remota L1.S11

Tale servizio richiesto dovrà consentire alle Amministrazioni di dare efficacia probatoria ai documenti informatici firmati digitalmente, favorendo così i processi di dematerializzazione e consentendo l'automazione e l'ottimizzazione dei processi aziendali.

Servizi Specialistici L1.S15

Si richiede l'erogazione di tali servizi finalizzati:

- alla migrazione dai sistemi di end-point protection attuali (Kaspersky) a quelli previsti dalla convenzione, comprese tutte le attività di analisi e configurazione per l'attivazione di configurazioni ad hoc, raccolta informazioni, meeting tecnici, ecc.; supporto nell'analisi dei deliverable raccolti a seguito di rilevazioni di violazioni.
- alle attività d'analisi, raccolta informazioni, meeting tecnici, configurazioni personalizzate, predisposizione connettori ed integrazione dei sistemi di firma digitale con gli applicativi aziendali.

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 36 mesi.

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	1001	1001	1001	0
				> 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	1	0	0	0
				SSL OV Wildcard				
				SSL EV				
				SSL DV				
				SSL Code signing				
				SSL Client Auth				

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	501	501	501	0
				> 1.000 utenti				
				Garantita - N. 1 firma				
				Garantita - N. 5 firme aggiuntive				

- ***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 le sedi dell'Amministrazione ove specificato dall'Amministrazione stessa; in alternativa presso la Sede del Fornitore.

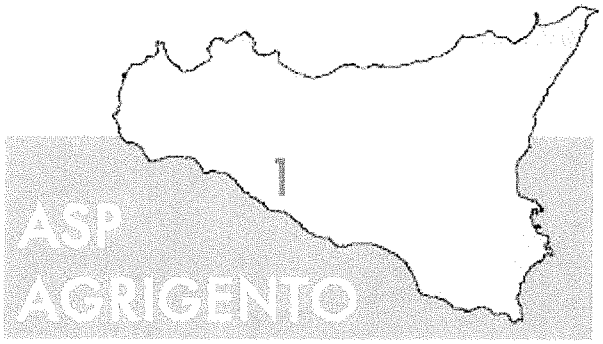
▪ INDICATORE DI PROGRESSO

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

Azienda Sanitaria Provinciale di Agrigento



PIANO DEI FABBISOGNI

P.O. Giovanni Paolo II Sciacca

(CUP C86G22001320006**, CIG_____)**

NOTA BENE:

Durante l'esecuzione contrattuale è possibile che il progresso tecnologico innovi i servizi di base con l'introduzione di nuove funzionalità e/o nuovi servizi in ogni caso complementari/supplementari ai servizi previsti in gara mediante procedura negoziata ai sensi dell'art. 63 co. 3 lett b), d.lgs. n. 50/2016 oppure mediante una modifica ai sensi dell'art. 106 co.1 lett. b) d.lgs. n. 50/2016.

L'organismo tecnico di Coordinamento e Controllo, raccolta la necessità di introduzione di un nuovo servizio, esclusivamente se lo stesso risulta nella disponibilità dell'aggiudicatario dell'Accordo Quadro, richiederà allo stesso, sulla base di un apposito documento di "specifiche tecniche" (con annessi i requisiti da garantire), la quotazione di un servizio da inserire nei servizi oggetto di fornitura. Tale nuovo servizio sarà dunque inserito in perimetro tra i servizi acquistabili.

INDICE

1. DATI ANAGRAFICI DELL'AMMINISTRAZIONE

Ragione sociale Amministrazione:	Azienda Sanitaria Provinciale di Agrigento
Indirizzo	Viale Della Vittoria, 321
CAP	92100
Comune	Agrigento
Provincia	AG
Regione	Sicilia
Codice Fiscale	02570930848
Codice IPA	asp_ag
Indirizzo mail	servizi.informatici@aspag.it
PEC	protocollo@pec.aspag.it

Referente Amministrazione	DOTT. RICCARDO INSALACO
Ruolo	Referente Informatico Aziendale
Telefono	3388002237
Indirizzo mail	riccardo.insalaco@aspag.it
PEC	servizi.informatici@pec.aspag.it

2. CONTESTO

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

L'Azienda Sanitaria, con sede legale in Viale della Vittoria 321 – 92100 Agrigento, è stata istituita con la Legge regionale 14 aprile 2009 N. 5 ed è divenuta operativa a partire dal 1° settembre 2009. L'organizzazione ed il funzionamento dell'azienda, disciplinati con atto aziendale di diritto privato, mirano ad assicurare l'erogazione delle prestazioni essenziali ed appropriate, lo sviluppo dei sistemi di qualità, la massima accessibilità ai servizi dei cittadini, l'equità delle prestazioni erogate, il raccordo istituzionale con gli Enti Locali, il collegamento con le altre organizzazioni sanitarie e di volontariato, nonché l'ottimalizzazione e l'integrazione delle risorse e delle risposte assistenziali.

Fine istituzionale dell' "Azienda Sanitaria Provinciale di Agrigento " è l'erogazione, sia in regime di ricovero che in forma ambulatoriale, di servizi e prestazioni di diagnosi e cura delle malattie acute e di quelle che richiedono interventi di urgenza.

Le prestazioni erogate dall'Azienda ospedaliera comprendono le visite mediche, l'assistenza infermieristica, e ogni atto e procedura diagnostica e terapeutica necessari per risolvere i problemi di salute di adulti e bambini, degenti e non degenti, compatibili con il livello di dotazione tecnologica delle singole strutture.

L'Azienda, dotata di oltre 500 posti letto, partecipa ai programmi nazionali e regionali nei settori dell'emergenza, dei trapianti, della prevenzione, della tutela materno-infantile e delle patologie oncologiche, e svolge attività didattiche e di ricerca.

L'attività ospedaliera, coordinata dalla direzione aziendale, è erogata attraverso due Distretti Ospedalieri dell'Azienda Sanitaria Provinciale (denominati AG1 e AG2) che operano mediante un'organizzazione in rete anche al fine di assicurare all'utente l'appropriatezza del percorso di accoglienza, presa in carico, cura e dimissione.

Del distretto AG1 fanno parte i seguenti Presidi Ospedalieri:

- S. Giovanni di Dio (Agrigento)
- Barone Lombardo (Canicattì)
- S. Giacomo D'Altopasso (Licata)

Del distretto AG2 fanno parte i seguenti Presidi Ospedalieri:

- Fratelli Parlapiano (Ribera)
- Giovanni Paolo II (Sciacca)

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

Di seguito si riporta una descrizione semplificata, relativa allo stato di fatto inerente vari aspetti di cybersecurity gestiti oggi presso l'Amministrazione ed in generale dell'architettura di rete dell'Azienda Sanitaria Provinciale di Agrigento.

L'Amministrazione si è dotata di una coppia di accessi dati alle reti INTERNET/INTRANET, in convenzione Consip SPC CONN. Tali collegamenti dati si trovano presso il CED di Viale Della Vittoria – Agrigento e sono in alta affidabilità con banda pari ad 600 Mbps. Le sedi periferiche dell'Amministrazione sono collegate al centro stella attraverso dei collegamenti VPN MPLS ed accedono alla rete INTERNET attraverso i firewall di centro stella.

Attualmente i servizi di sicurezza perimetrale, per tutti i server/Virtual Machine, vengono gestiti dall'Amministrazione attraverso dei firewall, brand Watchguard, attivi su appliance fisiche. Tutti i servizi vengono esposti alla rete pubblica attraverso questa appliance.

I server/VM sono collegati, attraverso l'infrastruttura LAN cliente, alla subnet *private* dei firewall perimetrali. La gestione della virtualizzazione viene garantita dal VMware Cluster Datastore. Tutti i server, su cui sono attive circa N.135 VM, e le

storage aziendali sono installati, quasi, nella loro totalità nel CED di Viale della Vittoria. Circa 10 VM risiedono invece tra i Presidi ospedalieri di Sciacca e Canicattì (i server totali tra fisici e virtuali sono circa 200). Non esiste un sito di Disaster-Recovery esterno al campus ed i backup vengono effettuati mediante il software VEEAM Backup, mentre i backup dei DB vengono effettuati su nastri esterni.

I PC dei dipendenti navigano protetti dai Watchguard, dove vengono applicate policy di navigazione, content-filtering, IDS, ecc..

La gestione da remoto sulle singole PDL (circa 2500) viene effettuata grazie al software di *remote control* Rustdesk.

La rete interna dell'Azienda dispone di N.2 core-switch, presso il CED di Viale della Vittoria, in alta affidabilità. Tali core-switch sono interconnessi ai router spc2. Gli switch che servono i padiglioni amministrativi e sanitari della sede di Viale della Vittoria vengono interconnessi con dorsali, sempre in F.O. ed a questi si attestano gli apparati Layer2 posti nei vari piani/reparti: il totale degli apparati per questo sito, al netto dei core-switch, è pari a N.35. Gli altri Presidi Ospedalieri contano una totalità di circa 154 *device*. La rete LAN è segmentata logicamente attraverso l'uso di VLAN dedicate e di access-list per consentire/negare (secondo necessità) la comunicazione tra le subnet all'interno del campus. Il numero complessivo degli apparati di rete è pari a 300.

La maggior parte degli apparati di rete sono managed ma esistono, pochissimi, apparati unmanaged nella rete cliente. Tutti gli switch, Access-Point ed UPS vengono monitorati attraverso il software Zabbix, gestito dal presidio tecnico.

Non esistono server syslog su cui si dovrebbero conservare, quantomeno, i log del Domain Controller, del server di posta elettronica e dell'antispam né tantomeno software per interpolare gli eventi tracciati.

Per ciò che riguarda l'accesso esterno, nella rete dell'Amministrazione, di fornitori/dipendenti sono state create, in un VPN Concentrator, delle utenze ad hoc. L'accesso avviene attraverso il solo inserimento della doppietta username/password.

La protezione delle macchine dell'Amministrazione è garantita ad oggi da un sistema antivirus di brand Kaspersky.

▪ DESCRIZIONE DELL'ESIGENZA

La trasformazione digitale nell'ambito sanitario gioca un ruolo chiave nell'evoluzione dei modelli assistenziali e organizzativi, soprattutto in un contesto come quello odierno che necessita di un'intensa collaborazione tra gli attori del Servizio Sanitario con lo scopo di offrire i servizi più idonei per la salvaguardia della salute e del benessere dei cittadini. La necessità di garantire i processi collaborativi tra diversi attori istituzionali e la spinta normativa del GDPR che sancisce l'obbligo di attuare le misure tecniche e organizzative atte a mitigare il rischio connesso ai trattamenti dei dati privati, attribuiscono alla sicurezza digitale un ruolo cruciale per la realizzazione di nuovi servizi che rispondano alla crescente domanda di efficacia, tempestività, sicurezza e appropriatezza delle prestazioni. La natura dei dati trattati da aziende sanitarie caratterizzate da un elevato grado di complessità organizzativa, richiede un focus specifico rispetto ai temi della cybersicurezza anche in relazione alla potenziale attribuzione dello status di infrastruttura critica di interesse nazionale (Commissione Europea - Council Directive 2008/114/EC of 8 December 2008, Ministero dell'Interno – Decreto del 9 gennaio 2008 "Individuazione delle infrastrutture critiche informatiche di interesse nazionale").

L' Azienda Sanitaria Provinciale di Agrigento è un'organizzazione al servizio del cittadino e detiene informazioni pubblicamente accessibili e informazioni riservate ai fini della privacy. La modifica non autorizzata delle informazioni pubblicate o la diffusione di quelle riservate possono avere un impatto rilevante sull'operatività aziendale:

- compromissione della mission aziendale
- danni a terzi con potenziali rischi di rivalsa
- sanzioni per violazione degli obblighi normativi
- danno alla reputazione e crollo della fiducia

In relazione alla protezione dei dati personali, il "Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016... (GDPR – General Data Protection Regulation)" sancisce l'obbligo di attuare le misure tecniche e organizzative atte a mitigare il rischio connesso ai trattamenti dei dati privati e a conseguire un adeguato livello di sicurezza, limitando, per quanto possibile, la distruzione accidentale o illecita, la perdita, la modifica, la rivelazione, l'accesso non autorizzato ai dati detenuti da un'organizzazione o ente titolare. L'individuazione e l'attuazione delle misure secondo un principio di proporzionalità tra mezzi e fini, rientra tra compiti dell'organizzazione attuatrice che, a tale fine, potrà avvalersi di codici di condotta o pratiche dettate da organismi accreditati o autorevoli nel campo della sicurezza delle informazioni.

La presente richiesta rientra nell'ambito delle misure e azioni intraprese per l'attuazione del PNRR MISSIONE 6 SALUTE - M6.C2 1.1.1.1 AMMODERNAMENTO DEL PARCO TECNOLOGICO E DIGITALE OSPEDALIERO (DIGITALIZZAZIONE DEA I E II) – Linea d'intervento Fabbisogni Ulteriori Tecnologie – "***Altro***" per:

- Il P.O. GIOVANNI PAOLO II - Contrada Seniazza - Sciacca.

Riguarda inoltre l'avvio di progetti finalizzati alla trasformazione digitale dei propri servizi in base al Modello strategico evolutivo dell'informatica della PA e ai principi afferenti al Piano Triennale per l'informatica della Pubblica Amministrazione.

Il presente capitolo ha lo scopo di descrivere le esigenze di Azienda Sanitaria Provinciale di Agrigento 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..

Azienda Sanitaria Provinciale di Agrigento necessita dei servizi di seguito indicati, al fine di assicurare, in caso di riscontro di eventi anomali, vulnerabilità critiche e altri eventi di sicurezza degni di nota, un'analisi approfondita degli eventi occorsi, dell'attuale livello di sicurezza dell'intera infrastruttura monitorata e allertare di conseguenza i corretti riferimenti aziendali indicati da Azienda Sanitaria Provinciale di Agrigento. In tal modo, le strutture interne preposte potranno di conseguenza intervenire con azioni correttive su indicazione dello stesso sistema di monitoraggio.

Il rilevamento delle vulnerabilità presenti all'interno del perimetro aziendale e la dotazione degli strumenti di efficacia probatoria e validità legale (Firme digitali remote) sono ulteriori obbiettivi che si pone questa azione.

Azienda Sanitaria Provinciale di Agrigento 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 per l'Ente coinvolto:

Servizi di gestione continua delle Vulnerabilità di Sicurezza L1.S4

Tale servizio dovrà consentire all'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.

Servizi di certificati SSL L1.S8

L'amministrazione necessita di un certificato SSL. Il certificato SSL (*Secure Sockets Layer*) e il suo successore TLS (*Transport Layer Security*), sono protocolli standard necessari a garantire affidabilità e sicurezza della comunicazione tra le componenti client e server di un'applicazione internet. Il certificato assicura che le informazioni sensibili fornite dagli utenti sul web rimangano riservate e non vengano in alcun modo intercettate da terze parti (comunicazione criptata tra il client server e il server web).

Servizi di firma digitale remota L1.S11

Tale servizio richiesto dovrà consentire all'Amministrazione di dare efficacia probatoria ai documenti informatici firmati digitalmente, favorendo così i processi di dematerializzazione e consentendo l'automazione e l'ottimizzazione dei processi aziendali.

Servizi Specialistici L1.S15

Si richiede l'erogazione di tali servizi finalizzati:

- raccolta informazioni, meeting tecnici e analisi per l'*assesment* di vulnerabilità prodotto e conseguenti attività propedeutiche;
- ad attività di delivery dei servizi oggetto di fornitura durante le operazioni di migrazione;
- al supporto nella definizione, configurazione ed erogazione del servizio di monitoraggio continuo delle vulnerabilità di sicurezza con particolare riferimento all'analisi dei deliverable raccolti a seguito dell'esecuzione da parte del fornitore delle sessioni di vulnerability assessment previsti nell'accordo quadro 2296.
- alle attività d'analisi, raccolta informazioni, meeting tecnici, configurazioni personalizzate, predisposizione connettori ed integrazione dei sistemi di firma digitale con gli applicativi aziendali.

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 36 mesi.

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	250	250	250	0

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	1	0	0	0
				SSL EV				
				SSL DV				
				SSL Code signing				
				SSL Client Auth				

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	501	501	501	0
				> 1.000 utenti				
				Garantita - N. 1 firma				
				Garantita - N. 5 firme aggiuntive				

- ***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 le sedi dell'Amministrazione ove specificato dall'Amministrazione stessa; in alternativa presso la Sede del Fornitore.

▪ 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		

All. 4

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

Rev.	Data	Descrizione delle modifiche	Autore
01	20/03/2023	Prima emissione	RTI

Registro delle versioni

Sommario

Indice delle tabelle

Indice delle figure

1 INTRODUZIONE

L'Azienda Sanitaria, con sede legale in Viale della Vittoria 321 – 92100 Agrigento (di seguito anche "Amministrazione" o "ASP"), è stata istituita con la Legge regionale 14 aprile 2009 N. 5 ed è divenuta operativa a partire dal 1° settembre 2009. L'organizzazione ed il funzionamento dell'azienda, disciplinati con atto aziendale di diritto privato, mirano ad assicurare l'erogazione delle prestazioni essenziali ed appropriate, lo sviluppo dei sistemi di qualità, la massima accessibilità ai servizi dei cittadini, l'equità delle prestazioni erogate, il raccordo istituzionale con gli Enti Locali, il collegamento con le altre organizzazioni sanitarie e di volontariato, nonché l'ottimalizzazione e l'integrazione delle risorse e delle risposte assistenziali.
Fine istituzionale dell'"Azienda Sanitaria Provinciale di Agrigento" è l'erogazione, sia in regime di ricovero che in forma ambulatoriale, di servizi e prestazioni di diagnosi e cura delle malattie acute e di quelle che richiedono interventi di urgenza.
Le prestazioni erogate dall'Azienda ospedaliera comprendono le visite mediche, l'assistenza infermieristica, e ogni atto e procedura diagnostica e terapeutica necessari per risolvere i problemi di salute di adulti e bambini, degenti e non degenti, compatibili con il livello di dotazione tecnologica delle singole strutture.
L'Azienda, dotata di oltre 500 posti letto, partecipa ai programmi nazionali e regionali nei settori dell'emergenza, dei trapianti, della prevenzione, della tutela materno-infantile e delle patologie oncologiche, e svolge attività didattiche e di ricerca.
L'attività ospedaliera, coordinata dalla direzione aziendale, è erogata attraverso due Distretti Ospedalieri dell'Azienda Sanitaria Provinciale (denominati AG1 e AG2) che operano mediante un'organizzazione in rete anche al fine di assicurare all'utente l'appropriatezza del percorso di accoglienza, presa in carico, cura e dimissione.

Del distretto AG1 fanno parte i seguenti Presidi Ospedalieri:

- S. Giovanni di Dio (Agrigento)
- Barone Lombardo (Canicattì)
- S. Giacomo D'Altopasso (Licata)

Del distretto AG2 fanno parte i seguenti Presidi Ospedalieri:

- Fratelli Parlapiano (Ribera)
- Giovanni Paolo II (Sciacca)

1.1 Descrizione del contesto Tecnologico, Applicativo e Procedurale

Di seguito si riporta una descrizione semplificata, relativa allo stato di fatto inerente vari aspetti di cybersecurity gestiti oggi presso l'Amministrazione ed in generale dell'architettura di rete dell'Azienda Sanitaria Provinciale di Agrigento.

L'Amministrazione è dotata di una coppia di accessi dati alle reti INTERNET/INTRANET, in convenzione Consip SPC CONN. Tali collegamenti dati si trovano presso il CED di Viale Della Vittoria – Agrigento e sono in alta affidabilità con banda pari ad 600 Mbps.
Le sedi periferiche dell'Amministrazione sono collegate al centro stella attraverso dei collegamenti VPN MPLS ed accedono alla rete INTERNET attraverso i firewall di centro stella.
Attualmente i servizi di sicurezza perimetrale, per tutti i server/Virtual Machine, vengono gestiti dall'Amministrazione attraverso dei firewall, di *brand* Watchguard, attivi su appliance fisiche. Tutti i servizi vengono esposti alla rete pubblica attraverso questa appliance.
I server/VM sono collegati, attraverso l'infrastruttura LAN cliente, alla subnet private dei firewall perimetrali. La gestione della virtualizzazione viene garantita dal VMware Cluster Datastore. Tutti i server, su cui sono attive circa N.135 VM, e le storage aziendali sono installati, quasi, nella loro totalità nel CED di Viale della Vittoria. Circa 10 VM risiedono tra i Presidi ospedalieri di Sciacca e Canicattì (i server totali tra fisici e virtuali sono circa 200). Non esiste un sito di Disaster-Recovery esterno al campus ed i backup vengono effettuati mediante il software VEEAM Backup, mentre i backup dei DB vengono effettuati su nastri esterni.
I PC dei dipendenti navigano protetti dai Watchguard, dove vengono applicate policy di navigazione, content-filtering, IDS, ecc..
La gestione da remoto sulle singole PDL (circa 2500) viene effettuata grazie al software di remote control Rustdesk.
La rete interna dell'Azienda dispone di N.2 core-switch, presso il CED di Viale della Vittoria, in alta affidabilità. Tali core-switch sono interconnessi ai router spc2. Gli switch che servono i padiglioni amministrativi e sanitari della sede di Viale della Vittoria vengono interconnessi con dorsali, sempre in F.O. ed a questi si attestano gli apparati Layer2 posti nei vari piani/reparti: il totale degli apparati per questo sito, al netto dei core-switch, è pari a N.35. Gli altri Presidi Ospedalieri contano una totalità di circa 154

device. La rete LAN è segmentata logicamente attraverso l'uso di VLAN dedicate e di access-list per consentire/negare (secondo necessità) la comunicazione tra le subnet all'interno del campus. Il numero complessivo degli apparati di rete è pari a 300.
La maggior parte degli apparati di rete sono managed ma esistono, pochissimi, apparati unmanaged nella rete cliente. Tutti gli switch, Access-Point ed UPS vengono monitorati attraverso il software Zabbix, gestito dal presidio tecnico.
Non esistono server syslog su cui si dovrebbero conservare, quantomeno, i log del Domain Controller, del server di posta elettronica e dell'antispam né tantomeno software per interpolare gli eventi tracciati.
Per ciò che riguarda l'accesso esterno, nella rete dell'Amministrazione, di fornitori/dipendenti sono state create, in un VPN Concentrator, delle utenze ad hoc. L'accesso avviene attraverso il solo inserimento della doppietta username/password.
La protezione delle macchine dell'Amministrazione è garantita ad oggi da un sistema antivirus di brand Kaspersky.

1.2 Scopo

Scopo del presente progetto è di fornire all'Azienda Sanitaria Provinciale di Agrigento i servizi mirati a garantire la corretta operatività dei sistemi attraverso la prevenzione, gestione, risoluzione di qualsiasi criticità di sicurezza che possa degradare il servizio all'utenza. La finalità principale è la gestione ed il monitoraggio dei servizi di sicurezza e, in aggiunta, la ricezione e l'analisi di reportistica (log) dando priorità ai processi di risoluzione e/o mitigazione delle minacce.
Ulteriore obiettivo che si vuole raggiungere è quello di assicurare, in caso di riscontro di eventi anomali nelle workstation o server aziendali e altri eventi di sicurezza degni di nota, un'analisi approfondita degli eventi occorsi, dell'attuale livello di sicurezza dell'intera infrastruttura monitorata e allertare di conseguenza i corretti riferimenti aziendali indicati dall'Amministrazione. In tal modo, le strutture interne preposte potranno di conseguenza intervenire con azioni correttive su indicazione dello stesso sistema di monitoraggio. L'ASP intende sostituire i sistemi di End Point Protection ad oggi in uso con quelli offerti dal RTI nell'ambito dell'AQ.
L'Azienda Sanitaria Provinciale di Agrigento 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.

1.3 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.

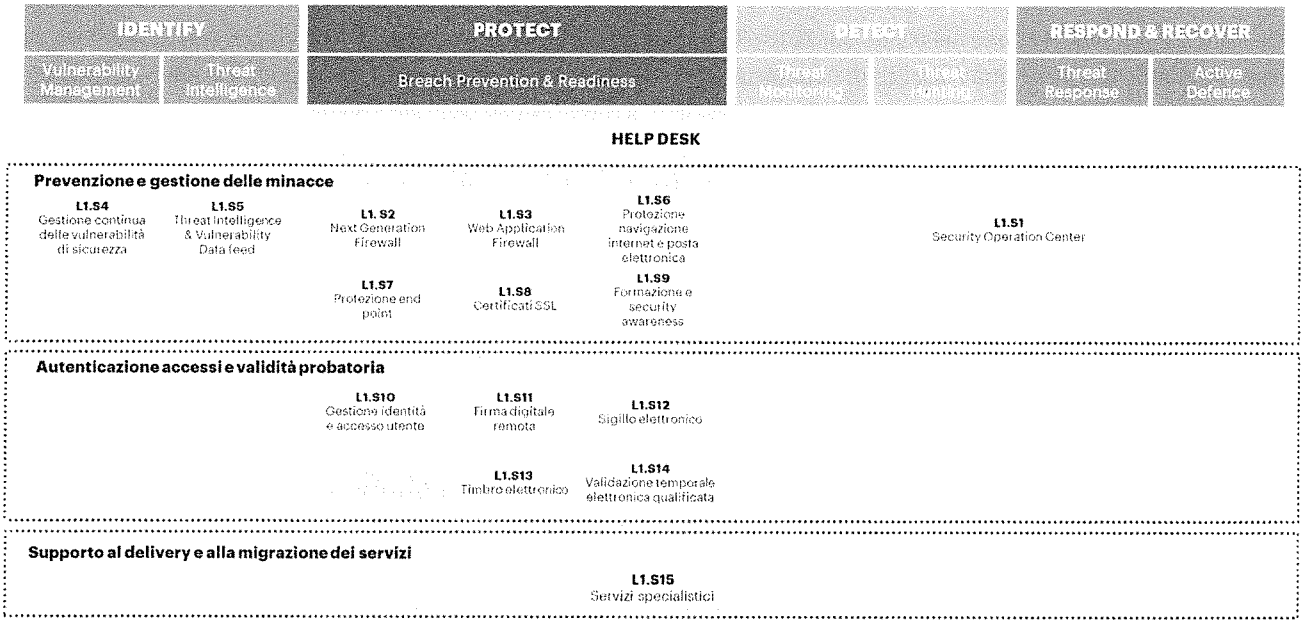


Figura 1 – Mappatura Servizi di Sicurezza e Framework NIST

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, **AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO**, intende avvalersi dei **servizi di Sicurezza da Remoto** previsti per il **Lotto 1**, secondo i termini e le condizioni dell'**Accordo Quadro per l'Affidamento di Servizi da Remoto, di Compliance e Controllo per le Pubbliche Amministrazioni – Lotto 1 ID2296 –** (Accordo Quadro o AQ), senza riaprire il confronto competitivo tra gli operatori economici parti dell'Accordo Quadro ("AQ a condizioni tutte fissate").

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

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

A tal fine, **AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO**, 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.

1.4 Assunzioni

ID	AMBITO	ASSUNZIONE
1	Adeguamenti Normativi	A fronte di eventuali novità di carattere normativo che riguardano i processi e i sistemi oggetto della presente fornitura, dovranno essere valutati e condivisi tra AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO 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 "PDF NO PNNR Sicurezza da Remoto_Template Piano dei fabbisogni_Final_rev2"

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

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

Tabella 4 - Acronimi

4 ORGANIZZAZIONE DEL CONTRATTO ESECUTIVO

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

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

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

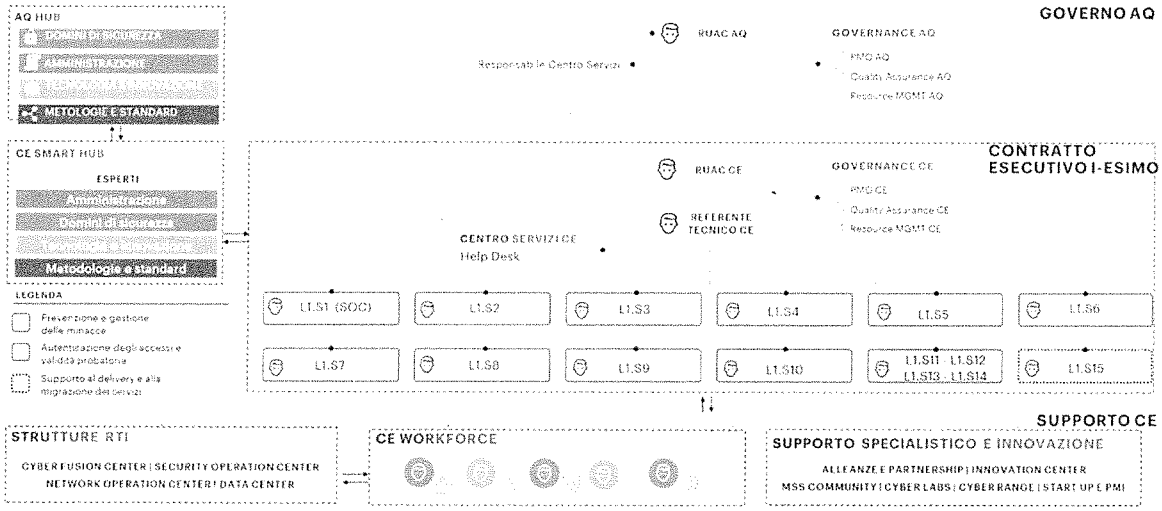


Figura 2 - Organizzazione dell'AQ proposta dal RTI

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

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

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

- team responsabili dell'erogazione dei servizi previsti.

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

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

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

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

4.1 Attività in carico alle aziende del RTI

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

SERVIZIO	ACCENTURE	FASTWEB	FINCANTIERI	DEAS
L1.S1 – Security Operation Center	X			
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		X		
L1.S8 – Certificati SSL				
L1.S9 – Formazione e Security Awareness				
L1.S10 – Gestione dell'Identità e dell'accesso dell'utente				
L1.S11 – Firma Digitale Remota				
L1.S12 – Sigillo Elettronico				
L1.S13 – Timbro Elettronico				
L1.S14 – Validazione temporale elettronica qualificata				
L1.S15 – Servizi Specialistici	X	X	X	X
TOTALE (%)	49,0484 %	50,6548 %	0,1484%	0,1484%
TOTALE (€)	161.296,00 €	166.578,71 €	488,00 €	488,00 €

Tabella 5 - Ripartizione attività in carico

4.2 Organizzazione e figure di riferimento del Fornitore

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

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

Tabella 6 - Figure di riferimento e referenti del Fornitore

4.3 Luogo di erogazione e di esecuzione della Fornitura

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

- per i servizi erogati da remoto: attraverso i Centri Servizi del Fornitore;
- per i servizi on-site: 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

Gli ambiti d'intervento oggetto di fornitura come di seguito elencati hanno l'obiettivo di soddisfare i requisiti di **AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO** così come riportati nel Piano dei Fabbisogni:

L1.S1 - Security Operation Center – sarà erogato un servizio da remoto che, attraverso adeguati strumenti tecnologici di back-end, 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 ai suggerimenti di azioni di contenimento, ripristino e prevenzione futura in stretta collaborazione con le strutture dell'Amministrazione preposte alla gestione sistemistica. Tra le funzioni fornite ci sono: la raccolta centralizzata dei log e degli eventi di sicurezza; la correlazione di più eventi che caratterizzano il potenziale incidente; la capacità di identificazione, gestione, mitigazione e risoluzione degli attacchi; la produzione di report periodici di sintesi. In aggiunta, anche l'invio e l'analisi della reportistica e dei log, con l'assegnazione della giusta priorità ai processi di risoluzione e/o mitigazione delle minacce, fanno parte del servizio.

L1.S7 - Servizi di protezione degli End-point

Servizio che consente la protezione dei dispositivi collegati alla rete (PC e Server) dall'accesso non autorizzato o dall'esecuzione di software dannoso. La protezione degli endpoint garantisce, inoltre, che i dispositivi (es. pc desktop, laptop, ecc.) raggiungano un livello di sicurezza definito e siano conformi alle policy e ai requisiti di conformità e sicurezza stabiliti dall'Ente. Nel dettaglio vengono fornite le funzioni di: protezione con sistemi antimalware; ispezione localmente anche del traffico HTTPS; controllo dell'uso o anche blocco dei dispositivi USB; trasmissione degli eventi alle piattaforme di correlazione; monitoraggio continuo delle minacce avanzate e protezione da malware basati su file e senza file; protezione e prevenzione dalla perdita di dati.

L1.S15 - Servizi Specialistici

I servizi di Supporto Specialistico hanno l'obiettivo di fornire ad AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO 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

I volumi e requisiti indicati nel Piano dei Fabbisogni dell'Amministrazione (sezione "Sintesi dei Servizi Richiesti"), relativamente ai servizi selezionati da quest'ultima, sono la base di partenza sulla quale il RTI ha definito le quantità e, quindi, il dimensionamento dei servizi ed il relativo periodo di riferimento, così come riportati nella seguente tabella. Si rende noto che in merito ai Servizi Specialistici L1.S15 richiesti espressamente dal Piano dei Fabbisogni, in cui tuttavia non sono indicati i dimensionamenti desiderati, il RTI propone il dimensionamento riportato nella tabella seguente al fine di rispondere ai requisiti richiesti dall'Amministrazione.

SERVIZIO	FASCIA	IMPORTO I ANNO/Quantità	IMPORTO II ANNO/Quantità	IMPORTO III ANNO/Quantità	IMPORTO IV ANNO/Quantità
L1.S1 – Security Operation Center	Fino a 6.000 Eps	43.680,00 €/200 (device equivalent)	43.680,00 €/200 (device equivalent)	43.680,00 €/200 (device equivalent)	0
L1.S7 – Protezione degli endpoint	Fino a 5.000 nodi	21.854,24 €/1699	21.854,24 €/1699	21.854,24 €/1699	0
L1.S15 – Servizi Specialistici a supporto di L1.S1 – Security Operation Center	Numero Giorni persona del team ottimale	10.248,00 €/42	10.248,00 €/42	10.248,00 €/42	0
L1.S15 –Servizi Specialistici a supporto di L1.S7 – Protezione degli endpoint	Numero Giorni persona del team ottimale	41.480,00 €/170	30.012,00 €/123	30.012,00 €/123	0

Tabella 7 - Servizi richiesti

5.3 Indicatore di progresso

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

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

Tabella 8 - Schema definizione Indicatore di Progresso

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

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

6 SOLUZIONE PROPOSTA

6.1 Descrizione dei servizi richiesti

Di seguito i servizi proposti in linea con le esigenze espresse da AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO.

6.1.1 L1.S1 Security Operation Center

La ventennale esperienza di Accenture, unitamente a quella di Fastweb nell'ambito della PA, ha permesso di consolidare e far evolvere un modello di servizio ponendo a fattor comune esperienze analoghe nella realizzazione ed erogazione di servizi di Security Operation Center per istituzioni governative nazionali ed internazionali. Si è giunti alla definizione ed ingegnerizzazione di un modello di "**Next Generation Security Operation Center (NG-SOC)**" basato sulla piattaforma tecnologica di Accenture denominata "**Advanced Security Monitoring & Detection (ASMD)**", la quale sfrutta un'architettura modulare flessibile e multicliente, che permette di scalare a seconda del numero e livello di integrazione delle amministrazioni coinvolte.
La soluzione ASMD di Accenture abilita ad un servizio di Managed Detection & Response (MDR), per offrire alle Amministrazioni aderenti servizi gestiti SIEM **segregati e integrati** con la piattaforma centralizzata SOAR, come nel seguito descritto. La soluzione opera in modalità 24x7x365 e viene erogata dai SOC di Napoli e Milano, operanti all'interno dei Centri Servizi in ambito della convenzione. Accenture ha selezionato e integrato nella piattaforma ASMD la tecnologia **Splunk** per la parte di "Security Information & Event Management (SIEM)" e **Palo Alto Cortex XSOAR** per la parte di "Security Orchestration, Automation & Response (SOAR)", entrambi leader di mercato secondo fonti affermate di analisti di settore quali Gartner e Forrester e partner decennali a livello globale delle aziende del RTI.
Il servizio proposto di SOC ha l'obiettivo di individuare nel minor tempo possibile potenziali incidenti di sicurezza, supportato dalle informazioni di dettaglio fornite dalle sorgenti di eventi di sicurezza dell'Amministrazione, contestualizzate e arricchite dagli ulteriori servizi oggetto della presente proposta quali ad esempio il 'Servizio di Gestione continua delle Vulnerabilità di Sicurezza' - per assegnare in fase di triage la corretta priorità all'incidente.
Il servizio SOC è erogato da un unico gruppo di lavoro (Accenture Cyber Fusion Center Napoli) che risponde a un Responsabile del Servizio SOC (RSOC, vale a dire il Service Manager) il quale rappresenterà il punto di contatto con il Referente tecnico dell'Amministrazione.

6.2 Team di servizio

Data la sua criticità, il servizio utilizza un framework di comunicazione che prevede allineamenti a differenti livelli, da quello operativo fino a quello Direzionale/Leadership.

Il team per il SOC del RTI è composto da:

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

Il RSOC rappresenta il punto di contatto tra il Referente Tecnico di AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO e il SOC Team ed ha le seguenti responsabilità:

- stilare e condividere il Questionario di Preinstallazione (QPI) adattato al contesto e perimetro di AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO. contenente le informazioni necessarie al processo di onboarding, i contatti dei referenti operativi di AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO. e i processi di escalation;
- valutare e convalidare il perimetro di monitoraggio, inteso come l'insieme di sorgenti di log (eventi di sicurezza) di AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO. identificati come fondamentali per la valutazione e la copertura del monitoraggio e, quindi, potenziali incidenti di sicurezza;
- valutare e convalidare la configurazione delle varie sorgenti di log di cui il punto precedente e, quindi, i collector/agent da utilizzare, aree geografiche coinvolte, canale di comunicazione protetto per il trasferimento di tali eventi di sicurezza dall'IT di AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO. verso il Centro Servizi, informazioni sugli use case e modello di automatizzazione e quanto altro al fine di definire al meglio il perimetro di lavoro;
- condividere e confermare le aspettative di AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO. ed evidenziare/indirizzare qualsiasi potenziale disallineamento;
- creare i collegamenti tra i vari referenti dei team coinvolti;

- raccogliere le procedure di escalation e di incident management per individuare i punti di aggiornamento;
- lavorare a contatto con i referenti di AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO. per recepire i riscontri operativi e tradurli in attività di miglioramento continuo;
- mantenere contatti regolari con eventuali altri team, esterni all'ambito sicurezza, per condividere informazioni rilevanti che possano aiutare/migliorare l'integrazione e la collaborazione;
- identificare i processi di automazione che facilitino la condivisione delle informazioni e la risposta alle minacce per guidare una reazione più rapida e accurata.

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

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

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

*Tabella **10** - Figure del SOC team*

Poiché prerequisiti per l'erogazione del servizio L1.S1 di seguito si elencano quelli che saranno i task in carico ad AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO, da pianificare durante la fase di onboarding:

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

6.3 Modello Operativo

Il modello operativo del servizio SOC proposto prevede il monitoraggio continuo delle informazioni prodotte dalle sorgenti di log (eventi di sicurezza) identificati come perimetro di monitoraggio da AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO.

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 AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO, 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 di AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO ed archiviate;
- Valutazione post incidente, in modo da individuare possibili azioni migliorative da implementare sui sistemi di sicurezza di AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO aumentando l'efficacia del SOC team.

6.4 Modalità di erogazione

Il modello di erogazione del servizio SOC si basa sulla logica che prevede la raccolta degli allarmi generati dal sistema di monitoraggio del Centro Servizi che, in seguito ad incidenti di sicurezza, apre il ticket verso il team "L1 SOC" sul sistema ITSM. Il team "L1 SOC" controllerà le informazioni evidenziate dall'allarme, ed eseguirà le prime verifiche per una eventuale escalation verso il team "L2 SOC" o/e il reperibile di AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO, 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 di AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO per segnalare/supportare azioni di remediation;
- verifica di chiusura del caso segnalato, da parte del team operativo di AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO.

6.4.1 L1.S7 – Protezione degli End-Point

Il servizio di protezione degli Endpoint rappresenta uno degli elementi chiave forniti dal Centro Servizi per garantire la sicurezza delle infrastrutture concordate con l'Amministrazione, operando direttamente sui dispositivi in uso agli utenti abilitando sia l'identificazione di anomalie di processo che le azioni di contenimento e reazione da implementare in caso di violazione. La soluzione tecnologica di Endpoint Protection proposta, riconosciuta come leader sul mercato, fornisce un'ampia e consolidata copertura dei requisiti di tecnico-funzionali e rappresenta un elemento fondamentale e raccomandato nel catalogo offerto del Centro Servizi. Nello specifico, il servizio consente di:

- effettuare l'ispezione del traffico generato dalla postazione di lavoro;
- controllare lo scambio di dati (Data Loss Prevention – DLP) in maniera tale che le informazioni sensibili non possano essere trasferite ad attori non autorizzati;
- controllare lo stato di compliance dei dispositivi rispetto a policy di sicurezza ben definite;
- inviare log al SOC e abilitando il monitoraggio 24x7.

Inoltre, il servizio prevede di sfruttare tecniche di rilevamento delle anomalie avanzate tramite:

- metodologie di ML prima e durante l'esecuzione dei file;
- tecniche di cancellazione del rumore di fondo, come censimento ed elenchi di utenti autorizzati, a ogni livello di rilevamento, per ridurre drasticamente i falsi positivi;
- tecniche specifiche per la protezione contro script, iniezioni, ransomware e attacchi a memoria e browser, grazie a un'innovativa analisi del comportamento.

Il numero di end point indicati nella richiesta di Azienda Sanitaria Provinciale di Agrigento (n. 1699) porta alla selezione della Fascia Fino a 5.000 nodi.

6.4.2 L1.S15 – Servizi Specialistici

Tale servizio prevede un supporto specialistico con l'obiettivo di fornire ad AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO supporto tecnico connesso ai servizi oggetto del presente Piano Operativo, come di seguito descritto.

6.4.2.1 Servizi Specialistici a supporto del Security Operation Center

I Servizi Specialistici a supporto del Servizio SOC, prevedono l'utilizzo in logica di progetto di personale specializzato che allo scopo di fornire controllo imparziale della corretta esecuzione del servizio, offra supporto nel processo di monitoraggio e gestione degli incidenti di sicurezza. In particolare, gli obiettivi di tale servizio specialistico sono i seguenti e saranno oggetto di pianifica-zione puntale in accordo con l'Amministrazione durante il periodo contrattuale di riferimento:

- Supporto nella gestione degli incidenti di sicurezza;
- Supporto nella identificazione e realizzazione di nuovi Use Case a supporto del processo di detection al fine di migliorare continuamente la libreria di casi dedicati;
- Supporto nella 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".

6.4.2.2 Servizi Specialistici a supporto della protezione degli End-Point

Il servizio prevede le azioni di setup negli end-point e la migrazione dai sistemi di end-point protection attuali (Kaspersky) a quelli previsti dalla convenzione, comprese tutte le attività di analisi e configurazione per l'attivazione di configurazioni ad hoc, raccolta informazioni, meeting tecnici, ecc.; supporto nell'analisi dei deliverable raccolti a seguito di rilevazioni di violazioni.

6.5 Utenza interessata / coinvolta

Personale di AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO.

6.6 Eventuali riferimenti / vincoli normativi

N.A.

7 PIANO DI PROGETTO

7.1 Cronoprogramma

L'erogazione dei servizi avrà durata 36 mesi, a decorrere dalla data di conclusione delle attività di presa in carico T0 (data di firma del contratto esecutivo + periodo di presa in carico), come indicato nella seguente tabella:

	ANNO I												ANNO II												ANNO III											
	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 SECURITY OPERATION CENTER																																				
L1.S7 PROTEZIONE DEGLI END POINT																																				
L1.S15 SERVIZI SPECIALISTICI																																				

Tabella 9 – Cronoprogramma

7.2 Data di Attivazione e Durata del Servizio

Il contratto esecutivo produrrà i suoi effetti dalla data di stipula e avrà una durata di 36 mesi a decorrere dalla data di conclusione delle attività di presa in carico.

7.3 Gruppo di Lavoro

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

7.4 Modalità di esecuzione dei Servizi

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

MILESTONE	DESCRIZIONE	ATTORE
Richiesta stima e Piano di Lavoro	Richiesta al fornitore di procedere alla stima dei tempi e costi del servizio	Amministrazione
Stima (pre-dimensionamento)	Comunicazione dei tempi e dei costi previsti per servizio	RTI

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

Tabella 10 - Descrizione milestone per obiettivo

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

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

7.5 Modalità di ricorso al Subappalto da parte del Fornitore

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

SERVIZIO	AZIENDA	QUOTA MASSIMA SUBAPPALTABILE
L1.S1 – Security Operation Center, L1.S15 – Servizi Specialistici	Accenture	50%
L1.S7 – Protezione degli endpoint, L1.S15 – Servizi Specialistici	Fastweb	50%
L1.S15 – Servizi Specialistici	Fincantieri	50%
L1.S15 – Servizi Specialistici	Deas	50%

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

8 DIMENSIONAMENTO ECONOMICO

8.1 Modalità di erogazione dei Servizi

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

ID SERVIZIO	METRICA	MODALITÀ EROGAZIONE	MODALITÀ CONSUNTIVAZIONE	PERIODICITÀ CONSUNTIVAZIONE	PREZZO UNITARIO OFFERTO	QUANTITÀ	VALORE ECONOMICO
L1.S1	Device Equivalente/anno	Da remoto	Canone	Mensile	218,40 €	600	131.040,00 € Per 3 anni
L1.S7	Nodi/anno	Da remoto	Canone	Mensile	12,863 €	5097	65.562,71 € Per 3 anni
L1.S15 per L1.S1	Giorni persona del team ottimale	Da remoto /on site	Progettuale a corpo	Mensile	244,00 €	126	30.744,00 € Per 3 anni
L1.S15 per L1.S7	Giorni persona del team ottimale	Da remoto /on site	Progettuale a corpo	Mensile	244,00 €	416	101.504,00 € Per 3 anni

Tabella 12 - Quadro economico di riferimento

L'importo complessivo dell'ordinativo di fornitura ammonta a **328.850,71 € (iva esclusa).**

8.2 Indicazioni in ordine alla fatturazione ed ai termini di pagamento

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

9 ALLEGATI

9.1 Piano di Lavoro Generale

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

9.2 Piano di Presa in Carico

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

9.3 Piano della Qualità Specifico

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

9.4 Curriculum Vitae dei Referenti

Si allega, nel Piano di Lavoro Generale, il CV del RUAC di CE. Per quanto concerne il Responsabile Tecnico, 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.

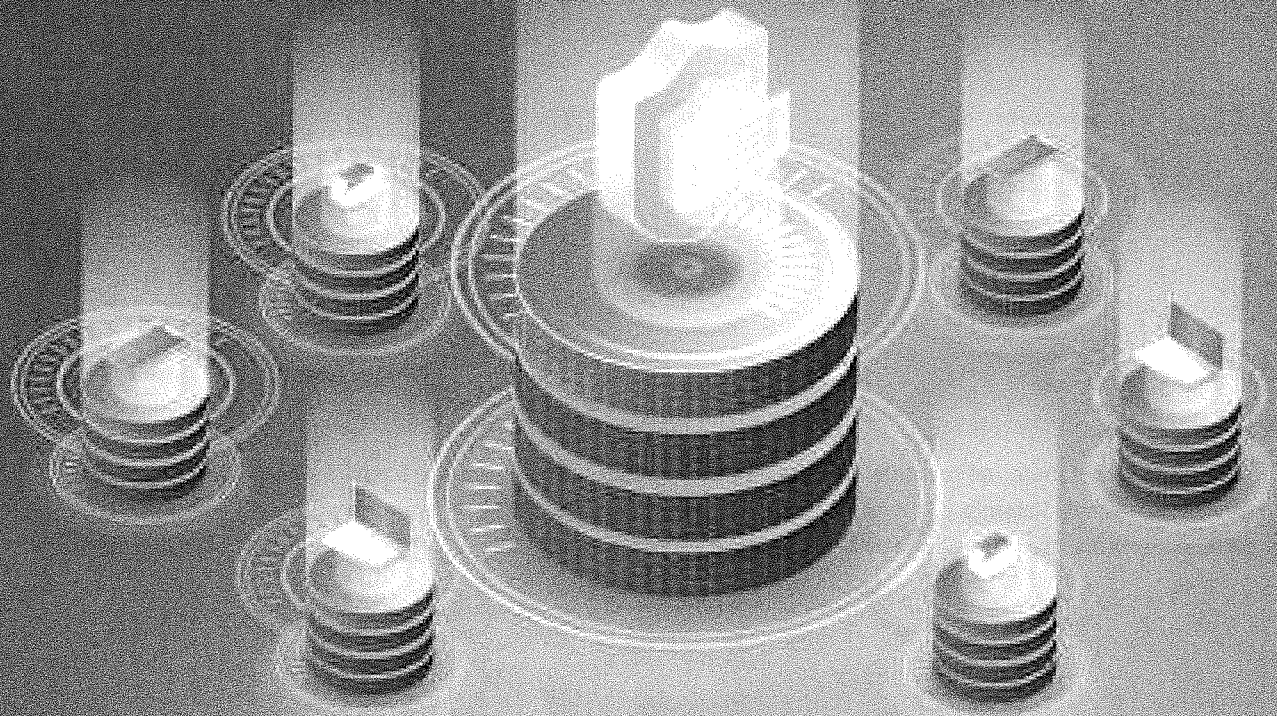
9.6 Documentazione relativa al principio "Do No Significant Harm" (DNSH)

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

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



accenture | FASTWEB | FINCANTIERI | RTI

Rev.	Data	Descrizione delle modifiche	Autore
01	20/03/2023	Prima emissione	RTI

Registro delle versioni

Sommario

Indice delle tabelle

Indice delle figure

1 INTRODUZIONE

L'Azienda Sanitaria, con sede legale in Viale della Vittoria 321 – 92100 Agrigento (di seguito anche "Amministrazione" o "ASP"), è stata istituita con la Legge regionale 14 aprile 2009 N. 5 ed è divenuta operativa a partire dal 1° settembre 2009. L'organizzazione ed il funzionamento dell'azienda, disciplinati con atto aziendale di diritto privato, mirano ad assicurare l'erogazione delle prestazioni essenziali ed appropriate, lo sviluppo dei sistemi di qualità, la massima accessibilità ai servizi dei cittadini, l'equità delle prestazioni erogate, il raccordo istituzionale con gli Enti Locali, il collegamento con le altre organizzazioni sanitarie e di volontariato, nonché l'ottimalizzazione e l'integrazione delle risorse e delle risposte assistenziali.
Fine istituzionale dell'"Azienda Sanitaria Provinciale di Agrigento" è l'erogazione, sia in regime di ricovero che in forma ambulatoriale, di servizi e prestazioni di diagnosi e cura delle malattie acute e di quelle che richiedono interventi di urgenza.
Le prestazioni erogate dall'Azienda ospedaliera comprendono le visite mediche, l'assistenza infermieristica, e ogni atto e procedura diagnostica e terapeutica necessari per risolvere i problemi di salute di adulti e bambini, degenti e non degenti, compatibili con il livello di dotazione tecnologica delle singole strutture.
L'Azienda Sanitaria, dotata di oltre 500 posti letto, partecipa ai programmi nazionali e regionali nei settori dell'emergenza, dei trapianti, della prevenzione, della tutela materno-infantile e delle patologie oncologiche, e svolge attività didattiche e di ricerca.
L'attività ospedaliera, coordinata dalla direzione aziendale, è erogata attraverso due Distretti Ospedalieri dell'Azienda Sanitaria Provinciale (denominati AG1 e AG2) che operano mediante un'organizzazione in rete anche al fine di assicurare all'utente l'appropriatezza del percorso di accoglienza, presa in carico, cura e dimissione.

Del distretto AG1 fanno parte i seguenti Presidi Ospedalieri:

- S. Giovanni di Dio (Agrigento)
- Barone Lombardo (Canicattì)
- S. Giacomo D'Altopasso (Licata)

Del distretto AG2 fanno parte i seguenti Presidi Ospedalieri:

- Fratelli Parlapiano (Ribera)
- Giovanni Paolo II (Sciacca)

Di seguito si riporta una descrizione semplificata, relativa allo stato di fatto inerente vari aspetti di cybersecurity gestiti oggi presso l'Amministrazione ed in generale dell'architettura di rete dell'Azienda Sanitaria Provinciale di Agrigento.

L'Amministrazione è dotata di una coppia di accessi dati alle reti INTERNET/INTRANET, in convenzione Consip SPC CONN. Tali collegamenti dati si trovano presso il CED di Viale Della Vittoria – Agrigento e sono in alta affidabilità con banda pari ad 600 Mbps.
Le sedi periferiche dell'Amministrazione sono collegate al centro stella attraverso dei collegamenti VPN MPLS ed accedono alla rete INTERNET attraverso i firewall di centro stella.
Attualmente i servizi di sicurezza perimetrale, per tutti i server/Virtual Machine, vengono gestiti dall'Amministrazione attraverso dei firewall, di *brand* Watchguard, attivi su appliance fisiche. Tutti i servizi vengono esposti alla rete pubblica attraverso questa appliance.
I server/VM sono collegati, attraverso l'infrastruttura LAN cliente, alla subnet private dei firewall perimetrali. La gestione della virtualizzazione viene garantita dal VMware Cluster Datastore. Tutti i server, su cui sono attive circa N.135 VM, e le storage aziendali sono installati, quasi, nella loro totalità nel CED di Viale della Vittoria. Circa 10 VM risiedono tra i Presidi ospedalieri di Sciacca e Canicattì (i server totali tra fisici e virtuali sono circa 200). Non esiste un sito di Disaster-Recovery esterno al campus ed i backup vengono effettuati mediante il software VEEAM Backup, mentre i backup dei DB vengono effettuati su nastri esterni.
I PC dei dipendenti navigano protetti dai Watchguard, dove vengono applicate policy di navigazione, content-filtering, IDS, ecc..
La gestione da remoto sulle singole PDL (circa 2500) viene effettuata grazie al software di remote control Rustdesk.
La rete interna dell'Azienda dispone di N.2 core-switch, presso il CED di Viale della Vittoria, in alta affidabilità. Tali core-switch sono interconnessi ai router spc2. Gli switch che servono i padiglioni amministrativi e sanitari della sede di Viale della Vittoria vengono interconnessi con dorsali, sempre in F.O. ed a questi si attestano gli apparati Layer2 posti nei vari piani/reparti: il totale degli apparati per questo sito, al netto dei core-switch, è pari a N.35. Gli altri Presidi Ospedalieri contano una totalità di circa 154 device. La rete LAN è segmentata logicamente attraverso l'uso di VLAN dedicate e di access-list per consentire/negare (secondo necessità) la comunicazione tra le subnet all'interno del campus. Il numero complessivo degli apparati di rete è pari a 300.

La maggior parte degli apparati di rete sono managed ma esistono, pochissimi, apparati unmanaged nella rete cliente. Tutti gli switch, Access-Point ed UPS vengono monitorati attraverso il software Zabbix, gestito dal presidio tecnico.
Non esistono server syslog su cui si dovrebbero conservare, quantomeno, i log del Domain Controller, del server di posta elettronica e dell'antispam né tantomeno software per interpolare gli eventi tracciati.
Per ciò che riguarda l'accesso esterno, nella rete dell'Amministrazione, di fornitori/dipendenti sono state create, in un VPN Concentrator, delle utenze ad hoc. L'accesso avviene attraverso il solo inserimento della doppietta username/password.
La protezione delle macchine dell'Amministrazione è garantita ad oggi da un sistema antivirus di brand Kaspersky.

1.1 Scopo

Scopo del presente progetto è di fornire all'Azienda Sanitaria Provinciale di Agrigento per il P.O. S. Giovanni di Dio gli strumenti necessari ad assicurare, in caso di riscontro di eventi anomali nelle workstation o server aziendali e altri eventi di sicurezza degni di nota, un'analisi approfondita degli eventi occorsi, dell'attuale livello di sicurezza dell'intera infrastruttura monitorata e allertare di conseguenza i corretti riferimenti aziendali che saranno indicati al RTI. In tal modo, le strutture interne preposte potranno di conseguenza intervenire con azioni correttive su indicazione dello stesso sistema di monitoraggio. L'ASP sostituirà i sistemi di End Point Protection ad oggi in uso con quelli offerti dal RTI nell'ambito dell'AQ.
È un ulteriore obiettivo di questa azione dotare l'Azienda Sanitaria degli strumenti di efficacia probatoria e validità legale (Firme digitali remote) oltre alla affidabilità, riservatezza e, quindi, sicurezza nella comunicazione tra le componenti client e server di un'applicazione internet (Certificati SSL), per i dipendenti del Presidio Ospedaliero S. Giovanni di Dio (Agrigento).

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.

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

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

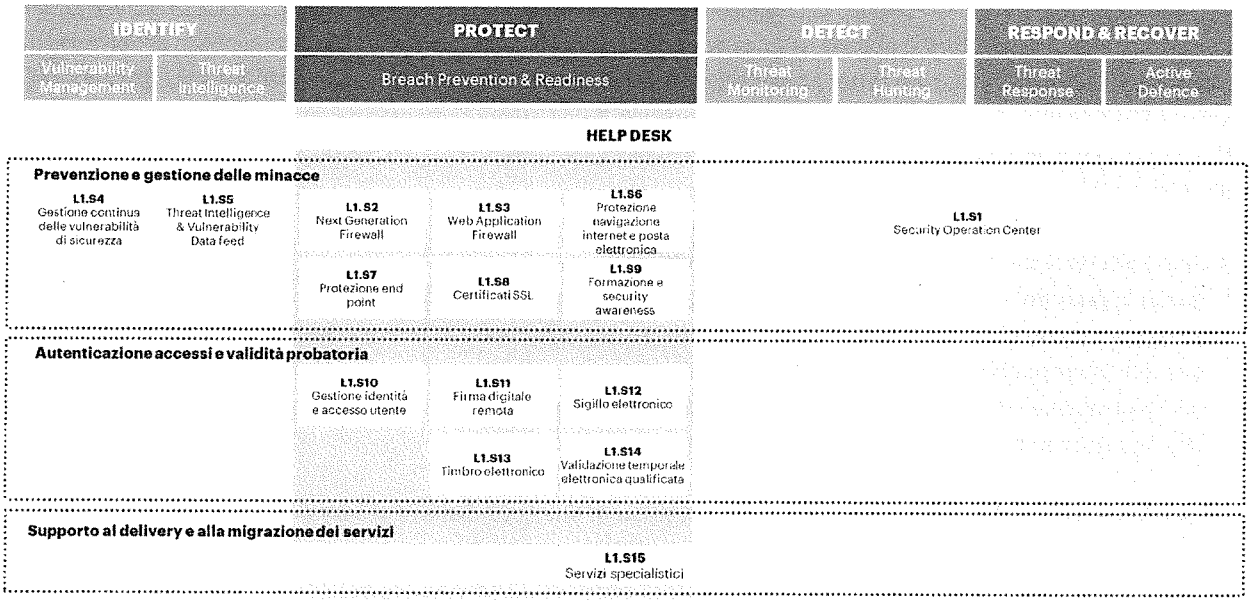


Figura 1 – Mappatura Servizi di Sicurezza e Framework NIST

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

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

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

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

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

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

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

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

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

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

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

- L1.S1 - Security Operation Center (SOC)
- L1.S2 - Next Generation Firewall

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

A tal fine, **AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO**, 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. Si precisa che, l'**AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO** beneficerà direttamente dei servizi e ne veicolerà l'erogazione nei confronti del **P.O. S. Giovanni di Dio**, fermo restando il rispetto da parte di entrambi dei relativi oneri verso il Fornitore.

1.3 Assunzioni

ID	AMBITO	ASSUNZIONE
1	Adeguamenti Normativi	A fronte di eventuali novità di carattere normativo che riguardano i processi e i sistemi oggetto della presente fornitura, dovranno essere valutati e condivisi tra AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO 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 *"PNNR AGRIGENTO Sicurezza da Remoto_Template Piano dei fabbisogni_Final_rev2"*

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

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

Tabella 4 - Acronimi

4 ORGANIZZAZIONE DEL CONTRATTO ESECUTIVO

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

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

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

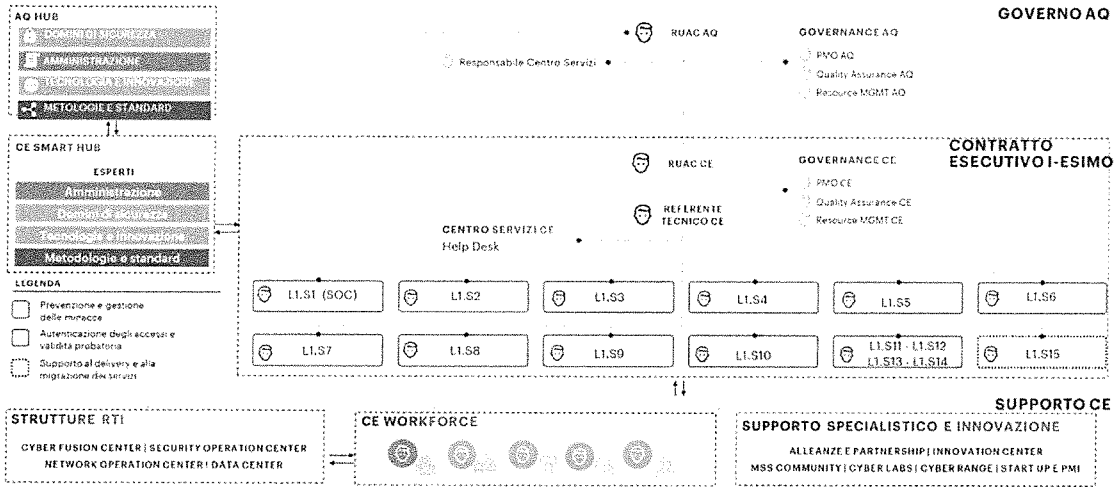


Figura 2 - Organizzazione dell'AQ proposta dal RTI

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

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

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

- team responsabili dell'erogazione dei servizi previsti.

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

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

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

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

4.1 Attività in carico alle aziende del RTI

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

SERVIZIO	ACCENTURE	FASTWEB	FINCANTIERI	DEAS
L1.S1 – Security Operation Center				
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		X		
L1.S8 – Certificati SSL		X		
L1.S9 – Formazione e Security Awareness				
L1.S10 – Gestione dell'Identità e dell'accesso dell'utente				
L1.S11 – Firma Digitale Remota		X		
L1.S12 – Sigillo Elettronico				
L1.S13 – Timbro Elettronico				
L1.S14 – Validazione temporale elettronica qualificata				
L1.S15 – Servizi Specialistici	X	X	X	X
TOTALE (%)	0,18 %	99,46 %	0,18 %	0,18 %
TOTALE (€)	244,00 €	134.950,73 €	244,00 €	244,00 €

Tabella 5 - Ripartizione attività in carico

4.2 Organizzazione e figure di riferimento del Fornitore

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

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

Tabella 6 - Figure di riferimento e referenti del Fornitore

4.3 Luogo di erogazione e di esecuzione della Fornitura

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

- per i servizi erogati da remoto: attraverso i Centri Servizi del Fornitore;
- per i servizi on-site: 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

Gli ambiti d'intervento oggetto di fornitura come di seguito elencati hanno l'obiettivo di soddisfare i requisiti di **AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO** così come riportati nel Piano dei Fabbisogni:

- L1.S7: Servizi di protezione degli End-point
- L1.S8: Certificati SSL
- L1.S11: Firma digitale remota
- L1.S15: Servizi Specialistici

L1.S7 - Servizi di protezione degli End-point

Servizio che consente la protezione dei dispositivi collegati alla rete (PC e Server) dall'accesso non autorizzato o dall'esecuzione di software dannoso. La protezione degli endpoint garantisce, inoltre, che i dispositivi (es. pc desktop, laptop, ecc.) raggiungano un livello di sicurezza definito e siano conformi alle policy e ai requisiti di conformità e sicurezza stabiliti dall'Ente. Nel dettaglio vengono fornite le funzioni di: protezione con sistemi antimalware; ispezione localmente anche del traffico HTTPS; controllo dell'uso o anche blocco dei dispositivi USB; trasmissione degli eventi alle piattaforme di correlazione; monitoraggio continuo delle minacce avanzate e protezione da malware basati su file e senza file; protezione e prevenzione dalla perdita di dati.

L1.S8 - Servizi di certificati SSL

Il certificato SSL (Secure Sockets Layer) e il suo successore TLS (Transport Layer Security), sono protocolli standard necessari a garantire affidabilità e sicurezza della comunicazione tra le componenti client e server di un'applicazione internet. Il certificato assicura che le informazioni sensibili fornite dagli utenti sul web rimangano riservate e non vengano in alcun modo intercettate da terze parti (comunicazione criptata tra il client server e il server web).

L1.S11 - Firma digitale remota - questo servizio consentirà all' Amministrazione di dare efficacia probatoria ai documenti informatici firmati digitalmente, favorendo così i processi di dematerializzazione e consentendo l'automazione e l'ottimizzazione dei processi aziendali. La firma digitale è il risultato di una procedura informatica, detta validazione, che garantisce l'autenticità, l'integrità e il non ripudio dei documenti informatici.

L1.S15 - Servizi Specialistici

I servizi di Supporto Specialistico hanno l'obiettivo di fornire ad AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO 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

I volumi e requisiti indicati nel Piano dei Fabbisogni dell'Amministrazione (sezione "Sintesi dei Servizi Richiesti"), relativamente ai servizi selezionati da quest'ultima, sono la base di partenza sulla quale il RTI ha definito le quantità e, quindi, il dimensionamento dei servizi ed il relativo periodo di riferimento, così come riportati nella seguente tabella.
Si rende noto che in merito ai Servizi Specialistici L1.S15 richiesti espressamente dal Piano dei Fabbisogni, in cui tuttavia non sono indicati i dimensionamenti desiderati, il RTI propone il dimensionamento riportato nella tabella seguente al fine di rispondere ai requisiti richiesti dall'Amministrazione.

SERVIZIO	FASCIA	IMPORTO I ANNO/Quantità	IMPORTO II ANNO/Quantità	IMPORTO III ANNO/Quantità	IMPORTO IV ANNO/Quantità
L1.S7 – Protezione degli endpoint	Fino a 5.000 nodi	12.875,86 €/1001	12.875,86 €/1001	12.875,86 €/1001	0
L1.S8 – Certificati SSL	SSL OV	32,72 €/1	0	0	0

SERVIZIO	FASCIA	IMPORTO I ANNO/Quantità	IMPORTO II ANNO/Quantità	IMPORTO III ANNO/Quantità	IMPORTO IV ANNO/Quantità
L1.S11 – Firma Digitale Remota	Fascia 3 - > 500 e fino a 1.000 utenti	2.491,473 €/501	2.491,473 €/501	2.491,473 €/501	0
L1.S15 – Servizi Specialistici a supporto di L1.S7 – Protezione degli endpoint	Numero Giorni persona del team ottimale	15.860,00 €/65	13.176,00 €/54	13.176,00 €/54	0
L1.S15 – Servizi Specialistici a supporto di L1.S11 – Firma digitale remota	Numero Giorni persona del team ottimale	19.520,00 €/80	13.908,00 €/57	13.908,00 €/57	0

Tabella 7 - Servizi richiesti

5.3 Indicatore di progresso

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

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

Di seguito i servizi proposti in linea con le esigenze espresse da AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO.

6.1 Descrizione dei servizi richiesti

6.1.1 L1.S7 – Protezione degli End-Point

Il servizio di protezione degli Endpoint rappresenta uno degli elementi chiave forniti dal Centro Servizi per garantire la sicurezza delle infrastrutture concordate con l'Amministrazione, operando direttamente sui dispositivi in uso agli utenti abilitando sia l'identificazione di anomalie di processo che le azioni di contenimento e reazione da implementare in caso di violazione. La soluzione tecnologica di Endpoint Protection proposta, riconosciuta come leader sul mercato, fornisce un'ampia e consolidata copertura dei requisiti di tecnico-funzionali e rappresenta un elemento fondamentale e raccomandato nel catalogo offerto del Centro Servizi. Nello specifico, il servizio consente di:

- effettuare l'ispezione del traffico generato dalla postazione di lavoro;
- controllare lo scambio di dati (Data Loss Prevention – DLP) in maniera tale che le informazioni sensibili non possano essere trasferite ad attori non autorizzati;
- controllare lo stato di compliance dei dispositivi rispetto a policy di sicurezza ben definite;
- inviare log al SOC e abilitando il monitoraggio 24x7.

Inoltre, il servizio prevede di sfruttare tecniche di rilevamento delle anomalie avanzate tramite:

- metodologie di ML prima e durante l'esecuzione dei file;
- tecniche di cancellazione del rumore di fondo, come censimento ed elenchi di utenti autorizzati, a ogni li-vello di rilevamento, per ridurre drasticamente i falsi positivi;
- tecniche specifiche per la protezione contro script, iniezioni, ransomware e attacchi a memoria e browser, grazie a un'innovativa analisi del comportamento.

Il numero di end point indicati nella richiesta di Azienda Sanitaria Provinciale di Agrigento (n. 1001) porta alla selezione della Fascia Fino a 5.000 nodi.

6.1.2 L1.S8 – Certificati SSL

Nell'ambito di tale progetto sarà fornito all'amministrazione un certificato SSL OV per la durata di un anno, diversamente dagli altri servizi.

6.1.3 L1.S11 – Firma Digitale Remota

Il servizio prevede la modalità di utilizzo "da remoto" ossia una firma digitale generata usando strumenti di autenticazione (tipicamente user id+ password +OTP o telefono cellulare) che consentono la generazione della firma su un dispositivo (HSM) custodito dal prestatore del servizio fiduciario qualificato.
Il servizio verrà configurato come un servizio "online" nel quale la chiave privata del firmatario viene generata e conservata assieme al certificato di firma rilasciato da parte di un Certificatore accreditato, all'interno di un server remoto sicuro (basa-to su un HSM conforme alla normativa vigente in materia).

Viene utilizzato un sistema di autenticazione forte che prevede l'uso, oltre alla conoscenza di un codice segreto (es. PIN), di sistemi OTP logici (es. USB, telefono cellulare, token).
L'attività di verifica dell'identità dei titolari dei certificati di firma digitali, propedeutica al loro rilascio, è effettuata a cura e sotto la responsabilità dell'Amministrazione.
Il servizio viene reso in modo da garantire la conformità alla normativa vigente in materia di firme digitali (CAD d.lgs. 82 del 7 marzo 2005 e successive modifiche) e la Determinazione Commissariale n. 63/2014 dell'Agenzia per l'Italia Digitale.
Il servizio include la fornitura dei certificati digitali rilasciati da un Certificatore accreditato e delle relative coppie di chiavi pubblica/privata con lunghezza minima di 2048 bit, necessarie alla generazione delle firme.
L'Amministrazione usufruirà di N.501 firme per ognuno dei tre anni di contratto.

6.1.4 L1.S15 – Servizi Specialistici

Tale servizio prevede un supporto specialistico con l'obiettivo di fornire ad AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO supporto tecnico connesso ai servizi oggetto del presente Piano Operativo, come di seguito descritto- nel dettaglio per ciascun servizio.

6.1.4.1 Servizi Specialistici a supporto della protezione degli End-Point

Il servizio prevede le azioni di setup negli end-point e la migrazione dai sistemi di end-point protection attuali (Kaspersky) a quelli previsti dalla convenzione, comprese tutte le attività di analisi e configurazione per l'attivazione di configurazioni ad hoc, raccolta informazioni, meeting tecnici, ecc.; supporto nell'analisi dei deliverable raccolti a seguito di rilevazioni di violazioni.

6.1.4.2 Servizi Specialistici a supporto della Firma Digitale Remota

Tale servizio prevede giornate di supporto necessarie all'integrazione dei sistemi di firma digitale remota con gli applicativi sanitari dell'Amministrazione. L'attività comprende le fasi di assessment, meeting tecnici verticali col personale IT dell'Amministrazione, analisi, sviluppo tecnico della soluzione d'integrazione con predisposizione connettori.

6.2 Utenza interessata / coinvolta

Personale di AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO e del P.O. S. Giovanni di Dio.

6.3 Eventuali riferimenti / vincoli normativi

N.A.

7 PIANO DI PROGETTO

7.1 Cronoprogramma

L'erogazione dei servizi avrà durata 36 mesi, a decorrere dalla data di conclusione delle attività di presa in carico T0 (data di firma del contratto esecutivo + periodo di presa in carico), come indicato nella seguente tabella:

	ANNO I												ANNO II												ANNO III											
	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.S7 PROTEZIONE DEGLI END POINT																																				
L1.S8 Certificati SSL																																				
L1.S11 FIRMA DIGITALE REMOTA																																				
L1.S15 SERVIZI SPECIALISTICI																																				

Tabella 9 – Cronoprogramma

7.2 Data di Attivazione e Durata del Servizio

Il contratto esecutivo produrrà i suoi effetti dalla data di stipula e avrà una durata di 36 mesi a decorrere dalla data di conclusione delle attività di presa in carico.

7.3 Gruppo di Lavoro

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

7.4 Modalità di esecuzione dei Servizi

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

MILESTONE	DESCRIZIONE	ATTORE
Richiesta stima e Piano di Lavoro	Richiesta al fornitore di procedere alla stima dei tempi e costi del servizio	Amministrazione
Stima (pre-dimensionamento)	Comunicazione dei tempi e dei costi previsti per servizio	RTI

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

Tabella 10 - Descrizione milestone per obiettivo

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

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

7.5 Modalità di ricorso al Subappalto da parte del Fornitore

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

SERVIZIO	AZIENDA	QUOTA MASSIMA SUBAPPALTABILE
L1.S15 – Servizi Specialistici	Accenture	50%
L1.S7 – Protezione degli endpoint, L1.S8 – Certificati SSL, L1.S11 – Firma Digitale Remota, L1.S15 – Servizi Specialistici	Fastweb	50%
L1.S15 – Servizi Specialistici	Fincantieri	50%
L1.S15 – Servizi Specialistici	Deas	50%

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

8 DIMENSIONAMENTO ECONOMICO

8.1 Modalità di erogazione dei Servizi

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

ID SERVIZIO	METRICA	MODALITÀ EROGAZIONE	MODALITÀ CONSUNTIVAZIONE	PERIODICITÀ CONSUNTIVAZIONE	PREZZO UNITARIO OFFERTO	QUANTITÀ	VALORE ECONOMICO
L1.S7	Nodi/anno	Da remoto	Canone	Mensile	12,863 €	3003	38.627,59 €
L1.S8	Numero certificati/anno	Da remoto	Canone	Annuale	32,717 €	1	32,717 €
L1.S11	Utenti/anno	Da remoto	Canone	Mensile	4,973 €	1503	7.474,42 €
L1.S15 per L1.S7	Giorni persona del team ottimale	Da remoto /on site	Progettuale a corpo	Mensile	244,00 €	173	42.212,00 €
L1.S15 per L1.S11	Giorni persona del team ottimale	Da remoto /on site	Progettuale a corpo	Mensile	244,00 €	194	47.336,00 €

Tabella 12 - Quadro economico di riferimento

L'importo complessivo dell'ordinativo di fornitura arrotondato per eccesso ammonta a **135.682,73 € (iva esclusa).**

8.2 Indicazioni in ordine alla fatturazione ed ai termini di pagamento

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

9 ALLEGATI

9.1 Piano di Lavoro Generale

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

9.2 Piano di Presa in Carico

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

9.3 Piano della Qualità Specifico

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

9.4 Curriculum Vitae dei Referenti

Si allega, nel Piano di Lavoro Generale, il CV del RUAC di CE. Per quanto concerne il Responsabile Tecnico, 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).

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

Rev.	Data	Descrizione delle modifiche	Autore
01	20/03/2023	Prima emissione	RTI

Registro delle versioni

Sommario

Indice delle tabelle

Indice delle figure

1 INTRODUZIONE

L'Azienda Sanitaria con sede legale in Viale della Vittoria 321 – 92100 Agrigento (di seguito anche "Amministrazione"), è stata istituita con la Legge regionale 14 aprile 2009 N. 5 ed è divenuta operativa a partire dal 1° settembre 2009. L'organizzazione ed il funzionamento dell'azienda, disciplinati con atto aziendale di diritto privato, mirano ad assicurare l'erogazione delle prestazioni essenziali ed appropriate, lo sviluppo dei sistemi di qualità, la massima accessibilità ai servizi dei cittadini, l'equità delle prestazioni erogate, il raccordo istituzionale con gli Enti Locali, il collegamento con le altre organizzazioni sanitarie e di volontariato, nonché l'ottimalizzazione e l'integrazione delle risorse e delle risposte assistenziali.
Fine istituzionale dell'"Azienda Sanitaria Provinciale di Agrigento " è l'erogazione, sia in regime di ricovero che in forma ambulatoriale, di servizi e prestazioni di diagnosi e cura delle malattie acute e di quelle che richiedono interventi di urgenza.
Le prestazioni erogate dall'Azienda ospedaliera comprendono le visite mediche, l'assistenza infermieristica, e ogni atto e procedura diagnostica e terapeutica necessari per risolvere i problemi di salute di adulti e bambini, degenti e non degenti, compatibili con il livello di dotazione tecnologica delle singole strutture.
L'Azienda, dotata di oltre 500 posti letto, partecipa ai programmi nazionali e regionali nei settori dell'emergenza, dei trapianti, della prevenzione, della tutela materno-infantile e delle patologie oncologiche, e svolge attività didattiche e di ricerca.
L'attività ospedaliera, coordinata dalla direzione aziendale, è erogata attraverso due Distretti Ospedalieri dell'Azienda Sanitaria Provinciale (denominati AG1 e AG2) che operano mediante un'organizzazione in rete anche al fine di assicurare all'utente l'appropriatezza del percorso di accoglienza, presa in carico, cura e dimissione.

Del distretto AG1 fanno parte i seguenti Presidi Ospedalieri:

- S. Giovanni di Dio (Agrigento)
- Barone Lombardo (Canicattì)
- S. Giacomo D'Altopasso (Licata)

Del distretto AG2 fanno parte i seguenti Presidi Ospedalieri:

- Fratelli Parlapiano (Ribera)
- Giovanni Paolo II (Sciacca)

1.1 Descrizione del contesto Tecnologico, Applicativo e Procedurale

Di seguito si riporta una descrizione semplificata, relativa allo stato di fatto inerente vari aspetti di cybersecurity gestiti oggi presso l'Amministrazione ed in generale dell'architettura di rete dell'Azienda Sanitaria Provinciale di Agrigento.

L'Amministrazione è dotata di una coppia di accessi dati alle reti INTERNET/INTRANET, in convenzione Consip SPC CONN. Tali collegamenti dati si trovano presso il CED di Viale Della Vittoria – Agrigento e sono in alta affidabilità con banda pari ad 600 Mbps.
Le sedi periferiche dell'Amministrazione sono collegate al centro stella attraverso dei collegamenti VPN MPLS ed accedono alla rete INTERNET attraverso i firewall di centro stella.
Attualmente i servizi di sicurezza perimetrale, per tutti i server/Virtual Machine, vengono gestiti dall'Amministrazione attraverso dei firewall, di *brand* Watchguard, attivi su appliance fisiche. Tutti i servizi vengono esposti alla rete pubblica attraverso queste appliance.
I server/VM sono collegati, attraverso l'infrastruttura LAN cliente, alla subnet private dei firewall perimetrali. La gestione della virtualizzazione viene garantita dal VMware Cluster Datastore. Tutti i server, su cui sono attive circa N.135 VM, e le storage aziendali sono installati, quasi, nella loro totalità nel CED di Viale della Vittoria. Circa 10 VM risiedono tra i Presidi ospedalieri di Sciacca e Canicattì (i server totali tra fisici e virtuali sono circa 200). Non esiste un sito di Disaster-Recovery esterno al campus ed i backup vengono effettuati mediante il software VEEAM Backup, mentre i backup dei DB vengono effettuati su nastri esterni.
I PC dei dipendenti navigano protetti dai Watchguard, dove vengono applicate policy di navigazione, content-filtering, IDS, ecc..
La gestione da remoto sulle singole PDL (circa 2500) viene effettuata grazie al software di remote control Rustdesk.
La rete interna dell'Azienda dispone di N.2 core-switch, presso il CED di Viale della Vittoria, in alta affidabilità. Tali core-switch sono interconnessi ai router spc2. Gli switch che servono i padiglioni amministrativi e sanitari della sede di Viale della Vittoria vengono interconnessi con dorsali, sempre in F.O. ed a questi si attestano gli apparati Layer2 posti nei vari piani/reparti: il totale degli apparati per questo sito, al netto dei core-switch, è pari a N.35. Gli altri Presidi Ospedalieri contano una totalità di circa 154 device. La rete LAN è segmentata logicamente attraverso l'uso di VLAN dedicate e di access-list per consentire/negare (secondo necessità) la comunicazione tra le subnet all'interno del campus. Il numero complessivo degli apparati di rete è pari a 300.

La maggior parte degli apparati di rete sono managed ma esistono, pochissimi, apparati unmanaged nella rete cliente. Tutti gli switch, Access-Point ed UPS vengono monitorati attraverso il software Zabbix, gestito dal presidio tecnico.
Non esistono server syslog su cui si dovrebbero conservare, quantomeno, i log del Domain Controller, del server di posta elettronica e dell'antispam né tantomeno software per interpolare gli eventi tracciati.
Per ciò che riguarda l'accesso esterno, nella rete dell'Amministrazione, di fornitori/dipendenti sono state create, in un VPN Concentrator, delle utenze ad hoc. L'accesso avviene attraverso il solo inserimento della doppietta username/password.
La protezione delle macchine dell'Amministrazione è garantita ad oggi da un sistema antivirus di brand Kaspersky.

1.2 Scopo

Scopo del presente progetto è di fornire all'Azienda Sanitaria Provinciale di Agrigento per il P.O. Giovanni Paolo II di Sciacca gli strumenti necessari ad assicurare un'analisi approfondita dell'attuale livello di sicurezza dell'intera infrastruttura monitorata e allertare di conseguenza i corretti riferimenti aziendali che saranno indicati al RTI. In tal modo, le strutture interne preposte potranno di conseguenza intervenire con azioni correttive a fronte del rischio identificato sui vari sistemi informatici inerente a potenziali falle dal punto di vista della sicurezza. Per consentire l'espletamento di tale servizio, l'amministrazione verrà dotata di uno strumento che, tramite un processo automatico di assesment delle vulnerabilità, le consentirà di ottenere una fotografia precisa del livello e gravità del rischio a cui, in quel momento, sono esposti i propri sistemi oggetto di tali valutazioni ripetute nel tempo.
E' un ulteriore obiettivo di questa azione dotare l'azienda degli strumenti di efficacia probatoria e validità legale (Firme digitali remote) oltre alla affidabilità, riservatezza e, quindi, sicurezza nella comunicazione tra le componenti client e server di un'applicazione internet (Certificati SSL), per i dipendenti degli Enti beneficiari.

1.3 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.

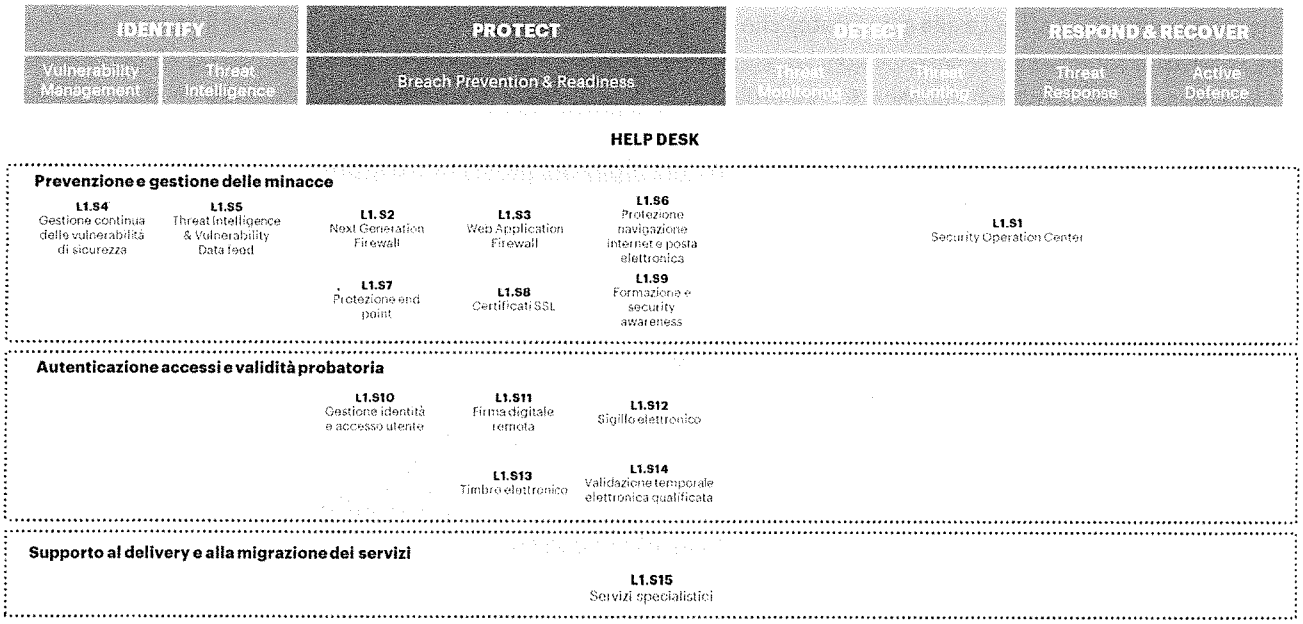


Figura 1 – Mappatura Servizi di Sicurezza e Framework NIST

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, **AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO**, intende avvalersi dei **servizi di Sicurezza da Remoto** previsti per il **Lotto 1**, secondo i termini e le condizioni dell'**Accordo Quadro per l'Affidamento di Servizi da Remoto, di Compliance e Controllo per le Pubbliche Amministrazioni – Lotto 1 ID2296 –** (Accordo Quadro o AQ), senza riaprire il confronto competitivo tra gli operatori economici parti dell'Accordo Quadro ("AQ a condizioni tutte fissate").

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

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

A tal fine, **AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO**, 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. Si precisa che, l'**AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO** beneficerà direttamente dei servizi e ne veicolerà l'erogazione nei confronti del **P.O. Giovanni Paolo II di Sciacca**, fermo restando il rispetto da parte di entrambi dei relativi oneri verso il Fornitore.

1.4 Assunzioni

Indicare le assunzioni (N.A. se non ce ne sono).

ID	AMBITO	ASSUNZIONE
1	Adeguamenti Normativi	A fronte di eventuali novità di carattere normativo che riguardano i processi e i sistemi oggetto della presente fornitura, dovranno essere valutati e condivisi tra AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO 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 "PDF PNNR SCIACCA Sicurezza da Remoto Template Piano dei fabbisogni_Final_rev2"

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

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

Tabella 4 - Acronimi

4 ORGANIZZAZIONE DEL CONTRATTO ESECUTIVO

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

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

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

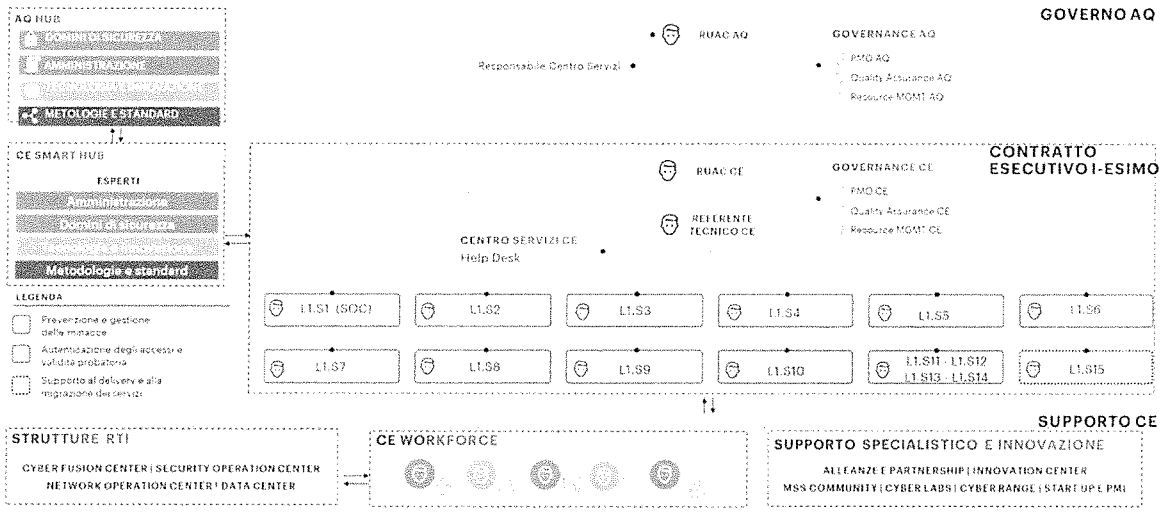


Figura 2 - Organizzazione dell'AQ proposta dal RTI

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

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

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

- team responsabili dell'erogazione dei servizi previsti.

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

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

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

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

4.1 Attività in carico alle aziende del RTI

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

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

SERVIZIO	ACCENTURE	FASTWEB	FINCANTIERI	DEAS
L1.S2 – Next Generation Firewall				
L1.S3 – Web Application Firewall				
L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza	X			
L1.S5 – Threat Intelligence & Vulnerability Data Feed				
L1.S6 – Protezione Navigazione Internet e Posta Elettronica				
L1.S7 – Protezione degli endpoint				
L1.S8 – Certificati SSL		X		
L1.S9 – Formazione e Security Awareness				
L1.S10 – Gestione dell'Identità e dell'accesso dell'utente				
L1.S11 – Firma Digitale Remota		X		
L1.S12 – Sigillo Elettronico				
L1.S13 – Timbro Elettronico				
L1.S14 – Validazione temporale elettronica qualificata				
L1.S15 – Servizi Specialistici	X	X	X	X
TOTALE (%)	19,873 %	79,739 %	0,194 %	0,194 %
TOTALE (€)	24.990,00 €	100.268,52 €	244,00 €	244,00 €

Tabella 5 - Ripartizione attività in carico

4.2 Organizzazione e figure di riferimento del Fornitore

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

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

Tabella 6 - Figure di riferimento e referenti del Fornitore

4.3 Luogo di erogazione e di esecuzione della Fornitura

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

- per i servizi erogati *da remoto* - attraverso i Centri Servizi del Fornitore;
- per i servizi on-site - 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

Gli ambiti d'intervento oggetto di fornitura come di seguito elencati hanno l'obiettivo di soddisfare i requisiti di **AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO** così come riportati nel Piano dei Fabbisogni:

- L1.S4: Gestione continua delle vulnerabilità
- L1.S8: Certificati SSL
- L1.S11: Firma digitale remota
- L1.S15: Servizi Specialistici

5.2 Servizi

I volumi e requisiti indicati nel Piano dei Fabbisogni dell'Amministrazione (sezione "Sintesi dei Servizi Richiesti"), relativamente ai servizi selezionati da quest'ultima, sono la base di partenza sulla quale il RTI ha definito le quantità e, quindi, il dimensionamento dei servizi ed il relativo periodo di riferimento, così come riportati nella seguente tabella. Si rende noto che in merito ai Servizi Specialistici L1.S15 richiesti espressamente dal Piano dei Fabbisogni, in cui tuttavia non sono indicati i dimensionamenti desiderati, il RTI propone il dimensionamento riportato nella tabella seguente al fine di rispondere ai requisiti richiesti dall'Amministrazione.

SERVIZIO	FASCIA	IMPORTO I ANNO/Quantità	IMPORTO II ANNO/Quantità	IMPORTO III ANNO/Quantità	IMPORTO IVANNO/Quantità
L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza	Fascia 3 > 200 IP	3.450,00 €/250	3.450,00 €/250	3.450,00 €/250	0
L1.S8 – Certificati SSL	SSL OV WILD-CARD	74,102 €/1	0	0	0
L1.S11 – Firma Digitale Remota	Fascia 3 - > 500 e fino a 1.000 utenti	2.491,473 €/501	2.491,473 €/501	2.491,473 €/501	0
L1.S15 – Servizi Specialistici a supporto di L1.S11 – Firma digitale remota	Numero Giorni persona del team ottimale	73.200,00 €/300	10.004,00 €/41	10.004,00 €/41	0
L1.S15 – Servizi Specialistici a supporto di L1.S4 - Vulnerability Management	Numero Giorni persona del team ottimale	7.320,00 € /30	3.660,00 €/15	3.660,00 €/15	0

Tabella 7 - Servizi richiesti

5.3 Indicatore di progresso

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

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

Tabella 8 - Schema definizione Indicatore di Progresso

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

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

6 SOLUZIONE PROPOSTA

6.1 Descrizione dei servizi

Di seguito i servizi proposti in linea con le esigenze espresse da AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO.

6.1.1 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.) del RTI. Il servizio prevede:

- Rilevazione delle vulnerabilità presenti in sistemi, apparati di rete, applicazioni (web, mobile, client-server, etc.), dispositivi ad uso professionale, con rendicontazione delle tecniche, dirette od articolate (OWASP, MITRE kill-chain, etc.) capaci di sfruttarle; la fase di ricerca delle vulnerabilità agevola peraltro la ricostruzione (ove non presente) di un 'Asset Inventory' (con CCE e CPE) del patrimonio informativo del AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO 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) usate per il servizio L1.S5 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'AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO che l'asset abilita, dalla **sensibilità dei dati trattati** e delle **interdipendenze** (con altre funzioni e/o sistemi), unitamente alle indicazioni sulle modalità tecniche, organizzative e procedurali di risoluzione (o mitigazione) delle problematiche riscontrate;
- **Supporto per la pianificazione, su base priorità** (stante la misura del rischio residuo corrente), delle azioni di risoluzione o mitigazione delle problematiche di sicurezza individuate e delle fasi di controllo orientate al rientro dalle non conformità e al miglioramento continuo;
- **Supporto tecnico-organizzativo** e **tecnico-funzionale;**
- **Reportistica** relativa alle scansioni con un alto grado di personalizzazione di elementi quali la superficie d'attacco esposta, livelli di rischio residuo, vulnerabilità associate agli asset (pregresse ed attuali) e stato d'avanzamento dei piani di rientro.

I volumi identificati per il servizio di Vulnerability scanning è pari a 250 IP/anno.

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'AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO 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'AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO e quest'ultimo abiliterà la comunicazione verso tutte le porte TCP e UDP dei i sistemi informativi presenti nelle reti in perimetro per eseguire le scansioni.
- Una **console di gestione,** installata presso il Centro Servizi, da cui è possibile pianificare le analisi infrastrutturali e applicative, visualizzare i risultati e gestire la reportistica per mantenere una visione complessiva dello stato di esposizione del contraente; la console di gestione comunica con le sonde tramite una connessione VPN.
- Una **console per il dashboarding avanzato e l'automazione**, installata presso il Centro Servizi, per la configurazione e la gestione remota delle sonde; la console di gestione comunica con le sonde tramite una connessione VPN.
- Un **modulo di supporto** con acceleratori e strumenti di diagnostica per l'esecuzione delle scansioni manuali, le analisi delle evidenze e la rappresentazione dei risultati.
- Un **modulo di monitoraggio del rischio** calcolato sui **processi**.

- Una **knowledge base contestualizzata** e aperta all'**information sharing**.

Nell'ambito delle attività sopra riportate, ed in particolare per la verifica delle vulnerabilità eseguita in ambiente di produzione, gli Enti beneficiari, approveranno formalmente l'esecuzione di questi test sui propri Sistemi, manlevando il Fornitore nel caso in cui l'esecuzione dei test approvati provochi degli impatti e/o danni. Resta inteso che il Fornitore segnalerà agli Enti beneficiari, 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'Ente beneficiario dovrà fornire specifica autorizzazione in tal senso, pertanto, qualora tale autorizzazione non venga fornita il Fornitore non potrà procedere. Fermo restando quanto sopra, gli Enti beneficiari si impegnano a verificare che siano resi al Fornitore tutti i consensi, le autorizzazioni e le manleve suddette e necessarie.

6.1.2 L1.S8 – Certificati SSL

Nell'ambito di tale progetto sarà fornito all'amministrazione un certificato SSL OV WILDCARD per la durata di un solo anno, diversamente dagli altri servizi.

6.1.3 L1.S11 – Firma Digitale Remota

Il servizio prevede la modalità di utilizzo "da remoto" ossia una firma digitale generata usando strumenti di autenticazione (tipicamente user id+ password +OTP o telefono cellulare) che consentono la generazione della firma su un dispositivo (HSM) custodito dal prestatore del servizio fiduciario qualificato.
Il servizio verrà configurato come un servizio "online" nel quale la chiave privata del firmatario viene generata e conservata assieme al certificato di firma rilasciato da parte di un Certificatore accreditato, all'interno di un server remoto sicuro (basa-to su un HSM conforme alla normativa vigente in materia).
Verrà utilizzato un sistema di autenticazione forte che prevede l'uso, oltre alla conoscenza di un codice segreto (es. PIN), di sistemi OTP logici (es. USB, telefono cellulare, token).
L'attività di verifica dell'identità dei titolari dei certificati di firma digitali, propedeutica al loro rilascio, verrà effettuata a cura e sotto la responsabilità dell'Amministrazione.
Il servizio verrà reso in modo da garantire la conformità alla normativa vigente in materia di firme digitali (CAD d.lgs. 82 del 7 marzo 2005 e successive modifiche) e la Determinazione Commissariale n. 63/2014 dell'Agenzia per l'Italia Digitale.
Il servizio includerà la fornitura dei certificati digitali rilasciati da un Certificatore accreditato e delle relative coppie di chiavi pubblica/privata con lunghezza minima di 2048 bit, necessarie alla generazione delle firme.
Infine, l'Amministrazione usufruirà di N.501 firme per ognuno dei tre anni di contratto.

6.1.4 L1.S15 – Servizi Specialistici

Tale servizio prevede un supporto specialistico con l'obiettivo di fornire all'AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO supporto tecnico connesso ai servizi oggetto del presente Piano Operativo, come di seguito descritto.

6.1.4.1 Servizi Specialistici a supporto della Firma Digitale Remota

Tale servizio prevede giornate di supporto necessarie all'integrazione dei sistemi di firma digitale remota con gli applicativi sanitari dell'Amministrazione. L'attività comprende le fasi di assessment, meeting tecnici verticali col personale IT dell'Amministrazione, analisi, sviluppo tecnico della soluzione d'integrazione con predisposizione connettori.

6.1.4.2 Servizi Specialistici a supporto della Gestione Continua delle Vulnerabilità di Sicurezza

Il servizio prevede, un supporto specialistico per la consegna del report delle vulnerabilità periodico sui sistemi e una assistenza all'Amministrazione nella valutazione delle vulnerabilità per identificare un piano di rientro in base alle priorità dettate dall'Amministrazione 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

Personale di AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO e del P.O. Giovanni Paolo II di Sciacca.

6.3 Eventuali riferimenti / vincoli normativi

N.A.

7 PIANO DI PROGETTO

7.1 Cronoprogramma

L'erogazione dei servizi avrà durata 36 mesi, a decorrere dalla data di conclusione delle attività di presa in carico T0 (data di firma del contratto esecutivo + periodo di presa in carico), come indicato nella seguente tabella:

	ANNO I												ANNO II												ANNO III											
	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.S4 Gestione Continua delle Vulnerabilità di Sicurezza																																				
L1.S8 Certificati SSL																																				
L1.S11 FIRMA DIGITALE REMOTA																																				
L1.S15 SERVIZI SPECIALISTICI																																				

Tabella 9 – Cronoprogramma

7.2 Data di Attivazione e Durata del Servizio

Il contratto esecutivo produrrà i suoi effetti dalla data di stipula e avrà una durata di 36 mesi a decorrere dalla data di conclusione delle attività di presa in carico.

7.3 Gruppo di Lavoro

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

7.4 Modalità di esecuzione dei Servizi

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

MILESTONE	DESCRIZIONE	ATTORE
Richiesta stima e Piano di Lavoro	Richiesta al fornitore di procedere alla stima dei tempi e costi del servizio	Amministrazione
Stima (pre-dimensionamento)	Comunicazione dei tempi e dei costi previsti per servizio	RTI

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

Tabella 10 - Descrizione milestone per obiettivo

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

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

7.5 Modalità di ricorso al Subappalto da parte del Fornitore

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

SERVIZIO	AZIENDA	QUOTA MASSIMA SUBAPPALTABILE
L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza, L1.S15 – Servizi Specialistici	Accenture	50%
L1.S8 – Certificati SSL, L1.S11 – Firma Digitale Remota, L1.S15 – Servizi Specialistici	Fastweb	50%
L1.S15 – Servizi Specialistici	Fincantieri	50%
L1.S15 – Servizi Specialistici	Deas	50%

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

8 DIMENSIONAMENTO ECONOMICO

8.1 Modalità di erogazione dei Servizi

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

ID SERVIZIO	METRICA	MODALITÀ EROGAZIONE	MODALITÀ CONSUNTIVAZIONE	PERIODICITÀ CONSUNTIVAZIONE	PREZZO UNITARIO OFFERTO	QUANTITÀ	VALORE ECONOMICO
L1.S4	Numero IP /anno	Da remoto	Canone	Mensile	13,80 €	750	10.350,00 € Per 3 anni
L1.S8	Numero certificati/anno	Da remoto	Canone	Mensile	74,102 €	1	74,10 € Per 1 anno
L1.S11	Utenti/anno	Da remoto	Canone	Mensile	4,973 €	1503	7.474,42 € Per 3 anni
L1.S15 per L1.S4	Giorni persona del team ottimale	Da remoto /on site	Progettuale a corpo	Mensile	244,00 €	60	14.640,00 € Per 3 anni
L1.S15 per L1.S11	Giorni persona del team ottimale	Da remoto /on site	Progettuale a corpo	Mensile	244,00 €	382	93.208,00 € Per 3 anni

Tabella 12 - Quadro economico di riferimento

L'importo complessivo dell'ordinativo di fornitura ammonta arrotondato per difetto a **125.746,52 € (iva esclusa).**

8.2 Indicazioni in ordine alla fatturazione ed ai termini di pagamento

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

9 ALLEGATI

9.1 Piano di Lavoro Generale

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

9.2 Piano di Presa in Carico

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

9.3 Piano della Qualità Specifico

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

9.4 Curriculum Vitae dei Referenti

Si allega, nel Piano di Lavoro Generale, il CV del RUAC di CE. Per quanto concerne il Responsabile Tecnico, 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)

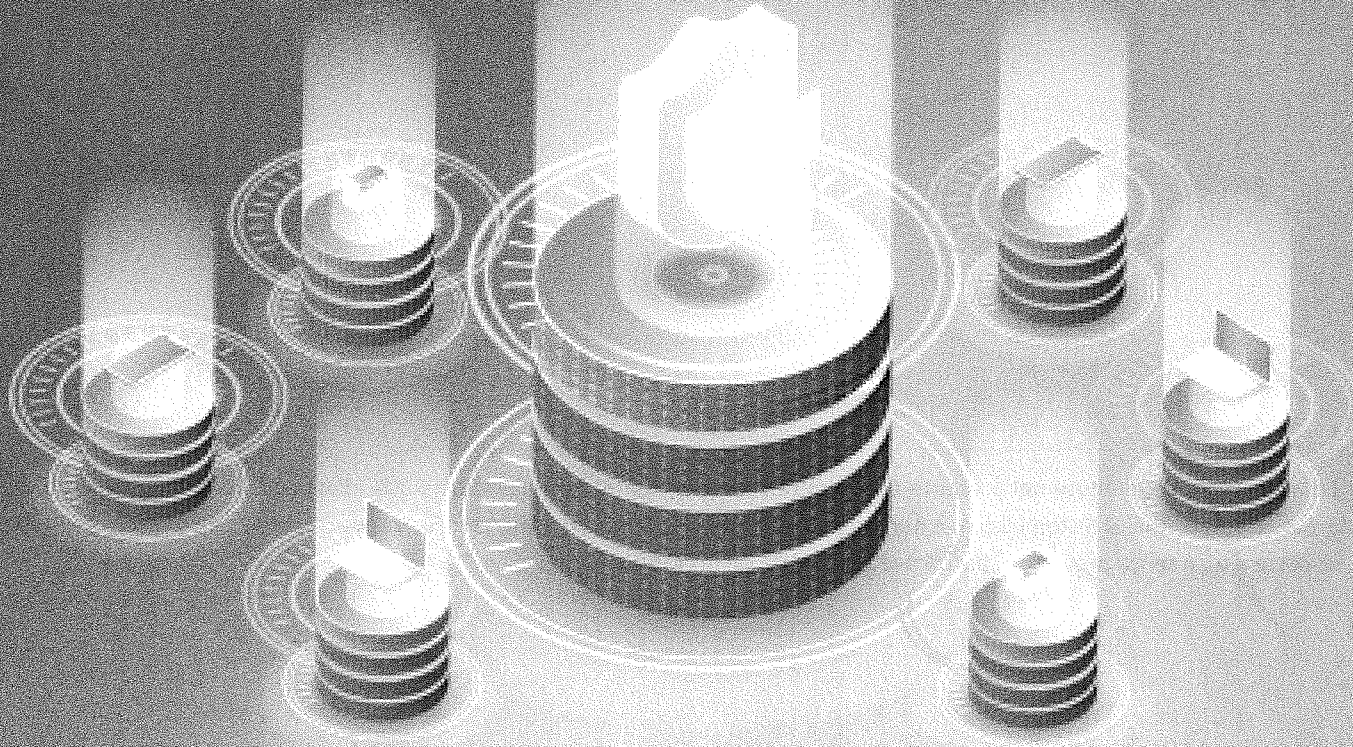
Si allega la documentazione trasmessa a Consip tramite pec in data 11/11/2022, relativa al principio "Do No Significant Harm" (DNSH).

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



Rev.	Data	Descrizione delle modifiche	Autore
01	20/03/2023	Prima emissione	RTI

Registro delle versioni

Sommario

Indice delle tabelle

Indice delle figure

1 INTRODUZIONE

L'Azienda Sanitaria, con sede legale in Viale della Vittoria 321 – 92100 Agrigento (di seguito anche "Amministrazione" o "Azienda Sanitaria" o "ASP"), è stata istituita con la Legge regionale 14 aprile 2009 N. 5 ed è divenuta operativa a partire dal 1° settembre 2009. L'organizzazione ed il funzionamento dell'Azienda Sanitaria, disciplinati con atto aziendale di diritto privato, mirano ad assicurare l'erogazione delle prestazioni essenziali ed appropriate, lo sviluppo dei sistemi di qualità, la massima accessibilità ai servizi dei cittadini, l'equità delle prestazioni erogate, il raccordo istituzionale con gli Enti Locali, il collegamento con le altre organizzazioni sanitarie e di volontariato, nonché l'ottimalizzazione e l'integrazione delle risorse e delle risposte assistenziali.
Fine istituzionale dell'"Azienda Sanitaria Provinciale di Agrigento" è l'erogazione, sia in regime di ricovero che in forma ambulatoriale, di servizi e prestazioni di diagnosi e cura delle malattie acute e di quelle che richiedono interventi di urgenza.
Le prestazioni erogate dall'Azienda ospedaliera comprendono le visite mediche, l'assistenza infermieristica, e ogni atto e procedura diagnostica e terapeutica necessari per risolvere i problemi di salute di adulti e bambini, degenti e non degenti, compatibili con il livello di dotazione tecnologica delle singole strutture.
L'Azienda Sanitaria, dotata di oltre 500 posti letto, partecipa ai programmi nazionali e regionali nei settori dell'emergenza, dei trapianti, della prevenzione, della tutela materno-infantile e delle patologie oncologiche, e svolge attività didattiche e di ricerca.
L'attività ospedaliera, coordinata dalla direzione aziendale, è erogata attraverso due Distretti Ospedalieri dell'Azienda Sanitaria Provinciale (denominati AG1 e AG2) che operano mediante un'organizzazione in rete anche al fine di assicurare all'utente l'appropriatezza del percorso di accoglienza, presa in carico, cura e dimissione.

Del distretto AG1 fanno parte i seguenti Presidi Ospedalieri:

- S. Giovanni di Dio (Agrigento)
- Barone Lombardo (Canicattì)
- S. Giacomo D'Altopasso (Licata)

Del distretto AG2 fanno parte i seguenti Presidi Ospedalieri (di seguito "P.O."):

- Fratelli Parlapiano (Ribera)
- Giovanni Paolo II (Sciacca)

1.1 Descrizione del contesto Tecnologico, Applicativo e Procedurale

Di seguito si riporta una descrizione semplificata, relativa allo stato di fatto inerente vari aspetti di cybersecurity gestiti oggi presso l'Amministrazione ed in generale dell'architettura di rete dell'Azienda Sanitaria Provinciale di Agrigento.

L'Amministrazione è dotata di una coppia di accessi dati alle reti INTERNET/INTRANET, in convenzione Consip SPC CONN. Tali collegamenti dati si trovano presso il CED di Viale Della Vittoria – Agrigento e sono in alta affidabilità con banda pari ad 600 Mbps.
Le sedi periferiche dell'Amministrazione sono collegate al centro stella attraverso dei collegamenti VPN MPLS ed accedono alla rete INTERNET attraverso i firewall di centro stella.
Attualmente i servizi di sicurezza perimetrale, per tutti i server/Virtual Machine, vengono gestiti dall'Amministrazione attraverso dei firewall, di *brand* Watchguard, attivi su appliance fisiche. Tutti i servizi vengono esposti alla rete pubblica attraverso questa appliance.
I server/VM sono collegati, attraverso l'infrastruttura LAN cliente, alla subnet private dei firewall perimetrali. La gestione della virtualizzazione viene garantita dal VMware Cluster Datastore. Tutti i server, su cui sono attive circa N.135 VM, e le storage aziendali sono installati, quasi, nella loro totalità nel CED di Viale della Vittoria. Circa 10 VM risiedono tra i Presidi ospedalieri di Sciacca e Canicattì (i server totali tra fisici e virtuali sono circa 200). Non esiste un sito di Disaster-Recovery esterno al campus ed i backup vengono effettuati mediante il software VEEAM Backup, mentre i backup dei DB vengono effettuati su nastri esterni.
I PC dei dipendenti navigano protetti dai Watchguard, dove vengono applicate policy di navigazione, content-filtering, IDS, ecc..
La gestione da remoto sulle singole PDL (circa 2500) viene effettuata grazie al software di remote control Rustdesk.
La rete interna dell'Azienda dispone di N.2 core-switch, presso il CED di Viale della Vittoria, in alta affidabilità. Tali core-switch sono interconnessi ai router spc2. Gli switch che servono i padiglioni amministrativi e sanitari della sede di Viale della Vittoria vengono interconnessi con dorsali, sempre in F.O. ed a questi si attestano gli apparati Layer2 posti nei vari piani/reparti: il totale degli apparati per questo sito, al netto dei core-switch, è pari a N.35. Gli altri Presidi Ospedalieri contano una totalità di circa 154 device. La rete LAN è segmentata logicamente attraverso l'uso di VLAN dedicate e di access-list per consentire/negare (secondo

necessità) la comunicazione tra le subnet all'interno del campus. Il numero complessivo degli apparati di rete è pari a 300.
La maggior parte degli apparati di rete sono managed ma esistono, pochissimi, apparati unmanaged nella rete cliente. Tutti gli switch, Access-Point ed UPS vengono monitorati attraverso il software Zabbix, gestito dal presidio tecnico.
Non esistono server syslog su cui si dovrebbero conservare, quantomeno, i log del Domain Controller, del server di posta elettronica e dell'antispam né tantomeno software per interpolare gli eventi tracciati.
Per ciò che riguarda l'accesso esterno, nella rete dell'Amministrazione, di fornitori/dipendenti sono state create, in un VPN Concentrator, delle utenze ad hoc. L'accesso avviene attraverso il solo inserimento della doppietta username/password.
La protezione delle macchine dell'Amministrazione è garantita ad oggi da un sistema antivirus di brand Kaspersky.

1.2 Scopo

Scopo del presente progetto è di fornire all'Azienda Sanitaria Provinciale di Agrigento per il P.O. Fratelli Parlapiano di Ribera gli strumenti necessari ad assicurare, in caso di riscontro di eventi anomali nelle workstation o server aziendali e altri eventi di sicurezza degni di nota, un'analisi approfondita degli eventi occorsi, dell'attuale livello di sicurezza dell'intera infrastruttura monitorata e allertare di conseguenza i corretti riferimenti aziendali che saranno indicati al RTI. In tal modo, le strutture interne preposte potranno di conseguenza intervenire con azioni correttive a fronte del rischio identificato sui vari sistemi informatici inerente a potenziali falle dal punto di vista della sicurezza. Per consentire l'espletamento di tale servizio, l'Amministrazione verrà dotata di uno strumento che, tramite un processo automatico di assesment delle vulnerabilità, le consentirà di ottenere una fotografia precisa del livello e gravità del rischio a cui, in quel momento, sono esposti i propri sistemi oggetto di tali valutazioni ripetute nel tempo.
È un ulteriore obiettivo di questa azione dotare l'azienda degli strumenti di efficacia probatoria e validità legale (Firme digitali remote) oltre alla affidabilità, riservatezza e, quindi, sicurezza nella comunicazione tra le componenti client e server di un'applicazione internet (Certificati SSL), per i dipendenti del P.O. Fratelli Parlapiano di Ribera.

1.3 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.

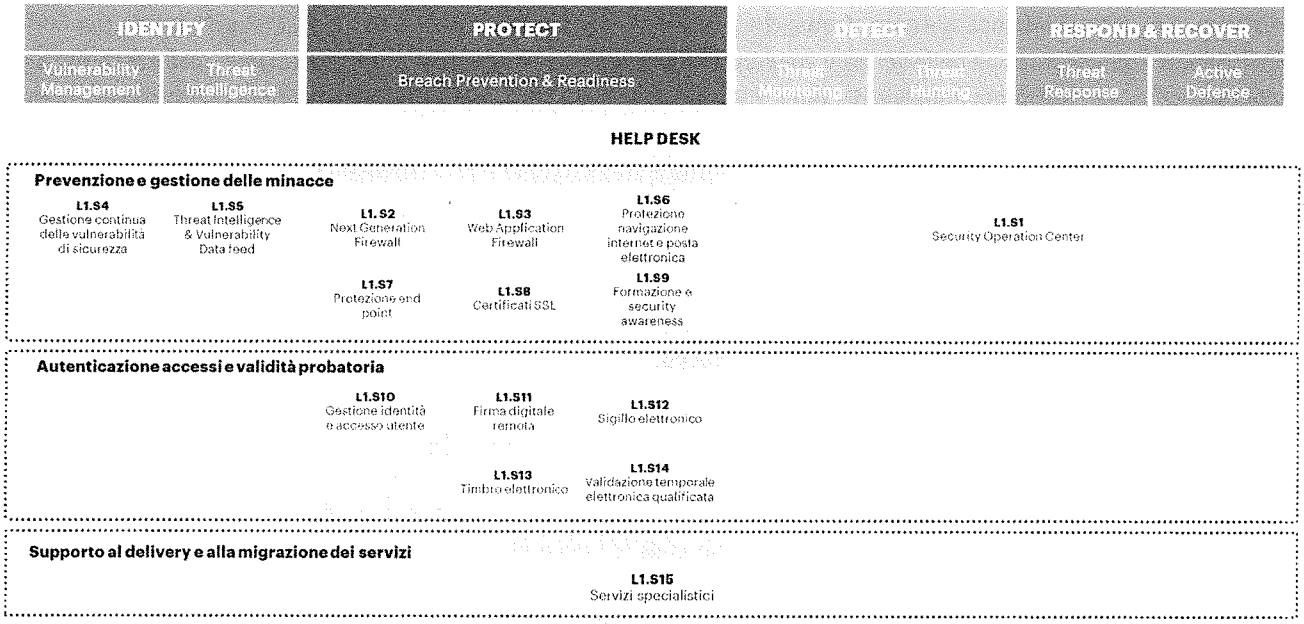


Figura 1 – Mappatura Servizi di Sicurezza e Framework NIST

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, **AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO**, intende avvalersi dei **servizi di Sicurezza da Remoto** previsti per il **Lotto 1**, secondo i termini e le condizioni dell'**Accordo Quadro per l'Affidamento di Servizi da Remoto, di Compliance e Controllo per le Pubbliche Amministrazioni – Lotto 1 ID2296** – (Accordo Quadro o AQ), senza riaprire il confronto competitivo tra gli operatori economici parti dell'Accordo Quadro ("AQ a condizioni tutte fissate").

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

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

A tal fine, **AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO**, 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. Si precisa che, l'**AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO** beneficerà direttamente dei servizi e ne veicolerà l'erogazione nei confronti del **P.O. Fratelli Parlapiano di Ribera**, fermo restando il rispetto da parte di entrambi dei relativi oneri verso il Fornitore.

1.4 Assunzioni

ID	AMBITO	ASSUNZIONE
1	Adeguamenti Normativi	A fronte di eventuali novità di carattere normativo che riguardano i processi e i sistemi oggetto della presente fornitura, dovranno essere valutati e condivisi tra AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO 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 *"PDF PNNR RIBERA Sicurezza da Remoto_Template Piano dei fabbisogni_Final_rev2"*

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

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

Tabella 4 - Acronimi

4 ORGANIZZAZIONE DEL CONTRATTO ESECUTIVO

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

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

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

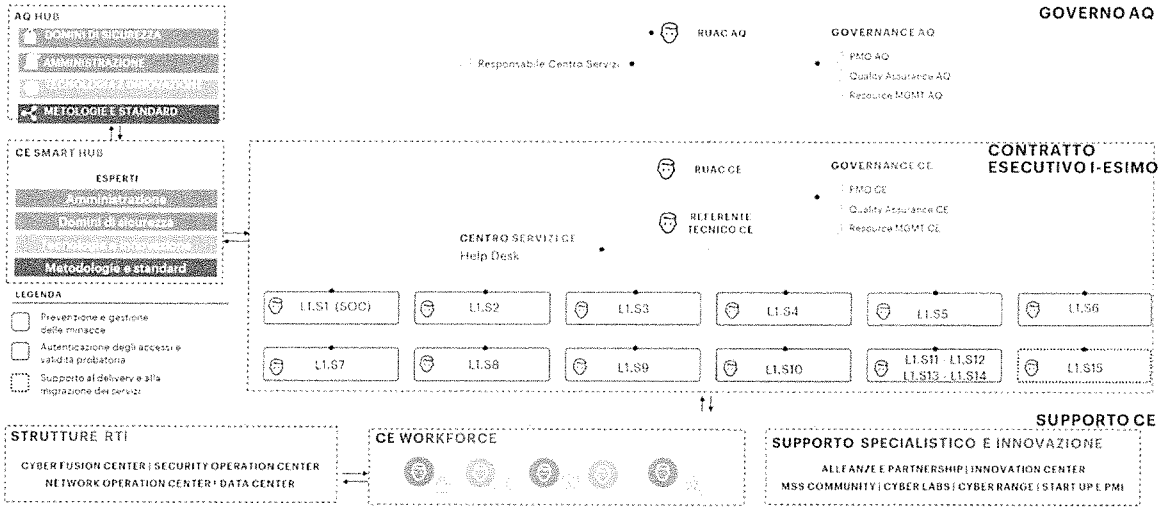


Figura 2 - Organizzazione dell'AQ proposta dal RTI

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

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

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

- team responsabili dell'erogazione dei servizi previsti.

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

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

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

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

4.1 Attività in carico alle aziende del RTI

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

SERVIZIO	ACCENTURE	FASTWEB	FINCANTIERI	DEAS
L1.S1 – Security Operation Center				
L1.S2 – Next Generation Firewall				
L1.S3 – Web Application Firewall				
L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza	X			
L1.S5 – Threat Intelligence & Vulnerability Data Feed				
L1.S6 – Protezione Navigazione Internet e Posta Elettronica				
L1.S7 – Protezione degli endpoint				
L1.S8 – Certificati SSL		X		
L1.S9 – Formazione e Security Awareness				
L1.S10 – Gestione dell'Identità e dell'accesso dell'utente				
L1.S11 – Firma Digitale Remota		X		
L1.S12 – Sigillo Elettronico				
L1.S13 – Timbro Elettronico				
L1.S14 – Validazione temporale elettronica qualificata				
L1.S15 – Servizi Specialistici	X	X	X	X
TOTALE (%)	37,5521 %	61,5255 %	0,4612 %	0,4612 %
TOTALE (€)	19.866,00 €	32.548,56 €	244,00 €	244,00 €

Tabella 5 - Ripartizione attività in carico

4.2 Organizzazione e figure di riferimento del Fornitore

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

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

Tabella 6 - Figure di riferimento e referenti del Fornitore

4.3 Luogo di erogazione e di esecuzione della Fornitura

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

- per i servizi erogati *da remoto* - attraverso i Centri Servizi del Fornitore;
- per i servizi *on-site* - 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

Gli ambiti d'intervento oggetto di fornitura come di seguito elencati hanno l'obiettivo di soddisfare i requisiti di **AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO** così come riportati nel Piano dei Fabbisogni:

- L1.S4: Gestione continua delle vulnerabilità
- L1.S8: Certificati SSL
- L1.S11: Firma digitale remota
- L1.S15: Servizi Specialistici

5.2 Servizi

I volumi e requisiti indicati nel Piano dei Fabbisogni dell'Amministrazione (sezione "Sintesi dei Servizi Richiesti"), relativamente ai servizi selezionati da quest'ultima, sono la base di partenza sulla quale il RTI ha definito le quantità e, quindi, il dimensionamento dei servizi ed il relativo periodo di riferimento, così come riportati nella seguente tabella.
Si rende noto che in merito ai Servizi Specialistici L1.S15 richiesti espressamente dal Piano dei Fabbisogni, in cui tuttavia non sono indicati i dimensionamenti desiderati, il RTI propone il dimensionamento riportato nella tabella seguente al fine di rispondere ai requisiti richiesti dall'Amministrazione.

.

SERVIZIO	FASCIA	IMPORTO I ANNO/Quantità	IMPORTO II ANNO/Quantità	IMPORTO III ANNO/Quantità	IMPORTO IV ANNO/Quantità
L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza	Fascia 3 > 200 IP	3.450,00 €/250	3.450,00 €/250	3.450,00 €/250	0
L1.S8 – Certificati SSL	SSL OV WILDCARD	74,10 €/1	0	0	0
L1.S8 – Certificati SSL	SSL OV	32,72 €/1	0	0	0
L1.S11 – Firma Digitale Remota	Fascia 2 - > 200 e fino a 500 utenti	1.135,248 €/201	1.135,248 €/201	1.135,248 €/201	0
L1.S15 – Servizi Specialistici a supporto di L1.S11 – Firma digitale remota	Numero Giorni persona del team ottimale	18.300,00 €/75	5.612,00 €/23	5.368,00 €/22	0
L1.S15 – Servizi Specialistici a supporto di L1.S4 - Vulnerability Management	Numero Giorni persona del team ottimale	4.880,00 € /20	2.440,00 €/10	2.440,00 €/10	0

Tabella 7 - Servizi richiesti

5.3 Indicatore di progresso

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

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

Tabella 8 - Schema definizione Indicatore di Progresso

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

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

6 SOLUZIONE PROPOSTA

6.1 Descrizione dei servizi

Di seguito i servizi proposti in linea con le esigenze espresse da AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO.

6.1.1 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.) del RTI. Il servizio prevede:

- Rilevazione delle vulnerabilità presenti in sistemi, apparati di rete, applicazioni (web, mobile, client-server, etc.), dispositivi ad uso professionale, con rendicontazione delle tecniche, dirette od articolate (OWASP, MITRE kill-chain, etc.) capaci di sfruttarle; la fase di ricerca delle vulnerabilità agevola peraltro la ricostruzione (ove non presente) di un 'Asset Inventory' (con CCE e CPE) del patrimonio informativo di AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO 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) usate per il servizio L1.S5 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** di AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO che l'asset abilita, dalla **sensibilità dei dati trattati** e delle **interdipendenze** (con altre funzioni e/o sistemi), unitamente alle indicazioni sulle modalità tecniche, organizzative e procedurali di risoluzione (o mitigazione) delle problematiche riscontrate;
- **Supporto per la pianificazione, su base priorità** (stante la misura del rischio residuo corrente), delle azioni di risoluzione o mitigazione delle problematiche di sicurezza individuate e delle fasi di controllo orientate al rientro dalle non conformità e al miglioramento continuo;
- **Supporto tecnico-organizzativo** e **tecnico-funzionale;**
- **Reportistica** relativa alle scansioni con un alto grado di personalizzazione di elementi quali la superficie d'attacco esposta, livelli di rischio residuo, vulnerabilità associate agli asset (pregresse ed attuali) e stato d'avanzamento dei piani di rientro.

I volumi identificati per il servizio di Vulnerability scanning è pari a 250 IP/anno.

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

- Una sonda fisica o virtuale, da installare da parte di AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO 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 di AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO e quest'ultimo abiliterà la comunicazione verso tutte le porte TCP e UDP dei i sistemi informativi presenti nelle reti in perimetro per eseguire le scansioni.
- Una **console di gestione,** installata presso il Centro Servizi, da cui è possibile pianificare le analisi infrastrutturali e applicative, visualizzare i risultati e gestire la reportistica per mantenere una visione complessiva dello stato di esposizione del contraente; la console di gestione comunica con le sonde tramite una connessione VPN.
- Una **console per il dashboarding avanzato e l'automazione**, installata presso il Centro Servizi, per la configurazione e la gestione remota delle sonde; la console di gestione comunica con le sonde tramite una connessione VPN.
- Un **modulo di supporto** con acceleratori e strumenti di diagnostica per l'esecuzione delle scansioni manuali, le analisi delle evidenze e la rappresentazione dei risultati.
- Un **modulo di monitoraggio del rischio** calcolato sui **processi**.
- Una **knowledge base contestualizzata** e aperta all'**information sharing**.

Nell'ambito delle attività sopra riportate, ed in particolare per la verifica delle vulnerabilità eseguita in ambiente di produzione, gli Enti beneficiari, approveranno formalmente l'esecuzione di questi test sui propri Sistemi, manlevando il Fornitore nel caso in cui l'esecuzione dei test approvati provochi degli impatti e/o danni. Resta inteso che il Fornitore segnalerà agli Enti beneficiari, 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'Ente beneficiario dovrà fornire specifica autorizzazione in tal senso, pertanto, qualora tale autorizzazione non venga fornita il Fornitore non potrà procedere. Fermo restando quanto sopra, gli Enti beneficiari si impegnano a verificare che siano resi al Fornitore tutti i consensi, le autorizzazioni e le manleve suddette e necessarie.

6.1.2 L1.S8 – Certificati SSL

Nell'ambito di tale progetto sarà fornito all'amministrazione un certificato SSL OV WILDCARD ed un certificato SSL OV per la durata di un anno, diversamente dagli altri servizi.

6.1.3 L1.S11 – Firma Digitale Remota

Il servizio prevede la modalità di utilizzo "da remoto" ossia una firma digitale generata usando strumenti di autenticazione (tipicamente user id+ password +OTP o telefono cellulare) che consentono la generazione della firma su un dispositivo (HSM) custodito dal prestatore del servizio fiduciario qualificato.
Il servizio verrà configurato come un servizio "online" nel quale la chiave privata del firmatario viene generata e conservata assieme al certificato di firma rilasciato da parte di un Certificatore accreditato, all'interno di un server remoto sicuro (basa-to su un HSM conforme alla normativa vigente in materia).
Viene utilizzato un sistema di autenticazione forte che prevede l'uso, oltre alla conoscenza di un codice segreto (es. PIN), di sistemi OTP logici (es. USB, telefono cellulare, token).
L'attività di verifica dell'identità dei titolari dei certificati di firma digitali, propedeutica al loro rilascio, è effettuata a cura e sotto la responsabilità dell'Amministrazione.
Il servizio viene reso in modo da garantire la conformità alla normativa vigente in materia di firme digitali (CAD d.lgs. 82 del 7 marzo 2005 e successive modifiche) e la Determinazione Commissariale n. 63/2014 dell'Agenzia per l'Italia Digitale.
Il servizio include la fornitura dei certificati digitali rilasciati da un Certificatore accreditato e delle relative coppie di chiavi pubblica/privata con lunghezza minima di 2048 bit, necessarie alla generazione delle firme.
L'Amministrazione usufruirà di N.201 firme per ognuno dei tre anni di contratto.

6.1.4 L1.S15 – Servizi Specialistici

Tale servizio prevede un supporto specialistico con l'obiettivo di fornire ad AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO supporto tecnico connesso ai servizi oggetto del presente Piano Operativo, come di seguito descritto.

6.1.4.1 Servizi Specialistici a supporto della Firma Digitale Remota

Tale servizio prevede giornate di supporto necessarie all'integrazione dei sistemi di firma digitale remota con gli applicativi sanitari dell'Amministrazione. L'attività comprende le fasi di assessment, meeting tecnici verticali col personale IT dell'Amministrazione, analisi, sviluppo tecnico della soluzione d'integrazione con predisposizione connettori.

6.1.4.2 Servizi Specialistici a supporto della Gestione Continua delle Vulnerabilità di Sicurezza

Il servizio prevede, un supporto specialistico per la consegna del report delle vulnerabilità periodico sui sistemi e una assistenza all'Amministrazione nella valutazione delle vulnerabilità per identificare un piano di rientro in base alle priorità dettate dall'Amministrazione 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

Personale di AZIENDA SANITARIA PROVINCIALE DI AGRIGENTO e del P.O. Fratelli Parlapiano di Ribera.

6.3 Eventuali riferimenti / vincoli normativi

N.A.

7 PIANO DI PROGETTO

7.1 Cronoprogramma

L'erogazione dei servizi avrà durata 36 mesi, a decorrere dalla data di conclusione delle attività di presa in carico T0 (data di firma del contratto esecutivo + periodo di presa in carico), come indicato nella seguente tabella:

	ANNO I												ANNO II												ANNO III											
	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.S4 Gestione Continua delle Vulnerabilità di Sicurezza																																				
L1.S8 Certificati SSL																																				
L1.S11 FIRMA DIGITALE REMOTA																																				
L1.S15 SERVIZI SPECIALISTICI																																				

Tabella 9 – Cronoprogramma

7.2 Data di Attivazione e Durata del Servizio

Il contratto esecutivo produrrà i suoi effetti dalla data di stipula e avrà una durata di 36 mesi a decorrere dalla data di conclusione delle attività di presa in carico.

7.3 Gruppo di Lavoro

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

7.4 Modalità di esecuzione dei Servizi

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

MILESTONE	DESCRIZIONE	ATTORE
Richiesta stima e Piano di Lavoro	Richiesta al fornitore di procedere alla stima dei tempi e costi del servizio	Amministrazione
Stima (pre-dimensionamento)	Comunicazione dei tempi e dei costi previsti per servizio	RTI

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

Tabella 10 - Descrizione milestone per obiettivo

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

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

7.5 Modalità di ricorso al Subappalto da parte del Fornitore

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

SERVIZIO	AZIENDA	QUOTA MASSIMA SUBAPPALTABILE
L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza, L1.S15 – Servizi Specialistici	Accenture	50%
L1.S8 – Certificati SSL, L1.S11 – Firma Digitale Remota, L1.S15 – Servizi Specialistici	Fastweb	50%
L1.S15 – Servizi Specialistici	Fincantieri	50%
L1.S15 – Servizi Specialistici	Deas	50%

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

8 DIMENSIONAMENTO ECONOMICO

8.1 Modalità di erogazione dei Servizi

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

ID SERVIZIO	METRICA	MODALITÀ EROGAZIONE	MODALITÀ CONSUNTIVAZIONE	PERIODICITÀ CONSUNTIVAZIONE	PREZZO UNITARIO OFFERTO	QUANTITÀ	VALORE ECONOMICO
L1.S4	Numero IP /anno	Da remoto	Canone	Mensile	13,80 €	750	10.350,00 € Per 3 anni
L1.S8	Numero certificati/anno	Da remoto	Canone	Mensile	74,10 €	1	74,10 € Per 1 anno
L1.S8	Numero certificati/anno	Da remoto	Canone	Mensile	32,72 €	1	32,72 € Per 1 anno
L1.S11	Utenti/anno	Da remoto	Canone	Mensile	5,648 €	603	3.405,74 € Per 3 anni
L1.S15 per L1.S4	Giorni persona del team ottimale	Da remoto /on site	Progettuale a corpo	Mensile	244,00 €	40	9.760,00 € Per 3 anni
L1.S15 per L1.S11	Giorni persona del team ottimale	Da remoto /on site	Progettuale a corpo	Mensile	244,00 €	120	29.280,00 € Per 3 anni

Tabella 12 - Quadro economico di riferimento

L'importo complessivo dell'ordinativo di fornitura ammonta a **52.902,56 € (iva esclusa).**

8.2 Indicazioni in ordine alla fatturazione ed ai termini di pagamento

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

9 ALLEGATI

9.1 Piano di Lavoro Generale

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

9.2 Piano di Presa in Carico

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

9.3 Piano della Qualità Specifico

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

9.4 Curriculum Vitae dei Referenti

Si allega, nel Piano di Lavoro Generale, il CV del RUAC di CE. Per quanto concerne il Responsabile Tecnico, 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).

All. 5

SERVIZIO SANITARIO NAZIONALE - REGIONE SICILIANA
Azienda Sanitaria Provinciale di Agrigento
Sede legale : Viale della Vittoria n.321 92100 Agrigento
Partita IVA - Codice Fiscale : 02570930848
Sistemi Informatici Aziendali

Tel. 0922407111
cell: 3388002237
EMail : riccardo.insalaco@aspag.it

Prot.n. 00 49544 *del* 24/03/2023

Al Direttore U.O.C. Servizio Provveditorato

e.p.c. Al Commissario Straordinario
Al Direttore Amministrativo

SEDE

Oggetto: *Procedura di adesione all'Accordo Quadro per l'affidamento di Servizi di Sicurezza da Remoto, di compliance e controllo per le pubbliche amministrazioni - lotto 1 - ID 2296.*
- Valutazione Piani Operativi proposti dal fornitore. -

In data 21 marzo u.s. la RTI Accenture S.p.A., Fincantieri Nextech S.p.A., Fasteweb S.p.A., Deas, Difesa e Analisi Sistemi S.p.A. ha consegnato, a mezzo PEC all'indirizzo Aziendale forniture@pec.aspag.it, quattro distinti Piani Operativi relativi alle richieste d'ordine prodotte da questa Amministrazione e legati ai Piani dei Fabbisogni che lo scrivente ha redatto in tema di Cyber Security.

Più precisamente, i Piani Operativi prodotti dal RTI per i Presidi Ospedalieri Aziendali DEA di I livello fanno riferimento alle attività incidenti sulle UU.OO. aziendali investite dagli obiettivi PNRR Missione 6 – Ammodernamento tecnologico digitalizzazione DEA di I Livello che risultano essere i PP.OO. di Agrigento, Sciacca e Ribera. Il quarto piano operativo, invece, risponde ai fabbisogni della restante parte dell'Azienda non ricompresa nel PNRR.

Io scrivente ha operato la verifica di congruità e corrispondenza tra la "Richiesta preliminare di fornitura" e i predetti "Piani Operativi" *accertandone la correttezza formale delle quantità e qualità dei servizi offerti rispetto ai fabbisogni rilevati da questa Azienda* e tecnicamente rivalutato dal RTI aggiudicatario dell'AQ Consip ID 2296 – Sicurezza da remoto e servizi di Compliance e controllo, Lotto 1.
Relativamente ai Piani Operativi legati ai PP.OO. DEA di I livello si rileva una completa sovrapposizione economica rispetto agli importi assegnati sugli interventi legati al PNRR per come di seguito dettagliati in tabella:

Presidio	***Intervento***	***Importo***
PO Ribera	parte del 5	64.556,62 €
PO Sciacca	parte del 13	153.416,58 €
PO Agrigento	parte del 21	165.547,10 €
		383.520,31 €

Detta differenziazione ha consentito di realizzare una netta suddivisione dei progetti tra quelli finanziati con il PNRR e la restante parte da finanziare con il bilancio aziendale.

Tanto premesso e tenuto conto dei numerosi e continui rischi sulla sicurezza dovuti agli attacchi hacker che stanno costantemente mettendo a dura prova la sicurezza dei dati e dei sistemi Aziendali, si suggerisce di procedere rapidamente all'adozione degli atti necessari all'adesione all'A.Q. in esame che, peraltro, consentirebbe all'Azienda di dotarsi di sistemi di firma remota la cui necessità è ampiamente conosciuta dalla Direzione Strategica, che legge per conoscenza.

Il Referente Sistemi Informatici Aziendali
Dott. Riccardo Insalaco


SERVIZIO SANITARIO NAZIONALE REGIONE SICILIA - Azienda Sanitaria Provinciale Agrigento

PUBBLICAZIONE

Si dichiara che la presente deliberazione, a cura dell'incaricato, è stata pubblicata in forma digitale all'albo pretorio on line dell'ASP di Agrigento, ai sensi e per gli effetti dell'art. 53, comma 2, della L.R. n.30 del 03/11/93 e dell'art. 32 della Legge n. 69 del 18/06/09 e s.m.i., dal_____ al _____

L'Incaricato

_____

Il Funzionario Delegato
Il Collaboratore Amministrativo Prof.le
Sig.ra Sabrina Terrasi

Notificata al Collegio Sindacale il _____ con nota prot. n._____

DELIBERA SOGGETTA AL CONTROLLO

Dell'Assessorato Regionale della Salute ex L.R. n. 5/09 trasmessa in data _____ prot. n. _____

SI ATTESTA

Che l'Assessorato Regionale della Salute:

- Ha pronunciato **l'approvazione** con provvedimento n. _____ del _____
- Ha pronunciato **l'annullamento** con provvedimento n. _____ del _____

come da allegato.

Delibera divenuta esecutiva per decorrenza del termine previsto dall'art. 16 della L.R. n. 5/09 dal _____

DELIBERA NON SOGGETTA AL CONTROLLO

- Esecutiva ai sensi dell'art. 65 della L. R. n. 25/93, così come modificato dall'art. 53 della L.R. n. 30/93 s.m.i., per decorrenza del termine di 10 gg. di pubblicazione all'Albo, dal _____

X Immediatamente esecutiva dal 14 APR. 2023

Agrigento, lì 14 APR. 2023

Il Referente Ufficio Atti deliberativi
Il Collaboratore Amm.vo Prof.le
Sig.ra Sabrina Terrasi

Sig. DOMENICO ALAIMO
Coadiutore Amministrativo

REVOCA/ANNULLAMENTO/MODIFICA

- Revoca/annullamento in autotutela con provvedimento n. _____ del _____
- Modifica con provvedimento n. _____ del _____

Agrigento, lì

Il Referente Ufficio Atti deliberativi
Il Collaboratore Amm.vo Prof.le
Sig.ra Sabrina Terrasi