Determina nr. 531 del 26/09/2024

ADOTTATA DAL DIRETTORE S.C. GESTIONE OPERATIVA NEXTGENERATIONEU E SISTEMI INFORMATIVI AI SENSI DEL DECRETO N. 220 DEL 21.03.2024

OGGETTO: **ATTUAZIONE DEL PIANO NAZIONALE DI RIPRESA E RESILIENZA – MISSIONE 6 COMPONENT 2: AMMODERNAMENTO DEL PARCO TECNOLOGICO E DIGITALE OSPEDALIERO (DIGITALIZZAZIONE DEA): ADESIONE AD ACCORDO QUADRO CONSIP DENOMINATO CYBERSECURITY 2 - LOTTO 2 - PER LA FORNITURA DI APPARATI PER LA SICUREZZA PERIMETRALE DELLA RETE AZIENDALE (CIG AQ: 8898075BC5 - CUP: D11B22001420001)**

IL DIRETTORE S.C.

RICHIAMATO il Regolamento (UE) 2021/241 del Parlamento Europeo e del Consiglio del 12 febbraio 2021, che ha istituito il Dispositivo per la ripresa e resilienza;

RICHIAMATO il Piano Nazionale di Ripresa e Resilienza (PNRR), approvato dal Governo, trasmesso il 30 aprile alla Commissione Europea e definitivamente approvato il 13 luglio 2021, con Decisione di esecuzione del Consiglio Europeo che comprende, fra le 6 Missioni in cui è suddiviso, la Missione numero 6, dedicata alla Salute;

PREMESSO che, la D.G.R. 23 maggio 2022, n. XI/6426 ad oggetto "Piano Nazionale di Ripresa e Resilienza PNRR - missione 6 component 1 e component 2 e PNC – approvazione del piano operativo regionale (POR) e contestuale individuazione degli interventi, con ripartizione delle corrispondenti quote di finanziamento PNRR/PNC - individuazione dei soggetti attuatori esterni", tra l'altro:

- determina quali Soggetti attuatori esterni, per l'esecuzione degli interventi, ai sensi dell'art.5, comma 2 del CIS, gli Enti del Servizio Sanitario Regionale, ATS, ASST ed IRCCS, rinviando a successivo provvedimento la delega puntuale delle attività elencate all'art. 5 c.1 del CIS;
- suddivide le quote di finanziamento a carico di PNRR e PNC;
- dettaglia i cronoprogrammi di attuazione e lo scadenziario Milestone & Target;

PREMESSO che, nell'ambito dei finanziamenti PNRR della Missione 6 Cap. 2 – 1.1.1. "Ammodernamento del parco tecnologico e digitale ospedaliero (Digitalizzazione delle strutture ospedaliere DEA di livello I e II)" con delibera D.G. n. 673 del 16/09/2022, la scrivente ASST ha preso atto dell'approvazione del progetto di trasformazione digitale dei processi clinici sanitari proposto a Regione Lombardia, trasmesso al Ministero della Salute attraverso l'apposito portale AGENAS e inserito nel Piano Operativo Regionale (D.G.R. n.XI/6426 del 23/05/2022);

PREMESSO che, con decreto della D.G.W. n. 11264 del 28/07/2022, Regione Lombardia ha formalmente assegnato all'Azienda un finanziamento pari a € 5.300.000,00 per la trasformazione digitale;

DATO ATTO che l'Allegato 2 al POR adottato con la suddetta D.G.R, per l'ASST del Garda prevede, tra gli altri, i seguenti interventi:

CUP	Titolo Progetto	Presidio Ospedaliero	DEA di I o II livello	Importo Intervento PNRR
D11B22001440001	Ammodernamento del parco tecnologico e digitale ospedaliero (digitalizzazione delle strutture ospedaliere – DEA I e II) MANERBIO	030184 - PO Manerbio	DEA I	€ 1.840.000,00
D11B22001420001	Ammodernamento del parco tecnologico e digitale ospedaliero (digitalizzazione delle strutture ospedaliere – DEA I e II) DESENZANO	030156 - PO Desenzano del Garda	DEA I	€ 3.460.000,00

CONSIDERATO che, con decreto n. 74 del 01/02/2024, è stata temporaneamente nominata R.U.P. dei predetti due interventi PNRR per i presidi di Manerbio e Desenzano l'Ing. Marta Carubelli, Direttore S.C. Gestione Operativa Nextgenerationeu e Sistemi Infomativi;

DATO ATTO che, tale progetto include, tra i diversi interventi, anche il potenziamento della sicurezza informatica, attraverso il rafforzamento del sistema di controllo perimetrale IDS/IPS, l'ASST del Garda si pone l'obbiettivo inderogabile di innalzare i propri standard di sicurezza informatica adeguandosi alle attuali norme. In particolare, si prevede di elevare lo standard di sicurezza legato alle VPN SSL e tunnel IPSEC, protezione IOT dei dispositivi medicali, sistema HIP, PAM, log administrators;

CONSIDERATO inoltre che, la fornitura in oggetto si inserisce nel contesto della sicurezza informatica aziendale più precisamente nella protezione perimetrale aziendale e messa in sicurezza delle connessioni remote;

EVIDENZIATA, pertanto, la necessità di acquisire n.2 nuovi firewall (comprensivi di servizio specialistico di supporto e manutenzione) come di seguito indicato in tabella:

Descrizione	**Quantità [nr.]**
Fornitura in opera NGFW-F3-PA-PAN-PA-3420-CONSIP-BUN-F3	2
Manutenzione annuale HP Next Generation Firewall Fascia 3	2
Servizio di supporto specialistico - Security Principal - fascia standard	8
Servizio di supporto specialistico - Security Principal - fascia straordinaria	1

SOTTOLINEATO che i predetti due nuovi "Next Generation Firewall" consentirebbero l'ispezione dei pacchetti di rete a differenza dei firewall "tradizionali". Non si occuperebbero solamente di analizzare e filtrare i pacchetti dati sulla base della porta e/o protocollo ma permetterebbero di eseguire l'ispezione a livello applicativo, fornendo inoltre funzionalità di prevenzione dalle intrusioni, analisi e rilevamento dei malware e capacità di utilizzo di sorgenti esterne a supporto dell'attività di protezione aziendale;

PRESO ATTO delle linee guida regionali in materia di acquisti di beni e servizi, confermate e ribadite, da ultimo, nella D.G.R. 1827/2024 – cosiddette "Regole di Sistema 2024" e la normativa nazionale in materia di contenimento della spesa, prevedono per gli Enti Sanitari l'obbligo di verificare la possibilità di adesione alle Convenzioni stipulate da CONSIP S.p.A. e/o dalle Centrali Regionali di Committenza, per Regione Lombardia ARIA S.p.A.;

CONSIDERATO che, l'obbligo di approvvigionarsi attraverso le Convenzioni stipulate da CONSIP S.p.A., ovvero dalle centrali di committenza regionali, è stato ribadito dall'art. 510 della Legge 208/2015;

DATO atto che nessuna convenzione ARIA risulta attualmente attivata per quanto in argomento;

PRESO ATTO che, per quanto in oggetto, risulta ad oggi attivo l'Accordo Quadro CONSIP denominato "CYBERSECURITY 2 - LOTTO 2" (CIG AQ: 8898075BC5) con affidataria la RTI TELECOM ITALIA S.p.A. - MATICMIND SPA - DGS SPA - SCAI SOLUTION GROUP S.p.A.;

VERIFICATO che è stata inviata, tramite portale "Acquistinretepa" di CONSIP, alla predetta RTI TELECOM ITALIA S.p.A. - MATICMIND S.p.A. - DGS S.p.A. - SCAI SOLUTION GROUP S.p.A. apposita procedura d'acquisto nr. 749871 contenente la "richiesta preliminare di fornitura" per quanto inserito nella suindicata tabella, secondo i format previsti dall'iter di adesione;

PERVENUTO a quest'Azienda, tramite nota a prot. ASST del Garda n. 40769/2024 del 27/08/2024, da parte della suddetta RTI TELECOM ITALIA S.p.A. - MATICMIND S.p.A. - DGS S.p.A. - SCAI SOLUTION GROUP S.p.A., il "Piano Operativo" nel quale viene quantificato il costo complessivo

inerente i prodotti e i servizi richiesti nella predetta tabella in € 35.387,04 (IVA esclusa) come da Allegato 1 al presente provvedimento a formarne parte integrante e sostanziale, composto da n. 10 pagine;

EVIDENZIATA l'esigenza di procedere con l'affidamento di quanto indicato in tabella alla RTI TELECOM ITALIA S.p.A. - MATICMIND S.p.A. - DGS S.p.A. - SCAI SOLUTION GROUP S.p.A. in regime di adesione ad Accordo Quadro CONSIP denominato "Cybersecurity 2 - Lotto 2" (CIG AQ: 8898075BC5) approvando il predetto "Piano Operativo" e prevedendo un impegno di spesa di € 43.172,18 (IVA inclusa) come di seguito dettagliato:

Descrizione	**Q.tà**	**Costo unit. (IVA esclusa)**	**Costo totale (IVA esclusa)**	**Costo totale (IVA inclusa)**
Fornitura in opera NGFW-F3-PA-PAN-PA-3420-CONSIP-BUN-F3	2	€ 15.062,48	€ 30.124,96	€ 36.752,45
Manutenzione annuale HP Next Generation Firewall Fascia 3	2	€ 1.205,04	€ 2.410,08	€ 2.940,29
Servizio di supporto specialistico - Security Principal - fascia standard	8	€ 310,00	€ 2.480,00	€ 3.025,60
Servizio di supporto specialistico - Security Principal - fascia straordinaria	1	€ 372,00	€ 372,00	€ 453,84
Totale fornitura			€ 35.387,04	**€ 43.172,18**

DATO atto che il presente provvedimento, in parte finanziato dall'Unione Europea – Next Generation EU mediante i fondi PNRR destinati alla "Missione 6 - Componente 2 - Investimento 1.1: Ammodernamento del parco tecnologico e digitale ospedaliero – Sub investimento 1.1.1. (Digitalizzazione DEA I e II livello)", viene emanato nel rispetto di quanto stabilito dalla disciplina nell'ambito del PNRR, ed in particolare:

- sulle condizioni da adottare al fine di non arrecare un danno significativo agli obiettivi ambientali, ai sensi dell'art. 17 del Regolamento UE 852/2020, in coerenza con i principi e gli obblighi relativamente al principio del "Do No Significant Harm" (DNSH) e, ove applicabili;
- sul principio degli obiettivi climatici e di trasformazione digitale (c.d. tagging ambientale e digitale), ai sensi di quanto disposto dall'art. 18, paragrafo 4, lettere e) e f) del Regolamento (UE) n. 241/2021 e dagli allegati VI e VII del Regolamento (UE) n. 241/2021;
- nel rispetto del principio di addizionalità del sostegno dell'Unione Europea previsto dall'art. 9 del Regolamento (UE) n. 241/2021, in conformità con quanto indicato dalla circolare del MEF n. 33 del 31 dicembre 2021, recante chiarimenti in merito a "Addizionalità, finanziamento complementare e obbligo di assenza del c.d. doppio finanziamento", attestando in particolare che il medesimo costo del suddetto intervento non è stato rimborsato due volte a valere su fonti di finanziamento pubbliche, anche di natura diversa, in conformità al Piano Operativo Regionale (POR) di cui alla D.G.R. XI/6426 del 23 maggio 2022 e successive modifiche, integrazioni e rimodulazioni;
- nel rispetto del principio di sana gestione finanziaria secondo quanto disciplinato nel Regolamento finanziario (UE, Euratom) n. 1046/2018 e nell'art. 22 del Regolamento (UE) n. 241/2021, in particolare in materia di prevenzione dei conflitti di interessi, delle frodi, della corruzione e di recupero e restituzione di fondi indebitamente assegnati. Sono, altresì, acquisite ed archiviate le autodichiarazioni attestanti l'assenza del conflitto di interessi rilasciate ai sensi del D.P.R. n. 445/2000 da parte di tutti i soggetti, sia interni che esterni, direttamente coinvolti

nell'attuazione del progetto, assoggettate ai controlli previsti dalla nota integrativa alla Direttiva Operativa MDS-UMPNRR-08- 15/06/2022, del 6 ottobre 2022;
- nel rispetto del principio delle pari opportunità in materia di non discriminazione, trasparenza, proporzionalità, pubblicità, uguaglianza di genere (Gender Equality), tutela dei diversamente abili;

DATO ATTO che, pur non riportando i riferimenti espliciti per quanto attiene il richiamo normativo contenuto nella circolare REGIS: "recante istruzioni tecniche per la redazione dei sistemi di gestione e controllo delle amministrazioni centrali titolari di interventi del PNRR", l'Amministrazione ha formalmente individuato i soggetti deputati ai controlli di primo livello con nota protocollo n. 30927 del 24/07/2023;

DATO ATTO che, la documentazione istruttoria è conservata agli atti presso la S.C. Gestione Operativa Nextgenerationeu e Sistemi Informativi dell'ASST del Garda;

VISTA l'istruttoria compiuta dal Responsabile del procedimento, Ing. Marta Carubelli, che ai sensi del Capo II della Legge 7 agosto 1990 n. 241 e successive modificazioni e integrazioni, ne attesta la completezza;

VISTA l'attestazione del Direttore S.C. Bilancio e Rendicontazione in ordine alla regolarità contabile;

DETERMINA

Per i motivi in premessa indicati:

1. di aderire all'Accordo Quadro CONSIP denominato "Cybersecurity 2 - Lotto 2" (CIG AQ: 8898075BC5);

2. di approvare il "Piano Operativo" (Allegato 1, composto da n. 10 pagine) recepito con nota a prot. ASST del Garda n. 40769/2024 del 27/08/2024 e di procedere all'acquisto di quanto in oggetto per un importo di € 43.172,18 (iva inclusa);

3. di affidare al RTI TELECOM ITALIA S.p.A. - MATICMIND S.p.A. - DGS S.p.A. - SCAI SOLUTION GROUP S.p.A., quale aggiudicatario dell'AQ, la fornitura di quanto in oggetto alle condizioni contenute nel citato Accordo Quadro, così come pubblicato nel portale CONSIP "Acquistinretepa", per un importo complessivo di € 43.172,18 (IVA inclusa) e di procedere a relativo OdA (Ordine di Acquisto);

4. di precisare che l'Allegato 1 è parte integrante e sostanziale del presente provvedimento, composto da n. 10 pagine;

5. di nominare Direttore dell'Esecuzione del Contratto, ai sensi del comma 1 dell'art. 114, del D. Lgs. n. 36/2023, Paolo Sartorelli cui demandare, congiuntamente al R.U.P., le attività individuate nel citato articolo;

6. di dare atto che, l'acquisizione in argomento è in parte finanziata dall'Unione Europea – Next Generation EU mediante i fondi PNRR destinati alla "Missione 6 - Componente 2 - Investimento 1.1: Ammodernamento del parco tecnologico e digitale ospedaliero – Sub investimento 1.1.1. (Digitalizzazione DEA I e II livello)";

7. di dare atto che l'onere di spesa derivante dal presente provvedimento, qui quantificato in € 43.172,18 IVA Inclusa, verrà registrato nella contabilità aziendale come di seguito indicato:

   - PNRR € 41.702,04 IVA Inclusa anno 2025 con imputazione al conto _____ e sarà gestito con il codice _____;
   - AREA OSPEDALIERA € 1.470,14 IVA inclusa anno 2026 con imputazione al conto "manutenzione assicurativa impianti" e sarà gestito con il codice 1320040002/INF/_____;

8. di dare mandato alla S.C. Gestione Operativa Nextgenerationeu e Sistemi Informativi per la comunicazione del presente provvedimento a tutti i Servizi e/o Strutture aziendali interessate, per i successivi adempimenti di competenza;

9. di incaricare l'Ufficio Inventario Beni Mobili, in conformità al Titolo V° della L.R. 31/12/1980 n. 106 e s.m.i., dell'iscrizione nell'inventario generale dei beni immobili di questa ASST delle acquisizioni oggetto del presente provvedimento, dando atto che il costo è finanziato con le somme assegnate nell'ambito del PNRR e che, pertanto, si provvederà alla sterilizzazione della relativa quota di ammortamento;

10. di dare atto che il presente provvedimento è sottoposto al controllo del Collegio Sindacale, in conformità ai contenuti dell'art. 3-ter del D.Lgs. n. 502/1992 e ss.mm.ii. e dell'art. 12, comma 14, della L.R. 33/2009;

11. di disporre, a cura della S.C. Affari Generali e Legali, la pubblicazione all'Albo pretorio on-line dell'ASST del Garda– ai sensi dell'art. 17, comma 6, della L.R. n. 33/2009, e dell'art. 32 della L. n. 69/2009, ed in conformità alle disposizioni ed ai provvedimenti nazionali e comunitari in materia di protezione dei dati personali.

Firmata digitalmente
IL DIRETTORE S.C.
GESTIONE OPERATIVA NEXTGENERATIONEU E SISTEMI INFORMATIVI
(Ing. Marta Carubelli)

PIANO OPERATIVO PER L'AFFIDAMENTO DI PRODOTTI PER LA SICUREZZA PERIMETRALE, PROTEZIONE DEGLI ENDPOINT E ANTI-APT

LOTTO 2

ASST DEL GARDA

Tabella Revisioni

Revisione	Descrizione modifiche	Data
1.0	Prima emissione	26/08/2024

Indice

1. INTRODUZIONE

1.1 PREMESSA

Il presente documento descrive il Piano Operativo TIM, relativamente alla richiesta di fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt per il ASST DEL GARDA, in conformità alle richieste espresse dall'Amministrazione nel Piano dei Fabbisogni (identificato dal codice: RPO 8023181 – Richiesta Piano Operativo/Ordine 8023181).

Con questo progetto il Cliente intende acquisire:

- Next Generation Firewall
- Servizi di supporto specialistico

1.2 SCOPO

Lo scopo del documento è quello di formulare una proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nell'Accordo Quadro ed in risposta al Piano dei Fabbisogni inviato dal cliente.

1.3 RIFERIMENTI

Identificativo
Piano dei Fabbisogni – ASST DEL GARDA – Richiesta Piano Operativo/Ordine 8023181
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT – Lotti 1,2,3 - Capitolato Tecnico Speciale
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT – Lotti 1,2,3 - Capitolato Tecnico Generale
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT – Lotti 1,2,3 - Capitolato d'oneri
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT –- Offerta Tecnica Lotto Lotti 1,2,3

1.4 ACRONIMI E GLOSSARIO

Definizione / Acronimo	Descrizione
AgID	Agenzia per l'Italia Digitale
Consip	Consip S.p.a.
RTI	Raggruppamento Temporaneo d'Impresa

2. ORGANIZZAZIONE DEL CONTRATTO ESECUTIVO

Per il coordinamento delle attività contrattuali previste il RTI impiegherà i referenti di seguito indicati:

- **Responsabile Unico della Attività Contrattuali dell'Accordo Quadro (RUAC-AQ)**, che dovrà riferire, per quanto di competenza, a Consip/Organismo Tecnico di Coordinamento e Controllo, ove richiesto, su tutte le tematiche contrattuali relative all'Accordo Quadro:

  Loredana Ferraiuolo – loredana.ferraiuolo@telecomitalia.it

- **Responsabile dell'Amministrazione**, identificato nel "Piano dei Fabbisogni":

  Marta Carubelli- informatica.aziendale@asst-garda.it

- **Responsabile del Fornitore** (cfr. par. 2.4.1.2 del Capitolato Tecnico Generale), che riferirà, per quanto di competenza, all'Amministrazione su tutte le tematiche contrattuali relative al Contratto Esecutivo:

  Roberto Telloni - roberto.telloni@telecomitalia.it

- **Referente Tecnico per l'erogazione dei servizi**, che dovrà garantire il corretto svolgimento delle attività e dei servizi ed il relativo livello di qualità di erogazione nel rispetto dei KPI previsti dal Capitolato Tecnico – Parte speciale (cfr. capitolo 5):

  Carlo Omini – carlo.omini@telecomitalia.it

2.1 CATEGORIZZAZIONE DEGLI INTERVENTI

In relazione al Piano Triennale per l'Informatica delle Pubbliche Amministrazioni, di seguito si riporta "l'inquadramento o categorizzazione" degli interventi che l'Amministrazione intende realizzare.

Ambito (layer)	Obiettivi Piano Triennale
□ Servizi	□ Servizi al cittadino
	□ Servizi a imprese e professionisti
	x Servizi interni alla propria PA
	□ Servizi verso altre PA
□ Dati	□ Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese
	□ Aumentare la qualità dei dati e dei metadati
	□ Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati
□ Piattaforme	□ Favorire l'evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l'azione amministrativa

	□ Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle PA
	□ Incrementare e razionalizzare il numero di piattaforme per le amministrazioni
□ Infrastrutture	□ Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni locali favorendone l'aggregazione e la migrazione sul territorio (Riduzione Data Center sul territorio)
	□ Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni centrali favorendone l'aggregazione e la migrazione su infrastrutture sicure ed affidabili (Migrazione infrastrutture interne verso il paradigma cloud)
	□ Migliorare la fruizione dei servizi digitali per cittadini ed imprese tramite il potenziamento della connettività per le PA
□ Interoperabilità	□ Favorire l'applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API
	□ Adottare API conformi al Modello di Interoperabilità
□ Sicurezza Informatica	x Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA
	□ Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione

3. PROGETTO DI ATTUAZIONE

Il progetto di attuazione come da richieste del cliente prevede l'installazione di 2 'PAN-PA-3420- CONSIPBUN-F nella sede centrale.

Le attività verranno eseguite come da piano di Lavoro descritto nel paragrafo 7.

4. PRODOTTI RICHIESTI

PRODOTTI	BRAND	FASCIA	MODELLO	CODICE ARTICOLO PRODUTTORE	N.
NGFW - Fascia 3	Palo alto	3	NGFW-F3-PA	'PAN-PA-3420- CONSIPBUN-F	2

CODICE ARTICOLI PRODUTTORE.docx

Nel seguente paragrafo è riportata la descrizione tecnica dei prodotti forniti.

4.1 NEXT GENERATION FIREWALL

I "Next Generation Firewall" sono apparati che consentono l'ispezione dei pacchetti di rete e si differenziano dai firewall "tradizionali" in quanto non si occupano solamente di analizzare e filtrare i pacchetti dati sulla base della porta e/o protocollo ma consentono di eseguire l'ispezione a livello applicativo, fornendo inoltre funzionalità di prevenzione dalle intrusioni, analisi e rilevamento dei malware e capacità di utilizzo di sorgenti esterne a supporto della propria attività di protezione. Nell'Accordo quadro sono previste sei fasce dimensionali e 4 Vendor, per i quali di seguito alleghiamo le specifiche tecniche delle soluzioni proposte.

PALOALTO NGFW.docx

5.SERVIZIO DI SUPPORTO SPECIALISTICO

Il servizio di Supporto Specialistico consente alle Amministrazioni Contraenti di richiedere del personale specializzato con l'obiettivo di essere supportata in varie attività inerenti sia la fornitura specifica acquistata in AQ sia, in maniera più generale, la propria infrastruttura di sicurezza informatica. Il servizio riguarderà esclusivamente le attività riportate nel seguito:

- l'effettuazione, nelle fasi successive all'implementazione dei prodotti, di attività di analisi specifiche che consentano di stabilire le policy di sicurezza maggiormente adeguate da implementare nel complesso dei sistemi dell'Amministrazione

Di seguito si riporta quanto richiesto dal cliente nel Piano dei fabbisogni:

Servizio Supporto Specialistico			
Fascia di acquisizione	Codice Servizio	Codice Fornitore	Quantità (gg/uomo)
Security Principal - fascia standard	SP-STA	SEC_PRINC_STD	**8**
Security Principal - fascia straordinaria	SP-STR	SEC_PRINC_STR	**1**

Per le competenze che ciascuna risorsa specialistica deve possedere si rimanda a quanto previsto nell'allegato 2 – Capitolato Tecnico – Parte Speciale (paragrafo 3.2.4), e come di seguito riportate:

Security Principal: in possesso della certificazione ISACA CISM (Certified Information Security Manager)

Durante le giornate uomo sopra indicate saranno svolte le attività di supporto specialistico in base alle esigenze del CLIENTE e comunque in funzione della fornitura prodotti richiesta tramite questo piano. Qualsiasi altra necessità sarà valutata di volta in volta in accordo con il cliente.

6. SERVZIO DI MANUTENZIONE

La manutenzione comprende le attività volte a garantire una pronta correzione dei malfunzionamenti e il ripristino delle funzionalità, anche attraverso attività di supporto on-site.
Il servizio manutenzione prevede 2 profili di qualità, *Low Profile* (*Business Day*) o *High Profile* (*H24*),
Il servizio di manutenzione è offerto per annualità, quindi per 12 mesi o massimo 24 mesi.
Può essere fornita anche con un accesso remoto sicuro (utilizzando account VPN personali configurati e abilitati opportunamente, con tracciatura degli accessi per eventuali successivi audit, accessi che comunque dovranno essere limitati al tempo strettamente necessario all'esecuzione dell'attività, ad esempio mediante utenze token create all'occorrenza) a supporto delle stesse (ad. es. effettuazione di diagnosi attraverso i propri sistemi di gestione e di management per analisi di problematiche e malfunzionamenti segnalati dall'Amministrazione).
Le attività di manutenzione sono previste per i soli elementi di fornitura acquistati nell'ambito del presente AQ.

Le attività di manutenzione possono riassumersi in:

- ricezione della chiamata di assistenza da parte dell'Amministrazione e assegnazione del Severity Code
- risoluzione del problema tramite supporto telefonico all'utente (ove possibile) e/o eventuale intervento/i remoto/i;
- risoluzione della causa del guasto tramite, ove necessario:
- intervento presso la sede/luogo interessato

- ripristino del servizio/funzionalità sui livelli preesistenti al guasto/anomalia, secondo gli SLA contrattualizzati, anche attraverso sostituzioni di elementi danneggiati o verifica funzionale del sistema per assicurare l'eliminazione della causa del guasto.

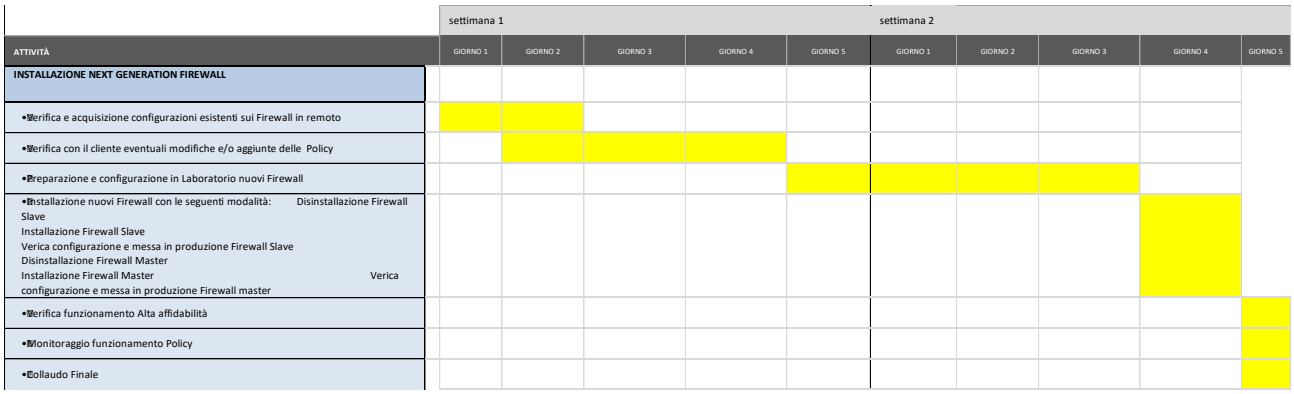
7. PIANO DI LAVORO

Al fine della corretta implementazione ed inizializzazione del servizio proposto, saranno necessarie le seguenti fasi operative:

INSTALLAZIONE NEXT GENERATION FIREWALL PALO ALTO SEDE CENTRALE

- Verifica e acquisizione configurazioni esistenti sui Firewall (da remoto)
- Verifica con il cliente di eventuali bonifica\creazione delle policy di sicurezza
- Installazione nuovo Firewall con le seguenti modalità:
  - Verifica configurazione e messa in produzione in area pilota Firewall
  - Verifica configurazione e rilascio in produzione Firewall sede centrale
- Verifica funzionamento
- Collaudo Finale e GO LIVE

7.1 GANTT



7.2 PIANO DI PRESA IN CARICO

L'attività di presa in carico del sistema consiste nell'acquisire tutte le informazioni che sono necessarie all'erogazione dei servizi e di quanto indicato nel sopra riportato piano di lavoro, con l'obiettivo di acquisire know how relativo al contesto organizzativo, tecnologico e funzionale dell'Amministrazione oltre a standard, modalità operative, linee guida, ove presenti.
Come specificato da piano dei fabbisogni l'amministrazione contraente fornirà la configurazione esistente degli apparati al fine di permettere la corretta sostituzione e implementazione delle regole di sicurezza attualmente in esercizio
L'attività potrà consistere, ad esempio, in riunioni di lavoro, rilevazione delle configurazioni in essere sui vari sistemi, esame della documentazione esistente (es. schemi logici e di low level design dell'infrastruttura di rete, informative sulle connettività presenti, piani di indirizzamento etc) con assistenza di personale esperto e affiancamento condotta con eventuali ulteriori fornitori dell'amministrazione contraente.
Se previsto e/o richiesto dall'amministrazione contraente saranno altresì forniti i dettagli necessari (es. tools IT Management) alla corretta implementazione dei processi di Incident, Change e Deploy Management richiesta per l'espletamento dei servizi descritti nei successivi paragrafi.
Si noti che qualora la documentazione disponibile risultasse non aggiornata e/o incompleta, tutto ciò dovrà risultare in modo dettagliato in un verbale attestante il completamento del piano di

presa in carico.
Durante le attività di Presa in carico si dovrà garantire:

- la presenza di tutte le figure coinvolte per l'erogazione dei servizi nonché dovranno essere reperibili e disponibili i Referenti Tecnici;
- la predisposizione di un verbale attestante il completamento della presa in carico da redigere secondo le indicazioni fornite dall'Amministrazione e che dovrà essere sottoscritto dal RTI e dall'Amministrazione.

SPECIFICHE DI COLLAUDO

Per ciascun elemento che compone le macroaree di progetto, verranno effettuate prove di esercibilità e test funzionali secondo il piano di seguito riportato. Le date di collaudo potranno essere definite in accordo al piano riportato al paragrafo precedente.

- Verifica funzionalità di base degli apparati
- Verifica funzionamento Alta affidabilità
- Monitoraggio funzionamento Policy

Per ciascun elemento che compone le macroaree di progetto, verranno effettuate prove di esercibilità e test funzionali secondo il piano di seguito riportato. Le date di collaudo potranno essere definite in accordo al piano riportato al paragrafo precedente.
Per il servizio di NGF saranno eseguite le seguenti attività di verifica e test da affinare in sede del cliente.

Tipologia	Descrizione
Test Funzionale	Verifica che i dispositivi funzionino come previste siano in grado di eseguire le funzionalità base come la prevenzione dell'intrusione, la verifica delle autorizzazione agli accessi, delle politiche di sicurezza
Test di sicurezza	Verificare la capacità dei dispositivi di rilevare e prevenire possibili compromissioni e attacchi all'infrastruttura IT. Questi test possono includere simulazioni in ambiente controllato, test di identificazione e blocco di Virus e malware
Test di compatibilità	Questi tipi di test verificano la capacità dei dispositivi di funzionare correttamente con gli altri componenti dell'infrastruttura IT

8. TABELLA RIEPILOGATIVA

Codice Articolo Convenzione	Quantità	Durata	Prezzo Totale
CS2L2-NGFW-F3-PA	2		30.124,96 €
CS2L2-MANHP-NGFW-F3-PA	2	24	2.410,08 €
CS2L2-SP-STA	8		2.480,00 €
CS2L2-SP-STR	1		372,00
		Tot	**35.387,04 €**

9. PRESTAZIONEI DI SUBAPPALTO

Nell'ambito dell'Accordo Quadro Cybersecurity 2 per le prestazioni erogate in subappalto è previsto quanto segue:

- Quota massima del subappalto: 50%
- Servizi per i quali è prevista la prestazione in subappalto:
  - Formazione;
  - Hardening;
  - Supporto Specialistico.
  - Manutenzione

Nella tabella sottostante è necessario riportare la quota, le prestazioni e il nome delle aziende che erogheranno i servizi in subappalto, nel rispetto di quanto indicato nel Piano dei fabbisogni:

Servizi	Quota subappalto	Azienda del RTI che eroga il servizio	Nome dell'azienda che eroga la prestazione in subappalto
Supporto specialistico e Manutenzione	15%	TIM	LANTECHLONGWAVE