

ID AQ 2367

## PIANO DEI FABBISOGNI SERVIZI

Spett.le  
TELECOM ITALIA S.p.A.

Lo scrivente A.O. Ordine Mauriziano, C.F. / P.IVA 09059340019

Codice IPA asoom\_to Codice Univoco Ufficio: UFHCOM

con sede legale in Torino, Prov. TO Nazione Italia

Indirizzo Via Magellano, 1

chiede che venga realizzato quanto di seguito indicato (barrare i servizi richiesti con il presente piano dei fabbisogni):

<input type="checkbox"/> <b>EDP/EPR</b> (compilare il Quadro A)	<input type="checkbox"/> <b>NAC</b> (compilare il Quadro B)
<input checked="" type="checkbox"/> <b>NGFW</b> (compilare il Quadro C)	<input type="checkbox"/> <b>ANTI - APT</b> (Compilare il Quadro D)
<input type="checkbox"/> <b>Server Protection</b> (compilare il Quadro E)	<input type="checkbox"/> <b>Servizio di Hardening</b> (compilare il Quadro F)
<input type="checkbox"/> <b>Servizio di Formazione</b> (compilare il Quadro G)	<input checked="" type="checkbox"/> <b>Servizio di Supporto Specialistico</b> (compilare il Quadro H)
<input checked="" type="checkbox"/> <b>Servizio di di Manutenzione</b> (compilare il Quadro I)	

### Invio delle fatture

**Codice Univoco Ufficio:**

**CIG** (quando disponibile):

**NSO** (quando disponibile):

**CUP:** G16G22000070005

### Domicilio fattura:

Località Torino Prov. TO CAP 10128 Nazione Italia

Indirizzo Via Magellano n. 1

### Responsabile dell'Amministrazione per i rapporti con TELECOM ITALIA

Nome Silvia Cognome Torrenco

Telefono 011 5082241- 335 7068310 Fax \_\_\_\_\_

E-mail storrenco@mauriziano.it

DATA

TIMBRO E FIRMA DEL CLIENTE



## **Descrizione del Contesto di Riferimento in cui si riferisce la fornitura dell'Amministrazione**

I device IoMT (Internet of Medical Things ovvero dispositivi medici connessi) sono essenziali per le organizzazioni sanitarie perché svolgono e aiutano a ottimizzare varie funzioni essenziali per la cura del paziente.

Tali dispositivi spesso non sono progettati pensando alla sicurezza, il che li rende particolarmente vulnerabili alle minacce informatiche. A questo va aggiunto che la compromissione di dispositivi IoMT può avere conseguenze più disastrose rispetto a qualsiasi altro sistema cyber-fisico, perché i dispositivi IoMT comportano rischi e pericoli per la sicurezza stessa del paziente.

Per tale motivo è necessaria un'adeguata soluzione di sicurezza cyber-fisica, perché potendo contare sulla visibilità e sulla protezione del dispositivo, l'organizzazione sanitaria può mitigare in modo proattivo i rischi e le vulnerabilità sfruttabili e impedire ai criminali informatici di eseguire una serie di azioni dannose, con conseguenze che vanno dall'ottenimento di informazioni sensibili sui pazienti (ad esempio dati sanitari, personali) ad attacchi ransomware.

Il primo passo per proteggere l'ecosistema IoMT è quello che concerne il rilevamento dei dispositivi che consente alle organizzazioni di capire come e quali dispositivi comunicano attraverso la rete e fornisce visibilità a livello aziendale, permettendo di implementare controlli granulari durante i passaggi successivi.

Tracciando in tempo reale tutto ciò che è fisico e virtuale durante il percorso del paziente, le organizzazioni sanitarie possono iniziare a proteggere il proprio ecosistema da attacchi informatici e tempi di inattività e garantire un'erogazione ottimale dell'assistenza ai pazienti.

Una volta che tutti i dispositivi sono stati individuati e catalogati all'interno di un inventario centralizzato in tempo reale, per costruire una solida sicurezza IoMT occorre valutare quali vulnerabilità sono presenti all'interno di tali dispositivi e nell'ambiente ad essi correlato e quindi intraprendere un percorso ottimale per la correzione dei rischi.

## **Macro Requisiti ed Obiettivi che l'Amministrazione si propone con la fornitura**

Innalzare il livello di sicurezza dei dispositivi IOMT: in particolare si intende censire tutti i dispositivi medicali e non, connessi in rete verificandone le vulnerabilità.

**Indicazione se il contratto esecutivo è finanziato, in tutto o in parte, con le risorse previste dal Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021 e dal Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, nonché dal PNC**

Il contratto è interamente finanziato dal PNRR all'interno del progetto CUP G16G22000070005.

**Tempistiche richieste per la realizzazione della fornitura, con descrizione di eventuali vincoli e/o criticità**

Il nuovo sistema dovrà essere messo in produzione entro il 31/03/2025 e il collaudo entro il 30/4/2025.

**Indicazione del/i luogo/ghi di interesse della fornitura**

A.O. Ordine Mauriziano  
S.C. Sistemi Informativi  
Via Magellano 1  
10128 Torino (TO)

**Durata del Contratto Esecutivo**

24 mesi

**Informazioni tecniche quali schemi di rete, piani di indirizzamento, apparati già in essere, utili a meglio comprendere il perimetro di interesse e indirizzare la migliore soluzione tecnologica, specificare:**

**Alloggiamento ed eventuale fissaggio sullo specifico supporto che sarà messo a disposizione dall'Amministrazione (rack, ripiano, ...) in relazione alla tipologia apparato.**

**Indicazione del/i luogo/ghi di interesse della fornitura**

Collocato su Rack 12-0 presso la sala CED dell'A.O. Ordine Mauriziano, I° piano.  
In merito all'indirizzamento di rete il sistema dovrà rimanere in ascolto di tutte le VLAN su Span Port collegata in fibra.

**Collegamento alla rete di alimentazione, presso il punto di presenza della rete indicato dall'Amministrazione.**

**Indicazione del/i luogo/ghi di interesse della fornitura**

Presso la sala CED dell'A.O. Ordine Mauriziano, I° piano.

**Collegamento alla rete dati, presso il punto di presenza della rete indicato dall'Amministrazione.**

Collegamento in fibra a 1 GB presso la sala CED

**Se prodotto hardware non è acquistato in sostituzione di un prodotto già presente l'amministrazione dovrà indicare i prerequisiti necessari all'installazione e configurazione :**

1. **schemi logici dell'architettura:** collegamento in fibra su Span Port dello switch Centro Stella per monitoraggio di tutto il traffico
2. **schemi di indirizzamento:** Per il management dell'apparato sarà assegnata la classe di indirizzamento 192.168.39.128/29
3. **requisiti delle policy di sicurezza stabiliti dall'Amministrazione:** il sistema dovrà essere configurato rispettando le best practices di settore nell'ambito della cyber sicurezza. In particolare dovranno essere garantiti accessi protetti da password e sistemi MFA e dovrà essere possibile limitare le comunicazioni verso l'esterno alle sole destinazioni "sicure".

**Se il prodotto hardware è acquistato in sostituzione di un prodotto già presente presso l'Amministrazione oltre agli schemi logici e di indirizzamento indicare le impostazioni/policy/configurazioni attive e attualmente in esercizio**

Il prodotto non è in sostituzione di altri prodotti già presenti presso la nostra Azienda

**Se il prodotto software è acquistato in sostituzione di un prodotto software già presente presso l'Amministrazione indicare il tipo di prodotto attualmente utilizzato e se è un prodotto SaaS o On premise. La migrazione di un prodotto che sia SaaS oppure On premise necessita di un supporto di servizi professionali.**

Il prodotto non è in sostituzione di altri prodotti già presenti presso la nostra Azienda

**Se il prodotto software non è acquistato in sostituzione di un prodotto software già presente presso l'Amministrazione indicare la tipologia dei Client/Server sui quali dovrà essere installato il software.**

L'accesso al software dovrà essere via browser

**Le installazioni di prodotti software richiedono la configurazione del software di management sia per la componente Client (EPP) che Server (SPP). L'amministrazione dovrà mettere a disposizione ambienti virtuali o fisici**

I servizi EPP e SPP non sono richiesti. L'Azienda non metterà a disposizione ambienti virtuali o fisici, in quanto gli eventuali software dovranno essere ospitati su apparati fornito o in ambiente cloud

**Ulteriori informazioni che l'Amministrazione ritieni utili per lo svolgimento dell'attività del fornitore**

Si prevede un numero indicativo di circa 3.700 dispositivi connessi in rete, di cui circa 400 IOMT

## QUADRO A - EDP/EPR

### Descrizione del Servizio

Una soluzione EPP/EDR consente di proteggere gli endpoint di tipo client da minacce quali virus, trojan, worm, etc, bloccando le attività di applicazioni che risultano potenzialmente dannose, fornendo inoltre funzionalità utili all'investigazione e al ripristino in seguito a violazioni di sicurezza.

Per l'EPP/EDR sono previste quattro fasce dimensionali:

- EPP\_EDR\_1 (fascia 1): fino a 500 client
- EPP\_EDR\_2 (fascia 2): fino a 1000 client
- EPP\_EDR\_3 (fascia 3): fino a 5000 client
- EPP\_EDR\_4 (fascia 4): oltre 5000 client

Endpoint Protection Platform & Endpoint Detection and Response				
Fascia di acquisizione	Codice Servizio	Brand	Codice Fornitore	Quantità (moduli)
EPP & EDR - Fascia 1	EPP-F1-CYN	CYNET	Cynet-360-EPP-EDR-C-F1	0
	EPP-F1-TM	TRENDMICRO	OS01141-EPP-C-F1	0
	EPP-F1-MCA	MCAFEE	MV6DEE-AA-BA+DLPECE-AT-BA-F1	0
	EPP-F1-BIT	BITDEFENDER	GZ ULTRA - GOV 2 Y - C - F1	0
EPP & EDR - Fascia 2	EPP-F2-BIT	BITDEFENDER	GZ ULTRA - GOV 2 Y - C - F2	0
	EPP-F2-TM	TRENDMICRO	OS01141-EPP-C-F2	0
	EPP-F2-CYN	CYNET	Cynet-360-EPP-EDR-C-F2	0
	EPP-F2-MCA	MCAFEE	MV6DEE-AA-BA+DLPECE-AT-BA-F2	0
EPP & EDR - Fascia 3	EPP-F3-BIT	BITDEFENDER	GZ ULTRA - GOV 2 Y - C - F3	0
	EPP-F3-TM	TRENDMICRO	OS01141-EPP-C-F3	0
	EPP-F3-CYN	CYNET	Cynet-360-EPP-EDR-C-F3	0
	EPP-F3-MCA	MCAFEE	MV6DEE-AA-DA+DLPECE-AT-DA-F3	0
EPP & EDR - Fascia 4	EPP-F4-BIT	BITDEFENDER	GZ ULTRA - GOV 2 Y - C - F4	0
	EPP-F4-TM	TRENDMICRO	OS01141-EPP-C-F4	0
	EPP-F4-CYN	CYNET	Cynet-360-EPP-EDR-C-F4	0
	EPP-F4-MCA	MCAFEE	MV6DEE-AA-EA+DLPECE-AT-EA-F4	0

L'Azienda non intende acquisire la soluzione EPP/EDR

## QUADRO B - NAC

### Descrizione del Servizio

Il NAC consente l'implementazione di regole per il controllo degli accessi all'infrastruttura aziendale da parte degli utenti, siano essi "umani" (attraverso personal computer, apparati mobili, ...) oppure "cose" (elementi in ambito IoT). Le regole possono basarsi su più modalità quali l'autenticazione degli utenti, la configurazione degli apparati che accedono alla rete, il ruolo degli utenti. Per mezzo del NAC è inoltre possibile applicare regole successive alla connessione degli utenti, in base ad eventi che possono provenire da altri elementi di sicurezza.

Per i NAC sono previste sei fasce dimensionali/prestazionali:

- NAC\_1 (fascia 1): fino a 100 Endpoint concorrenti
- NAC\_2 (fascia 2): fino a 500 Endpoint concorrenti
- NAC\_3 (fascia 3): fino a 1.000 Endpoint concorrenti
- NAC\_4 (fascia 4): fino a 10.000 Endpoint concorrenti
- NAC\_5 (fascia 5): fino a 25.000 Endpoint concorrenti
- NAC\_6 (fascia 6): fino a 50.000 Endpoint concorrenti.

Network Access Control				
Fascia di acquisizione	Codice Servizio	Brand	Codice Fornitore	Quantità (moduli)
NAC- Fascia 1	NAC-F1-HPE	HPE	JZ508AM-3Y-100C	0
	NAC-F1-FN	FORTINET	FNC-CA-500C-BDL-C1	0
NAC- Fascia 2	NAC-F2-HPE	HPE	JZ508AM-3Y-500C	0
	NAC-F2-FN	FORTINET	FNC-CA-500C-BDL-C2	0
NAC- Fascia 3	NAC-F3-HPE	HPE	JZ508AM-3Y-1000C	0
	NAC-F3-FN	FORTINET	FNC-CA-500C-BDL-C3	0
NAC- Fascia 4	NAC-F4-HPE	HPE	R1V81AM-3Y-10000C	0
	NAC-F4-FN	FORTINET	FNC-CA-700C-BDL-C1	0
NAC- Fascia 5	NAC-F5-HPE	HPE	R1V82AM-3Y-25000C	0
	NAC-F5-FN	FORTINET	FNC-CA-700C-BDL-C2	0
NAC- Fascia 6	NAC-F6-HPE	HPE	R1V82AM-3Y-50000C	0
	NAC-F6-FN	FORTINET	FNC-CA-700C-BDL-C3	0

L'Azienda non intende acquisire la soluzione NAC

### QUADRO C - NGFW

#### Descrizione del Servizio

I NGFW 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.

Per i NGFW sono previste sei fasce dimensionali.

Next Generation Firewall				
Fascia di acquisizione	Codice Servizio	Brand	Codice Fornitore	Quantità (moduli)
NGFW - Fascia 1	NGFW-F1-FN	FORTINET	FG-60F-BDL-C	
	NGFW-F1-CI	CISCO	CISCO-FPR1010-F1C	
	NGFW-F1-FP	FORCEPOINT	N120-C-F1	
	NGFW-F1-PA	PALO ALTO	PAN-PA-440-CONSIP-BUN-F1	
NGFW - Fascia 2	NGFW-F2-CI	CISCO	CISCO-FPR2110-F2C	
	NGFW-F2-FN	FORTINET	FG-200F-BDL-C	
	NGFW-F2-FP	FORCEPOINT	N2101-C-F2	
	NGFW-F2-PA	PALO ALTO	PAN-PA-1410-CONSIP-BUN-F2	1
NGFW - Fascia 3	NGFW-F3-CI	CISCO	CISCO-FPR2130-F3C	
	NGFW-F3-FP	FORCEPOINT	N2101-C-F3	

	NGFW-F3-FN	FORTINET	FG-600E-BDL-C	
	NGFW-F3-PA	PALO ALTO	PAN-PA-3420-CONSIP-BUN-F3	
NGFW - Fascia 4	NGFW-F4-PA	PALO ALTO	PAN-PA-5220-CONSIP-BUN-F4	
	NGFW-F4-CI	CISCO	CISCO-FPR2140-F4C	
	NGFW-F4-FP	FORCEPOINT	N3401-C-F4	
	NGFW-F4-FN	FORTINET	FG-1100E-BDL-C	
NGFW - Fascia 5	NGFW-F5-PA	PALO ALTO	PAN-PA-5250-CONSIP-BUN-F5	
	NGFW-F5-CI	CISCO	CISCO-FPR4115-F5C	
	NGFW-F5-FP	FORCEPOINT	N3405-C-F5	
	NGFW-F5-FN	FORTINET	FG-2600F-BDL-C	
NGFW - Fascia 6	NGFW-F6-PA	PALO ALTO	PAN-PA-5260-CONSIP-BUN-F6	
	NGFW-F6-CI	CISCO	CISCO-FPR9300-F6C	
	NGFW-F6-FP	FORCEPOINT	N3410-C-F6	
	NGFW-F6-FN	FORTINET	FG-3400E-BDL-C	

L'Azienda intende acquisire un firewall NGFW – fascia 2 PAN-PA-1410-CONSIP-BUN-F2 – Palo Alto

#### QUADRO D - ANTI - APT

#### Descrizione del Servizio

La soluzione di Anti-APT consente l'analisi di file che possono essere inviati all'elemento da altri dispositivi di sicurezza o direttamente dal personale che si occupa di sicurezza. All'interno dell'ambiente protetto (sandbox) è quindi possibile, attraverso varie tecniche, esaminare i file e i loro comportamenti per determinare se questi siano o meno malevoli, assegnando loro un grado di severità.

Per l'Anti-APT sono previste due fasce dimensionali/prestazionali:

- Anti\_APT\_1 (fascia 1): fino a 450 file/ora
- Anti\_APT\_2 (fascia 2): fino a 1000 file/ora

Protezione anti-Advanced Persistent Threat				
Fascia di acquisizione	Codice Servizio	Brand	Codice Fornitore	Quantità (moduli)
Anti-APT - Fascia 1	Anti-APT-F1-CP	CHECKPOINT	SandBlast TE Appliance TE100X-C	0
	Anti-APT-F1-TM	TRENDMICRO	ADAXZZE5XL-C-F1	0
Anti-APT - Fascia 2	Anti-APT-F2-CP	CHECKPOINT	SandBlast TE Appliance TE250X-C	0
	Anti-APT-F2-TM	TRENDMICRO	ADAXZZE5XL-C-F2	0

L'Azienda non intende acquisire una soluzione Anti-APT

#### QUADRO E - Server Protection

#### Descrizione del Servizio

La soluzione SPP consente di proteggere gli endpoint di tipo server da minacce quali virus, trojan, worm, malware, bloccando le attività di applicazioni che risultano potenzialmente dannose, fornendo inoltre funzionalità utili all'investigazione e al ripristino in seguito a violazioni di sicurezza.

Per la SPP sono previste quattro fasce dimensionali:

- SPP\_1 (fascia 1): fino a 50 server
- SPP\_2 (fascia 2): fino a 100 server
- SPP\_3 (fascia 3): fino a 500 server
- SPP\_4 (fascia 4): oltre 500 server

Server Protection Platform				
Fascia di acquisizione	Codice Servizio	Brand	Codice Fornitore	Quantità (moduli)
SPP - Fascia 1	SPP-F1-CP	CHECKPOINT	CP-HAR-EP-COMLETE-SPP-C-F1	0
	SPP-F1-TM	TRENDMICRO	DX0099-SPP-C-F1	0
SPP - Fascia 2	SPP-F2-CP	CHECKPOINT	CP-HAR-EP-COMLETE-SPP-C-F2	0
	SPP-F2-TM	TRENDMICRO	DX0099-SPP-C-F2	0
SPP - Fascia 3	SPP-F3-CP	CHECKPOINT	CP-HAR-EP-COMLETE-SPP-C-F3	0
	SPP-F3-TM	TRENDMICRO	DX0099-SPP-C-F3	0
SPP - Fascia 4	SPP-F4-CP	CHECKPOINT	CP-HAR-EP-COMLETE-SPP-C-F4	0
	SPP-F4-TM	TRENDMICRO	DX0099-SPP-C-F4	0

L'Azienda non intende acquisire una soluzione SPP

## QUADRO F - Servizio di Hardening

### Descrizione del Servizio

Il servizio di hardening fornisce all'Amministrazione il supporto operativo necessario per rendere sicuri i client utilizzati. Le attività effettuate dovranno essere aderenti a quanto previsto dalle "Linee guida per adeguare la sicurezza del software di base" rilasciate da AgID.

Le specifiche attività che dovranno essere eseguite sono dipendenti dagli specifici software utilizzati sui client, ma in linea generale possono essere riassunte in:

- eliminazione di programmi non necessari dalle postazioni utente. Potenzialmente ogni programma è una porta di accesso per soggetti non legittimati e dunque la loro diminuzione consente di limitare i rischi di intrusioni. Tutti i programmi che non sono stati autorizzati e controllati e che non sono strettamente utili all'esecuzione delle attività lavorative dovrebbero essere rimossi;
- supporto ai sistemisti PA nelle fasi di monitoraggio e controllo che il sistema operativo e i programmi leciti siano aggiornati alle ultime versioni e agli ultimi "service pack" disponibili;
- controllo che sui client siano abilitati i servizi autorizzati, ossia che non vi siano "demoni" in ascolto sulle porte di rete se non quelli strettamente necessari;
- verifica che gli utenti abbiano i corretti privilegi in relazione al loro ruolo e che appartengono ai corretti gruppi utenti;
- verifica della consistenza delle password richieste e della periodicità di cambio password richiesta agli utenti;

- supporto ai sistemisti PA nella definizione di gruppi di policy che potranno essere applicati agli utenti sulla base dei loro ruoli;
- verifica che gli eventi di sicurezza siano correttamente storicizzati (logging) ai fini del controllo e dell'audit;
- supporto al personale dell'Amministrazione nella distribuzione delle azioni correttive individuate (ad es. installazione di eventuali *patch* mancanti, realizzazione e installazione di fix temporanee, etc..) siano esse relative al sistema operativo che ai programmi utilizzati.

Il servizio dovrà essere effettuato sulle postazioni di tipo client e dovrà includere almeno i seguenti software:

- Sistemi operativi Windows Client;
- Sistemi operativi macOS;
- Sistemi operativi UNIX/Linux di tipo Client;
- Principali Web Browser (Edge, Explorer, Firefox, Chrome);
- Principali applicativi software di produttività (Microsoft Office/OpenOffice, Pdf Readers, Outlook).

Servizio di Hardening			
Fascia di acquisizione	Codice Servizio	Codice Fornitore	Quantità (moduli)
Fase di assessment	ASS	HARD_ASSMNT	0
Fase di distribuzione degli interventi -1001_5000	DISINT 1001-5000	HARD_DISTR_1001_5000	0
Fase di distribuzione degli interventi - 2_1000	DISINT 2-1000	HARD_DISTR_2_1000	0
Fase di distribuzione degli interventi - 5001_	DISINT>5000	HARD_DISTR_5001_	0
Fase di progettazione degli interventi	PRINT	HARD_PROG	0

L'Azienda non intende acquisire il servizio di Hardening

### QUADRO G - Servizio di Formazione

#### Descrizione del Servizio

Il servizio di formazione e affiancamento consente la fruizione di sessioni formative impartite presso le sedi dell'Amministrazione Contraente che permettano di istruire i discenti sulle specifiche tecnologie acquistate nell'AQ, e deve avere l'obiettivo di:

- istruire i discenti sulle principali minacce che i prodotti acquistati si prefiggono di contrastare;
- descrivere gli apparati installati in termini di caratteristiche, configurazione e funzionalità, con particolare enfasi sulle componenti software;
- mettere il personale designato dall'Amministrazione Contraente in grado di provvedere alla gestione delle componenti installate in maniera autonoma ed ottimale;
- descrivere le eventuali attività di integrazione effettuate con altri prodotti acquistati o con prodotti già presenti presso l'Amministrazione e le relative finalità;
- realizzare demo e/o attività di test che consentano ai discenti di apprendere le principali funzionalità dei prodotti attraverso l'esperienza diretta.

È richiesto che tali attività formative siano erogate in moduli da massimo 16 ore e che per ogni modulo siano previsti al massimo 10 discenti. Ogni modulo è composto da due sezioni indicativamente di 8 ore ciascuna:

- una sezione teorica, in cui sono descritti i sistemi interessati e le relative funzionalità previste;
- una sezione pratica, in cui il personale dell'Amministrazione opererà attivamente sui sistemi, secondo una modalità *training on the job*.

Formazione			
Fascia di acquisizione	Codice Servizio	Codice Fornitore	Quantità (moduli)
Modulo Formativo	FOR	FORMAZIONE	0

L'Azienda non intende acquisire il servizio di Formazione

## QUADRO H - Servizio di Supporto Specialistico

### Descrizione del Servizio

Il servizio 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 le attività riportate nel seguito:

- la realizzazione di specifiche integrazioni tra i prodotti acquistati e prodotti già presenti presso l'Amministrazione al fine di massimizzare l'efficacia dei prodotti acquisiti e garantire la sicurezza del sistema nel suo complesso
- 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
- il supporto operativo al personale dell'Amministrazione nella gestione della sua infrastruttura, fornendo competenze specifiche in ambito di sicurezza informatica. Tale supporto potrà essere sia in modalità "a chiamata" sia in modalità "presidio" laddove l'Amministrazione, in ragione della complessità della propria infrastruttura, ravveda la necessità di avere del personale del Fornitore presso la propria sede in maniera continuativa

il supporto operativo al personale dell'Amministrazione nella gestione del suo centro operativo dedicato alla sicurezza (SOC), fornendo competenze specifiche in tale ambito.

Tale servizio potrà essere acquistato dalle Amministrazioni Contraenti unicamente in maniera contestuale ai prodotti e avere durata massima pari a 24 mesi.

Il servizio potrà essere prestato secondo le seguenti modalità:

- in fase iniziale - lett. a) del precedente elenco;
- in modalità "spot" - lett. b) e lett c) (limitatamente alla modalità "a chiamata") del precedente elenco
- con periodicità definita - lett. c) (limitatamente alla modalità "presidio") e d) del precedente elenco.

Servizio Supporto Specialistico			
Fascia di acquisizione	Codice Servizio	Codice Fornitore	Quantità (gg/uomo)
Junior Security Analyst - fascia standard	JSAN-STA	JR_SEC_AN_STD	<b>79</b>
Junior Security Analyst - fascia straordinaria	JSAN-STR	JR_SEC_AN_STR	
Security Principal - fascia standard	SP-STA	SEC_PRINC_STD	
Security Principal - fascia straordinaria	SP-STR	SEC_PRINC_STR	
Senior Security Analyst - fascia standard	SSAN-STA	SR_SEC_AN_STD	<b>80</b>
Senior Security Analyst - fascia straordinaria	SSAN-STR	SR_SEC_AN_STR	
Senior Security Architect - fascia standard	SSAR-STA	SR_SEC_ARCH_STD	
Senior Security Architect - fascia straordinaria	SSAR-STR	SR_SEC_ARCH_STR	
Senior Security Tester - fascia standard	SST-STA	SR_SEC_TEST_STD	
Senior Security Tester - fascia straordinaria	SST-STR	SR_SEC_TEST_STR	

## QUADRO I - Servizio di Manutenzione

### Descrizione del Servizio

Il servizio di manutenzione comprende le attività volte a garantire una pronta correzione dei malfunzionamenti e il ripristino delle funzionalità.

La manutenzione, in base alla qualità del servizio richiesto per i servizi erogati, prevede due profili *Low Profile (Business Day)* o *High Profile (H24)* e potrà essere offerta per annualità, quindi per 12 mesi o massimo 24 mesi.

Le attività di manutenzione sono associate ai soli elementi di fornitura acquistati nell'ambito del presente AQ e potranno essere acquistate solo contestualmente alla fornitura.

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:
  1. intervento presso la sede/luogo interessato;
  2. ripristino del servizio/funzionalità sui livelli preesistenti al guasto/anomalia, secondo gli SLA contrattualizzati, anche attraverso sostituzioni di elementi danneggiati;
  3. verifica funzionale del sistema per assicurare l'eliminazione della causa del guasto.

Servizio di manutenzione		
Fascia di acquisizione	Codice Servizio	Quantità (mesi)
Manutenzione LP	MANLP-EPP-F1	
	MANLP-EPP-F2	
	MANLP-EPP-F3	
	MANLP-EPP-F4	
	MANLP-NAC-F1	
	MANLP-NAC-F2	
	MANLP-NAC-F3	
	MANLP-NAC-F4	
	MANLP-NAC-F5	
	MANLP-NAC-F6	
	MANLP-NGFW-F1	
	MANLP-NGFW-F2	
	MANLP-NGFW-F3	
	MANLP-NGFW-F4	
	MANLP-NGFW-F5	
	MANLP-NGFW-F6	
	MANLP-Anti-APT-F1	
	MANLP-Anti-APT-F2	
	MANLP-SPP-F1	
	MANLP-SPP-F2	
MANLP-SPP-F3		
MANLP-SPP-F4		

Manutenzione HP

MANHP-EPP-F1	
MANHP-EPP-F2	
MANHP-EPP-F3	
MANHP-EPP-F4	
MANHP-NAC-F1	
MANHP-NAC-F2	
MANHP-NAC-F3	
MANHP-NAC-F4	
MANHP-NAC-F5	
MANHP-NAC-F6	
MANHP-NGFW-F1	
MANHP-NGFW-F2	24
MANHP-NGFW-F3	
MANHP-NGFW-F4	
MANHP-NGFW-F5	
MANHP-NGFW-F6	
MANHP-Anti-APT-F1	
MANHP-Anti-APT-F2	
MANHP-SPP-F1	
MANHP-SPP-F2	
MANHP-SPP-F3	
MANHP-SPP-F4	

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

## LOTTO 2



ASOOM\_TO\_Azienda Ospedaliera Ordine Mauriziano di Torino - Rep. DG 09/12/2024.0000946.I



## Tabella Revisioni

Revisione	Descrizione modifiche	Data
1.0	Prima emissione	26/11/2024
2.0	Aggiunta fornitura NAC Fortinet	04/12/2024

## Indice

1. INTRODUZIONE.....	3
1.1 Premessa.....	3
1.2 Scopo.....	3
1.3 Riferimenti.....	3
1.4 Acronimi e glossario .....	3
2. ORGANIZZAZIONE DEL CONTRATTO ESECUTIVO.....	4
2.1 Categorizzazione degli interventi.....	4
3. PROGETTO DI ATTUAZIONE .....	5
4. PRODOTTI RICHIESTI .....	6
5. PRODOTTI DELLA FORNITURA.....	6
5.1 Next Generation Firewall .....	6
5.2 Network Access Control .....	6
6. Prerequisiti dei PRODOTTI .....	7
7. SERVIZIO DI SUPPORTO SPECIALISTICO.....	7
8. SERVIZIO DI FORMAZIONE .....	9
9. SERVIZIO DI HARDENING.....	9
10. SERVIZIO DI MANUTENZIONE .....	9
11. PIANO DI LAVORO.....	10
11.1 GANTT.....	11
11.2 Piano di presa in carico .....	11
11.3 Specifiche di collaudo.....	12
12. TABELLA RIEPILOGATIVA dei servizi e relativi importi contrattuali .....	13
13. PRESTAZIONI DI SUBAPPALTO .....	14

## 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 Cliente Azienda Ospedaliera Ordine Mauriziano di Torino (di seguito il Cliente), in conformità alle richieste espresse dall'Amministrazione nel Piano dei Fabbisogni (Richiesta Piano Operativo/Ordine 8170131).

Con questo progetto il Cliente intende acquisire:

- Next Generation Firewall
- Network Access Control

### 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 – A.O. Mauriziano di Torino – Richiesta Piano Operativo/Ordine 8170131
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)**

**Massimiliano Materazzi**  
*massimiliano.materazzi@telecomitalia.it*

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.

✓ **Responsabile del Fornitore**

**Cristina Moscato**  
 335 5644666  
*Cristina.moscato@telecomitalia.it*

che riferirà, per quanto di competenza, all'Amministrazione su tutte le tematiche contrattuali relative al Contratto Esecutivo.

✓ **Referente Tecnico per l'erogazione dei servizi**

**Simona Lunetta**  
 335 6339151  
*Simona.lunetta@telecomitalia.it*

che dovranno 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).

### 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	<input type="checkbox"/> Servizi al cittadino
	<input type="checkbox"/> Servizi a imprese e professionisti
	<input checked="" type="checkbox"/> Servizi interni alla propria PA
	<input type="checkbox"/> Servizi verso altre PA
☐ Dati	<input type="checkbox"/> Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese
	<input type="checkbox"/> Aumentare la qualità dei dati e dei metadati
	<input type="checkbox"/> 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
	x Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione

### 3. PROGETTO DI ATTUAZIONE

Il progetto contempla l'attivazione di un NGFW sulla rete dell'Azienda Ospedaliera Mauriziano di Torino, sita a Torino, Via Magellano 1, con l'obiettivo di aumentare il livello di sicurezza dei dispositivi IOMT: in particolare si intende censire tutti i dispositivi medicali e non connessi in rete verificandone le vulnerabilità.

L'apparato dovrà essere collocato su Rack 12-0 presso la sala CED dell'A.O. Ordine Mauriziano, 1° piano.

In merito all'indirizzamento di rete il sistema dovrà rimanere in ascolto di tutte le VLAN su Span Port collegata in fibra 1 Gbps.

Per il management dell'apparato sarà assegnata la classe di indirizzamento 192.168.39.128/29.

Il sistema dovrà essere configurato rispettando le best practices di settore nell'ambito della cyber sicurezza. In particolare, dovranno essere garantiti accessi protetti da password e sistemi MFA e dovrà essere possibile limitare le comunicazioni verso l'esterno alle sole destinazioni "sicure".

Si prevede un numero indicativo di circa 3.700 dispositivi connessi in rete, di cui circa 400 IOMT.

Successivamente, il Cliente ha chiesto di integrare il progetto con la fornitura in opera di un NAC Fortinet.

#### 4. PRODOTTI RICHIESTI

PRODOTTI	BRAND	FASCIA	MODELLO	CODICE PRODUTTORE	ARTICOLO	N.
NGFW Fascia 2	PALO ALTO	2	PAN-PA-1410- CONSIP-BUN-F2	PAN-PA-1410-CONSIP- BUN-F2		1
NAC-F4-	FORTINET	4	FORTINET FNC- CA-700C-BDL-C1	FNC-CA-700C-BDL-C1		1

#### 5. PRODOTTI DELLA FORNITURA

---

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

##### 5.1 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. Alleghiamo le specifiche tecniche della soluzione Palo Alto.



##### 5.2 NETWORK ACCESS CONTROL

---

Il NAC consente l'implementazione di regole per il controllo degli accessi all'infrastruttura aziendale da parte degli utenti, siano essi "umani" (attraverso personal computer, apparati mobili, ...) oppure "cose" (elementi in ambito IoT). Le regole possono basarsi su più modalità quali l'autenticazione degli utenti, la configurazione degli apparati che accedono alla rete, il ruolo degli utenti. Per mezzo del NAC è inoltre possibile applicare regole successive alla connessione degli utenti, in base ad eventi che possono provenire da altri elementi di sicurezza. Nell'Accordo quadro sono previste e sei fasce dimensionali/prestazionali e 2 Vendor. Alleghiamo le specifiche tecniche della soluzione Fortinet.



## 6. PREREQUISITI DEI PRODOTTI

N.A.

## 7.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:

- b) 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 riportano gli impegni previsti nel progetto:

Servizio Supporto Specialistico			
Fascia di acquisizione	Codice Servizio	Codice Fornitore	Quantità (gg/uomo)
Junior Security Analyst - fascia standard	JSAN-STA	JR_SEC_AN_STD	<b>79</b>
Junior Security Analyst - fascia straordinaria	JSAN-STR	JR_SEC_AN_STR	
Security Principal - fascia standard	SP-STA	SEC_PRINC_STD	
Security Principal - fascia straordinaria	SP-STR	SEC_PRINC_STR	
Senior Security Analyst - fascia standard	SSAN-STA	SR_SEC_AN_STD	<b>73</b>
Senior Security Analyst - fascia straordinaria	SSAN-STR	SR_SEC_AN_STR	
Senior Security Architect - fascia standard	SSAR-STA	SR_SEC_ARCH_STD	
Senior Security Architect - fascia straordinaria	SSAR-STR	SR_SEC_ARCH_STR	
Senior Security Tester - fascia standard	SST-STA	SR_SEC_TEST_STD	
Senior Security Tester - fascia straordinaria	SST-STR	SR_SEC_TEST_STR	

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:

**Junior Security Analyst:** in possesso di almeno una delle seguenti certificazioni: EC-Council CSA (Certified SOC Analyst) e/o CompTIA CySA+ (Cyber Security Analyst) e/o GIAC Certified Intrusion Analyst,

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

Security Manager)

**Senior Security Architect:** in possesso della certificazione (ISC)<sup>2</sup> CISSP (Certified Information System Security Professional)

**Senior Security Analyst:** in possesso di almeno una delle seguenti certificazioni:  
EC-Council CSA (Certified SOC Analyst) e/o CompTIA CySA+ (Cyber Security Analyst) e/o  
GIAC Certified Intrusion Analyst

Durante le giornate uomo sopra indicate saranno svolte le attività di supporto specialistico per l'installazione dell'Hardware Palo Alto:

- il Firewall PA-1410 verrà montato in rack e connesso alla rete.  
Alimentazione e cavi (ethernet e console).

Configurazioni Preliminari:

- Definire le subnet interne (LAN, DMZ).
- Mappare le regole di sicurezza richieste.

Accesso al Firewall:

- Collegamento tramite console seriale o interfaccia management (MGMT).
- Credenziali di default per primo accesso.

Passaggi di Configurazione:

#### **Step 1: Configurazione Iniziale**

- Collegarsi alla porta di management (default: <https://192.168.1.1>).
- Cambiare credenziali di default.

Configurare:

- Hostname e dettagli base.
- NTP per sincronizzazione oraria.
- Indirizzo IP della porta di management.

#### **Step 2: Configurazione delle Interfacce**

- Assegnare le interfacce alle zone:
- Ethernet1/1: WAN (zona Untrust, IP pubblico).
- Ethernet1/2: LAN (zona Trust, IP privato).
- Ethernet1/3: DMZ (zona DMZ, IP privato).

Configurare le interfacce:

- Statico o DHCP per WAN.
- Statici per LAN e DMZ.

#### **Step 3: Creazione delle eventuali zone necessarie**

Creare zone logiche:

- Untrust, Trust, DMZ, VPN.
- Associare le interfacce fisiche alle zone.

#### **Step 4: Regole di Sicurezza**

#### **Step 5: Logging e Monitoraggio**

- Configurare Syslog per invio log a un server centrale.

- Configurare notifiche email per eventi critici.
- Monitorare il traffico e ottimizzare le regole.

## 6. Test e Validazione

- Verifica connettività:
- LAN → WAN.
- Accesso VPN remoto.
- Accesso a server nella DMZ.
- Test delle regole:

Controllo dei permessi e blocchi definiti.

Simulare attacchi per verificare la protezione.

Durante le giornate uomo sopra indicate saranno svolte le attività di supporto specialistico per l'installazione della soluzione FortiNAC:

- ASSESSMENT
- DESIGN HLD soluzione centralizzata + meeting
- ANALISI dei dati raccolti dall'assessment
- DESIGN HLD soluzione centralizzata + meeting
- PROGETTO LLD gantt + meeting
- INST E CONF PARTE WIRED (1°STEP)
- Ambiente pilota
- Messa in produzione area pilota
- TUNING PARTE WIRED
- Collaudo finale
- FORMAZIONE
- Rilascio documentazione
- CONF PARTE WIRELESS (2°STEP)
- Ambiente pilota
- Messa in produzione area pilota
- Collaudo finale
- Rilascio documentazione
- FORMAZIONE

## 8. SERVIZIO DI FORMAZIONE

---

N.A.

## 9. SERVIZIO DI HARDENING

---

N. A.

## 10. SERVIZIO 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),

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.

Nel progetto è prevista l'assistenza tecnica per 24 mesi di tipo High Profile H24.

## 11 PIANO DI LAVORO

---

Il nuovo firewall Palo Alto Networks sarà installato nel sit indicato dall'Amministrazione, e sarà dedicato alle funzioni cui l'Amministrazione deciderà di adibirlo.

Gli step implementativi prevedono le seguenti attività:

- Verifica configurazioni necessarie sul nuovo Firewall (da remoto)
- Verifica in accordo con il cliente eventuali bonifica\creazione policy di sicurezza
- Installazione nuovo Firewall con le seguenti modalità:
  - Installazione Firewall
  - Verica configurazione e rilascio in produzione Firewall
- Monitoraggio funzionamento Policy di sicurezza
- Collaudo Finale e GO LIVE

Il nuovo FORTINAC sarà installato nel sito indicato dall'Amministrazione, e sarà dedicato alle funzioni cui l'Amministrazione deciderà di adibirlo.

Gli step implementativi prevedono le seguenti attività:

- ASSESSMENT
- DESIGN HLD soluzione centralizzata + meeting
- ANALISI dei dati raccolti dall'assessment
- DESIGN HLD soluzione centralizzata + meeting
- PROGETTO LLD gantt + meeting
- INST E CONF PARTE WIRED (1°STEP)
- Ambiente pilota
- Messa in produzione area pilota
- TUNING PARTE WIRED
- Collaudo finale
- FORMAZIONE
- Rilascio documentazione
- CONF PARTE WIRELESS (2°STEP)
- Ambiente pilota
- Messa in produzione area pilota
- Collaudo finale



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

### 11.3 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
- 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
<b>Test Funzionale</b>	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
<b>Test di sicurezza</b>	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
<b>Test di compatibilità</b>	Questi tipi di test verificano la capacità dei dispositivi di funzionare correttamente con gli altri componenti dell'infrastruttura IT

## 12. TABELLA RIEPILOGATIVA DEI SERVIZI E RELATIVI IMPORTI CONTRATTUALI

Famiglia	Codice Articolo Convenzione	Descrizione Articolo Convenzione	Produttore	Quantità	Durata	Unità di misura	Prezzo senza IVA	UT Totale	Canone Anno 1 Totale	Canone Anno 2 Totale
Next Generation Firewall	CS2L1-NGFW-F2-PA	Fornitura in opera NGFW-F2-PA-PAN-PA-1410-CONSIP-BUN-F2	PALO ALTO	1		Pezzo	8951,15	8951,15		
			TELECOMITALIA							
Next Generation Firewall	CS2L1-MANHP-NGFW-F2-PA	Manutenzione mensile HP Next Generation Firewall Fascia 2	TELECOMITALIA	1	12	Pezzo/mese	29,84		358,08	
Next Generation Firewall	CS2L1-MANHP-NGFW-F2-PA	Manutenzione mensile HP Next Generation Firewall Fascia 2	TELECOMITALIA	1	12	Pezzo/mese	29,84			358,08
Network Access Control	CS2L1-NAC-F4-FN	Fornitura in opera NAC-F4-FN-FNC-CA-700F-BDL-C1	FORTINET	1		Pezzo	66577,91	66577,91		
Network Access Control	CS2L1-MANHP-NAC-F4-FN	Manutenzione mensile HP Network Access Control Fascia 4	TELECOMITALIA	1	12	Pezzo/mese	221,93		2663,16	
Network Access Control	CS2L1-MANHP-NAC-F4-FN	Manutenzione mensile HP Network Access Control Fascia 4	TELECOMITALIA	1	12	Pezzo/mese	221,93			2663,16
Servizi	CS2L1-JSAN-STA	Servizio di supporto specialistico - Junior Security Analyst - fascia standard	TELECOMITALIA	79		gg/uomo	227,50	17972,50		
Servizi	CS2L1-SSAN-STA	Servizio di supporto specialistico - Senior Security Analyst - fascia standard	TELECOMITALIA	73		gg/uomo	271,00	19783,00		
							<b>TOTALE</b>	<b>113284,56</b>	<b>3021,24</b>	<b>3021,24</b>

### 13. PRESTAZIONI DI SUBAPPALTO

---

La tabella sottostante riporta le quote di subappalto, nel rispetto di quanto indicato nel Piano dei fabbisogni:

<b>Servizi</b>	<b>Quota subappalto</b>	<b>Azienda del RTI che eroga il servizio</b>	<b>Nome dell'azienda che eroga la prestazione in subappalto</b>
Manutenzione	5,06%	TIM	LantechLongwave
Supporto Specialistico	63,30%	TIM	LantechLongwave