COMUNE DI VANZAGHELLO

Città Metropolitana di Milano
Via Donatori Volontari del Sangue, 3
Mail: info@comune.vanzaghello.mi.it – PEC: comune.vanzaghello@postecert.it
P.TA IVA 02937320154 – RUP – Cristina Crupi

ID AQ 2367

PIANO DEI FABBISOGNI SERVIZI

ID:

Spett.le
TELECOM ITALIA S.p.A.

Lo scrivente **COMUNE DI VANZAGHELLO** C.F. / P.IVA 02937320154
Codice IPA L_664
con sede legale in Vanzaghella Prov.MI CAP20020 Nazione ITALIA
Indirizzo Via donatori volontari del Sangue, 3
chiede che venga realizzato quanto di seguito indicato (barrare i servizi richiesti con il presente piano dei fabbisogni):

X **EDP/EPR** (compilare il Quadro **A**)	☐ **NAC** (compilare il Quadro **B**)
☐ **NGFW** (compilare il Quadro **C**)	☐ **ANTI - APT** (Compilare il Quadro **D**)
☐ **Server Protection** (compilare il Quadro **E**)	☐ **Servizio di Hardening** (compilare il Quadro **F**)
☐ **Servizio di Formazione** (compilare il Quadro **G**)	X **Servizio di Supporto Specialistico** (compilare il Quadro **H**)
☐ **Servizio di di Manutenzione** (compilare il Quadro **I**)	

Invio delle fatture

Codice Univoco Ufficio:
CIG (quando disponibile)**:**
NSO (quando disponibile)**:**
CUP:

Domicilio fattura:

Località VANZAGHELLO Prov. MI CAP 20020 Nazione ITALIA
Indirizzo Via Donatori Volontari del Sangue, 3

☐ Cliente esente IVA in base a _____ (allegare dichiarazione di intento)

Responsabile dell'Amministrazione per i rapporti con TELECOM ITALIA[1]

Nome CRISTINA Cognome CRUPI
Tel. 0331308927 fax 0331658355
E-mail**(obbligatoria)info@comune.vanzaghello.mi.it – pec: comune.vanzaghello@postecert.it**

1 Tale nominativo sarà l'unico riconosciuto da TELECOM ITALIA per qualsiasi contatto inerente. a problematiche di tipo amministrativo/commerciale anche relative all'indicazione del/i luogo/ghi di esecuzione dei servizi. In caso di variazione il Cliente è tenuto a trasmettere a Telecom Italia, come indicato nella Richiesta di Adesione al Servizio, una comunicazione scritta.

DATA 11/06/2024 TIMBRO E FIRMA DEL CLIENTE

Firmato digitalmente

Descrizione del Contesto di Riferimento in cu si riferisce la fornitura dell'Amministrazione
Attualmente è presente una soluzione di protezione degli endpoint basata su tecnologia Webroot

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

Sosituire n.45 licenze antivirus Webroot in scadenza

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

NO

Tempistiche richieste per la realizzazione della fornitura, con descrizione di eventuali vincoli e/o criticità
Scadenza licenza 25-06-2025

Indicazione del/i luogo/ghi di interesse della fornitura
COMUNE DI VANZAGHELLO Via Donatori Volontari del Sangue 3 – cap. 20020 - MI
Durata del Contratto Esecutivo

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

Collegamento alla rete di alimentazione, presso il punto di presenza della rete indicato dall'Amministrazione.
Indicazione del/i luogo/ghi di interesse della fornitura

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

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**
2. **schemi di indirizzamento**
3. **requisiti delle policy di sicurezza stabiliti dall'Amministrazione**

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

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 nesessità di un supporto di servizi professionali.

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.

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

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

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	
	EPP-F1-TM	TRENDMICRO	OS01141-EPP-C-F1	
	EPP-F1-MCA	MCAFEE	MV6DEE-AA-BA+DLPECE-AT-BA-F1	
	EPP-F1-BIT	BITDEFENDER	GZ ULTRA - GOV 2 Y - C - F1	**45**
EPP & EDR - Fascia 2	EPP-F2-BIT	BITDEFENDER	GZ ULTRA - GOV 2 Y - C – F2	
	EPP-F2-TM	TRENDMICRO	OS01141-EPP-C-F2	
	EPP-F2-CYN	CYNET	Cynet-360-EPP-EDR-C-F2	
	EPP-F2-MCA	MCAFEE	MV6DEE-AA-BA+DLPECE-AT-BA-F2	
EPP & EDR - Fascia 3	EPP-F3-BIT	BITDEFENDER	GZ ULTRA - GOV 2 Y - C – F3	
	EPP-F3-TM	TRENDMICRO	OS01141-EPP-C-F3	
	EPP-F3-CYN	CYNET	Cynet-360-EPP-EDR-C-F3	
	EPP-F3-MCA	MCAFEE	MV6DEE-AA-DA+DLPECE-AT-DA-F3	
EPP & EDR - Fascia 4	EPP-F4-BIT	BITDEFENDER	GZ ULTRA - GOV 2 Y - C – F4	
	EPP-F4-TM	TRENDMICRO	OS01141-EPP-C-F4	
	EPP-F4-CYN	CYNET	Cynet-360-EPP-EDR-C-F4	
	EPP-F4-MCA	MCAFEE	MV6DEE-AA-EA+DLPECE-AT-EA-F4	

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	
	NAC-F1-FN	FORTINET	FNC-CA-500C-BDL-C1	
NAC- Fascia 2	NAC-F2-HPE	HPE	JZ508AM-3Y-500C	
	NAC-F2-FN	FORTINET	FNC-CA-500C-BDL-C2	
NAC- Fascia 3	NAC-F3-HPE	HPE	JZ508AM-3Y-1000C	
	NAC-F3-FN	FORTINET	FNC-CA-500C-BDL-C3	
NAC- Fascia 4	NAC-F4-HPE	HPE	R1V81AM-3Y-10000C	
	NAC-F4-FN	FORTINET	FNC-CA-700C-BDL-C1	
NAC- Fascia 5	NAC-F5-HPE	HPE	R1V82AM-3Y-25000C	
	NAC-F5-FN	FORTINET	FNC-CA-700C-BDL-C2	
NAC- Fascia 6	NAC-F6-HPE	HPE	R1V82AM-3Y-50000C	
	NAC-F6-FN	FORTINET	FNC-CA-700C-BDL-C3	

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-3220-CONSIP-BUN-F2	
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-3260-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	

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	
	Anti-APT-F1-TM	TRENDMICRO	ADAXZZE5XL-C-F1	
Anti-APT - Fascia 2	Anti-APT-F2-CP	CHECKPOINT	SandBlast TE Appliance TE250X-C	
	Anti-APT-F2-TM	TRENDMICRO	ADAXZZE5XL-C-F2	

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-COMPLETE-SPP-C-F1	
	SPP-F1-TM	TRENDMICRO	DX0099-SPP-C-F1	
SPP - Fascia 2	SPP-F2-CP	CHECKPOINT	CP-HAR-EP-COMPLETE-SPP-C-F2	
	SPP-F2-TM	TRENDMICRO	DX0099-SPP-C-F2	
SPP - Fascia 3	SPP-F3-CP	CHECKPOINT	CP-HAR-EP-COMPLETE-SPP-C-F3	
	SPP-F3-TM	TRENDMICRO	DX0099-SPP-C-F3	
SPP - Fascia 4	SPP-F4-CP	CHECKPOINT	CP-HAR-EP-COMPLETE-SPP-C-F4	
	SPP-F4-TM	TRENDMICRO	DX0099-SPP-C-F4	

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	
Fase di distribuzione degli interventi -1001_5000	DISINT 1001-5000	HARD_DISTR_1001_5000	
Fase di distribuzione degli interventi - 2_1000	DISINT 2-1000	HARD_DISTR_2_1000	
Fase di distribuzione degli interventi - 5001_	DISINT>5000	HARD_DISTR_5001_	
Fase di progettazione degli interventi	PRINT	HARD_PROG	

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 *traning on the job*.

Formazione			
Fascia di acquisizione	Codice Servizio	Codice Fornitore	Quantità (moduli)
Modulo Formativo	FOR	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 riguarderda le attività riportate nel seguito:
a) 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

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

c) 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:
i. in fase iniziale - lett. a) del precedente elenco;

ii. in modalità "*spot*" - lett. b) e lett c) (limitatamente alla modalità "a chiamata") del precedente elenco

iii. 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	**2**
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	**1**
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	24
	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	
	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	