Copia dell'originale conservato presso la Pubblica Amministrazione (Art.85sexies,co.2-4,D156/05 smi)

**UFFICIO INFORMATICA, SICUREZZA,
RETI E PROTEZIONE DEI DATI PERSONALI**
Dipartimento Funzione Pubblica

Massimiliano Casali
Firmato digitalmente da Massimiliano Casali
Data: 2026.11.10 09:18:38 +01'00'

Interna: AOO AOO-02, N. Prot. 00109303 del 10/11/2026

ALLEGATO "A"

CAPITOLATO SPECIALE
PER LA FORNITURA, L'INSTALLAZIONE E LA MIGRAZIONE DI UNA SOLUZIONE NEXT GENERATION FIREWALL (NGFW)

Oggetto

La presente Asta Pubblica, composta da n. 01 lotto, prevede la fornitura, l'installazione e la migrazione di una soluzione Next Generation Firewall (NGFW).

Dichiarazione di confidenzialità

I documenti e le informazioni trasmessi nell'ambito della presente Asta pubblica, sono da considerarsi strettamente confidenziali; in particolare, le informazioni contenute nei relativi allegati non possono essere copiate, riprodotte, divulgate, trasferite, trasformate in qualsiasi forma, trasmesse o pubblicate. L'Impresa Appaltatrice s'impegna, inoltre, al rispetto delle disposizioni della Legge n. 171/2018 e successive modifiche, circa la protezione dei dati personali.

Riservatezza

L'impresa partecipante, e tutte le figure ad essa collegate, dovrà tenere riservate tutte le informazioni concernenti le attività di cui sia venuta o potrà venire a conoscenza in occasione della definizione ed esecuzione della presente Asta. Il medesimo impegno sarà a carico dell'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali dal momento della ricezione delle offerte.

DESCRIZIONE GENERALE

1 - OGGETTO

Il presente capitolato disciplina la fornitura, l'installazione, la configurazione e la migrazione di una soluzione Next Generation Firewall (NGFW) a protezione delle reti della Pubblica Amministrazione, in sostituzione dell'attuale sistema firewall giunto a fine ciclo di vita.
Ai fini del presente capitolato, per Stazione Appaltante si intende l'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali del Dipartimento Funzione Pubblica della Repubblica di San Marino.
La fornitura comprende:

- Quattro apparati NGFW, installati in due cluster di alta affidabilità;
- La fornitura di un apparato centralizzato di raccolta e analisi dei log, in hardware, che riceve i log dei quattro apparati, li analizza e li inoltra al SIEM dell'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali;
- Le licenze e i servizi di sicurezza per **36 mesi**;
- I servizi di preanalisi, installazione, configurazione, migrazione, collaudo, formazione e assistenza;
- Il supporto tecnico e i livelli di servizio per 12 mesi.

La procedura è aperta a tutte le soluzioni presenti sul mercato.

Copia dell'originale conservato presso la Pubblica Amministrazione (Art.85sexies,co.2-4,D156/05 smi)

Interna: AOO AOO-02, N. Prot. 00109303 del 10/11/2026

2 - SITUAZIONE ATTUALE

L'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali gestisce due perimetri di sicurezza distinti, ciascuno protetto da due apparati in alta affidabilità:

- Perimetro esterno;
- Perimetro interno.

La topologia, l'indirizzamento, la collocazione degli apparati e le funzioni svolte da ciascun perimetro sono forniti all'aggiudicatario all'avvio della preanalisi, previa sottoscrizione dell'impegno di riservatezza, e non sono riportati nel presente documento.
Gli apparati in uso sono firewall di tecnologia Forcepoint. La raccolta dei log è affidata a un apparato dedicato della stessa tecnologia, che sarà sostituito dalla sonda fornita dall'aggiudicatario.
L'indicazione della tecnologia attualmente installata ha finalità puramente descrittiva del contesto: non costituisce requisito di compatibilità.

La configurazione da migrare comprende:

Elemento	**Quantità**
Regole di sicurezza del perimetro esterno	2.263
Regole di sicurezza del perimetro interno	2.058
Inspection policy	148
Regole NAT	202
Reti e subnet	520
Host e dispositivi	2.700
Utenti VPN per accesso remoto	circa 500

Il numero di tunnel VPN site-to-site, di oggetti e di utenti di dominio sarà verificato in fase di preanalisi. Il vecchio firewall sarà spento entro la fine di marzo 2027. Il nuovo sistema deve pertanto essere installato, migrato e collaudato prima di tale data.

3 - ARCHITETTURA DELLA SOLUZIONE

La soluzione comprende:

1. Due apparati NGFW in alta affidabilità per il perimetro esterno;
2. Due apparati NGFW in alta affidabilità per il perimetro interno;
3. Una sonda che raccoglie, analizza e correla i log dei quattro apparati e li inoltra al SIEM.

Tutti gli apparati sono amministrati da un'unica console di gestione.
I quattro apparati NGFW devono appartenere alla stessa famiglia e impiegare lo stesso sistema operativo, al fine di garantire omogeneità delle policy e degli aggiornamenti.
Ciascun cluster deve operare in alta affidabilità con sincronizzazione delle sessioni, commutazione automatica senza perdita di servizio e collegamento di heartbeat dedicato. Ogni apparato deve disporre di una porta di gestione separata dal traffico.
Per motivi di sicurezza il presente documento non riporta schemi di rete, indirizzamenti né planimetrie delle sedi. Tali informazioni sono fornite al fornitore aggiudicatario all'avvio della preanalisi, previa sottoscrizione dell'impegno di riservatezza richiesto dalla Stazione Appaltante.

3.1 Apparato centralizzato di raccolta e analisi dei log (sonda)

La soluzione deve comprendere un apparato centralizzato di raccolta e analisi dei log, di seguito la sonda, fornito dall'aggiudicatario, in hardware e non virtuale, che non si limita a raccogliere i log dei

Copia dell'originale conservato presso la Pubblica Amministrazione (Art.85sexies,co.2-4,D156/05 smi)

quattro apparati: li conserva, li analizza e li correla, produce report e avvisi e li inoltra al SIEM dell'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali. L'analisi e la reportistica della sonda riguardano il traffico e le minacce dei firewall; la correlazione di sicurezza a livello di sistema resta affidata al SIEM.

I valori indicati nella tabella costituiscono requisiti minimi obbligatori.

Requisito	**Valore minimo**
Formato e alimentazione	1U rack, doppia alimentazione ridondante
Porte	almeno 4 porte GE RJ45 o SFP
Capacità di raccolta	80 GB di log al giorno
Velocità di elaborazione dei log	almeno 1800 eventi al secondo in modalità analitica, con report, dashboard e ricerca storica disponibili
Funzioni di analisi	correlazione degli eventi, ricerca storica sui log, report e dashboard predefiniti e personalizzabili
Storage per la conservazione dei log	Due unità disco RAID1 da almeno 3TB ciascuna

4 - REQUISITI MINIMI DEGLI APPARATI

I valori indicati costituiscono requisiti minimi per singolo apparato. Il fornitore è tenuto a comprovarli mediante datasheet ufficiale del produttore; la verifica avviene in fase di aperture caratteristiche tecnico amministrative.

Tutte le funzioni richieste dal presente capitolato devono essere disponibili nella versione offerta e in quella consegnata; non sono ammesse funzionalità annunciate o previste in rilasci futuri.

Formato	1U rack, doppia alimentazione ridondante
Porte	almeno 2 x 25 GbE SFP28, 4 x 10 GbE SFP+, 8 x 1 GbE SFP e 4 x RJ45 GbE
Porte dedicate	una per la gestione e una per l'alta affidabilità, separate dal traffico
Throughput firewall con pacchetti da 1518 byte	150 Gbps
Throughput firewall con pacchetti da 64 byte	120 Gbps
Capacità di elaborazione	200 milioni di pacchetti al secondo
Throughput IPS	25 Gbps
Throughput NGFW con firewall, IPS e controllo applicativo attivi	12 Gbps
Throughput ispezione TLS con IPS attivo	10 Gbps
Throughput IPsec VPN	50 Gbps
Sessioni concorrenti	20 milioni
Nuove sessioni al secondo	500.000
Tunnel VPN site-to-site	1.500
Utenti VPN simultanei	4.000
Accelerazione hardware	accelerazione mediante ASIC o tecnologia equivalente per le funzioni di rete e di sicurezza, con offload automatico e protezione DDoS come da paragrafo 4.1

Interna: AOO AOO-02, N. Prot. 00109303 del 10/11/2026

Copia dell'originale conservato presso la Pubblica Amministrazione (Art.85sexies,co.2-4,D156/05 smi)

Interna: AOO AOO-02, N. Prot. 00109303 del 10/11/2026

4.1 Accelerazione hardware

La piattaforma deve disporre di accelerazione hardware dedicata alle funzioni di rete e di sicurezza, realizzata mediante circuiti integrati dedicati (ASIC) o tecnologia equivalente. Il sistema deve delegare automaticamente le sessioni ai componenti di accelerazione, senza moduli aggiuntivi né configurazioni separate, in modo che l'elaborazione delle funzioni ripetitive non gravi sulla CPU.
L'accelerazione deve riguardare almeno: ispezione delle sessioni, traduzione degli indirizzi, VPN, routing, qualità del servizio, controllo applicativo, prevenzione delle intrusioni, ispezione del traffico cifrato e filtro dei contenuti.
La protezione dagli attacchi volumetrici (DDoS) è requisito obbligatorio: deve essere operativa nella versione offerta, con mitigazione automatica e soglie configurabili.
Il rispetto di tali requisiti è obbligatorio ed è verificato sui datasheet ufficiali del produttore.

5 - FUNZIONI DI SICUREZZA RICHIESTE

Le funzioni indicate nella tabella costituiscono requisiti minimi obbligatori e sono richieste per il perimetro o i perimetri ivi specificati.

Funzione	**Perimetro**
Firewall stateful con policy per zona, indirizzo, servizio, utente e applicazione; NAT sorgente e destinazione	Esterno e interno
Prevenzione delle intrusioni con firme aggiornate, firme personalizzate, rilevamento comportamentale e modelli di machine learning	Esterno e interno
Virtual patching per i sistemi non aggiornabili	Esterno e interno
Controllo applicativo, con throughput di almeno 45 Gbps	Esterno e interno
Filtro URL e filtro DNS per categorie	Esterno e interno
Ispezione TLS, con gestione delle esenzioni e dei certificati	Esterno e interno
Applicazione dei profili di sicurezza anche al traffico cifrato	Esterno e interno
VPN IPsec site-to-site e VPN per utenti remoti	Esterno e interno
Gestione centralizzata dei nodi, con backup e ripristino delle configurazioni	Esterno e interno
Ruoli amministrativi differenziati, registro di audit	Esterno e interno
Reportistica su traffico, minacce e applicazioni	Esterno e interno
Integrazione con Active Directory per policy basate su utente e gruppo e per l'autenticazione	Esterno e interno
Invio degli eventi al SIEM in tempo reale	Esterno e interno

Copia dell'originale conservato presso la Pubblica Amministrazione (Art.85sexies,co.2-4,D156/05 smi)

Interna: AOO AOO-02, N. Prot. 00109303 del 10/11/2026

6 - LICENZE E AGGIORNAMENTI

6.1 Le licenze e le sottoscrizioni indicate nella tabella sono comprese nel prezzo e hanno durata di 36 mesi. I perimetri sono quelli definiti all'articolo 2.

Voce	Apparati esterni (2)	Apparati interni (2)	Sonda (1)
Prevenzione delle intrusioni, con firme aggiornate, rilevamento comportamentale e modelli di machine learning, comprensiva di virtual patching	sì	sì	-
Controllo applicativo	sì	sì	-
Filtro URL e filtro DNS per categorie	sì	no	-
Supporto del produttore, aggiornamento del firmware e sostituzione dell'hardware guasto	sì	sì	sì
Aggiornamento del software e spazio di conservazione dei log della sonda	-	-	sì

6.2 Durante i 36 mesi nessuna funzione richiesta può essere limitata o subordinata all'acquisto di licenze ulteriori.

6.3 Le licenze e le sottoscrizioni sono rese disponibili e visualizzabili dagli account della Stazione Appaltante. Il fornitore consegna, all'atto della fornitura, i codici di licenza, le chiavi di attivazione e i seriali, e indica per ciascuna voce della tabella il costo del rinnovo annuale alla scadenza, a titolo informativo.

7 - SERVIZI RICHIESTI

Tutti i servizi di cui al presente articolo sono compresi nel prezzo. Il fornitore li descrive nell'offerta tecnica indicando metodologia, tempi e risultati attesi.

Preanalisi e installazione comportano complessivamente un impegno non inferiore a 20 giornate lavorative, di cui almeno 10 da remoto per l'analisi e la redazione del report e almeno 10 in sede. Il fornitore ripartisce le giornate in sede tra la preanalisi e l'installazione e indica la ripartizione nell'offerta tecnica; resta fermo l'obbligo di presenza in sede durante le finestre di cut-over. Le giornate sono anche non consecutive, secondo un calendario concordato con l'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali, e si intendono di 8 ore.

Il progetto si articola nelle fasi seguenti:

Fase	Risultato
Preanalisi	Report sulla configurazione esistente e piano di migrazione delle policy
Installazione e configurazione	Apparati installati, cluster in alta affidabilità, integrazioni attive, configurazione delle policy
Test prima del cut-over	Esito positivo dei test concordati
Migrazione e cut-over	Configurazione migrata e verifica di equivalenza
Presidio in sede	presenza fino al superamento delle criticità emerse dopo la migrazione, e comunque non inferiore a 5 giorni lavorativi consecutivi
Formazione e documentazione	Manuale operativo e documentazione as-built

Nessuna fase può iniziare senza l'approvazione della fase precedente da parte dell'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali. Fa eccezione la preanalisi, che ha inizio alla stipula del contratto e si svolge in parallelo alla consegna degli apparati, al fine di rispettare i tempi di cui all'articolo 8.

Copia dell'originale conservato presso la Pubblica Amministrazione (Art.85sexies,co.2-4,D156/05 smi)

Interna: AOO AOO-02, N. Prot. 00109303 del 10/11/2026

7.1 Preanalisi

La preanalisi inizia alla stipula del contratto, senza attendere la consegna degli apparati, con accesso agli apparati e alla configurazione. Le giornate sono ripartite come previsto dall'introduzione del presente articolo; la preanalisi si conclude con la consegna del report approvato dell'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali.
Il fornitore consegna un report contenente:

- L'inventario della configurazione esistente, con riferimento a regole, NAT, oggetti, VPN, routing, VLAN e utenti;
- La corrispondenza regola per regola tra la configurazione Forcepoint in uso e il nuovo sistema, con indicazione di quelle non convertibili e della relativa motivazione;
- L'analisi delle integrazioni con Active Directory e SIEM;
- L'elenco delle regole obsolete, duplicate o non utilizzate, con proposta di razionalizzazione;
- La verifica del dimensionamento rispetto al traffico rilevato;
- I rischi individuati e le relative misure di mitigazione;
- Il piano di migrazione, con tempi, responsabilità e finestre di intervento.

Il report è illustrato in una riunione di condivisione ed è approvato dell'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali.

7.2 Installazione e configurazione

Il fornitore installa i quattro apparati NGFW e la sonda, configura i due cluster in alta affidabilità, imposta policy, NAT, VPN, routing e profili di sicurezza, attiva le integrazioni con Active Directory e SIEM, verifica che la sonda riceva i log da tutti i nodi, verifica che le licenze e le sottoscrizioni corrispondano alla tabella dell'articolo 6 e consegna le credenziali amministrative all'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali.

7.3 Test prima del cut-over

Prima del passaggio in produzione il fornitore esegue i test concordati, che comprendono almeno:

- Conversione delle regole e degli oggetti, con confronto dei conteggi;
- Funzionamento dei servizi critici e delle applicazioni soggette a policy specifiche;
- VPN site-to-site e accessi remoti con autenticazione degli utenti;
- Commutazione automatica, con simulazione del guasto di un nodo;
- Invio dei log al SIEM;
- Prestazioni, ove misurabili.

Il cut-over è ammesso quando tutti i test concordati hanno esito positivo. I difetti che impediscono l'esercizio di una funzione richiesta o compromettono la sicurezza impediscono il passaggio in produzione; i difetti di gravità inferiore sono eliminati entro 15 giorni dalla messa in esercizio.

7.4 Migrazione e cut-over

La migrazione avviene in due finestre distinte, una per il perimetro esterno e una per il perimetro interno, secondo il piano approvato dall'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali. La migrazione comprende la conversione delle regole, degli oggetti, delle regole NAT, delle VPN e delle policy di sicurezza dal firewall Forcepoint in uso. Al fine di minimizzare il fermo dei servizi, la migrazione potrà essere programmata in orari notturni, festivi o prefestivi.
Sono richiesti i seguenti requisiti:

Copia dell'originale conservato presso la Pubblica Amministrazione (Art.85sexies,co.2-4,D156/05 smi)

Interna: AOO AOO-02, N. Prot. 00109303 del 10/11/2026

- il giorno dello spegnimento del vecchio firewall il nuovo sistema deve essere pienamente funzionante, collaudato e in grado di svolgere tutte le funzioni oggetto della fornitura; il vecchio sistema non può essere spento in presenza di difetti aperti o di funzioni non operative;
- la sostituzione deve risultare trasparente, senza modifiche sui client, senza interruzioni dei servizi e con continuità delle VPN;
- al termine deve essere prodotta la verifica di equivalenza tra configurazione di partenza e configurazione migrata;
- il vecchio sistema resta disponibile per 30 giorni quale ulteriore possibilità di ripristino;
- il rollback deve essere eseguibile in ogni momento della finestra, con competenze e accessi disponibili in sede.
- il vecchio apparato di raccolta dei log può essere spento solo dopo che la sonda riceve correttamente i log dei quattro nodi e li inoltra al SIEM.

Il rollback si attiva qualora, durante la finestra, servizi critici risultino non disponibili, le VPN non funzionino, le policy di sicurezza non vengano applicate o si perda la connettività verso sedi o servizi.

7.5 Assistenza post-migrazione

Dopo la messa in esercizio il fornitore garantisce:

- presenza in sede fino al superamento delle criticità emerse dopo la migrazione, e comunque non inferiore a 5 giorni lavorativi consecutivi, negli orari di servizio, con un tecnico in grado di intervenire autonomamente sulla configurazione;
- analisi giornaliera dei log e ottimizzazione delle policy;
- report giornaliero con gli interventi eseguiti e i problemi aperti;
- una riunione di punto quotidiana con il referente dell'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali;
- assistenza prioritaria per i primi 60 giorni dalla messa in esercizio, con canale diretto dedicato e presa in carico entro 1 ora lavorativa per le criticità bloccanti;
- un referente tecnico nominato, con recapiti diretti.
- Il servizio di supporto è garantito per 12 mesi dalla data del collaudo, senza interruzioni.

7.6 Formazione e documentazione

Il fornitore eroga 2 giornate di formazione a almeno 8 tecnici, prima del collaudo, con una parte esercitativa sulle procedure di emergenza.
Al termine delle attività consegna la documentazione as-built, l'elenco delle regole migrate con la corrispondenza rispetto alla configurazione di partenza, il manuale operativo, le procedure di backup e ripristino e l'attestazione dei test eseguiti.

7.7 Aggiornamenti del firmware

Gli aggiornamenti del firmware sono eseguiti dal fornitore previa comunicazione all'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali e in una finestra concordata, un nodo alla volta e mantenendo la continuità del servizio. Prima dell'aggiornamento il fornitore verifica la compatibilità, predispone il backup della configurazione e informa l'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali dei rischi e delle modalità di ripristino.
Qualora l'aggiornamento provochi malfunzionamenti, il fornitore ripristina la versione precedente e la configurazione salvata entro i tempi di intervento previsti per le criticità bloccanti.

Copia dell'originale conservato presso la Pubblica Amministrazione (Art.85sexies,co.2-4,D156/05 smi)

Interna: AOO AOO-02, N. Prot. 00109303 del 10/11/2026

8 - TEMPI DI ESECUZIONE

Attività	Termine
Consegna dell'hardware	30 giorni dalla data dell'ordine
Conclusione di installazione, migrazione e collaudo	entro il 31 marzo 2027
Spegnimento del vecchio firewall	entro il 31 marzo 2027, a nuovo sistema pienamente funzionante

Il fornitore avvia la preanalisi alla stipula del contratto, in parallelo alla consegna degli apparati, secondo l'articolo 7.1. Le finestre di cut-over sono proposte dal fornitore e approvate dall'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali.
Il termine del 31 marzo 2027 è essenziale. Il suo mancato rispetto costituisce inadempimento grave, comporta una penale pari all'1 per cento del valore del contratto per ogni giorno di sforamento del termine e legittima la Stazione Appaltante alla risoluzione del contratto. La penale è dovuta fino a un massimo del 25 per cento del valore del contratto.

9 - SUPPORTO TECNICO E LIVELLI DI SERVIZIO

9.1 Modalità operative

Il servizio di supporto è garantito per 12 mesi dalla data del collaudo, senza interruzioni.
Il servizio si integra nel processo di Incident & Service Request Management dell'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali ed è articolato su due livelli:

- primo livello: U.O. Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali, che raccoglie la segnalazione e apre la richiesta;
- secondo livello: supporto specialistico del fornitore, da remoto e, ove necessario, in sede.

Il fornitore descrive nell'offerta il modello di assistenza proposto, indicando canali, orari, procedura di escalation, referenti, tempi e reportistica periodica. L'assistenza è erogata preferibilmente in lingua italiana.
Le richieste di assistenza al supporto del produttore fanno capo all'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali. Il fornitore la affianca nella loro gestione: la assiste nella compilazione e nell'inoltro e, quando l'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali glielo deleghi, apre e segue le richieste per suo conto, nell'ambito del servizio di cui al presente articolo. Per le richieste delegate il fornitore comunica il riferimento assegnato dal produttore e lo stato di avanzamento entro un giorno lavorativo dall'apertura e ne cura il tracciamento fino alla chiusura. Resta ferma la facoltà dell'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali di aprire direttamente le richieste tramite gli account di cui all'articolo 6.5.

9.2 Tempi di intervento e livelli di servizio

Per le criticità bloccanti delle attività gli interventi devono essere garantiti:

- presa in carico entro 1 ora lavorativa dall'apertura del ticket o dalla chiamata;
- intervento da remoto entro 2 ore lavorative dalla presa in carico;
- intervento in sede entro 8 ore lavorative dalla presa in carico.

Sono considerate criticità bloccanti l'indisponibilità del firewall, il guasto di un nodo con perdita della ridondanza, l'interruzione delle VPN e la mancata applicazione delle policy di sicurezza.
Verranno applicate le seguenti penali in caso di superamento degli SLA:

- per ritardo sino a 3 ore, pari allo 0,5 per cento del valore del contratto;

Copia dell'originale conservato presso la Pubblica Amministrazione (Art.85sexies,co.2-4,D156/05 smi)

Interna: AOO AOO-02, N. Prot. 00109303 del 10/11/2026

- per ritardo superiore a 3 ore, pari all'1 per cento del valore del contratto.

Per le criticità non bloccanti gli interventi saranno garantiti in modalità best-effort.
Le ore indicate si intendono lavorative, secondo l'orario di apertura dell'Ufficio.

9.3 Sostituzione dell'hardware

In caso di guasto hardware non risolvibile da remoto, il fornitore provvede alla sostituzione dell'apparato entro 3 (tre) giorni lavorativi dalla presa in carico della richiesta. L'obbligo si applica per l'intera durata del servizio di cui all'articolo 9.1.
La sostituzione avviene senza oneri per la Stazione Appaltante, nell'ambito del supporto del produttore compreso nella fornitura ai sensi dell'articolo 6.1. Il termine comprende il trasporto e la messa in servizio dell'apparato sostitutivo, che deve avere caratteristiche non inferiori a quelle dell'apparato guasto ed essere riconsegnato con la configurazione ripristinata.
Nell'offerta tecnica il fornitore indica il tempo di sostituzione proposto. Un tempo inferiore a 3 giorni lavorativi costituisce elemento di valutazione della qualità dell'offerta e non requisito di ammissione.
Resta ferma la facoltà della Stazione Appaltante di risolvere il contratto in caso di inadempimenti reiterati, secondo quanto previsto dal capitolato generale.

10 – COLLAUDO

Il collaudo è eseguito dalla Stazione Appaltante con la partecipazione del fornitore e accerta la piena rispondenza della fornitura ai requisiti del presente capitolato e dell'offerta.
Il fornitore produce il piano di collaudo, con i casi di test, e lo sottopone all'approvazione della Stazione Appaltante.
Non sono previste prove strumentali di throughput: i valori prestazionali si verificano sui datasheet ufficiali del produttore.
L'esito del collaudo è formalizzato in un verbale firmato da entrambe le parti. Il collaudo si intende superato quando tutte le verifiche hanno esito positivo; in caso di esito negativo il fornitore elimina le difformità entro 15 giorni e comunque non oltre il 31 marzo 2027.

11 - REQUISITI DEL FORNITORE

11.1 Requisiti di ammissione

Il fornitore deve dimostrare:

- Esperienza comprovata in sicurezza informatica;
- Esperienza su sistemi firewall o NGFW;
- Personale certificato sulla tecnologia offerta;
- Certificazioni tecniche del produttore sulla tecnologia offerta;
- La disponibilità di un referente tecnico dedicato per tutta la durata delle attività;
- La capacità di erogare l'assistenza in lingua italiana.

Il fornitore allega i curricula delle risorse impiegate.

11.2 Installazioni dichiarate

Nell'offerta tecnica il fornitore allega l'elenco delle installazioni realizzate negli ultimi cinque anni, con gli elementi necessari alla loro valutazione.
Il numero e la rilevanza delle installazioni analoghe costituiscono elemento di valutazione dell'offerta tecnica, secondo i criteri e i punteggi di cui all'Allegato C.
La Stazione Appaltante si riserva di verificare le installazioni dichiarate.

Copia dell'originale conservato presso la Pubblica Amministrazione (Art.85sexies,co.2-4,D156/05 smi)

12 – RINVIO

Per quanto non previsto dal presente capitolato e dagli atti di gara si rinvia al Capitolato Generale d'Appalto e alla normativa vigente in materia.

Nomina del Direttore dell'esecuzione

Divenuta efficace la delibera di aggiudicazione, a seguito del controllo preventivo di legittimità da parte del competente organo di controllo, la Stazione Appaltante nominerà il Direttore dell'esecuzione, in conformità a quanto previsto all'articolo 30, comma 2, del Decreto Delegato n. 26/2015 e successive modifiche. Nel contratto sarà indicato il nominativo ed il recapito del Direttore dell'esecuzione.

Interna: AOO AOO-02, N. Prot. 00109303 del 10/11/2026

REPUBBLICA DI SAN MARINO
Via 28 Luglio, 192 - 47893 Borgo Maggiore
T +378 (0549) 885150
Mail: info.informatica@pa.sm