**ALLEGATO "A"**

# CAPITOLATO SPECIALE
# PER LA FORNITURA DI SERVIZI DI MANUTENZIONE, LICENZE E SUPPORTO SPECIALISTICO AI SISTEMI DI SICUREZZA E ALL'INFRASTRUTTURA DI RETE DELLA PUBBLICA AMMINISTRAZIONE DELLA REPUBBLICA DI SAN MARINO

## Oggetto

La presente Asta Pubblica, costituita da **n. 3 lotti funzionali**, ha per oggetto la fornitura dei servizi di manutenzione, rinnovo licenze software, supporto specialistico e assistenza tecnica relativi ai sistemi di sicurezza informatica e agli apparati di rete installati nella rete dati della Pubblica Amministrazione della Repubblica di San Marino.

I lotti previsti sono:

- **Lotto 1 – Manutenzione e licenze sistemi Firewall Forcepoint**
- **Lotto 2 – Manutenzione e licenze apparati di rete Extreme Networks / Enterasys e sistema NAC**
- **Lotto 3 – Manutenzione, licenze e supporto specialistico piattaforma SIEM SGBox**

La durata dei servizi richiesti è pari a **12 (dodici) mesi**, con decorrenza dal **01 aprile 2026 al 31 marzo 2027**.

## 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

## LOTTO 1 – MANUTENZIONE E LICENZE SISTEMI FIREWALL FORCEPOINT

### Oggetto del lotto

Il lotto riguarda il servizio di manutenzione hardware e software dei sistemi di sicurezza firewall e gateway installati presso la rete dati della Pubblica Amministrazione.
Il supporto ufficiale dei prodotti è fornito dal costruttore **Forcepoint**.
Il servizio ha come obiettivo la correzione e l'eliminazione di guasti o malfunzionamenti garantendo la continuità operativa dei sistemi di sicurezza perimetrale, nonché in caso di guasti hardware, la sostituzione degli apparati o componenti.
Il servizio ha durata pari a **12 (dodici) mesi**, con decorrenza dal **01 aprile 2026 al 31 marzo 2027**.

### Servizi richiesti

Il servizio dovrà comprendere:

- Interventi tecnici per la risoluzione di guasti o malfunzionamenti;
- Eventuale sostituzione di componenti difettosi;
- Aggiornamenti software e firmware rilasciati dal produttore;
- Supporto remoto tramite connessione sicura;
- Attività preventive;
- Personalizzazione e aggiornamento delle policy di sicurezza;
- Interfacciarsi con Forcepoint per supporto software e hardware (sostituzione apparati guasti) forniti dal Vendor.

### Apparati attualmente installati

| Codice | Descrizione | Q.tà | Start | End |
|---|---|---|---|---|
| N2101 | Forcepoint NGFW 211 Appliance | 4 | 01.04.2026 | 31.03.2027 |
| ACPA2200 | AC Power Supply | 4 | 01.04.2026 | 31.03.2027 |
| N2101 | Forcepoint Sonda | 1 | 01.04.2026 | 31.03.2027 |
| ESESPT | Essential Support | 1 | 01.04.2026 | 31.03.2027 |
| SMC | NGFW Management Center | 5 | 01.04.2026 | 31.03.2027 |

### Supporto specialistico

Gli strumenti installati di diagnostica ed eventi producono documentazione complessa che necessita di un'accurata analisi fatta possibilmente da più esperti per evitare situazioni di saturazioni di banda trasmissiva o, peggio ancora, blocchi di trasmissioni causate da ritardi sui tempi di risposta tra applicativi.

Per questo viene richiesto un supporto specialistico qualificato da effettuarsi indispensabilmente con il personale responsabile dell'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali per:

- Analisi eventi di sicurezza;
- Tuning configurazioni;
- Verifica policy;
- Prevenzione attacchi informatici.

**Servizi previsti**

| Servizio | Giornate |
|---|---|
| Supporto remoto a chiamata, anche a frazione di ore se da remoto, o minimo ½ giornata se on site, comprensiva di:<br>- Servizio specialistico da remoto a chiamata da lunedì a venerdì;<br>- Presa in carico del problema;<br>- Intervento da remoto;<br>- Intervento on site. | 3 gg |
| Intervento periodico programmato, da concordare con il responsabile dell'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali per:<br>- Analisi verifica;<br>- Tuning;<br>- Report mensili ed eventualmente modifica o aggiornamento delle policy di governo della sicurezza informatica. | 6 gg |

**Modalità operative**

Il servizio si integra nel processo di Incident & Service Request Management della Stazione Appaltante.

- Primo livello: Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali
- Secondo livello: Supporto specialistico remoto.

**Tempi di intervento, SLA**

Per criticità bloccanti delle attività gli interventi dovranno 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 on-site entro **8 ore lavorative** dalla presa in carico.

Verranno applicate le seguenti penali in caso di superamento degli SLA:
per ritardo sino alle 3 ore, pari allo 0,5% del valore del lotto;
per ritardo superiore alle 3 ore, pari all'1% del valore del lotto;
per criticità non bloccanti, gli interventi saranno garantiti in modalità Best-Effort.

Orario servizio:
Lunedì – Venerdì
08:30 – 17:30
(esclusi festivi)

**Requisiti del fornitore**

Il fornitore dovrà dimostrare:

- Esperienza comprovata in cyber security;
- Certificazioni vendor;
- Personale certificato;
- Esperienza su Firewall.

Dovranno essere forniti i CV delle risorse.

**Requisiti mandatori**

- Sede operativa a San Marino o in Italia;
- Lingua italiana;
- Certificazioni tecniche vendor.

## LOTTO 2 - MANUTENZIONE E LICENZE APPARATI DI RETE EXTREME NETWORKS / ENTERASYS E SISTEMA NAC

**Oggetto del lotto**

Servizio di manutenzione TAC&OS e licenze Platform ONE, rinnovo licenze e supporto degli apparati di rete core, distribuzione e accesso della rete della Pubblica Amministrazione.
Il servizio ha come obiettivo la correzione e l'eliminazione di guasti o malfunzionamenti garantendo la continuità operativa dei sistemi si rete nonché in caso di guasti hardware, la sostituzione degli apparati o sue componenti.
Il servizio ha durata pari a **12 (dodici) mesi**, con decorrenza dal **01 aprile 2026 al 31 marzo 2027**.

**Apparati soggetti a manutenzione TAC&OS**

| Modello | Q.tà |
|---|---|
| VSP-7400-48Y-8C | 6 |
| X435-24P-4S | 18 |
| X435-8T-4S | 19 |
| 4220-24T | 1 |
| 5320-24T-8XE-SwitchEngine | 9 |
| 5320-48T-8XE-SwitchEngine | 20 |
| 5420F-48P-4XE-SwitchEngine | 5 |

**Licenze Platform One (ExtremeCloud IQ)**

Applicato solo per apparati che possono supportare licenze TAC&OS

| Tipologia Apparato | Q.tà | Licenza |
|---|---|---|
| Licenze XIQ | | |
| XIQ-SE | 1 | Tier A (EP1-STD-TA-S-C) |
| NAC | 2 | Tier A (EP1-STD-TA-S-C) |
| Analytics | 1 | Tier A (EP1-STD-TA-S-C) |
| | | |
| AP305C | 141 | Tier A (EP1-STD-TA-S-C) |
| | | |
| A-Series | 1 | Pilot |
| B-Series | 65 | Pilot |
| C-Series | 4 | Pilot |
| S-Series | 4 | Pilot |
| Summit Series (x435) | 37 | Tier A (EP1-STD-TA-S-C) |
| Universal Switch Engine 5320 / 4220 | 30 | Tier A (EP1-STD-TA-S-C) |
| Universal Switch Engine 5420 | 13 | Tier B (EP1-STD-TB-S-C) |
| Universal Switch Fabric Engine 5420 | 4 | Tier B (EP1-STD-TB-S-C) |
| Universal Switch Fabric Engine 5520 | 1 | Tier C (EP1-STD-TC-S-C) |
| VSP-7400-48Y-8C | 6 | Tier D (EP1-STD-TD-S-C) |
| | | |
| Wireless Controller | 2 | Navigator |
| AP Identify | 38 | Navigator |
| | | |
| D2, 800, V2 | 173 | Navigator |

Comprensivo di:

- 2000 licenze NAC da rinnovare.

**Servizi richiesti**

- Aggiornamenti OS;
- Supporto vendor TAC;
- Troubleshooting avanzato;
- Supporto configurazioni rete;
- Integrazione NAC;
- Supporto tramite una connessione remota in modalità sicura per un supporto anche preventivo
- Intervento tecnico di 2° livello entro i termini riportati per la correzione/eliminazione di guasti o malfunzionamenti tramite sostituzione della parte difettosa.

**Supporto specialistico**

Servizi specialistici richiesti come personalizzazione nell'ambito NAC (Network Access Control), sicurezza informatica che controlla l'accesso alle reti aziendali verificando l'identità di utenti e dispositivi (compliance) prima di concedere l'accesso, garantendo che solo dispositivi conformi e autorizzati entrino, bloccando gli accessi non autorizzati.

| Servizio | Giornate |
|---|---|
| Supporto remoto a chiamata, anche a frazione di ore se da remoto, o minimo ½ giornata se on site, comprensiva di:<br>- Intervento tecnico per la correzione /eliminazione di guasti o malfunzionamenti;<br>- Eventuali aggiornamenti software, qualora resi disponibili dal produttore;<br>- Supporto tramite una connessione remota in modalità sicura. | 6 gg |

**Modalità operative**

Il servizio si integra nel processo di Incident & Service Request Management della Stazione Appaltante.

- Primo livello: Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali
- Secondo livello: Supporto specialistico remoto.

Il fornitore dovrà inoltre interfacciarsi direttamente con il vendor per eventuali sostituzioni hardware.

**Tempi di intervento, SLA**

Per criticità bloccanti delle attività gli interventi dovranno 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 on-site entro **8 ore lavorative** dalla presa in carico.

Verranno applicate le seguenti penali in caso di superamento degli SLA:
per ritardo sino alle 3 ore, pari allo 0,5% del valore del lotto;
per ritardo superiore alle 3 ore, pari all'1% del valore del lotto;
per criticità non bloccanti, gli interventi saranno garantiti in modalità Best-Effort.

Orario servizio:
Lunedì – Venerdì
08:30 – 17:30
(esclusi festivi)

**Requisiti del fornitore**

Il fornitore dovrà dimostrare:

- Esperienza comprovata in networking;
- Certificazioni vendor;
- Personale certificato;
- Esperienza su NAC.

Dovranno essere forniti i CV delle risorse.

**Requisiti mandatori**

- Sede operativa a San Marino o in Italia;
- Lingua italiana;
- Certificazioni tecniche vendor.

# LOTTO 3 – MANUTENZIONE, LICENZE E SUPPORTO SPECIALISTICO PIATTAFORMA SIEM SGBOX

### Oggetto del lotto

Fornitura, manutenzione licenze e supporto specialistico della piattaforma SGBox Next Generation SIEM & SOAR.

Particolare attenzione è richiesta per:

- Gestione correlazione eventi;
- Analisi sicurezza;
- Compliance normativa.

Il servizio ha durata pari a **12 (dodici) mesi**, con decorrenza dal **01 aprile 2026 al 31 marzo 2027**.

### Licenze

| Prodotto | Codice | Descrizione | Q.tà |
|---|---|---|---|
| SGBox Premium | PM200-1N | Subscription 200 IP | 1 |
| Change Management | PM200-CM-1N | Subscription | 1 |
| Start-up | PM200-STP | Attivazione remota | 1 |

### Servizi richiesti

- Ottimizzazione del software SIEM SGBOX con predisposizione invio allarmi e accessi;
- Intervento tecnico per la correzione/eliminazione degli errori o malfunzionamenti tramite l'invio di aggiornamenti o reinstallazione del software;
- Tuning regole correlazione;
- Gestione allarmi;
- Upgrade software;
- Supporto incident response;
- Report compliance GDPR, ISO27001, PCI DSS;
- Formazione.

### Funzionalità minime richieste

- Log Management avanzato
- Event Correlation Engine
- SOAR
- Incident Management

### Servizi previsti

| Servizio | Giornate |
|---|---|
| Supporto remoto a chiamata, anche a frazione di ore se da remoto, o minimo ½ giornata se on site, comprensiva di:<br>- Interventi specialistici per gestione di guasti e malfunzionamenti.<br>- Interventi specialistici per gestione eventi di correlazione. | 6 gg |

| Servizio | Giornate |
|---|---|
| - Interventi specialistici per il coordinamento con il SOC esterno. | |

**Modalità operative**

Il servizio si integra nel processo di Incident & Service Request Management della Stazione Appaltante.

- Primo livello: Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali
- Secondo livello: Supporto specialistico remoto.

Il fornitore dovrà inoltre interfacciarsi direttamente con il vendor per eventuali sostituzioni hardware.

**Tempi di intervento, SLA**

Per criticità bloccanti delle attività gli interventi dovranno 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 on-site entro **8 ore lavorative** dalla presa in carico.

Verranno applicate le seguenti penali in caso di superamento degli SLA:
per ritardo sino alle 3 ore, pari allo 0,5% del valore del lotto;
per ritardo superiore alle 3 ore, pari all'1% del valore del lotto;
per criticità non bloccanti, gli interventi saranno garantiti in modalità Best-Effort.

Orario servizio:
Lunedì – Venerdì
08:30 – 17:30
(esclusi festivi)

**Requisiti del fornitore**

Il fornitore dovrà dimostrare:

- Esperienza comprovata in cybersecurity;
- Certificazioni vendor;
- Personale certificato;
- Esperienza comprovata su SIEM SGBox.

Dovranno essere forniti i CV delle risorse.

**Requisiti mandatori**

- Sede operativa a San Marino o in Italia;
- Lingua italiana;
- Certificazioni tecniche vendor.

**Requisiti**

Le aziende partecipanti al presente bando d'asta dovranno dimostrare di avere esperienza nella fornitura di prodotti e servizi analoghi.

**Modalità e tempi di consegna**

La Stazione Appaltante si riserva, a suo insindacabile giudizio, il diritto di non procedere all'effettiva aggiudicazione, anche a seguito dell'emissione del presente bando.
Pertanto la presente richiesta di preventivo NON comporta alcun impegno da parte della Stazione Appaltante e non sorgeranno nei partecipanti diritti di sorta fino a quando l'eventuale aggiudicazione non sia stata deliberata con formale provvedimento della Stazione Appaltante, reso esecutivo a norma di legge e firmato il relativo contratto.

Le attività comprenderanno dove previsto:

- Analisi preliminare;
- Pianificazione;
- Configurazione sistemi;
- Test e collaudo;
- Formazione;
- Documentazione tecnica.

Il servizio di Supporto Specialistico Remoto specifico di ogni lotto, si integrerà nell'attuale processo complessivo di incident & service request management che provvederà a gestire un eventuale tiket aperto del I° livello.
Ad effettuare una prima analisi del malfunzionamento saranno i tecnici dell'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali di San Marino che successivamente apriranno un ticket per un'analisi al II° livello con il Supporto Specialistico Remoto, oggetto dell'appalto.
Il supporto specialistico remoto a sua volta prenderà in carico il problema collegandosi, qualora sia possibile, oppure on site presso la sede dell'Ufficio Informatica, Sicurezza, Reti e Protezione dei Dati Personali di San Marino risolvendo il problema in maniera risolutiva o mediante workaround.

Con riferimento alla sostituzione di apparati e/o componenti guasti, sarà altresì cura del supporto specialistico remoto interfacciarsi con il Vendor al fine di richiedere, ottenere e consegnare l'eventuale sostituzione dell'apparato.

**Orario di lavoro**

Gli orari degli interventi dovranno essere concordati con il Direttore dell'esecuzione.

**Interferenze con altre imprese**

L'Impresa Appaltatrice dovrà prendere atto che durante il servizio potrà incontrarsi con altre ditte, di conseguenza, s'impegna a condurre i propri lavori in armonia con le esigenze delle anzidette ditte, senza recare intralcio ed evitando contestazioni pregiudizievoli per l'andamento generale dei lavori. Resta inteso che per le accennate interferenze e per gli oneri conseguenti, l'Impresa Appaltatrice non potrà accampare nessuna pretesa, richiesta di compenso o richiesta di proroga. In caso di divergenza, l'Impresa Appaltatrice s'impegna ad accettare ed osservare le disposizioni e decisioni che il Direttore dell'esecuzione, a suo insindacabile giudizio, riterrà opportuno prendere, tenendo presente il migliore andamento dei lavori, salvo esporre le proprie riserve.

**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.