# ALLEGATO 4

# CAPITOLATO TECNICO

*INDICE*

## 1 OGGETTO

Il presente Capitolato tecnico ha lo scopo di definire le specifiche tecniche ed i requisiti minimi relativi ai seguenti beni e servizi da acquisire:

a) manutenzione e supporto tecnico per i Sottosistemi di Sicurezza di proprietà del Ministero dell'Economia e delle Finanze ubicati nelle diverse sedi romane e nel CED di Latina;
b) rinnovo Software Subscription dei Sottosistemi di Sicurezza di proprietà del Ministero dell'Economia e delle Finanze, ubicati nelle diverse sedi romane e nel CED di Latina;
c) consulenza e supporto specialistico, a richiesta, per un totale massimo fruibile di 200 gg/persona.

Per l'erogazione dei servizi oggetto del presente capitolato tecnico, l'Impresa dovrà definire le seguenti figure professionali:

- **Responsabile del Contratto**, ha la responsabilità di gestire e risolvere tutte le problematiche legate al corretto svolgimento del contratto (es: fatturazione, verifica del rispetto dei livelli di servizio, definizione e aggiornamento del Team di manutenzione – di cui al successivo paragrafo 3.1), nonché delle eventuali variazioni dell'elenco dei sottosistemi in manutenzione;

- **Responsabile tecnico per l'erogazione dei servizi**, ha la responsabilità di coordinare dal punto di vista operativo tutte le attività legate ai servizi oggetto del presente capitolato tecnico, e di essere il punto di riferimento per l'attivazione del servizio di supporto specialistico (di cui al successivo capitolo 3).

L'Impresa dovrà comunicare alla Committente il numero di telefono e l'e-mail con le quali contattare tali figure professionali, il cui ruolo potrà essere assunto anche dalla medesima persona.

Le prestazioni oggetto del presente capitolato dovranno essere erogate nei locali delle sedi del MEF situate all'interno dei comuni di Roma e Latina, a titolo esemplificativo ma non esaustivo, si indicano di seguito i CED di primaria importanza:
- il Centro Comunicativo, ubicato in via Pastrengo, n. 1, Roma;
- nel CED della sede di La Rustica, ubicato in via A. Soldati, n. 80, Roma;
- nel CED della sede di Piazza Dalmazia, n. 1, Roma;
- nel CED ubicato in viale Nervi, Latina;
- nel CED ubicato in Via Mario Carucci, n. 99, Roma.

Nel corpo del capitolato, ai termini di cui appresso, viene attribuito il significato riportato a fianco di ciascuno di essi:

- ***Sottosistema***, l'insieme delle componenti hardware, software (di base ed applicativo), delle licenze e degli accessori (es. HUB/Switch per il collegamento di rete, Rack, Switch delle Consolle) che realizzano una specifica funzionalità di sicurezza (es. sicurezza perimetrale, AAA per accesso remoto, analisi del traffico);

- ***Sistema di Sicurezza***, l'insieme dei *Sottosistemi* installati presso le varie sedi del MEF e della Consip atti a realizzare l'infrastruttura di sicurezza;

- ***Committente***, la Sogei S.p.A.;

- ***Best Practices*****,** sono un insieme di raccomandazioni fornite da gruppi, enti, organizzazioni o produttori, riconosciuti dalla comunità tecnologica, per la corretta esecuzione di determinate attività, non solo dal punto di vista tecnico, ma anche sotto il profilo dell'esperienza d'uso;

- ***Dispositivi UTM, o "Unified Threat Management" (letteralmente: "gestione delle minacce unificata"),*** si occupano di effettuare molte tipologie di controlli sulla pericolosità e sul tipo

del traffico che si muove da e verso la rete. Per svolgere tale attività tipicamente combinano più funzionalità di sicurezza informatica (come ad esempio: firewall, IPS, antivirus, URL filtering, etc.) in uno stesso hardware;

- ***Sistema Blade*,** è composto da un blade server e da uno chassis. Un blade server è un server auto-contenuto pensato per minimizzare l'occupazione di spazio. Uno *chassis* per *blade server*, è il contenitore dei blade server che fornisce servizi come l'alimentazione, il raffreddamento, la rete e facilita la gestione centralizzata; uno chassis potrà anche contenere più blade server;

- ***SIEM (Security Information e Event Management)*,** centralizza, aggrega, normalizza e correla eventi eterogenei provenienti da diverse tipologie di sistemi/apparati. Effettua l'analisi in tempo reale dei log e degli eventi provenienti da sistemi di sicurezza ed apparati di rete, eventualmente anche sistemi operativi, data base e storage. Supporta la gestione delle minacce interne ed esterne all'organizzazione.

- ***Log management*,** fornisce l'archiviazione di eventi e flow, anche a lungo termine, con funzionalità di query. Supporta la gestione delle minacce interne e facilita il monitoraggio degli accessi alle risorse effettuati dalle utenze privilegiate, inoltre, facilita la compliance alle normative (es.: privacy).

- ***MEF e Amministrazione*:** Ministero dell'Economia e delle Finanze.

- ***Malfunzionamento*** si intende qualsiasi anomalia funzionale o fermo dei Sottosistemi che, direttamente o indirettamente, provochi l'interruzione, la non completa disponibilità del servizio all'utenza o il degrado delle prestazioni dei Sottosistemi stessi.
- ***Software Subscription***: si intendono tutti gli aggiornamenti relativi ai prodotti software installati sul Sistema di Sicurezza del MEF.

## 2 IL SERVIZIO DI MANUTENZIONE DEL SISTEMA DI SICUREZZA DEL MEF

Per razionalizzare e centralizzare il servizio di manutenzione dei sottosistemi di sicurezza del MEF, attualmente siti nelle varie sedi romane e nel CED di Latina, si è ritenuto opportuno bandire una gara europea per l'affidamento ad un unico gestore, del servizio di assistenza e manutenzione dei suddetti sottosistemi di sicurezza.
Tale servizio avrà efficacia triennale dal momento della "Dichiarazione di inizio del servizio" che sarà comunicata dalla Committente all'Impresa successivamente alla consegna della **documentazione di startup,** di cui al successivo paragrafo 3.2.

Per agevolare il compito dei fornitori nella valutazione del servizio da erogare, si è ritenuto opportuno descrivere i Sottosistemi di sicurezza attualmente installati aggregando i dati raccolti nella seguente tabella.

Il Sistema di Sicurezza del MEF è attualmente costituito dai seguenti Sottosistemi, la seguente tabella ha carattere puramente informativo e non esaustivo.

| Sede | Note |
|---|---|
| Via XX Settembre (RM) | 2 nodi appliance Checkpoint 12600 in HA, vers R75.20 |
| Via XX Settembre (RM) | 2 Nodi appliance Checkpoint 4607 in HA, vers R75.20 |
| Via XX Settembre (RM) | 2 Nodi appliance Checkpoint 4607 in HA, vers R75.20 |
| Via XX Settembre (RM) | 2 Nodi Juniper SSG 140 + SW in HA |
| Via XX Settembre (RM) | Firepass 4300 HF-70-7 |
| Via XX Settembre (RM) | 2 nodi Contivity 1010 + SW in HA |
| Via XXSett-Soldati (RM) | 2 Nodi Appliance RSA ACE Server in Fault Tolerance |
| Via XX Settembre (RM) | 10 IPS GX4004 + 10 sonde Host ISS + Enterprise Scanner ISS + Fusion Module + SP Application Gateway + DB |
| Via XX Settembre (RM) | 2 Nodi Appliance UTM 3077 in HA, vers R75.20 |
| Via XX Settembre (RM) | 2 Nodi Appliance UTM 3073 in HA, vers R75.20 |
| Via XX Settembre (RM) | 3 nodi McAfee WG 5500 Secure Gateway + WebReporter |
| Via XX Settembre (RM) | 2 HP DL 380 + DC + CA |
| Via XX Settembre (RM) | 2 nodi Cisco ASA 5510 in HA |
| Via XX Settembre (RM) | 3 nodi Palo Alto Next Generation Firewall PA-5020 + Panorama |
| Via XX Settembre (RM) | 2 Nodi appliance Checkpoint 4607 in HA, vers R75.20 |
| Via XX Settembre (RM) | 2 Nodi appliance Checkpoint 4607 in HA, vers R75.20 |
| Via XX Settembre (RM) | 2 nodi appliance Smart-1 50 in HA |
| Via XX Settembre (RM) | HP Proliant ML 570 SkyBox Firewall Assurance |
| Viale Nervi (LT) | 2 Nodi appliance Checkpoint 4607 in HA, vers R75.20 |
| Via XX Settembre (RM) | RSA Envision PowerEgde R710 |
| Via XX Settembre (RM) | 2 Nodi appliance Checkpoint 12400 in HA, vers R7520 |
| Via XX Settembre (RM) | 2 Nodi appliance Checkpoint 4607 in HA, vers R75.20 |
| Via XX Settembre (RM) | 2 Nodi UTM Checkpoint 572 in HA vers R75.20 |
| Via A.Soldati (RM) | 2 nodi appliance Checkpoint 12400 in HA, vers R75.40 – Gaia |

| | |
|---|---|
| Via A.Soldati (RM) | 2 Nodi appliance Checkpoint 4600 in HA, vers R75.40 - Gaia |
| Via A.Soldati (RM) | 1 Server di Management IBM system 3650 vers vers R75.40 – Gaia |
| Via A.Soldati (RM) | 2 HP WKS xw8200 |
| Via A.Soldati (RM) | Appliance Dell RSA Envision PowerEgde R710 |

Tabella 1

## 2.1 CLASSI DI MANUTENZIONE DEI SISTEMI DI SICUREZZA

Per semplificare sia l'offerta dei canoni di manutenzione, sia la gestione del servizio, disciplinato dal presente capitolato (garantendo flessibilità sul numero e le tipologie dei Sottosistemi che di volta in volta potranno essere inseriti o esclusi dal contratto), si sono definite le 22 seguenti classi di manutenzione.
Tali Classi sono applicabili a tutte le famiglie dei sottosistemi che implementano funzionalità per la sicurezza delle informazioni (fisica/logica/organizzativa), come ad esempio i firewall, gli antivirus, i software per il monitoraggio degli eventi e le piattaforme per la gestione del rischio.
Le 22 Classi vengono individuate attraverso la correlazione dei seguenti tre elementi:

1. la tipologia dell'hardware che costituisce il sottosistema (Host based, Appliance o Blade);
2. il numero di nodi che compongono il singolo sottosistema (l'enclosure è considerato un nodo; stesso criterio è utilizzato per la consolle del sottosistema qualora risieda su un hardware aggiuntivo);
3. fattore di complessità del sottosistema, (numero di funzionalità, anche chiamate blade software, attive sul sottosistema):
    - Fattore 1 = massimo 2 funzionalità (esempio: firewall + IPS);
    - Fattore 2 = più di 2 funzionalità.

Inoltre, nella definizione delle seguenti classi si è considerata anche la possibilità di attivare il servizio di manutenzione soltanto sulla componente software applicativa del sottosistema (funzionalità di sicurezza), conservando soltanto l'elemento 'fattore di complessità' (*Classe11* e *Classe22*).
Infine, in caso di attivazione del servizio di manutenzione (software e hardware) per sottosistemi residenti in ambienti virtualizzati, nel canone di manutenzione sarà compresa anche la manutenzione dell'ambiente di virtualizzazione (ad esempio VmWare).

La seguente tabella descrive le 22 Classi individuate da cui partire per la definizione dei canoni di manutenzione:

| Classi | Descrizione |
|---|---|
| ***Fattore di Complessità = 1*** | |
| *Classe1* | contiene apparati HOST BASED con nodi/guest da 1 a 4 |
| *Classe2* | contiene apparati HOST BASED con nodi/guest da 5 a 10 |
| *Classe3* | contiene apparati HOST BASED con nodi/guest da 11 a 20 |
| *Classe4* | contiene apparati APPLIANCE con nodi/guest da 1 a 4 |
| *Classe5* | contiene apparati APPLIANCE con nodi/guest da 5 a 10 |
| *Classe6* | contiene apparati APPLIANCE con nodi/guest da 11 a 20 |
| *Classe7* | contiene apparati APPLIANCE con nodi/guest superiori a 20 |
| *Classe8* | contiene apparati Blade con nodi/guest da 1 a 4 |
| *Classe9* | contiene apparati Blade con nodi/guest da 5 a 10 |
| *Classe10* | contiene apparati Blade con nodi/guest da 11 a 20 |
| *Classe11* | Solo manutenzione software applicativo dei sottosistemi |

| *Fattore di Complessità = 2* | |
|---|---|
| *Classe12* | contiene apparati HOST BASED con nodi/guest da 1 a 4 |
| *Classe13* | contiene apparati HOST BASED con nodi/guest da 5 a 10 |
| *Classe14* | contiene apparati HOST BASED con nodi/guest da 11 a 20 |
| *Classe15* | contiene apparati APPLIANCE con nodi/guest da 1 a 4 |
| *Classe16* | contiene apparati APPLIANCE con nodi/guest da 5 a 10 |
| *Classe17* | contiene apparati APPLIANCE con nodi/guest da 11 a 20 |
| *Classe18* | contiene apparati APPLIANCE con nodi/guest superiore a 20 |
| *Classe19* | contiene apparati Blade con nodi/guest da 1 a 4 |
| *Classe20* | contiene apparati Blade con nodi/guest da 5 a 10 |
| *Classe21* | contiene apparati Blade con nodi/guest da 11 a 20 |
| *Classe 22* | Solo manutenzione software applicativo dei sottosistemi |

Tabella 2

Combinando le **22 classi** sopra indicate con i due ulteriori parametri descritti di seguito, si arriva ad individuare i **132 canoni di manutenzione** (22 classi x 3 fasce di prodotto x 2 livelli di servizio) oggetto di offerta da parte del fornitore:

1. fascia di prodotto **HIGH, MEDIUM e LOW (H, M, L)** definita in base al throughput dell'apparato (vedi paragrafo 2.4);
2. livello di servizio **A** e **B** (vedi paragrafo 2.5).

A titolo esemplificativo, il canone con identificativo **1LA** è il canone relativo alla Classe **1**, fascia di prodotto **LOW** e livello di servizio **A.**

## 2.2 SERVIZIO DI MANUTENZIONE DEL SISTEMA DI SICUREZZA

Il servizio di manutenzione del Sistema di Sicurezza dovrà essere erogato sulle componenti hardware e software dei sottosistemi che lo compongono.
Tale servizio è suddiviso in due macro attività, la manutenzione preventiva e la manutenzione correttiva. Di seguito vengono descritti in maniera dettagliata i task da svolgere per ogni macro attività.
Sia per la manutenzione preventiva, sia per quella correttiva, per gli interventi per i quali si renderà necessaria la sostituzione di una o più parti, l'Impresa dovrà utilizzare parti di ricambio nuove, di primaria qualità, garantite dallo stesso costruttore del sottosistema; solo in caso di irreperibilità del ricambio originale per cessata produzione, è ammessa la fornitura di un ricambio commerciale di pari caratteristiche. Si richiede inoltre che l'Impresa garantisca la sostituzione di una parte guasta nei tempi di ripristino previsti dal presente capitolato, eventualmente anche predisponendo una scorta presso le sedi del MEF interessate dal servizio. Le parti sostituite verranno ritirate e smaltite dall'Impresa, ad eccezione delle componenti che contengono dati che rimarranno nella disponibilità della Committente, nel rispetto della normativa vigente in materia di smaltimento dei rifiuti.

### 2.2.1 MANUTENZIONE PREVENTIVA

L'Impresa si impegna a realizzare gli interventi tecnici (controlli, regolazioni, sostituzioni) finalizzati a ottimizzare il funzionamento dei Sottosistemi e prevenirne futuri malfunzionamenti; i tempi e le modalità degli interventi dovranno essere concordati con la Committente ed effettuati periodicamente, almeno una volta al mese.

La Manutenzione preventiva comprende altresì l'implementazione delle modifiche tecniche, consistenti in miglioramenti e/o aggiornamenti, al fine di elevare il grado di affidabilità del Sistema di Sicurezza del MEF, di migliorarne il funzionamento e di aumentare la sicurezza.

L'Impresa dovrà definire e consegnare alla Committente un **Piano tecnico di manutenzione preventiva**, sia hardware, sia software, per ogni Sottosistema di sicurezza oggetto del contratto, entro 20 giorni lavorativi dalla comunicazione da parte della Committente della messa in manutenzione del Sottosistema, pena l'applicazione delle penali di cui alla schema di contratto; tale piano dovrà essere verificato ed approvato dalla Committente.

In assenza del suddetto documento non può essere attivato il servizio.

Nel piano dovranno essere contenute tutte le indicazioni tecniche e procedurali indicate dal produttore del sottosistema stesso per la realizzazione della manutenzione a regola d'arte.
In ogni caso il suddetto piano dovrà contenere le "Best practices" indicate dalle normative vigenti per quanto riguarda la manutenzione di sistemi altamente tecnologici.

È a carico dell'Impresa l'aggiornamento e l'integrazione del piano di manutenzione, a fronte di nuove indicazioni dei produttori, della pubblicazione di nuove "Best practices" o di eventuali indicazioni della Committente.

Su richiesta della Committente, inoltrata al **Responsabile tecnico per l'erogazione dei servizi**, il **Piano tecnico di manutenzione preventiva** deve essere aggiornato entro e non oltre i successivi 30 giorni lavorativi, pena l'applicazione delle penali di cui alla schema di contratto.

Ogni aggiornamento e/o integrazione del **Piano tecnico di manutenzione preventiva** è sottoposto ad approvazione della Committente.

L'Impresa dovrà monitorare costantemente ed in maniera continuativa:
- il rilascio di aggiornamenti, di nuove versioni o correzioni (hardware, software di base, software applicativo e firmware) rilasciate dai produttori,
- le scadenze delle licenze dei prodotti software installati sui sottosistemi, lo stato di end of support (EoS) e lo stato di end of life (EoL) rilasciate dai produttori,

di tutti i componenti dei Sottosistemi di sicurezza oggetto del servizio di manutenzione e darne pronta segnalazione alla Committente entro un tempo massimo di 15 giorni lavorativi dalla data di rilascio/comunicazione delle stesse, pena l'applicazione delle penali di cui alla schema di contratto.

Inoltre, l'Impresa dovrà verificare e segnalare alla Committente, mediante un rapporto tecnico, la compatibilità e l'impatto tecnologico degli aggiornamenti, delle nuove versioni o delle correzioni con l'ambiente di esercizio, entro 15 giorni lavorativi dalla data della pubblicazione della notizia, da parte dei produttori, pena l'applicazione delle penali di cui alla schema di contratto. Tale rapporto tecnico dovrà essere validato dal vendor produttore della tecnologia oggetto di manutenzione.

Il rapporto tecnico sarà soggetto alla validazione da parte della Committente che, in caso di esito positivo, deciderà i tempi e le modalità di intervento che l'Impresa dovrà rispettare per rendere operative (installare, configurare e personalizzare) le modifiche segnalate, oppure di non procedere all'applicazione degli aggiornamenti segnalati.

In caso di esito negativo della valutazione del rapporto tecnico, segnalato a mezzo posta elettronica al Responsabile tecnico per l'erogazione dei servizi secondo le modalità di cui allo schema di Contratto, l'Impresa dovrà produrre un nuovo rapporto tecnico entro e non oltre 5 giorni lavorativi dalla data della segnalazione, pena l'applicazione delle penali di cui alla schema di contratto.

A fronte dell'acquisizione da parte della Committente di nuove versioni dei software dei Sottosistemi di sicurezza (sia di base, sia applicativo), finalizzata ad elevare il grado di affidabilità del Sistema, di migliorarne il funzionamento e di aumentarne la sicurezza, l'Impresa, su richiesta

della Committente, dovrà installare, configurare e personalizzare tale software.

Tutte le attività che verranno eseguite sui Sottosistemi oggetto della manutenzione preventiva dovranno essere prontamente registrati sui libri macchina dei sistemi informatici che li compongono.

Qualora, durante lo svolgimento della manutenzione preventiva l'Impresa riscontrasse dei malfunzionamenti dei Sottosistemi di sicurezza dovrà immediatamente comunicare tale evidenza alla Committente, pena l'applicazione delle penali di cui al contratto, che provvederà di conseguenza ad aprire una chiamata di manutenzione correttiva, di cui al successivo paragrafo 2.2.2.

### 2.2.2 MANUTENZIONE CORRETTIVA

L'Impresa dovrà fornire la manutenzione correttiva, ovvero dovrà provvedere alla riparazione dei guasti, blocchi o altri inconvenienti non bloccanti che dovessero verificarsi, anche se causati da parti del Sistema ridondate (ad esempio alimentatori), effettuando tutte le attività necessarie a garantire il ripristino del pieno funzionamento dei Sottosistemi di Sicurezza. Anche gli interventi su componenti ridondate saranno soggetta a Sla.

Le attività di manutenzione correttiva saranno rivolte a tutte le componenti del Sottosistema ed in particolare riguarderanno: componenti hardware, aggiornamenti software e configurazioni di sistema.
La manutenzione correttiva dovrà essere prestata nel rispetto dei livelli di servizio indicati nel successivo paragrafo 2.5.
Il servizio di manutenzione correttiva è a tutti gli effetti un'attività complementare alla manutenzione preventiva, a tal fine, il personale che sarà chiamato ad effettuare gli interventi di manutenzione correttiva dovrà essere perfettamente a conoscenza dello stato dei Sottosistemi e quindi delle attività svolte (aggiornamenti, modifiche, etc.) nell'ambito del servizio di manutenzione preventiva.

## 2.3 PRODOTTI IN END OF LIFE

Qualora gli aggiornamenti dei prodotti software installati sui Sottosistemi di Sicurezza del MEF comportino anche la sostituzione delle componenti hardware dei Sottosistemi stessi (esempio EoL del prodotto), su richiesta della Committente (nei limiti di valore di Euro 40.000,00) l'Impresa ha la facoltà di fornire il nuovo hardware necessario alla continuità dei servizi di sicurezza del MEF; la Committente ha la facoltà di acquisire tale hardware al valore del prezzo di listino pubblicato dal produttore, alla data della sostituzione, scontato almeno del 20%; resta salva la facoltà della Committente di acquisire diversamente l'HW necessario.
Resta fermo che la Committente è tenuta ad applicare i contratti in essere con altri fornitori ed eventuali Convenzioni Consip e Contratti Quadro aventi ad oggetto le medesime componenti hardware.

## 2.4 FASCIA DI PRODOTTO

Ai fini della definizione dei canoni di manutenzione, vengono identificate le seguenti fasce di prodotto:

- **HIGH (H)**: I sistemi/apparati che hanno un throughput superiore a 35Gbps;
- **MEDIUM (M)**: I sistemi/apparati che hanno un throughput compreso fra 10Gbps e 35Gbps;
- **LOW (L)**: I sistemi/apparati che hanno un throughput inferiore a 10Gbps.

## 2.5 LIVELLI DI SERVIZIO

Al servizio di manutenzione erogato sui singoli sottosistemi potranno essere associati i seguenti livelli di servizio:

| Livello di servizio | Giorni | Orario |
|---|---|---|
| **A** | 365 giorni all'anno | H24 |
| **B** | Dal lunedì al venerdì | 8:00 – 20:00 |
| | sabato | 8:00 – 13:00 |

Il livello di servizio assegnato ad un particolare sottosistema verrà definito dalla Committente e potrà essere modificato su sua richiesta in qualsiasi momento del periodo di efficacia del contratto.

A fronte di malfunzionamenti e/o guasti sui sottosistemi, l'Impresa dovrà garantire un servizio di manutenzione i cui livelli di servizio sono dettagliati nel seguito.

Se durante l'erogazione di tale servizio, non venissero rispettati i suddetti livelli di servizio, fermo restando l'applicazione delle penali, il Committente si riserva la facoltà, a suo insindacabile giudizio, di far intervenire una società terza per la risoluzione dei problemi e il riavvio dei servizi. Il costo sostenuto dal Committente verrà detratto dal canone dovuto al fornitore del servizio di manutenzione.

### 2.5.1 LIVELLO DI SERVIZIO DI TIPO A

Il servizio di manutenzione di tipo **A** dovrà essere erogato **7 giorni la settimana per 24 ore al giorno 365 giorni l'anno.**

Gli interventi effettuati dovranno eliminare gli inconvenienti che hanno determinato la richiesta di intervento e ripristinare le normali condizioni di funzionamento.

Gli eventuali workaround che verranno implementati nella fase iniziale dell'intervento al fine di mitigare gli effetti dell'anomalia, non comporteranno la chiusura del "problem".

Il servizio di manutenzione dovrà essere erogato con le seguenti caratteristiche:

*a)* supporto remoto di un tecnico qualificato (vedi paragrafo 3.1) entro 30 minuti solari dalla chiamata della Committente effettuata con le modalità di cui al successivo paragrafo 2.5.3;
*b)* intervento on-site, qualora il problema non sia risolvibile telefonicamente, entro un tempo massimo di 2 ore solari dalla chiamata della Committente;
*c)* il tempo globale di ripristino non dovrà comunque superare le 4 ore solari dalla chiamata della Committente;
*d)* l'Impresa si impegna in ogni caso a garantire che il Sistema di Sicurezza del MEF sia disponibile, e cioè correttamente funzionante in tutte le sue componenti, per una percentuale non inferiore al 99,86% dell'orario di erogazione del servizio di tipo A, calcolato su base trimestrale.

La violazione dei precedenti livelli di servizio comporterà l'applicazione delle penali contrattuali.

### 2.5.2 LIVELLO DI SERVIZIO DI TIPO B

Il servizio di manutenzione di tipo **B** dovrà essere erogato dal **lunedì al venerdì dalle ore 8.00 alle ore 20.00 ed il sabato dalle ore 8.00 alle ore 13.00** (esclusi domenica e festivi). Esso avrà le seguenti caratteristiche:

*a)* supporto remoto di un tecnico qualificato (vedi paragrafo 3.1) entro 30 minuti lavorativi dalla chiamata della Committente effettuata con le modalità di cui al successivo paragrafo 2.5.3;
*b)* intervento on-site, qualora il problema non sia risolvibile telefonicamente, entro un tempo massimo di 2 ore lavorative dalla chiamata della Committente;
*c)* il tempo globale di ripristino non dovrà comunque superare le 4 ore lavorative dalla chiamata della Committente;
*d)* l'Impresa si impegna in ogni caso a garantire che il Sistema di Sicurezza del MEF sia disponibile, ovvero correttamente funzionante in tutte le sue componenti, per una percentuale non inferiore al 99,86% dell'orario di erogazione del servizio di tipo B, calcolato su base trimestrale.

La violazione dei precedenti livelli di servizio comporterà l'applicazione delle penali contrattuali.

Gli interventi effettuati dovranno eliminare gli inconvenienti che hanno determinato la richiesta di intervento e ripristinare le normali condizioni di funzionamento.

Gli eventuali workaround che verranno implementati nella fase iniziale dell'intervento al fine di mitigare gli effetti dell'anomalia, non comporteranno la chiusura del "problem".

### 2.5.3 GESTIONE CHIAMATA E TRACCIAMENTO INTERVENTI

A fronte di un malfunzionamento del Sistema, della necessità di pianificazione di un intervento correttivo/migliorativo del Sistema stesso o di un'anomalia relativa alle Software Subscription/Licenze (di cui al successivo capitolo 4) la Committente e/o l'Amministrazione, anche tramite Call Center di aziende diverse dall'Amministrazione, all'uopo preposte, aprirà una chiamata ("ticket") all'Impresa secondo le modalità di seguito descritte.
L'intervento sarà attivato mediante chiamata telefonica ad un numero di rete fissa (preferibilmente un numero verde) da parte della Committente, confermata via e-mail ad un indirizzo di posta elettronica, entrambi comunicati dall'Impresa.
Si precisa che l'ora di invio della e-mail da parte della Committente è considerata come l'ora di apertura della chiamata.
In ogni caso l'Impresa dovrà dare comunicazione della presa in carico della richiesta di assistenza inviando una e-mail di conferma all'indirizzo **gruppo.sicurezza.cc@tesoro.it** e **gruppo.sicurezza.lr@tesoro.it**.
Quest'ultima e-mail dovrà contenere data ed ora di apertura della chiamata, identificativo (n° di intervento) della richiesta di assistenza, i riferimenti relativi al sottosistema oggetto dell'intervento e una sintetica descrizione della richiesta di supporto.

L'impresa dovrà disporre di un sistema di gestione atto a garantire il tracciamento della chiamata (stato dell'intervento) in tutte le sue fasi, fino alla chiusura della stessa.

Alla chiusura della chiamata sarà a carico del tecnico che ha eseguito l'intervento (anche solo telefonico) la redazione di una **nota d'intervento**, associata ad un numero identificativo, da recapitare sia in formato cartaceo, sia elettronico all'indirizzo sopra indicato, mediante i quali l'Impresa dovrà mantenere traccia delle azioni intraprese per il ripristino delle corrette funzionalità del Sottosistema, per consentire alla Committente la verifica dell'attività svolta.

La nota d'intervento dovrà essere approvata dalla Committente.

Su tale nota dovranno essere presenti almeno le seguenti informazioni:

- numero identificativo della nota d'intervento (numero progressivo assegnato dal tecnico);
- numero identificativo della chiamata (assegnato dal sistema di gestione);
- ora di inizio intervento telefonico;
- ora di inizio intervento "on-site" (se effettuato);
- ora ripristino del Sottosistema/termine attività pianificata;
- nome del tecnico che ha effettuato l'intervento;
- nome del referente della Committente;
- descrizione dettagliata del problema;
- soluzione adottata;
- esito della chiamata.

Rimane a carico del personale dell'Impresa, che ha eseguito l'intervento, l'aggiornamento del "libro macchina" del Sottosistema dove sono riportate le attività eseguite sullo stesso.

Alla fine di ogni trimestre, il Fornitore dovrà produrre il documento chiamato "Elenco degli interventi" contenente tutti gli interventi eseguiti nel corso di tale periodo, con evidenziati quelli che non hanno rispettati gli SLA previsti e le note di intervento ad essi associate.

## 2.6 RECESSO DI UN SOTTOSISTEMA DAL CONTRATTO DI MANUTENZIONE

Per ogni tipo di sottosistema, la cui manutenzione è disciplinata dal presente capitolato, è previsto il recesso dal servizio di manutenzione in ogni momento del periodo di efficacia del contratto. Il recesso deve essere formalizzato, mediante apposita comunicazione al Fornitore da parte della Committente con un preavviso di 15 giorni. Ciò comporterà, dal mese successivo alla scadenza del preavviso, la detrazione del canone di spesa, relativo alla apparecchiatura dismessa, dal canone globale del contratto di manutenzione.

## 2.7 INSERIMENTO DI UN SOTTOSISTEMA NEL CONTRATTO DI MANUTENZIONE

La Committente e/o Amministrazione potrà inserire ogni tipo di sottosistema acquisito ex-novo dall'Amministrazione o già facente parte della sua infrastruttura di sicurezza, appartenente alle 22 classi precedentemente descritte, nel suddetto contratto di manutenzione, in qualsiasi momento del periodo di efficacia del contratto.

Inoltre, per ogni sottosistema già inserito nel contratto di manutenzione con un determinato LdS (A, B), deve essere prevista, solo ed esclusivamente su indicazione della Committente, la possibilità di cambiare il LdS stesso.

I cambiamenti sopra indicati non potranno essere rifiutati dall'Impresa e verranno richiesti dalla Committente via e-mail al Responsabile del Contratto con 15 giorni di preavviso.

L'inserimento di un nuovo sottosistema o la modifica di un LdS associato ad un sottosistema già in manutenzione, comporterà dal mese successivo alla scadenza del preavviso l'aggiunta o l'aggiornamento del canone di spesa al canone globale del contratto di manutenzione.

L'inserimento di un nuovo sottosistema nel contratto comporterà l'individuazione della *Classe* corrispondente e, considerati i parametri 'fascia di prodotto' e 'livello di servizio', il relativo canone di manutenzione.

L'individuazione della *Classe* più adeguata per ogni Sottosistema, avverrà basandosi sui criteri definiti nel paragrafo 2.1.

Nel caso in cui un Sottosistema sarà costituito da apparati misti (alcuni in tecnologia HOST BASED, alcuni in tecnologia APPLIANCE - Blade), la *Classe* di appartenenza verrà individuata basandosi sulla

tecnologia prevalente.

È altresì previsto lo spostamento di un sottosistema di sicurezza da una *Classe* ad un'altra, a seguito di un possibile potenziamento o parziale dismissione degli apparati costituenti il sottosistema oppure in conseguenza ad un cambio tecnologico.

## 3 SERVIZIO DI CONSULENZA E SUPPORTO SPECIALISTICO

Si richiede l'erogazione di un servizio di supporto specialistico, sotto forma di giornate persona a richiesta, dedicate allo sviluppo e all'evoluzione delle configurazioni dei Sottosistemi di sicurezza, anche se non inclusi nel servizio di manutenzione oggetto del presente capitolato. Tale servizio dovrà essere erogato dalle seguenti figure professionali:

- Sistemista senior: con consolidata esperienza almeno quinquennale sui sistemi di sicurezza, che lo abiliti ad operare in completa autonomia sul particolare Sottosistema per il quale è stata richiesta la consulenza;

- Specialista di prodotto: con elevata esperienza sullo specifico prodotto in quanto appartenente ai team di consultant del vendor. Focal point di prodotto per l'erogazione dei servizi di supporto a livello nazionale; partecipa all'aggiornamento del prodotto e alla risoluzione di problematiche particolarmente complesse.

L'Impresa dovrà erogare, su richiesta della Committente, il servizio di supporto specialistico per un massimo di 200 giornate complessive nel corso della validità del contratto. La stima attuale della ripartizione delle giornate per le due figure professionali è:

- Sistemista senior 100 giornate feriali;
- Sistemista senior 30 giornate notturno/festivo;
- Specialista di prodotto 56 giornate feriali;
- Specialista di prodotto 14 giornate notturno/festivo.

Si precisa che tali quantità sono da ritenersi puramente indicative ed in alcun modo vincolanti per l'Amministrazione, che potrà richiedere un quantitativo superiore o inferiore rispetto a quello stimato.

Il servizio comprende, a titolo esemplificativo ma non esaustivo:

- l'assistenza post installazione, mediante affiancamento al personale dei Ced allo scopo di realizzare uno skill-transfert;
- il supporto alla progettazione per l'evoluzione delle architetture dei Sottosistemi di sicurezza;
- l'installazione, la configurazione e la personalizzazione del software necessario al corretto funzionamento del nuovo hardware installato, a fronte dell'acquisizione da parte della Committente di un nuovo hardware in aggiunta o sostituzione dei Sottosistemi di sicurezza in corso di manutenzione.

Le figure professionali sopra indicate saranno caratterizzate dalle seguenti competenze di base:

- consolidata esperienza lavorativa in ambito della sicurezza informatica;
- consolidata esperienza nelle architetture di sicurezza e di rete;
- capacità di gestire la relazione con gli utenti;
- consolidata capacità di problem solving;
- capacità di gestione di sistemi complessi.

Inoltre, entrambe le figure professionali dovranno essere in possesso almeno delle certificazioni di cui alla successiva Tabella 3, previste dalle società produttrici dei Sottosistemi di sicurezza.

Il servizio di supporto specialistico verrà richiesto dalla Committente mediante l'invio di una e-mail al Responsabile tecnico per l'erogazione dei servizi, specificando il profilo professionale d'interesse.

Il servizio dovrà essere reso disponibile entro e non oltre il termine di 5 giorni lavorativi dall'invio della suddetta e-mail per la figura professionale 'sistemista senior', 15 giorni lavorativi dall'invio

della suddetta e-mail per la figura professionale 'specialista di prodotto' pena l'applicazione delle penali di cui allo schema di contratto.

Le attività di supporto specialistico saranno svolte presso le sedi dove sono ubicati i Sottosistemi, nell'arco delle 24 ore, per 365 giorni all'anno, in base all'esigenza manifestata dalla Committente.

Ogni attività di consulenza richiesta ed erogata sarà consuntivata mediante apposito "Resoconto di consulenza", redatto a cura dell'Impresa e sottoscritto dalle parti, nel quale verranno trascritti il tipo e la durata dell'intervento stesso. Solo dopo l'approvazione da parte della Committente di tale documento il Fornitore potrà procedere con la fatturazione dell'intervento erogato.

### 3.1 FIGURE PROFESSIONALI DEI TECNICI ADDETTI ALLA MANUTENZIONE E AL SERVIZIO DI SUPPORTO SPECIALISTICO

Sarà carico dell'Impresa fornire e mantenere aggiornato un elenco contenente il personale tecnico incaricato del servizio di manutenzione (**Team di manutenzione**) e il personale incaricato del servizio di Supporto Specialistico. Entro 10 giorni solari dalla data di stipula del contratto dovranno essere consegnati i curricula del personale incluso nel suddetto elenco, dando evidenza negli stessi dello skill tecnico professionale e delle certificazioni possedute. Si precisa che nel caso in cui venga prevista una risorsa professionale per l'erogazione dei suddetti servizi su più tecnologie la stessa dovrà essere in possesso di tutte le certificazioni richieste (Tabella 3 di seguito riportata). Sono richieste almeno le certificazioni di cui alla seguente Tabella 3, associate alle società di produzione dei Sottosistemi di sicurezza: ISS, Check Point, CISCO, RSA, McAfee, Juniper, Symantec e F5.

Tali certificazioni dovranno essere valide per l'intera durata del contratto e qualora vengano a scadenza in fase di esecuzione del contratto stesso l'Impresa si impegna entro 30 giorni a produrre idonea documentazione attestante il rinnovo delle stesse.

| Società di produzione | Servizio di Supporto Specialistico | Servizio di Manutenzione |
|---|---|---|
| ISS-IBM | ISS-CA | ISS-CE |
| Check Point | CCSA R.75 | CCSE R.75 |
| CISCO | CCNP Security + CCDP | CCNP Security |
| RSA | RSA SecurID Certified Systems Engineer, RSA SecurID Certified Administrator (CA), RSA enVision Certified Systems Engineer (CSE) | RSA SecurID Certified Systems Engineer, RSA SecurID Certified Administrator (CA), RSA enVision Certified Systems Engineer (CSE) |
| McAfee | TRN-TCL4-Z1 | TRN-TCL4-Z1 |
| Juniper | JNCIP, JNCIS-AC, JNCIS-SA | JNCIS |
| Symantec | Exam 250-530: Administration of Symantec Network Access Control 12.1 | Exam 250-403: Administration of Symantec Management Platform 7.1 |
| F5 | F5SE | F5PC-FP |
| HP | HP Technical Certified I – Fortify Security solutions | HP Technical Certified I – Fortify Security solutions |
| Skybox | SCSC, SACE, SCRE | SCSC, SACE, SCRE |
| Imperva | IWSS (WAF), IDSS (DAM), IFSS (FAM) | IWSS (WAF), IDSS (DAM), IFSS (FAM) |
| Palo Alto | Certificazioni ufficiali del vendor | |

Tabella 3

Nell'elenco fornito ad ogni nominativo dovrà essere opportunamente associato/i il/i Sottosistema/i

di competenza. L'elenco verrà sottoposto ad approvazione della Committente che ne abiliterà il personale elencato ad eseguire gli interventi.

Qualora l'Impresa non abbia alle proprie dipendenze tecnici in possesso delle certificazioni sopra richieste dovrà comunque avvalersi di specialisti che possiedano le suddette certificazioni.

Se i vendor nel corso della validità del contratto, apporteranno delle modifiche al loro programma di certificazione sostituendo alcune certificazioni presenti nell'elenco riportato nella Tabella 3, quest'ultimo verrà considerato automaticamente aggiornato, faranno comunque fede sempre le ultime versioni delle certificazioni ufficiali dichiarate dai vendor.

Qualora durante il periodo di vigenza contrattuale, vengano introdotti nel contratto di manutenzione Sottosistemi di sicurezza di tecnologia non elencata nella Tabella 1, sarà a carico dell'Impresa fornire personale avente la specifica certificazione (indicata dal produttore di tale tecnologia) per lo svolgimento delle attività di manutenzione, amministrazione e/o sviluppo e progettazione. Il **Responsabile Tecnico per l'erogazione dei servizi** dovrà quindi aggiornare l'elenco del personale addetto alla manutenzione (Team di manutenzione) e al servizio di Supporto Specialistico. L'aggiornamento di cui sopra verrà sottoposto all'approvazione della Committente.

### 3.1 STARTUP DEL SERVIZIO DI MANUTENZIONE DEI SOTTOSISTEMI

Lo startup del servizio di manutenzione dei Sottosistemi di sicurezza del MEF, avverrà a seguito dell'invio da parte della Committente, all'Impresa, della lettera di **"Dichiarazione di inizio del servizio"**.

Nella Dichiarazione di inizio del servizio sarà contenuto l'elenco dei Sottosistemi da mettere in manutenzione con associati i relativi canoni di manutenzione individuati in base a quanti riportato nel paragrafo 2.1.

La Committente produrrà la suddetta dichiarazione, solo dopo che l'Impresa avrà fornito, entro un tempo massimo di 20 giorni solari decorrenti dalla comunicazione della Committente circa la messa in manutenzione del Sottosistema, la **documentazione di startup**, composta dalle seguenti voci:

1. **Piano tecnico di manutenzione preventiva**, di cui al precedente paragrafo 2.2.1 (uno per ogni Sottosistema);
2. composizione del **Team di manutenzione**, di cui al precedente paragrafo 3.1;
3. **documenti di presa in carico** dei Sottosistemi, come di seguito descritto.

Prima della stipula del contratto il Fornitore dovrà comunicare: il nominativo del **Responsabile del Contratto**, di cui al precedente capitolo 1, il nominativo del **Responsabile tecnico per l'erogazione dei servizi,** di cui al precedente capitolo 1, e gli estremi telefonici e l'indirizzo e-mail per l'attivazione delle chiamate, di cui al precedente paragrafo 2.5.3.

Per quanto riguarda i documenti di presa in carico dei Sottosistemi sarà carico dell'Impresa eseguire una verifica puntuale dello stato della manutenzione per ogni Sottosistema indicato dalla Committente e redigere per ognuno di essi un **documento di presa in carico**.

Nel documento di presa in carico l'Impresa dove riportare il livello degli aggiornamenti hardware e software e le eventuali segnalazioni di errore o parti guaste riscontrate sul Sottosistema e dovrà dichiarare che nulla osta alla presa in carico del Sottosistema stesso.

Nel caso in cui la suddetta verifica evidenziasse eventuali problemi/anomalie sui Sottosistemi di sicurezza esaminati, l'Impresa dovrà comunicare alla Committente quali sono gli elementi che ostano alla presa in carico del Sottosistema di sicurezza e all'avvio del servizio di manutenzione. In tale situazione, il Committente, verificato quanto segnalato dall'impresa, avvierà le azioni necessarie alla rimozione dei problemi.

Rimane comunque facoltà della Committente richiedere all'Impresa la presa in carico del Sottosistema nello stato in cui si trova al momento della verifica, considerando il risultato della verifica stessa quale stato accettabile di funzionamento del Sottosistema e assumendolo come stato di riferimento per l'erogazione del servizio di manutenzione.

## 4 AGGIORNAMENTO DELLE SOFTWARE SUBSCRIPTION

L'obiettivo della presente iniziativa è quello di acquisire:
- un rinnovo per dodici mesi degli aggiornamenti software, di seguito indicati come Software Subscription, dei prodotti software installati sul Sistema di Sicurezza del MEF, le cui scadenze avverranno entro il 31 dicembre 2014;
- 2 successivi rinnovi di uguale durata relativamente alle Software Subscription che la Committente di volta in volta andrà specificamente ad individuare, in ragione delle sue specifiche esigenze.

In aggiunta a quanto sopra riportato, è facoltà della Committente utilizzare le quotazioni unitarie indicate nello schema di contratto per ulteriori acquisizioni delle Software Subscription la cui esigenza si dovesse manifestare nel corso dei 36 mesi di validità contrattuale.

Qualora gli aggiornamenti dei prodotti software installati sui Sottosistemi di Sicurezza del MEF non potranno essere effettuati a causa dello stato di end of support (EoS), end of life (EoL) o End of Sale degli stessi, si procederà come descritto nel paragrafo 2.3.

Per Software Subscription si intendono tutti gli aggiornamenti relativi ai prodotti software installati sul Sistema di Sicurezza del MEF, a titolo esemplificativo, ma non esaustivo, di seguito vengono elencati alcuni esempi di aggiornamenti software:

- patch correttive ed evolutive;
- fix di sicurezza;
- **nuove versioni dei prodotti software**;
- aggiornamento delle informazione necessarie ai riscontri di sicurezza (firme, "dat", etc.)
- **nuove release dei prodotti software**, **maggiori e minori** (per release maggiori si intendono gli aggiornamenti che sostituiscono uno specifico prodotto software con un nuovo prodotto completamente riscritto).

Si sottolinea che la registrazione delle suddette Software Subscription, con le case produttrici, dovrà avvenire a nome di SOGEI S.p.A., e sarà a carico dell'Impresa la gestione e l'eventuale aggiornamento degli account attivi presso i vari produttori, secondo le indicazioni della Committente.

L'Impresa dovrà mettere a disposizione della Committente una USERID ed una PASSWORD, per ognuno dei prodotti di seguito elencati, con le quali sia possibile accedere alle rispettive Software Subscription.

La USERID e la PASSWORD dovranno garantire l'accesso alle aree riservate dei siti Internet dei vari produttori di Software Subscription. Nel caso in cui il produttore di Software Subscription non eroghi le stesse in base alle modalità sopra descritte, l'Impresa, dopo la stipula, comunicherà alla Committente le diverse modalità di consegna della fornitura delle Software Subscription.

La mancata fornitura delle suddette informazioni determina l'applicazione delle penali di cui allo schema di contratto.

L'Impresa, procederà alla fornitura delle Software Subscription, da effettuarsi entro 20 giorni solari dalla data di invio di **"Richiesta di fornitura di Software Subscription"** che la Committente invierà al Responsabile del Contratto, durante l'intera durata contrattuale. Il Fornitore dovrà rilasciare la documentazione che attesti l'autorizzazione del produttore all'utilizzo delle Software Subscription e dell'eventuale supporto magnetico ad esse correlato, nonché il numero identificativo del prodotto, il numero identificativo della licenza/certificato e i termini temporali di utilizzo (date di inizio e di fine utilizzo). Tale modalità di fornitura sarà applicata anche nel caso di ulteriori acquisizioni di Software Subscription, la cui esigenza si dovesse manifestare nel corso dei 36 mesi di validità contrattuale. Ad esempio, a seguito della presa in manutenzione di un nuovo Sottosistema.

Vengono di seguito riportate le licenze dei prodotti software attualmente installati sul Sistema di Sicurezza del MEF e le relative Software Subscription attualmente in esercizio, suddivise per produttore.

## 4.1 SOFTWARE SUBSCRIPTION

Di seguito si riportano le tabelle con le Software Subscription suddivise per prodotto e casa produttrice, attualmente attive e di proprietà dell'Amministrazione.

| CheckPoint | | | |
|---|---|---|---|
| **Account: 0005834259, 0006837377, 0006812133, 0006739166, 0006811253** | | | |
| **Product SKU** | **Product Name** | **Description** | **Quantità** |
| CPAP-SG3077-HA-F | Secondary UTM-1 3077 (includes FW, VPN, IPS, AV, ASPM, URLF, IA) | Secondary Check Point UTM-1 3077 (includes FW, VPN, IPS, AV, ASPM, URLF, IA) | 1 |
| CPAP-SG3077-F | UTM-1 3077 (includes FW, VPN, IPS, AV, ASPM, URLF, IA) | Check Point UTM-1 3077 (includes FW, VPN, IPS, AV, ASPM, URLF, IA) | 1 |
| CPAP-SG572-HA | HA Check Point UTM-1 572 Total Security App with 2 Security blades | Secondary Check Point UTM-1 572 Total Security Appliance with 2 Security blades (FW, VPN) and 3 Management blades (NPM, EPM, LOGS) | 1 |
| CPAP-SG572 | Check Point UTM-1 572 Total Security Appliance | Check Point UTM-1 572 Total Security Appliance with 2 Security blades (FW, VPN) and 3 Management blades (NPM, EPM, LOGS) | 1 |
| CPAP-SG3073 | Check Point UTM-1 3073 Total Security Appliance | Check Point UTM-1 3073 Total Security Appliance with 3 Security blades (FW, VPN, IPS) and 3 Management blades (NPM, EPM, LOGS) | 1 |
| CPAP-SG3073-HA | HA Check Point UTM-1 3073 Total Security Appliance | Secondary Check Point UTM-1 3073 Total Security Appliance with 3 Security blades (FW, VPN, IPS) and 3 Management blades (NPM, EPM, | 1 |
| CPAC-4-1C | 4 Port 10/100/100 Base-T RJ45 interface card | 4 Port 10/100/100 Base-T RJ45 interface card | 10 |
| CPSG-P203iU-F-FM | Security Gateway with Container with 2 cores and unlimited users | Check Point Security Gateway pre-defined system including Container with 2 cores and unlimited users (including FW, IA and ACCL bla | 1 |
| CPSG-P203U-HA-F-FM | Secondary Security Gatewaywith container for 8 cores and 5 blades | Secondary Check Point Security Gateway pre-defined system including Container with 2 cores and U users (including FW, IA and ACCL b | 1 |
| CPSG-P203U-CPSM-PU003-F-EPC | Security bundle - including SG203U and SMU003 | Check Point Security bundle - including SG203U and SMU003 (FW, IA, ACCL ,NPM, EPM and LOGS) | 1 |
| CPFW-FM-U-NG | Security Gateway - Firewall-1 (unlimited users) | FireWall-1 Module for an unlimited number of IP addresses | 1 |
| CPAP-SG4607-HA | Check Point 4600 Appliance HA | Check Point 4600 Appliance with FW, VPN, IA, ADNC, MOB, IPS, and APCL for High Availability | 7 |
| CPAP-SG4607 | Check Point 4600 Appliance | Check Point 4600 Appliance with FW, VPN, IA, ADNC, MOB, IPS, and APCL | 7 |

| | | | |
|---|---|---|---|
| CPSG-P204iU-F | Security Gateway including container for 2 core and 4 blades | Check Point Security Gateway pre-defined system including container for 2 cores and 4 blades (FW, IA, VPN and ADN) | 2 |
| CPSG-P204U-CPSM-PU003-F | Security bundle - including SG204U and SMU003 | Check Point Security bundle - including SG204U and SMU003 (FW, IA, VPN, ADN, NPM, EPM and LOGS) | 2 |
| CPAP-SG12407 | Check Point 12400 Appliance | Check Point 12400 Appliance with FW, VPN, IA, ADNC, MOB, IPS, and APCL | 4 |
| CPAC-LOM | 2 unità | | 2 |
| CPSG-P204IU-CPSM-PU003-F-VEE | Security bundle - including SG204U and SMU003 | Check Point Security bundle - including SG204U and SMU003 (FW, IA, VPN, ACCL, NPM, EPM and LOGS) | 1 |
| CPAP-SG12207 | Check Point 12200 Appliance | Check Point 12200 Appliance with FW, VPN, IA, ADNC, MOB, IPS, and APCL | 7 |
| CPAP-SM504 | Smart-1 5 | Check Point Smart-1 Security Management managing 5 gateways with 4 Management blades (NPM, EPM, LOGS, PRVS) | 2 |
| CPAC-RAM4GB | 4GB Memory upgrade for 4800 and 12200 appliances. | 4GB Memory upgrade for 4800 and 12200 appliances. | 4 |
| CPAC-4-1F | 4 Port 1000Base-F SFP interface card | 4 Port 1000Base-F SFP interface card. Requires additional 1000Base SFP transceiver modules per interface port. | 5 |
| CPAC-PSU-4800/12200 | Additional/replacement AC Power Supply for 4800 and 12200 app | Additional/replacement AC Power Supply for 4800 and 12200 appliances | 4 |
| CPAC-TR-1SX | 16 unità | | 2 |
| CPIP-A-TR-1SX | 8 unità | | 1 |
| CPIP-A-TR-C | 8 unità | | 1 |
| CPSB-DMN200 | Security Management - Domain blade (2 Gateways) | Check Point Management Domain blade for managing 2 Gateways | 8 |
| CPAC-8-1C | 2 unità | | 1 |
| CPAC-RAM | 2 unità | | 1 |
| CPSB-IPS-S-1Y | F2GT0Q (22/6/13) | | 1 |
| CPSB-IPS-XL-1Y | R08UYFW (1/10) | | 1 |

Tabella 4

| IBM ISS | | | |
|---|---|---|---|
| **Prodotto** | **Certificate Key** | **Descrizione** | **Quantità** |
| SVP-WIN-001-PB-M (old)<br>E0C9CLL (new) | ND | Software Maintenance Real Secure Server | 5 |
| NSB-00250-PBM (old)<br><br>ESL-0000500-P-M (new) | ND | Software Maintenance Real SecureVulnerability<br><br>MAINT. PROVENTIA ENT SCANNER - LICENSE (500 USERS) | 500 |
| GX4002-C-1-PM | ND | Proventia G Maintenance | 1 |
| GX4004C-V2-1-P-M | ND | (ROHS) Proventia GX4004C-V2 Intr. Preven. App. Maintenance | 12 |
| | ND | Siteprotector unlimited software package management (1 quant.) | 2 |
| | ND | Maintenance Proventia Ent. Scanner 1500 | 1 |
| GX4004C-V2-1-P-M | ND | (ROHS) Proventia GX4004C-V2 Intr. Preven. App. Maintenance | 2 |
| | ND | Maintenance Proventia SVR for Linux per User (1 user) | 5 |

Tabella 5

| Symantec | | | |
|---|---|---|---|
| **Prodotto** | **Certificate Key** | **Descrizione** | **Quantità** |
| IX7DOZZ0-ER1N0 / RNW531-998-776 | 41670066 / 41670066 | symc network access control enforcer 12.1 server/device renewal essential 12 months | 2 |

Tabella 6

| RSA | | | |
|---|---|---|---|
| **Prodotto** | **Certificate Key** | **Descrizione** | **Quantità** |
| AUT0001500BE12 | ND | RSA Authentication Manager Base Edition SecurCare Extnd Maint 1 Year 755-1500 Users | 1 |
| enVision 7500 | seriale 39Q845J | RSA Envision 7500 | 1 |
| N.1 Appliance ES-7560 RSA enVision 7500 con | seriale 1B4H85J | RSA Envision 7560 (DT presso la Rustica) | 1 |
| enVision 5000 | seriale 7HCB15J | | 1 |
| enVision 5000 | seriale 4FSH45J | | 1 |

Tabella 7

| Juniper | | | |
|---|---|---|---|
| **Prodotto** | **Certificate Key** | **Descrizione** | **Quantità** |
| SVC-SDCE-SSG140 | ND | Juniper SSG 140 ONLY EMEA J-Care SameDay Onsite Support 1 Year | 2 |

Tabella 8

| F5 | | | |
|---|---|---|---|
| **Prodotto** | **Certificate Key** | **Descrizione** | **Quantità** |
| F5-SVC-FP-PRE-L2-3 | ND | Level 2-3 Premium Service for FirePass (7x24) - FirePass 4310 | 1 |
| F5-SVC-FP-PRE-L2-3 | ND | Level 2-3 Premium Service for FirePass (7x24) - FirePass 4300 Failover Unit | 1 |
| F5-SVC-FP-PRE-L2-3 | ND | Level 2-3 Premium Service for FirePass (7x24) - FirePass Host Adapter | 1 |

Tabella 9

| Mc Afee | | | |
|---|---|---|---|
| **Prodotto** | **Certificate Key** | **Descrizione** | **Quantità** |
| Change Platform | ND | Upgrade della piattaforma from gold to platinum | 10.000 |
| NYV5500SSMA | | MFE WEB GATEWAY WG5500 1YR GL+NBD | 3 |
| RU5500WBGXFA | | MFE WEB GATEWAY WG5500 1YR SD HW UPG | 3 |

Tabella 10

| Fortinet | | |
|---|---|---|
| **Codice** | **Descrizione** | **Quantità** |
| FORC-10-00312-247-02-121Yr | FORTICARE 24X7 FG310B RENEWAL FG300B3909602068 | 1 |
| FORC-10-00312-247-02-121Yr | FORTICARE 24X7 FG310B RENEWAL FG300B3909602071 | 1 |
| FORC-10-00312-108-02-121Yr | FORTIGUARD IPS FG310B RENEWAL FG300B3909602068 | 1 |

| | | |
|---|---|---|
| FORC-10-00312-108-02-121Yr | FORTIGUARD IPS FG310B RENEWAL FG300B3909602071 | 1 |
| FORC-10-00312-247-02-121Yr | FORTICARE 24X7 FG620B RENEWAL FG600B3909600123 | 1 |
| FORC-10-00312-247-02-121Yr | FORTICARE 24X7 FG620B RENEWAL FG600B3909600267 | 1 |
| FO FC-10-L0403-247-02-12 | Forti analyzer SR:FLG8003706000640 | 1 |

Tabella 11

| Palo Alto | | | | |
|---|---|---|---|---|
| **Device serial n.** | **Model** | **Tipologia** | **Feature** | **Quantità** |
| 0007D101357 | PRA-25 | Console Gestionale Panorama | Premium Partner Support | 1 |
| 0011C101843 | PA-5020 | Next Generation Firewal Node 2 | Premium Partner Support | 1 |
| 0011C101850 | PA-5020 | Next Generation Firewal Node 1 | Premium Partner Support | 1 |
| 0011C101863 | PA-5020 | Next Generation Firewal Node 3 | Premium Partner Support | 1 |

Tabella 12

Si sottolinea che a fronte del rilascio da parte delle case produttrici di nuovi release e/o di nuove versioni dei prodotti inseriti nelle tabelle che precedono, queste ultime si intendono automaticamente aggiornate e il relativo costo rimarrà invariato.

I 2 rinnovi, successivi al primo, ciascuno di 12 mesi, avranno ad oggetto le sole Software Subscription di cui alle Tabelle sopra indicate (eventualmente aggiornate) che la Committente di volta in volta richiederà, in termini di tipologia e quantità, in ragione delle sue specifiche esigenze.

L'Impresa, per tutta la durata del Contratto, avrà facoltà di richiedere l'aggiornamento delle Tabelle con le Software Subscription delle varie Case Produttrici per far fronte ad evoluzioni delle tecnologie.
Gli aggiornamenti dovranno essere adeguatamente motivati, proponendo la sostituzione di singoli Componenti software, o l'ampliamento delle soluzioni già presenti nelle Tabelle secondo parametri di equivalenza e funzionalità.
La Committente si riserva la facoltà di valutare le proposte dell'Impresa.
Se la proposta verrà accettata si procederà all'aggiornamento e/o all'ampliamento delle Tabelle, anche economico, con cadenza annuale (o semestrale).

Resta fermo che i prezzi da applicare ai nuovi prodotti della Casa Produttrice di una data tabella saranno pari al corrispondente prezzo di listino della stessa Casa Produttrice ridotto dello sconto medio praticato in sede di offerta dal Fornitore rispetto ai prodotti di quella Casa Produttrice.

## 5 VERIFICA DI CONFORMITÀ

Tutte le prestazioni oggetto del contratto saranno sottoposte a verifica di conformità, secondo le modalità indicate nello Schema di contratto condizioni speciali (Allegato 3 al Disciplinare di gara).

In particolare, entro il termine di 20 giorni solari decorrenti dalla data di consegna delle Software Subscription (vedi capitolo 4), le Software Subscription saranno sottoposte a verifica da parte della Committente in contraddittorio con l'Impresa. Solo in caso di esito positivo di tale verifica l'Impresa potrà procedere alla fatturazione delle Software Subscription stesse secondo le modalità di cui allo Schema di contratto speciale (Allegato 3). Delle operazioni di verifica verrà redatto un apposito **"Verbale di verifica"**.

Entro il termine di 20 giorni solari decorrenti dalla data di avvio operativo del Sottosistema, aggiornato a seguito dello stato di: end of support (EoS), end of life (EoL) o End of Sale dei Sottosistemi (o di loro componenti), le sue componenti hardware saranno sottoposte a verifica di conformità da parte della Committente in contraddittorio con l'Impresa. Entro il termine di 10 giorni solari decorrenti dalla data di ordine delle suddette componenti hardware del Sottosistema aggiornato il Fornitore dovrà redigere e consegnare un **"Piano di collaudo"**, che dovrà essere approvato dalla Committente, contenente l'articolazione delle prove proposte per la verifica di conformità dei Sottosistemi oggetto della fornitura.

L'Impresa prende atto e accetta che la verifica di conformità può comprendere anche prove diverse indicate dalla Committente.

La verifica di conformità dei Sottosistemi, anche in modalità integrata tra le componenti hardware e software, verrà eseguita da una Commissione, in contraddittorio con l'Impresa. Delle operazioni di verifica di conformità verrà redatto un apposito **"Verbale di verifica di conformità"** in contraddittorio con l'Impresa che dovrà prevedere, in allegato, un documento nel quale dovranno essere riportate le seguenti informazioni:

a) numero e matricola delle apparecchiature costituenti il Sottosistema, consegnato;
b) nome delle Software Subscription installate sul Sottosistema;
c) la descrizione della configurazione Hardware e Software dei Sottosistemi consegnati;
d) la descrizione delle operazioni e dei test effettuati;
e) la descrizione degli eventuali problemi riscontrati;
f) la descrizione delle soluzioni adottate a fronte dei problemi riscontrati.

La verifica di conformità del Sottosistema si intende positivamente superata solo se tutte le componenti hardware e software risultino funzionare correttamente, singolarmente e integrate tra loro, secondo le specifiche indicate nella documentazione tecnica e d'uso fornita dall'Impresa.
Nel caso di esito positivo della verifica di conformità la data del verbale verrà considerata quale "Data di Accettazione della Fornitura", da parte della Committente.

In sede di verifica di conformità, l'Impresa si impegna a fornire alla Committente tutta la documentazione tecnica ed i dati necessari al fine di consentire alla medesima di provvedere direttamente o tramite terzi alla gestione del Sottosistema.