ALLEGATO 4 - CAPITOLATO TECNICO

ACQUISIZIONE DI HARDWARE, SOFTWARE E SERVIZI PER L'EVOLUZIONE DELL'INFRASTRUTTURA FIREWALL E IPS DEL MINISTERO DELL'ECONOMIA E DELLE FINANZE E DELLA CORTE DEI CONTI – ID 1081

SOMMARIO

1 ACRONIMI

CMA	Customer Management Add-on
ETSI	European Telecommunications Standards Institute
HA	High Availability
ICSA	International Computer Security Association
IEEE	Institute of Electrical and Electronics Engineers
IPS	Intrusion Prevention System
MDS	Multi-Domain Security Management
MEF	Ministero dell'Economia e delle Finanze
NAC	Network Access Control
NGF	Next-Generation Firewall
OPSEC	Open Platform for Security
PoE	Power over Ethernet
RTI	Raggruppamento Temporaneo d'Imprese
SIEM	Security Information and Event Management
SOAP	Simple Object Access Protocol
SPOF	Single Point of Failure
UTM	Unified Threat Management
VdC	Verifica della Conformità
VLAN	Virtual Local Area Network
VoIP	Voice over IP
WAF	Web Application Firewall

2 INTRODUZIONE

Il presente Capitolato Tecnico disciplina gli aspetti tecnici della Fornitura dei sistemi hardware e software e dei servizi correlati necessari per l'evoluzione dell'infrastruttura di sicurezza del Ministero dell'Economia e delle Finanze (nel seguito indicato per comodità con MEF) e della Corte dei conti (nel seguito indicata per comodità con Cdc). Fanno parte della Fornitura anche le attività (esecutive) di consegna, installazione, configurazione e supporto alla Verifica della Conformità (nel seguito indicata per comodità con VdC).

Le attività di personalizzazione verranno eseguite dall'Impresa, su richiesta del Committente, facendo ricorso al supporto specialistico, anche questo compreso nell'Oggetto della Fornitura.

Nel seguito del documento si ricorrerà più volte ad alcuni termini cui è attribuito il seguente significato:

- **Capitolato Tecnico**, il presente documento;
- **Amministrazione/i**, la/le Amministrazione/i contraente/i, ovvero il MEF e la Cdc;
- **Committente**, la CONSIP S.p.A.;
- **Impresa**, l'Impresa aggiudicataria della gara, eventualmente mandataria di un RTI;
- **Fornitura**, quanto indicato al capitolo 3 come **Oggetto di Fornitura** e descritto dettagliatamente nel capitolo 4;
- **Listini,** elenchi di prodotti e di servizi, corrispondenti a varie tecnologie, predisposti dal Committente oppure offerti dall'Impresa sulla base dei requisiti del presente Capitolato, da cui è possibile attingere gli oggetti delle varie acquisizioni;
- **Manutenzione,** l'insieme delle operazioni volte a mantenere in efficienza e/o ripristinare la piena funzionalità dei Sistemi richiesti nel Capitolato Tecnico;
- **Infrastruttura di sicurezza**, l'insieme dei Sistemi e dei servizi correlati atti a garantire un'adeguata protezione delle informazioni e dei servizi erogati dai sistemi informativi del MEF e della Cdc;
- **Ordinativo/i successivo/i**, le acquisizioni, effettuate eventualmente dall'Amministrazione successivamente alla stipula del Contratto, necessarie per far fronte ad evoluzioni e/o adeguamenti tecnologici della propria infrastruttura di sicurezza;
- **Primo Ordinativo**, la prima acquisizione, descritta nel paragrafo 3.1 del presente Capitolato, effettuata all'atto della stipula del Contratto per far fronte alle esigenze attuali dell'Amministrazione;
- **Sistema di sicurezza (o Sistema)**, espressione architetturale di una o più

funzionalità dell'Infrastruttura di sicurezza, per esempio firewall, IPS, ecc.; ogni Sistema può essere costituito da uno o più Componenti di sicurezza;

- **Componente di sicurezza (o Componente),** un qualunque elemento hardware o software (per esempio nodo firewall, licenza software, interfaccia di rete, console di gestione, ecc.) dei Sistemi facenti parte dell'Infrastruttura di sicurezza;
- **Software di base e middleware,** l'insieme del software necessario per supportare il corretto funzionamento delle applicazioni, per esempio sistema operativo, file system, protocolli di comunicazione;
- **Software applicativo,** qualunque software diverso dal software di base e middleware;
- **Servizio/i,** il servizio o l'insieme dei servizi connessi alla Fornitura in oggetto.

3 CARATTERISTICHE DELLA FORNITURA

Il Committente ha inteso organizzare la presente iniziativa di acquisizione in maniera da rispondere in modo efficiente e flessibile alle esigenze attuali e future delle Amministrazioni in tema di Sistemi di sicurezza. A tal fine, all'Impresa verrà richiesto di quotare una serie di listini afferenti alle tecnologie di interesse.
Successivamente alla stipula del Contratto, la Consip invierà all'Impresa, mediante posta elettronica, una "Comunicazione di attivazione" relativamente alla Fornitura del primo ordinativo, attinto dai listini e descritto dettagliatamente nel presente Capitolato Tecnico al paragrafo 3.1.
L'Impresa dovrà indicare, entro 5 (cinque) giorni solari dalla stipula del Contratto, un apposito indirizzo di posta elettronica, al quale la Consip inoltrerà le richieste di ordinativo ed un numero telefonico/fax per tutte le altre comunicazioni.

L'Amministrazione si riserva di attingere dai Listini, così come fissati all'atto dell'Offerta e/o, eventualmente, aggiornati/integrati.

Le modalità di aggiornamento dei Listini sono descritte nel paragrafo 4.8 del presente Capitolato Tecnico.

3.1 OGGETTO DELLA FORNITURA

Di seguito sono descritte le specifiche tecniche e le funzionalità relative alla **Fornitura**:

- **Infrastruttura di sicurezza**, secondo quanto descritto al paragrafo 4.1;
- **Manutenzione in garanzia** dell'"Infrastruttura di Sicurezza", secondo quanto descritto al paragrafo 4.3;
- **Consulenza specialistica,** secondo quanto descritto al paragrafo 4.4;
- **Supporto specialistico di prodotto**, secondo quanto descritto al paragrafo 4.5
- **Addestramento**, secondo quanto descritto al paragrafo 4.6.

L'Impresa, assumendo verso le Amministrazioni il ruolo di "fornitore globale", dovrà garantire la completezza e l'omogeneità della Fornitura stessa.

La Fornitura dovrà conformarsi ai requisiti di base di seguito indicati:

1. tutti i Componenti dovranno soddisfare i requisiti e presentare caratteristiche tecniche non inferiori a quanto riportato nel presente Capitolato Tecnico;
2. i Componenti, laddove di pertinenza, dovranno essere forniti secondo le quantità, indicate al capitolo 4 del presente Capitolato Tecnico;
3. l'Infrastruttura di Sicurezza nel suo complesso ed i servizi ad essa correlati dovranno rispettare le normative vigenti in materia di sicurezza dell'informazione, di privacy, emissioni elettromagnetiche e sicurezza sul lavoro specificati nel capitolo 7.

In merito alla presente Fornitura, si precisa inoltre che:

1. tutti gli apparati forniti dovranno essere nuovi di fabbrica ed essere costruiti utilizzando parti nuove;
2. l'Impresa dovrà garantire l'interoperabilità e la compatibilità di tutti i Sistemi che costituiscono la soluzione proposta;
3. l'Impresa dovrà provvedere a consegnare, installare ed avviare tutti i Componenti presso le sedi indicate nel paragrafo 3.1.1;
4. l'Impresa dovrà provvedere a consegnare tutti i Componenti con software di base e middleware preinstallati, comprensivi di licenze e manuali d'uso, patch di sistema e di sicurezza aggiornate almeno alla data di firma del Contratto;
5. una volta effettuata la consegna secondo quanto indicato nel paragrafo 4.2, l'Impresa dovrà installare sui suddetti Sistemi il software, non oggetto della Fornitura (per esempio software di gestione e monitoraggio), fornito dall'Amministrazione;
6. con riferimento alla eventuale fornitura di sistemi operativi Microsoft, nel formulare l'Offerta l'Impresa dovrà fare riferimento ai listini relativi ai Contratti in essere con la relativa Amministrazione.

L'Impresa dovrà individuare un **Responsabile della Fornitura**, che costituirà il singolo punto di contatto nei confronti del Committente. Il **Responsabile della Fornitura** dovrà coordinare tutte le attività e produrre resoconti periodici, da presentare per discussione durante i SAL di progetto.

I SAL, da tenere con cadenza quindicinale o su esplicita richiesta del Committente, riguarderanno almeno i seguenti argomenti:

- percentuale di completamento del progetto, con il dettaglio delle attività già svolte e quelle ancora da svolgere;
- eventuali problematiche insorte;
- questioni aperte di carattere strategico/metodologico da sottoporre all'attenzione del Committente.

A fronte di eventuali problematiche che dovessero presentarsi, il SAL dovrà comprendere anche le relative proposte di risoluzione e la relativa ripianificazione delle attività impattate.

3.1.1 MODALITÀ DI ACQUISIZIONE

La modalità di acquisizione attuata adotta una logica basata sui Listini. Tale approccio garantisce da una parte il soddisfacimento delle esigenze attuali dell'Amministrazione, dall'altra un'efficiente acquisizione per eventuali nuove esigenze. La scontistica sui Listini, proposta dall'Impresa all'atto della presentazione dell'Offerta, rimarrà invariata per tutta la durata contrattuale.

È previsto un massimale contrattuale, dal cui ammontare, detratto l'importo del Primo Ordinativo, l'Amministrazione avrà facoltà di richiedere gli Ordinativi Successivi.

In ogni caso, del predetto massimale, il Committente garantisce l'attivazione del 10% dello stesso.

Le modalità di gestione degli Ordinativi Successivi sono descritte nel paragrafo 4.2.2 del presente Capitolato Tecnico.

3.2 SEDI DI FORNITURA

La consegna dei Componenti e l'erogazione dei Servizi previsti nel Capitolato Tecnico potrà avvenire all'interno dei comuni di Roma e Latina. Di seguito viene riportato un elenco non esaustivo delle sedi principali del MEF e della Cdc presenti all'interno dei suddetti comuni:

- Roma - Via XX Settembre;
- Roma - Via A. Soldati (La Rustica);
- Roma - Piazza Dalmazia;
- Latina - Viale Nervi;
- Roma - Via Sicilia;
- Roma - Via Baiamonti.

4 DESCRIZIONE DELLA FORNITURA

I paragrafi seguenti descrivono le caratteristiche del Primo Ordinativo della Fornitura.

4.1 INFRASTRUTTURA DI SICUREZZA

Nel prosieguo del presente Capitolato, laddove vengano riportate caratteristiche tecniche, queste sono sempre da intendersi come requisiti minimi della Fornitura, se non diversamente specificato.

L'Infrastruttura di sicurezza oggetto di acquisizione è composta da Sistemi appartenenti alle seguenti categorie tecnologiche:

- Firewall, delle seguenti tipologie:
  - Firewall perimetrali e di rete, secondo le quantità e le caratteristiche tecniche indicate al paragrafo 4.1.1;
  - Firewall applicativi (Web Application Firewall – WAF), secondo le quantità e le caratteristiche tecniche indicate al paragrafo 4.1.2;
  - Firewall di nuova generazione (Next-Generation Firewall – NGF), secondo le quantità e le caratteristiche tecniche indicate al paragrafo 4.1.3;
- Intrusion Prevention Systems (IPS), secondo le quantità e le caratteristiche tecniche indicate al paragrafo 4.1.4;
- Wireless Security, secondo le caratteristiche tecniche indicate al paragrafo 4.1.5;
- Security Lifecycle Management, secondo le quantità e le caratteristiche tecniche indicate al paragrafo 4.1.6.

Nel caso in cui i prodotti offerti non garantiscano la rispondenza nativa ai requisiti specificati, dovranno essere predisposte tutte quelle attività necessarie a garantirne il corretto funzionamento (per esempio, la realizzazione di specifici connettori o configurazioni). Tali attività saranno a totale carico dell'Impresa.

Si fa presente che, laddove applicabile, a tutela del precedente investimento dell'Amministrazione, l'Impresa dovrà prevedere il "trade-in" delle licenze.

4.1.1 Firewall perimetrali e di rete

4.1.1.1 CheckPoint

Il MEF implementa una infrastruttura firewall consolidata e piuttosto articolata, basata quasi esclusivamente su tecnologia CheckPoint. I firewall facenti parte della suddetta infrastruttura sono utilizzati sia per la protezione del perimetro della rete ministeriale sia per segregare le aree considerate a differenti livelli di sicurezza. La suddetta

infrastruttura firewall comprende attualmente una componente gestionale decentralizzata, costituita da un certo numero di console tra loro indipendenti. La componente gestionale sarà aggiornata, sostituendola con la piattaforma CheckPoint Provider-1, oggetto della presente fornitura.

Per consentire all'Impresa di individuare adeguatamente le Componenti dell'infrastruttura di sicurezza oggetto di Offerta, si precisa che la piattaforma di gestione richiesta è la Smart-1 MDS 50 in alta affidabilità, comprendente 5 CMA unlimited di default. A questa configurazione base, si aggiungono 20 CMA di taglio minimo (2 gateway).

Relativamente ai "Firewall perimetrali e di rete" di tecnologia CheckPoint, il primo ordinativo consta dei seguenti componenti:

Componente	**Quantità**
CPAP-SG2075	3
CPAP-SG2075-HA	6
CPAP-SG9077	2
Software blade con 12 mesi di aggiornamenti	Tutte quelle di serie negli apparati
CPAP-SM50-MD508	2
CPSB-DMN200	20

Tutte le CMA dovranno comprendere 12 mesi di aggiornamenti software.

4.1.1.2 Fortinet

La tecnologia di firewall Fortinet è utilizzata attualmente in uno specifico ambito dell'infrastruttura MEF, per svolgere funzioni di sicurezza ormai consolidate da tempo.

La Cdc possiede invece una infrastruttura di sicurezza con diversi sistemi firewall Fortinet, dislocati anche presso le sedi periferiche dell'Amministrazione.

Il primo ordinativo non prevede l'acquisizione di oggetti appartenenti a questa tecnologia.

4.1.2 Web Application Firewall

Il Sistema WAF riveste una funzionalità al momento non presente nell'infrastruttura di sicurezza dell'Amministrazione.

Relativamente a tale Sistema, il primo ordinativo consta dei seguenti Componenti:

Componente	**Quantità**
Appliance, con licenze software e 12 mesi di aggiornamenti	3, di cui 2 in HA

Componente	**Quantità**
Console di gestione centralizzata, con licenze software e 12 mesi di aggiornamenti	1

La componente di gestione centralizzata del Sistema WAF potrà essere offerta sottoforma di hardware o software. Nel caso di Componente realizzata mediante macchina virtuale, si fa presente che l'Amministrazione adotta un'infrastruttura virtualizzata basata su VMWare Vsphere 4.

Il Sistema offerto deve possedere le seguenti certificazioni specifiche per prodotti Web Application Firewall:

- Common Criteria EAL 2;
- ICSA Labs.

Il dimensionamento del Sistema WAF deve essere effettuato sulla base dei seguenti requisiti tecnici minimi:

- throughput: 500 Mbps;
- http Transactions/sec: 22.000;
- porte in rame 10/100/1000: 4;
- espandibilità con schede in fibra a 1 o 10 Gbps;
- scalabilità relativamente alle componenti hardware e software;
- modalità di funzionamento: in-line, proxy/reverse-proxy e tap. Qualora non fosse disponibile la modalità tap l'apparato deve essere in grado di simulare la funzionalità di port mirroring;
- implementazione in alta affidabilità: deve essere possibile configurare il Sistema WAF in modalità HA, secondo il paradigma active/passive o active/active; in questa seconda modalità, deve essere possibile anteporre al Sistema un apparato di bilanciamento in grado di gestire l'inoltro del traffico al Componente del Sistema ritenuto più scarico;
- possibilità di analizzare traffico SSL anche in modalità passiva (senza terminare la sessione cifrata);
- accelerazione dei flussi SSL;
- gestione centralizzata:
  - creazione e propagazione delle configurazioni e delle policy di sicurezza a tutti i componenti interessati;
  - raccolta e gestione in un unico log degli eventi generati da tutti i Componenti del Sistema WAF;
- autoapprendimento: il Sistema WAF deve essere in grado di definire automaticamente, per ogni applicazione, una *baseline* comportamentale ritenuta "normale";

- correlazione di eventi: il Sistema WAF deve essere in grado di identificare attacchi sofisticati, per esempio quelli condotti mediante più fasi successive;
- arricchimento: il Sistema WAF deve essere in grado di importare ed interpretare i risultati prodotti dalle scansioni del Web vulnerability scanner "HP Web Inspect" (attualmente in possesso dell'Amministrazione) al fine di verificare la effettiva presenza di vulnerabilità e bloccare in maniera proattiva solamente gli attacchi realmente pericolosi (virtual patching). Nel caso in cui il Sistema offerto non sia nativamente compatibile col prodotto Web Inspect, dovrà essere predisposto uno specifico connettore per l'integrazione. Tale attività farà parte della configurazione del prodotto e sarà quindi a totale carico dell'Impresa;
- compatibilità con i più noti sistemi SIEM (RSA n-Vision, ArcSight, etc.);
- supporto di base per la protezione dei Web Services, in particolare: ispezione e validazione del controllo della busta SOAP, conformità dello schema XML e controllo delle firme e dei profili XML/SOAP;
- alerting: invio automatico delle segnalazioni e degli allarmi in presenza di violazioni delle politiche di sicurezza;
- conformità: soddisfacimento dei requisiti di sicurezza per la compliance alle direttive del Payment Card Industry Data Security Standard (PCI DSS). Tra questi requisiti, quello di proteggere almeno contro le prime 10 minacce del programma Open Web Application Security Project (OWASP), aggiornandosi in accordo al progetto OWASP.

4.1.3 Next Generation Firewall

Il Sistema NGF riveste una funzionalità al momento non presente nell'infrastruttura di sicurezza dell'Amministrazione. La tecnologia che consente di rispondere al meglio alle esigenze dell'Amministrazione è quella della Palo Alto Networks.

Relativamente a tale Sistema, il primo ordinativo consta dei seguenti Componenti:

Componenti	**Quantità**
Palo Alto NGF PA-5020, con licenze software e 12 mesi di aggiornamenti	3, di cui 2 in HA
Panorama Central Management PAN-PRA-25, con licenze software e 12 mesi di aggiornamenti	1

4.1.4 Intrusion Prevention Systems

Il MEF implementa da diversi anni una infrastruttura di Intrusion Prevention costituita da apparati attestati sulle zone della rete ritenute maggiormente critiche. Tale infrastruttura

è costituita da un certo numero di sonde IBM/ISS e dalla relativa piattaforma software di gestione (SiteProtector).

La suddetta infrastruttura IPS comprende attualmente una componente gestionale decentralizzata, costituita da un certo numero di console tra loro indipendenti. L'aggiornamento della componente gestionale SiteProtector avverrà nell'ambito della presente fornitura.

Relativamente a tale Sistema, il primo ordinativo consta dei seguenti Componenti:

Componenti	**Quantità**
Proventia GX4004C-V2-1-P, con licenze software e 12 mesi di aggiornamenti	5
Host IPS Linux Red Hat, con 12 mesi di aggiornamenti	5

I Componenti Proventia oggetto di Fornitura saranno tutti implementati come nodi primari.

4.1.5 Wireless Security

La tecnologia Aruba Networks è implementata nell'infrastruttura Wi-Fi dell'Amministrazione per l'erogazione del servizio presso alcune specifiche aree. È previsto l'ampliamento di tale infrastruttura, volto alla diffusione del servizio Wi-Fi in altre sedi.

Il primo ordinativo non prevede l'acquisizione di Componenti appartenenti a questa tecnologia.

4.1.6 Security Lifecycle Management

La complessa infrastruttura firewall del MEF ha creato l'esigenza di implementare un Sistema per monitorare il ciclo di vita delle regole presenti, razionalizzare l'insieme delle policy e degli oggetti e supportare la struttura addetta alla gestione attraverso funzionalità di audit e reportistica.

A tale scopo, si intende acquisire nel primo ordinativo una soluzione di "Security Lifecycle Management" che soddisfi almeno i seguenti requisiti:

- Certificazioni di prodotto:
  - il Sistema offerto deve essere certificato secondo il modello architetturale OPSEC;
- Compatibilità:
  - il Sistema offerto deve essere in grado di gestire almeno le seguenti tecnologie firewall:

  - CheckPoint;
  - Palo Alto Networks;
  - Fortinet;
  - Juniper;
  - Cisco;
- Razionalizzazione delle policy al fine di:
  - individuare regole obsolete che potrebbero essere eliminate;
  - posizionare le regole in base al numero degli accessi per migliorare le performance;
  - individuare oggetti che non sono utilizzati all'interno di regole in uso;
  - individuare le regole ridondanti, contrastanti o logicamente errate;
- Funzionalità di analisi del rischio e best practices che consentano di:
  - rappresentare la distribuzione del rischio associando tipologia e livello di rischio alle regole presenti;
  - implementare funzionalità di "network topology discovery", producendo mappe topologiche della distribuzione dei firewall.

4.1.7 Componenti hardware e software forniti dall'Amministrazione a supporto della Fornitura

Gli apparati di rete (switch, switch PoE, hub, router, …) necessari per integrare i Sistemi oggetto di acquisizione all'interno dell'infrastruttura MEF, comprensivi della eventuale componente passiva del cablaggio, sono a carico dell'Amministrazione e non sono quindi oggetto di Fornitura.

Se necessario, per l'installazione delle soluzioni offerte, l'Amministrazione potrà mettere a disposizione server HP Proliant (modelli BL460c e BL680c) con sistema operativo Windows Server 2008-R2 (Standard o Enterprise) 64bit oppure Red Hat Enterprise Linux 5.x 64bit.
Si precisa che le Componenti basate su piattaforma Microsoft verranno arruolate su un dominio Active Directory dell'Amministrazione, secondo le politiche di sicurezza da questa adottate.

Inoltre, l'Amministrazione potrà mettere a disposizione le seguenti licenze software:
- Microsoft SQL Server Enterprise Edition 2008;
- Microsoft SQL Server Standard Edition 2008;
- Oracle RDBMS.

Per le soluzioni virtualizzabili, l'Amministrazione potrà mettere a disposizione l'ambiente VMWare VSphere 4.

Al fine di consentire all'Amministrazione un'adeguata e tempestiva predisposizione dei Componenti hardware e software necessari, l'Impresa dovrà eventualmente specificare di

quali Componenti intenda avvalersi tra quelli sopra menzionati, indicando il dimensionamento minimo degli stessi sulla base della soluzione fornita.

In tal caso, al fine di assicurarne una corretta gestione, sui Componenti suddetti, messi a disposizione dall'Amministrazione, dovranno essere installati, a carico dell'Impresa, alcuni dei software indicati di seguito:

- Antivirus:
  - Symantec Corporate Edition 11.x, se il sistema operativo è Microsoft;
  - F-Secure client versione 9.11;
- Monitoraggio:
  - Omnivision;
  - Tivoli;
  - NetX 2.5 e SCOM versione 2007 R2
- HP DataProtector 6.x per il back-up centralizzato.

L'Impresa dovrà garantire la piena compatibilità delle proprie soluzioni con i prodotti software sopra indicati.

4.2 RESPONSABILE DELLA FORNITURA, ATTIVITÀ ESECUTIVE

Entro 5 (cinque) giorni solari dalla stipula del Contratto, l'Impresa comunicherà alla Consip il nominativo del Responsabile della Fornitura, il quale assumerà il ruolo di referente per tutte le attività previste dal Contratto stesso.

Le attività esecutive, a carico dell'Impresa, sono strumentali alla corretta messa in opera della Fornitura. Tali attività, descritte nei paragrafi successivi, sono consegna, installazione, configurazione e supporto alla VdC.

4.2.1 ATTIVITÀ DI CONSEGNA, INSTALLAZIONE E CONFIGURAZIONE (PRIMO ORDINATIVO)

Entro 25 (venticinque) giorni solari, decorrenti dalla "Comunicazione di attivazione", l'Impresa dovrà ultimare la consegna delle apparecchiature e del software con relative licenze, documentazione e manuali d'uso.

I Componenti dovranno essere consegnati presso una o più sedi tra quelle elencate al paragrafo 3.1.1, secondo le indicazioni riportate nella "Comunicazione di attivazione". Sul Documento di Trasporto (DDT), l'Impresa si impegna a riportare il codice del Contratto comunicato dalla Consip.

La consegna e l'installazione dovranno essere effettuate dall'Impresa, attraverso proprio personale specializzato, nei locali indicati dal Committente.

In particolare, le attività di installazione e configurazione dovranno essere ultimate entro 45 (quarantacinque) giorni solari dalla data della "Comunicazione di attivazione".

Le attività esecutive si intendono comprensive di ogni relativo onere e spesa, ivi inclusi, a titolo meramente esemplificativo e non esaustivo, gli oneri relativi ad imballaggio, trasporto, facchinaggio, consegna "al piano", posa in opera, installazione fisica, supporto alla verifica delle funzionalità da parte del Committente, asporto e smaltimento dell'imballaggio e qualsiasi altra attività a queste strumentale.

Relativamente alla Fornitura, l'Impresa dovrà provvedere, a proprio esclusivo onere:

- a richiedere ed ottenere eventuali permessi o autorizzazioni che si rendessero necessari per la consegna/installazione;
- ad acquisire la disponibilità di mezzi speciali e/o di quant'altro necessario a trasportare, scaricare ed a collocare la Fornitura presso le sedi riportate al paragrafo 3.1.1, nei locali indicati dal Committente;
- a smaltire, secondo le normative in vigore, i rifiuti prodotti durante l'installazione degli apparati (imballaggi, residui metallici e plastici, ecc.);
- a collegare in rete i vari componenti della Fornitura, secondo le specifiche di configurazione indicate dal Committente;
- a consegnare, contestualmente alla fine delle attività, i seguenti documenti:
    - il **Rapporto di Fine Installazione**, contenente la dichiarazione di posa in opera dell'Infrastruttura a regola d'arte in base alle norme vigenti, nonché la **Dichiarazione di rispondenza** dei prodotti hardware e software forniti alle specifiche di cui al Capitolato Tecnico;
    - il **Piano di VdC**, condiviso precedentemente con il Committente al fine di recepirne le indicazioni, ed organizzato secondo un modello checklist o tabellare:
        - tipologia, modello, dotazione, numero seriale e posizionamento fisico di ciascuna apparecchiatura installata;
        - identificativi di tutto il software (codice prodotto e numero di licenza) installato su ciascuna apparecchiatura e relativa versione;
        - l'articolazione delle prove proposte per la VdC dei prodotti oggetto della Fornitura.

4.2.2 GESTIONE DEGLI EVENTUALI ORDINATIVI SUCCESSIVI

Il Committente, a seguito di sopravvenute esigenze di evoluzione/adeguamento dell'Infrastruttura di sicurezza si riserva di attivare Ordinativi Successivi.
Il Committente, nella predisposizione degli Ordinativi Successivi, fatto salvo l'ammontare minimo garantito del Contratto (pari al 10% del valore globale), si riserva di

variare, in base alle proprie esigenze tecniche, i massimali di ciascun Listino.

4.2.2.1 Richiesta di Ordinativi Successivi

Per effettuare una richiesta di Fornitura, il Committente comunicherà all'Impresa:

- l'elenco dei beni e dei servizi che intende acquisire (sulla base dei Listini attuali);
- il Dipartimento/Amministrazione ordinante e la/le sede/sedi dove tali beni/servizi dovranno essere consegnati/erogati;
- i tempi massimi delle attività esecutive.

La Richiesta di Fornitura avverrà mediante e-mail all'indirizzo di posta elettronica indicato dall'Impresa. La data della suddetta e-mail costituirà il riferimento per il rispetto dei tempi esecutivi della Fornitura.
All'interno delle fatture, l'Impresa dovrà inserire il riferimento al Dipartimento/Amministrazione ordinante.

4.2.2.2 Attività esecutive relative ad Ordinativi Successivi

L'Impresa, entro 5 (cinque) giorni solari dalla data di ricezione dell'e-mail di richiesta del Committente, dovrà trasmettere un "piano dei lavori" con la previsione delle attività di consegna, installazione e configurazione e di erogazione delle risorse professionali all'uopo destinate, rispettando le seguenti tempistiche:

- consegna: entro 30 (trenta) giorni solari dall'approvazione del piano dei lavori;
- installazione e configurazione: entro 40 (quaranta) giorni solari dall'approvazione del piano dei lavori.

La pianificazione, una volta concordata con il Committente, dovrà essere rispettata dall'Impresa pena l'applicazione delle penali previste nel Contratto.

Al termine delle fasi di consegna, installazione e configurazione, l'Impresa dovrà fornire il **Piano di VdC** ed il **Rapporto di Fine Installazione,** la cui data di consegna sarà considerata come **Data di ultimazione della Fornitura**.

4.2.3 SUPPORTO ALLA VERIFICA DELLA CONFORMITÀ

Entro 40 (quaranta) giorni solari, decorrenti dalla **Data di ultimazione della Fornitura,** questa sarà sottoposta a VdC, anche a campione, da parte di Consip/Amministrazione. La VdC verrà eseguita da una Commissione di Verifica della Conformità, in contraddittorio con l'Impresa.

A tal fine, l'Impresa dovrà:

- accettare che la VdC comprenda, oltre alle prove indicate nel Piano di VdC, anche ulteriori prove indicate da Consip/Amministrazione;

- fornire supporto durante la VdC.

La VdC delle apparecchiature si intende positivamente superata solo se tutte le componenti hardware e software risultino funzionare correttamente, singolarmente e integrate tra loro, secondo le specifiche del presente Capitolato e della documentazione tecnica e d'uso fornita dall'Impresa.

Al termine della VdC verrà redatto un apposito verbale e nel caso di esito positivo della VdC, verrà rilasciato al fornitore un "Certificato di verifica di conformità" la cui data . sarà considerata come **Data di accettazione della Fornitura**.

Nel caso di esito negativo della VdC, l'Impresa dovrà eliminare i vizi accertati entro il termine massimo di 5 (cinque) giorni solari. In tale ipotesi, la VdC verrà ripetuta e tutti gli oneri che la Consip dovrà sostenere saranno posti a carico dell'Impresa.

Nell'ipotesi in cui anche la successiva VdC abbia esito negativo, il Committente, ferma restando l'applicazione delle penali, avrà facoltà di dichiarare risolto di diritto il Contratto.

In sede di VdC, l'Impresa si impegna a fornire al Committente tutta la documentazione tecnica ed i dati necessari al fine di consentire al medesimo di provvedere direttamente o tramite terzi alla manutenzione delle apparecchiature.

L'Impresa, in sede di VdC, si impegna, altresì, a fornire al Committente tutte le informazioni di dettaglio necessarie per la presa in carico del bene da parte dell'Amministrazione.

4.3 MANUTENZIONE IN GARANZIA

Nell'ambito della presente Fornitura, è prevista la manutenzione in garanzia per 12 (dodici) mesi a partire dalla **Data di accettazione della Fornitura**, per tutti i componenti hardware e software oggetto di acquisizione.

Il servizio di manutenzione in garanzia dovrà essere erogato dall'Impresa a propria cura e spese, senza alcun onere aggiuntivo per l'Amministrazione, intendendosi ricompreso nel corrispettivo della Fornitura.

Il servizio di manutenzione comprende tutti gli oneri necessari per la perfetta e puntuale esecuzione del servizio stesso, nonché ogni altro onere per mantenere e/o riportare le apparecchiature hardware e i prodotti software in stato di funzionamento coerente con la documentazione.

Il servizio di manutenzione dovrà prevedere:

- apertura di ticket: su richiesta del Committente o di una società da questi indicata, mediante chiamata telefonica (confermata via fax o e-mail);
- supporto telefonico di primo e secondo livello sulle problematiche riguardanti le componenti software oggetto di acquisizione;
- fornitura degli aggiornamenti software e sottoscrizioni per 12 (dodici) mesi.

Il servizio di manutenzione sarà prestato dall'Impresa da lunedì a venerdì dalle ore 9.00 alle ore 18.00.

La Consip e/o l'Amministrazione comunicheranno all'Impresa i malfunzionamenti, via posta elettronica, confermata via fax.

Le richieste di intervento verranno gestite dall'Impresa tramite un tecnico specializzato.

Le parti di ricambio, che dovranno essere identiche alle parti sostituite, verranno fornite dall'Impresa senza alcun onere aggiuntivo per l'Amministrazione; le parti sostituite verranno ritirate dall'Impresa stessa, che ne acquisisce la proprietà. Per gli interventi per i quali si rendesse necessaria la sostituzione di una o più parti, l'Impresa dovrà utilizzare parti di ricambio originali e nuove di fabbrica.

Per ogni intervento di manutenzione dovrà essere redatta, da un incaricato della Consip e/o dell'Amministrazione e da un incaricato dell'Impresa, un'apposita nota di ripristino, in formato cartaceo od elettronico, nella quale dovranno essere registrati l'ora della chiamata e quella dell'avvenuto ripristino, nonché le prestazioni effettuate.

4.4 CONSULENZA SPECIALISTICA

Per tutta la durata del Contratto, il Committente potrà richiedere l'erogazione a consumo di un numero di giornate di Consulenza Specialistica fino all'erosione del sottomassimale previsto, che potranno essere utilizzate per la realizzazione di diverse attività. A titolo esemplificativo ma non esaustivo, ne sono riportate di seguito alcune:

- implementazione di nuove funzionalità derivanti da specifiche esigenze di evoluzione dell'Infrastruttura non note al momento;
- stesura di procedure e politiche di sicurezza inerenti il funzionamento in esercizio della nuova Infrastruttura;
- realizzazione di integrazioni personalizzate tra i Sistemi forniti e quelli presenti attualmente all'interno dell'Infrastruttura.

La Consulenza Specialistica potrà essere richiesta dal Committente o da una società da questi indicata, mediante e-mail o fax, dal lunedì al venerdì dalle ore 9.00 alle ore 18.00 e il sabato dalle ore 9.00 alle ore 13.00.

La Consulenza Specialistica dovrà essere erogata con i seguenti livelli di servizio:

- **tempo di presa in carico, 1 (uno) giorno lavorativo dalla ricezione della richiesta**: l'Impresa deve prendere in carico la chiamata inviando un fax o una e-mail di conferma alla persona di riferimento indicata dal Committente;
- **tempo di intervento 5 (cinque) giorni solari dalla presa in carico**: per intervento s'intende la presenza fisica della risorsa nella sede indicata nella chiamata.

La Consulenza Specialistica dovrà essere erogata dal lunedì al venerdì dalle 9.00 alle 18.00 ed anche in orari notturni o festivi.

Per l'espletamento delle suddette attività l'Impresa dovrà avvalersi di personale certificato nella tecnologia oggetto di intervento (e comunque compresa nell'ambito della Fornitura), ed in possesso di competenza ed esperienza su tematiche inerenti sia aspetti tecnologici sia aspetti di sicurezza informatica.

A seconda delle attività da svolgere, il Committente potrà richiedere che il personale di cui l'Impresa si avvarrà sia in possesso di determinati requisiti e competenze professionali. A titolo esemplificativo ma non esaustivo di seguito vengo indicati alcuni dei requisiti professionali che di volta in volta potrebbero essere richiesti dal Committente:

- almeno 5 anni di esperienza nella progettazione, e realizzazione di architetture di rete, sia cablate sia wireless;
- esperienza comprovata di configurazione e tuning relativa alle componenti dell'Infrastruttura oggetto di Fornitura;
- almeno 5 anni di esperienza in materia di sicurezza informatica, con particolare riferimento alla componente organizzativa, per la progettazione/realizzazione di Sistemi di Gestione della Sicurezza delle Informazioni (SGSI/ISMS);
- certificazione ISO 27001 o equivalenti.

L'Impresa dovrà produrre, di volta in volta, quanto necessario per consentire al Committente di comprovare l'esistenza della suddetta certificazione e dei requisiti professionali richiesti.

Il servizio comprende tutti gli oneri necessari per la perfetta e puntuale esecuzione del medesimo.

Tutte le attività e gli interventi richiesti ed erogati saranno consuntivati mediante apposita **Relazione delle attività di consulenza specialistica svolte**, redatta a cura dell'Impresa ed accettata dall'Amministrazione, nella quale verranno indicati l'orario di inizio, l'oggetto e la durata dell'intervento stesso (mezza giornata o giornata intera a seconda della durata dell'intervento).

4.5 SUPPORTO SPECIALISTICO DI PRODOTTO

Per tutta la durata del Contratto, il Committente potrà richiedere l'erogazione a consumo di un numero di giornate di Supporto specialistico di prodotto fino all'erosione del sottomassimale previsto, che potranno essere utilizzate per la realizzazione di attività tecniche specifiche. A titolo esemplificativo ma non esaustivo, ne sono riportate di seguito alcune:

- implementazione di nuove funzionalità derivanti da specifiche esigenze di evoluzione dell'infrastruttura non note al momento;
- diagnosi e risoluzione di difetti e/o malfunzionamenti dei prodotti.

Per l'espletamento delle suddette attività l'Impresa dovrà avvalersi di personale identificato come focal point del prodotto, riconosciuto dal vendor della tecnologia oggetto di analisi.
L'Impresa dovrà produrre, di volta in volta, quanto necessario per consentire al Committente di comprovare l'esistenza della suddetta qualità.

Il Supporto specialistico di prodotto potrà essere richiesto dal Committente o da una società da questi indicata, mediante mail o fax, dal lunedì al venerdì dalle ore 9.00 alle ore 18.00 e il sabato dalle ore 9.00 alle ore 13.00.

Il Supporto specialistico di prodotto dovrà essere erogato con i seguenti livelli di servizio:

- **tempo di presa in carico, 1 (uno) giorno lavorativo dalla ricezione della richiesta**: l'Impresa deve prendere in carico la chiamata inviando un fax o una e-mail di conferma alla persona di riferimento indicata dal Committente;
- **tempo di intervento 5 (cinque) giorni solari dalla presa in carico**: per intervento s'intende la presenza fisica della risorsa nella sede indicata nella chiamata.

Il Supporto Specialistico dovrà essere erogato dal lunedì al venerdì dalle 9.00 alle 18.00, ed anche in orari notturni o festivi.

Tutte le attività e gli interventi richiesti ed erogati saranno consuntivati mediante apposita **Relazione delle attività di supporto specialistico di prodotto svolte**, redatta a cura dell'Impresa ed accettata dall'Amministrazione, nella quale verranno indicati l'orario di inizio, l'oggetto e la durata dell'intervento stesso (mezza giornata o giornata intera a seconda della durata dell'intervento).

4.6 ADDESTRAMENTO

L'Impresa, nell'ambito del Primo Ordinativo, dovrà erogare un servizio di Addestramento rivolto al personale tecnico dell'Amministrazione, o eventuale personale

di società da questa designate, con lo scopo di fornire loro una adeguata conoscenza delle nuove tecnologie offerte, tale da consentire la gestione delle apparecchiature e dei prodotti software previsti nell'ambito della Fornitura.

L'Addestramento dovrà essere volto all'approfondimento di temi riguardanti l'utilizzo e la gestione dei nuovi prodotti oggetto di Fornitura comprendendo le caratteristiche e le funzionalità salienti, con particolare riferimento alle configurazioni hardware e software adottate. Inoltre dovrà comprendere le comuni problematiche riscontrabili nell'implementazione della tecnologia nell'ambiente applicativo dell'Amministrazione.

Le nuove tecnologie oggetto di addestramento sono le seguenti:

- Next-Generation Firewall;
- Web Application Firewall;
- Security Lifecycle Management.

L'Impresa dovrà erogare una sessione di Addestramento per ogni tecnologia di durata di 3 (tre) giorni, per un totale di 9 (nove) giorni. L'Impresa dovrà inoltre provvedere alla fornitura della documentazione didattica per i discenti, sia su supporto cartaceo, sia su supporto elettronico, comprendente una pianificazione delle sessioni di addestramento con gli argomenti trattati.

Le sessioni di Addestramento dovranno essere svolte da personale certificato sui prodotti offerti e verranno tenute presso un apposito locale, adeguatamente attrezzato, sito in Roma e messo a disposizione dall'Impresa.
L'Impresa dovrà produrre, di volta in volta, quanto necessario per consentire al Committente di comprovare l'esistenza della suddetta certificazione.

Le sessioni di Addestramento dovranno essere erogate, previo accordo con il Committente, entro un tempo massimo di 2 (due) mesi dalla **Data di accettazione della Fornitura**.

Il completo e corretto espletamento delle sessioni di Addestramento sarà certificato mediante apposita **Relazione sull'Addestramento svolto** comprendente un questionario che indichi il livello di gradimento del corso da parte dei discenti, redatta a cura dell'Impresa ed accettata dal personale dell'Amministrazione, nella quale verranno indicati l'oggetto e la durata delle sessioni di Addestramento svolte.

4.7 ULTERIORI REQUISITI DELLA FORNITURA

4.7.1 Affidabilità dell'hardware

Le apparecchiature richieste nell'ambito del Capitolato Tecnico dovranno presentare caratteristiche intrinseche di robustezza ed affidabilità tali da limitare le possibilità di malfunzionamento delle apparecchiature stesse, ed in maniera più generale, dell'intera infrastruttura.
L'affidabilità di una singola apparecchiatura è normalmente misurata utilizzando il parametro MTBF (Mean Time Between Failure).
In configurazioni ed architetture complesse, non è però immediatamente e linearmente definibile un requisito di MTBF dell'infrastruttura complessiva in funzione degli MTBF delle singole apparecchiature o addirittura del singolo Componente costituente l'apparecchiatura.
La misura indiretta dell'affidabilità di una apparecchiatura può essere peraltro valutata dalla sua presenza stabile e collaudata sul mercato, dato che i produttori, a fronte di problemi ripetitivi che scaturiscano da una insufficiente affidabilità di componenti o apparecchiature, normalmente provvedono ad un ritiro dal mercato ed a politiche di richiamo e sostituzione.

4.7.2 Inacessibilità

In merito agli aspetti relativi all'inaccessibilità dei Componenti e nell'ottica della riduzione dei potenziali rischi conseguenti a manomissioni, anche involontarie, da parte di personale non qualificato o non addetto, si richiede che i componenti oggetto della presente Fornitura consentano il blocco logico (con chiave) o la protezione fisica (con sportello dotato di serratura), laddove applicabile, dei comandi di accensione/spegnimento/reset.

4.8 MODALITÀ DI AGGIORNAMENTO DEI LISTINI

4.8.1 Aggiornamento tecnologico

L'Impresa, per tutta la durata del Contratto, avrà facoltà di richiedere l'aggiornamento dei Listini per far fronte ad evoluzioni delle tecnologie. Gli aggiornamenti dovranno essere adeguatamente motivati, proponendo la sostituzione di singoli Componenti hardware o software già presenti nel Listino con altri Componenti.

Il Committente si riserva la facoltà di valutare le motivazioni tecniche prodotte dell'Impresa, nonché di chiedere eventuali chiarimenti, e, se ritiene giustificata l'istanza, procederà all'aggiornamento dei Listini.

Resta fermo che la scontistica proposta dall'Impresa all'atto della presentazione dell'Offerta rimarrà invariata anche per i Listini aggiornati.

5 DOCUMENTAZIONE

Ai fini dell'esecuzione del Contratto, l'Impresa dovrà produrre tutta la documentazione tecnica contenente la descrizione dettagliata e le caratteristiche di tutti i prodotti hardware forniti (technical reference, installation guide, tuning guide, etc.).
Tale documentazione dovrà essere redatta in lingua italiana, o in subordine in lingua inglese, e dovrà essere fornita su supporto magnetico (CD-ROM/DVD-ROM).

Oltre alla documentazione descritta in precedenza, l'Impresa dovrà produrre i **Manuali di Gestione** sistemistica ed applicativa dei Sistemi dell'Infrastruttura, sulla base di un *template* fornito da Consip/Amministrazione. Tali Manuali di Gestione dovranno essere consegnati contestualmente con il **Piano di Verifica della Conformità** e la loro approvazione costituirà parte integrante delle verifiche comprese nell'attività di VdC.

5.1 ULTERIORE DOCUMENTAZIONE TECNICA DEGLI APPARATI

Allo scopo di consentire un eventuale adeguamento dell'ambiente in cui verranno ospitate le apparecchiature, l'Impresa dovrà fornire, 10 (dieci) giorni solari prima della consegna dei nuovi apparati, le seguenti informazioni:

- dimensioni volumetriche e peso dei singoli oggetti;
- specifiche di assorbimento elettrico di ogni apparato;
- quantità di calore emesso da ogni singolo Componente;
- documentazione relativa al rispetto delle norme di sicurezza e delle direttive europee di tutte le apparecchiature.

6 CERTIFICAZIONI DELL'IMPRESA

L'Impresa dovrà dimostrare, producendo tutta la relativa documentazione (anche in autocertificazione), la sussistenza dei requisiti per il rispetto delle seguenti normative:

- DPR. 27/04/1955 n. 547 e DPR. 07/01/1956, sull'osservanza da parte dei singoli lavoratori delle norme di sicurezza citate e sull'uso dei mezzi di protezione messi a loro disposizione;
- DPR. 19/03/1956 n. 303, Norme Generali per l'igiene del lavoro;
- D.Lgs. 19 settembre 1994 N. 626, attuazione direttive CEE riguardanti il miglioramento della sicurezza e della salute dei lavoratori sul luogo di lavoro e successivi aggiornamenti;
- Legge n. 46 del 05/03/1990: norme sulla sicurezza degli impianti e relativo DPR 447/91 di attuazione, per quanto attiene alla installazione dei Componenti.

All'Impresa viene inoltre richiesto che le apparecchiature offerte siano state prodotte in regime di qualità, certificato ISO-9001:2000 in corso di validità alla data di pubblicazione e di chiusura del Bando di Gara relativo alle apparecchiature in oggetto.
Il mantenimento della validità della certificazione viene richiesto anche per tutto l'arco della durata della manutenzione.
Dovrà essere prodotta tutta la documentazione (anche in autocertificazione) attestante la sussistenza di tutti i suddetti requisiti.

Dovrà inoltre essere prodotta tutta la certificazione (o autocertificazione) circa la sussistenza dei suddetti requisiti per le apparecchiature fornite.

7 REQUISITI DI CONFORMITÀ DELL'INFRASTRUTTURA

Dovranno essere rispettate tutte le disposizioni attualmente vigenti in materia di sicurezza dell'informazione, di privacy, emissioni elettromagnetiche, sia a livello nazionale che comunitario (o, in sua assenza, internazionale). A titolo puramente indicativo e non esaustivo, si riportano di seguito alcuni esempi:

- requisiti per i videoterminali indicati nella circolare 71911/10.0.296;
- requisiti indicati dal D.Lgs. 19 settembre 1994 n.626;
- D.Lgs. 9 aprile 2008 n. 81 in materia di tutela della salute e della sicurezza nei luoghi di lavoro;
- requisiti di ergonomia riportati nella direttiva CEE 90/270 recepita dalla legislazione italiana nella legge N.142 del 19 febbraio 1992;
- requisiti di sicurezza I.M.Q. (Istituto Marchio di Qualità) e di emissione elettromagnetica FCC (Federal Communications Commission); in alternativa, dovranno almeno rispettare analoghi requisiti certificati da altri Enti riconosciuti a livello europeo, nel qual caso l'Impresa dovrà allegare una descrizione delle prove effettuate e dei risultati ottenuti;
- Legge quadro 22 febbraio 2001, n. 36 "sulla protezione dalle esposizioni a campi elettrici, magnetici ed elettromagnetici"
- norme di sicurezza CEI 74/2 (EN 60950/IEC 950);
- norme di sicurezza CEI 110/5 (EN 55022/CISPR 22);
- cablaggio strutturato EN 50173 e ISO/IEC 11801;
- misure dei parametri elettrici e trasmissivi secondo la norma IEC 1156;
- guaine secondo norme IEC 332-3 C;