CLASSIFICAZIONE DEL DOCUMENTO: CONSIP PUBLIC

ALLEGATO 4

CAPITOLATO TECNICO

ACQUISIZIONE DI HARDWARE, SOFTWARE E SERVIZI PER L'EVOLUZIONE E L'AGGIORNAMENTO DELL'INFRASTRUTTURA DI SICUREZZA DEL MINISTERO DELL'ECONOMIA E DELLE FINANZE E DELLA CORTE DEI CONTI

Sommario

1 INTRODUZIONE

Il presente Capitolato Tecnico descrive gli aspetti tecnici della fornitura dei sistemi hardware e software e dei servizi correlati necessari per l'evoluzione e l'aggiornamento dell'infrastruttura di sicurezza del Ministero dell'Economia e delle Finanze (di seguito MEF) e della Corte dei conti (di seguito Cdc). La fornitura, oltre a comprendere le attività esecutive di consegna, installazione, configurazione e supporto alla verifica di conformità, prevede l'esecuzione di servizi correlati che consistono in manutenzione in garanzia nonché, su richiesta del Committente, supporto specialistico e addestramento.

Le caratteristiche tecniche indicate sono sempre da intendersi come requisiti minimi della fornitura, se non diversamente specificato.

2 DEFINIZIONI ED ABBREVIAZIONI

Si riportano di seguito le definizioni con cui interpretare termini, espressioni ed abbreviazioni che vengono utilizzati nella documentazione di gara, evidenziati nel presente documento in *grassetto corsivo*.

Tabella 1 Definizioni

Amministrazione	l'insieme delle strutture del Ministero dell'Economia e delle Finanze e della Corte dei conti, utenti dei servizi descritti nel presente Capitolato Tecnico;
Committente	Sogei, Società Generale di Informatica;
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*;
Fornitore/Impresa	l'impresa, RTI o Consorzio che risulterà aggiudicatario dell'appalto cui il presente Capitolato Tecnico si riferisce;
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*;
Listini	elenchi di prodotti e di servizi attinenti aspetti di sicurezza informatica, relativi alle diverse tecnologie di interesse, allegati in appendice 1 al presente Capitola Tecnico, da cui è possibile attingere gli oggetti delle varie acquisizioni;
Ordinativo successivo	le acquisizioni, eventualmente effettuate dalle *Amministrazioni* successivamente al *primo ordinativo*, necessarie per far fronte ad evoluzioni e/o adeguamenti tecnologici della propria infrastruttura di sicurezza;
Primo Ordinativo	la prima acquisizione, effettuata all'atto della stipula del Contratto per far fronte alle esigenze attuali delle *Amministrazioni*;
Responsabile della fornitura	svolge il ruolo di coordinamento generale e di figura unica di riferimento per conto del *Fornitore*;
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;

Stazione appaltante *Consip S.p.A.*

Tabella 2 - Abbreviazioni

Cdc	Corte dei conti
HA	High Availability
IPS	Intrusion Prevention System
MEF	Ministero dell'Economia e delle Finanze
PoE	Power over Ethernet
PoC	Proof of Concept
RTI	Raggruppamento Temporaneo d'Imprese

3 DEFINIZIONE DELLA FORNITURA

3.1 Oggetto

L'oggetto dell'appalto comprende le seguenti voci:

- Fornitura di *Componenti di sicurezza*, consistenti in apparecchiature hardware e software, comprensive dei servizi di consegna, installazione, configurazione e di manutenzione in garanzia, secondo le specifiche tecniche e le funzionalità descritte nel capitolo 4;
- Servizi di supporto specialistico ed addestramento, da erogarsi secondo le specifiche tecniche e le funzionalità descritte nel capitolo 5.

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

3.2 Sedi

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

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

3.3 Durata

La durata della fornitura è di 36 (trentasei) mesi, a decorrere dalla stipula del Contratto ed eventuali ulteriori 12 mesi, limitatamente all'erogazione del servizio di manutenzione in garanzia sui prodotti acquisiti nel periodo compreso tra il 24° e il 36° mese di vigenza contrattuale.

4 COMPONENTI DI SICUREZZA: CARATTERISTICHE, MODALITÀ DI ACQUISIZIONE E TECNOLOGIE

4.1 Caratteristiche della fornitura

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

1. tutti i *Componenti* dovranno soddisfare i requisiti e presentare caratteristiche tecniche non inferiori a quanto previsto nel presente Capitolato Tecnico;
2. i *Componenti* oggetto di acquisizione ed i servizi a questi correlati dovranno rispettare le normative vigenti in materia di sicurezza dell'informazione, di privacy, emissioni elettromagnetiche e sicurezza sul lavoro specificati al paragrafo 6.3;
3. tutti gli apparati forniti dall'*Impresa* dovranno essere nuovi di fabbrica ed essere costruiti utilizzando parti nuove;
4. l'*Impresa* dovrà garantire l'interoperabilità e la compatibilità di tutti i *Sistemi* che costituiscono la soluzione proposta di volta in volta in risposta al relativo ordinativo;
5. l'*Impresa* dovrà provvedere a consegnare, installare ed avviare tutti i *Componenti* presso le sedi indicate dal *Committente*;
6. 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 (o, nel caso di *Ordinativi Successivi*, alla data di invio della richiesta);
7. una volta effettuata la consegna l'*Impresa* dovrà installare sui suddetti *Componenti* l'eventuale software, non oggetto della fornitura (per esempio software di gestione e monitoraggio), fornito dall'Amministrazione.

Relativamente alle tecnologie oggetto della presente fornitura, nel caso in cui i prodotti forniti non garantiscano la rispondenza nativa ai requisiti di volta in volta specificati da *Sogei/Amministrazione*, l'*Impresa* dovrà predisporre, a suo totale carico, tutte le attività necessarie a garantirne il corretto funzionamento (per esempio, la realizzazione di specifici connettori o configurazioni).

Si fa presente che, laddove applicabile, a tutela del precedente investimento dell'Amministrazione, l'Impresa dovrà prevedere il "trade-in" delle licenze software e degli apparati hardware, ovvero la valorizzazione dei beni, di proprietà dell'Amministrazione stessa, eventualmente sostituiti in virtù di una nuova acquisizione.

4.1.1 *Affidabilità dell'hardware*

Le apparecchiature richieste 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.

4.2 Modalità di acquisizione di *Componenti di sicurezza*

Il *Committente* ha inteso organizzare l'acquisizione dei *Componenti di sicurezza* in maniera da rispondere in modo efficiente e flessibile alle esigenze attuali e future delle *Amministrazioni* in tema di *Infrastrutture di Sicurezza*.

Pertanto, al fine di garantire da una parte il soddisfacimento delle esigenze attuali delle Amministrazioni e dall'altra un efficiente approvvigionamento a fronte di eventuali nuove esigenze, il *Committente* ha predisposto dei *Listini,* riportati in appendice al presente Capitolato, in cui sono elencati i prodotti di interesse e le relative quotazioni massime. Le caratteristiche tecniche dei prodotti oggetto di acquisto corrispondono a quelle dei modelli presenti nei listini in appendice.

L'*Impresa* dovrà formulare la propria offerta indicando gli sconti, che rimarranno invariati per tutta la durata contrattuale, da praticare su ciascun *listino* previsto in gara. Successivamente alla stipula del Contratto, la *Sogei* invierà all'Impresa una "Comunicazione di attivazione" relativamente alla fornitura del "*Primo Ordinativo*", attinto dai *Listini* e descritto nel paragrafo 4.4.1.

Gli eventuali *ordinativi successivi*, relativi ai prodotti che di volta in volta l'*Amministrazione* tramite la Committente vorrà acquisire, potranno essere disposti fino alla scadenza o al raggiungimento dell'importo massimo contrattuale prefissato.

Il Committente garantisce che, nell'ambito del Contratto, verranno effettuati acquisti per un importo almeno pari al 10% del massimale contrattuale o il più alto valore corrispondente al primo ordinativo. Il *Committente* potrà superare i massimali dei *Listini* di prodotti fino ad un massimo pari al 20% del valore del massimale del corrispondente listino, comunque nel rispetto dell'importo contrattuale massimo complessivo.

Le modalità di gestione degli *Ordinativi Successivi* sono descritte nel paragrafo 4.4.2 .

L'Impresa dovrà indicare, entro 5 (cinque) giorni solari dalla stipula del Contratto, un apposito indirizzo di posta elettronica, al quale la *Sogei* inoltrerà le richieste di ordinativo ed un numero telefonico/fax per tutte le altre comunicazioni.

4.2.1 *Aggiornamento tecnologico dei listini*

Il *Committente*, per tutta la durata del Contratto, potrà proporre l'aggiornamento dei Listini per recepire le eventuali evoluzioni delle tecnologie ivi incluse.

Anche l'Impresa, per tutta la durata del Contratto, avrà facoltà di proporre l'aggiornamento dei **Listini** per recepire le evoluzioni delle tecnologie. Gli aggiornamenti dovranno essere adeguatamente motivati, proponendo la sostituzione di singoli *Componenti* hardware o software già presenti nel *Listino* (usciti di produzione) o l'aggiunta nel *Listino* di *Componenti* funzionalmente equivalenti a quelli presenti. Il *Committente* si riserva la facoltà di valutare le proposte e le motivazioni tecniche prodotte dall'Impresa nonché di chiedere eventuali chiarimenti, e, ove le condivida, di approvarle.

In seguito all'approvazione si procederà all'aggiornamento e/o all'ampliamento dei *Listini*.

In entrambi i casi resta fermo lo sconto offerto in fase di gara per ciascun *Listino* che si intende aggiornare.

4.2.2 *Aggiornamento economico dei listini*

L'Impresa, per tutta la durata del Contratto, avrà facoltà di richiedere, con cadenza annuale, l'aggiornamento economico dei listini, che sarà attuato sulla base di una richiesta del Fornitore, debitamente motivata (e documentata) rispetto alle effettive variazioni verificatesi sui prodotti dei *Listini* ufficiali oggetto di Fornitura, e della successiva accettazione del *Committente*.

Analogamente anche il Committente, per tutta la durata del Contratto e con cadenza annuale, avrà facoltà di proporre tale aggiornamento economico

Anche a fronte di tali aggiornamenti, la scontistica proposta dall'Impresa all'atto della presentazione dell'Offerta rimarrà invariata anche per il *Listino* eventualmente aggiornato.

4.3 Tecnologie

I *Componenti* oggetto di possibili acquisizioni nel corso del Contratto sono indicati nella tabella seguente :

Componente	Tecnologia
Firewall perimetrali e di rete	**Checkpoint** e **Fortinet**
Firewall applicativi e firewall di nuova generazione	**Imperva**, **Palo Alto Networks**

Intrusion Prevention System/Vulnerability Assessment dei sistemi	**IBM**, **Checkpoint**
Sistemi Wireless e soluzioni di Wireless Security	**Aruba Networks**
Security Lifecycle management	**Skybox**
Vulnerability Assessment delle applicazioni	**HP**
Performance monitoring	**Network Instruments**
Security Service Assurance	**VSS Monitoring**

In Appendice sono riportati, per ogni tecnologia, i *Listini* con l'elenco puntuale dei singoli *Componenti* oggetto di fornitura.

4.4 Ordinativi e consegne

4.4.1 Primo ordinativo

Le *Componenti* che fanno parte del *Primo Ordinativo* sono:

- 1 modulo "SkyBox Network Assurance" fino a 100 devices;
- 1 modulo " SkyBox Risk Control" fino a 500 devices.

Entro 25 (venticinque) giorni solari, decorrenti dalla data della "Comunicazione di attivazione" di cui al paragrafo 4.2, l'*Impresa* dovrà, pena l'applicazione delle penali previste nel Contratto, ultimare la consegna delle apparecchiature e del software con relative licenze, documentazione e manuali d'uso. Le attività di installazione e configurazione dovranno essere ultimate entro 45 (quarantacinque) giorni solari dalla "Comunicazione di attivazione", pena l'applicazione delle penali previste nel Contratto.

In Appendice 2 del presente Capitolato Tecnico viene riportata la descrizione dell'iniziativa di evoluzione della piattaforma Skybox di System Life Cicle Management da realizzare mediante i prodotti acquisiti con il primo ordinativo di cui al presente paragrafo.

4.4.2 Ordinativi successivi

Successivamente alla Stipula del Contratto, il *Committente*, a seguito di sopravvenute esigenze di evoluzione o adeguamento dell'Infrastruttura di sicurezza delle Amministrazioni, si riserva di attivare *Ordinativi Successivi*.

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

- l'elenco dei beni (contenuti nei *Listini*) e dei servizi che intende acquisire;
- *Amministrazione* ordinante e sede/sedi dove tali beni/servizi dovranno

essere consegnati/erogati;

- tempi per lo svolgimento delle attività esecutive.

La richiesta di fornitura avverrà mediante invio di una e-mail all'indirizzo indicato dall'*Impresa*. La data della suddetta e-mail costituirà il riferimento per il rispetto dei tempi esecutivi della fornitura.

L'*Impresa*, entro 5 (cinque) giorni solari dalla data di ricezione dell'e-mail di richiesta del *Committente*, dovrà, pena l'applicazione delle penali previste nel Contratto, trasmettere un "Piano di lavoro" con la previsione delle attività di consegna, installazione e configurazione e di erogazione delle risorse professionali all'uopo destinate, rispettando le seguenti tempistiche salvo diverso accordo con il Committente:

- consegna: entro 30 (trenta) giorni solari dall'approvazione del "Piano di lavoro", pena l'applicazione delle penali previste nel Contratto;
- installazione e configurazione: entro 40 (quaranta) giorni solari dall'approvazione del "Piano di lavoro", pena l'applicazione delle penali previste nel Contratto.

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

4.4.3 Consegna ed installazione

La consegna e l'installazione dovranno essere effettuate dall'*Impresa*, attraverso proprio personale specializzato, nei locali indicati dal *Committente* presso una o più sedi comprese tra quelle elencate al paragrafo 3.2.

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 di conformità da parte del *Committente*, asporto e smaltimento dell'imballaggio e qualsiasi altra attività a queste strumentale.

In particolare, l'*Impresa* dovrà provvedere, a proprio esclusivo onere:

- a richiedere ed ottenere eventuali permessi o autorizzazioni che si rendessero necessari per la consegna/installazione;
- a riportare il codice del Contratto, preventivamente comunicato dalla *Sogei* sul Documento di Trasporto (DDT);
- ad acquisire la disponibilità di mezzi speciali e/o di quant'altro necessario a trasportare, scaricare ed a collocare gli oggetti di fornitura presso le sedi

indicate;

- 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, alla fine delle attività di cui all'oggetto del presente paragrafo, 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 presente Capitolato Tecnico. La data di consegna suddetto rapporto sarà considerata come "Data di ultimazione della fornitura";
- a consegnare, pena l'applicazione delle penali previste nel Contratto, entro il termine di 5 (cinque) giorni solari dalla "Data di ultimazione della fornitura" il Piano di Collaudo, per approvazione del Committente, organizzato secondo un modello checklist o tabellare contenente almeno:
    - 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 le Verifiche di Conformità dei prodotti oggetto della fornitura.

4.5 Hardware e software a supporto della fornitura

Gli apparati di rete (switch, switch PoE, hub, router, etc.) necessari per integrare i Sistemi oggetto di acquisizione all'interno delle infrastrutture *MEF* e *Cdc*, comprensivi dell'eventuale componente passiva del cablaggio, sono a carico delle *Amministrazioni* e non sono, quindi, oggetto di fornitura.

Se necessario, per l'installazione delle soluzioni offerte, le *Amministrazioni* potranno mettere a disposizione server blade HP Proliant (modelli BL460c e BL680c) con sistema operativo Windows Server 2008-R2 (Standard o Enterprise) 64bit oppure Red Hat Enterprise Linux 6.x 64bit.

Si precisa che le *Componenti* basate su piattaforma Microsoft verranno arruolate ai domini Active Directory della rispettiva *Amministrazione*, secondo le politiche di sicurezza da questa adottate.

Inoltre, le *Amministrazioni* potranno eventualmente mettere a disposizione le

seguenti licenze software:

- Microsoft SQL Server Enterprise Edition 2008;
- Microsoft SQL Server Standard Edition 2008;
- Oracle RDBMS.

Per le soluzioni software virtualizzabili, le *Amministrazioni* potranno mettere a disposizione l'ambiente VMWare VSphere 5.

Al fine di consentire alle *Amministrazioni* un'adeguata e tempestiva predisposizione dei *Componenti* hardware e software necessari, l'*Impresa* dovrà specificare di quali *Componenti* intenda eventualmente 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;
  - Microsoft SCEP 2013;
- Monitoraggio:
  - Tivoli;
  - NetX versioni 2.5/3.3.1 e SCOM versione 2007 R2;
  - HP DataProtector 6.x e 8.x per il back-up centralizzato.

4.6 Verifica di Conformità

In corso di Contratto, all'esito dell'esecuzione di ogni fornitura e/o servizio, il *Committente* effettuerà la Verifica di Conformità delle prestazioni contrattuali volta a certificare che le stesse siano eseguite a regola d'arte sotto il profilo tecnico-funzionale.

Entro 20 (venti) giorni solari, decorrenti dalla data di ultimazione della fornitura, questa sarà sottoposta a Verifica di Conformità da parte di *Sogei*.

La Verifica verrà effettuata ai sensi dell'art. 314 del DPR 207/2010 a seconda della complessità dell'oggetto contrattuale e in contraddittorio con l'*Impresa*.

La Verifica di Conformità potrà comprendere, oltre alle prove indicate nel Piano di Collaudo, anche eventuali ulteriori prove proposte da *Sogei*.

In sede di Verifica, l'*Impresa* si impegna a fornire supporto al *Committente* ed a

consegnare tutta la documentazione tecnica ed i dati necessari per provvedere direttamente o tramite terzi alla manutenzione delle apparecchiature.

La Verifica di Conformità delle apparecchiature si intenderà positivamente superata solo qualora tutte le componenti hardware e software risultino funzionare correttamente, singolarmente ed integrate tra loro, secondo le specifiche del presente Capitolato Tecnico e della documentazione tecnica e d'uso fornita dall'*Impresa*.

Al termine della Verifica sarà redatto un apposito Verbale la cui data, nel caso di esito positivo, sarà considerata come "Data di accettazione della Fornitura".

Nel caso di esito negativo, l'*Impresa* dovrà eliminare i vizi accertati entro il termine massimo di 5 (cinque) giorni solari, pena l'applicazione delle penali previste nel Contratto. In tale ipotesi, la Verifica sarà ripetuta.

La Sogei si riserva la facoltà di eseguire la verifica a campione dei prodotti acquisiti

(che avverrà comunque almeno sul 10% dei prodotti hardware e software acquistati); in caso di esito negativo, l'*Impresa* dovrà eliminare i vizi accertati entro il termine massimo di 5 (cinque) giorni solari, pena l'applicazione delle penali previste nel Contratto. In tale ipotesi, la verifica potrà essere effettuata, oltre che sui prodotti già verificati, anche su altri prodotti, fermo restando che gli effetti che si produrranno saranno comunque quelli del secondo tentativo di verifica di cui all'art. 11S comma 14.

Tutti gli oneri che la *Sogei* dovrà sostenere in relazione alle verifiche saranno posti a carico dell'*Impresa*.

Qualora anche la successiva Verifica avesse esito negativo, il *Committente*, ferma restando l'applicazione delle penali, avrà facoltà di dichiarare risolto di diritto il Contratto con facoltà di richiedere il maggior danno.

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

Con riferimento al servizio di "supporto specialistico", la Verifica di Conformità sarà avviata entro il mese successivo a quello di riferimento, in seguito alla consegna della "Relazione delle attività svolte" di cui al successivo paragrafo 5.

Con riferimento al servizio di "Addestramento", la Verifica di Conformità sarà avviata entro il mese successivo a quello di riferimento, in seguito alla consegna della "Relazione delle attività svolte" di cui al successivo paragrafo 5.

4.7 Manutenzione in garanzia

Per tutti i componenti hardware e software oggetto di acquisizione è prevista la manutenzione in garanzia per 12 (dodici) mesi a partire dalla "Data di accettazione della Fornitura".

Il servizio di manutenzione in garanzia dovrà essere erogato dall'*Impresa* a propria cura e spese, senza alcun onere aggiuntivo per l'*Amministrazione*, intendendosi ricompresi nel corrispettivo della fornitura 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 in garanzia dovrà prevedere:

- disponibilità di un call center per l'apertura di ticket su richiesta del *Committente* o di una società da questi indicata;
- supporto telefonico di primo e secondo livello sulle problematiche riguardanti le componenti oggetto di acquisizione;
- fornitura degli aggiornamenti software e sottoscrizioni per 12 (dodici) mesi.

Il *Committente* comunicheranno all'*Impresa* i malfunzionamenti attraverso il Call center, che provvederà alla memorizzazione dei ticket e di tutte le informazioni relative alla gestione dei malfunzionamenti, rendendole accessibili al Committente.

I malfunzionamenti segnalati al Call center vengono classificati in due categorie (severity code), in funzione della gravità del disservizio:

Severity code 1 : guasto bloccante, che determina la non operatività delle funzionalità di base e/o maggiormente rilevanti;

Severity code 2 : guasto non bloccante che, pur non interrompendo il funzionamento, determina un degrado delle funzionalità.

La classificazione del malfunzionamento dovrà essere effettuata dal call center e il relativo security code dovrà essere associato al ticket contestualmente alla ricezione della segnalazione.

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

Le parti di ricambio, che dovranno essere identiche alle parti sostituite, saranno fornite dall'*Impresa* senza alcun onere aggiuntivo per l'*Amministrazione*; le parti sostituite saranno 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 in manutenzione dovrà essere redatta, da un incaricato della *Sogei* e da un incaricato dell'*Impresa*, un'apposita nota di ripristino (valida ai fine della verifica di conformità), in formato cartaceo od elettronico, nella quale registrare l'ora della chiamata e quella dell'avvenuto ripristino, nonché le prestazioni effettuate.

5 SERVIZI CORRELATI

I servizi correlati all'oggetto principale della fornitura, vengono eseguiti su richiesta del *Committente*. L'attivazione di tali servizi avviene attraverso una comunicazione via e-mail da parte del *Committente* o da una società da questi indicata.

Tutte le attività e gli interventi richiesti ed erogati saranno consuntivati mediante apposita "Relazione delle attività svolte", redatta a cura dell'*Impresa* ed accettata da *Sogei*, nella quale sono indicati l'orario di inizio, l'oggetto e la durata dell'intervento stesso, sulla base dei quali verrà valutato il rispetto dei livelli di servizio e la qualità delle prestazioni svolte.

5.1 Servizi di supporto specialistico

Per tutta la durata del Contratto, il *Committente* potrà richiedere l'erogazione a consumo di giornate di Supporto specialistico da parte di personale dell'*Impresa*, che potrà essere utilizzato per lo svolgimento 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 di sicurezza non note al momento;
- redazione di procedure e politiche di sicurezza inerenti il funzionamento in esercizio della nuova Infrastruttura;
- progettazione di infrastrutture di sicurezza secondo le specifiche tecniche, operative e funzionali indicate dalla *Sogei*;
- diagnosi e risoluzione di difetti e/o malfunzionamenti dei prodotti;
- progettazione/realizzazione di Sistemi di Gestione della Sicurezza delle Informazioni (SGSI) conformi a standard internazionali come, per esempio, ISO27001;
- progettazione di Security Operation Center (SOC) e di soluzioni destinate alla governance della sicurezza;
- realizzazione di integrazioni personalizzate tra i Sistemi forniti e quelli già presenti all'interno dell'Infrastruttura dell'Amministrazione (come ad esempio le Sonde IPS McAfee);
- supporto alla esecuzione di Proof of Concept (PoC), come descritto nel paragrafo 5.1.1;
- supporto alle iniziative connesse all'attuazione dell'Agenda Digitale in materia di sicurezza, secondo le indicazioni e gli obiettivi forniti da AgID.

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

Per l'esecuzione dei servizi 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. L'*Impresa* dovrà produrre, di volta in volta, quanto necessario per consentire al *Committente* di comprovare l'esistenza delle certificazioni e dei requisiti professionali richiesti.

In particolare, tale personale dovrà essere in possesso, a seconda della tematica oggetto di intervento, dei seguenti requisiti minimi che devono essere posseduti in fase di esecuzione contrattuale:

- almeno 3 anni di esperienza nella progettazione e realizzazione di architetture di rete, sia cablate sia wireless;
- almeno 5 anni di esperienza nella progettazione e realizzazione di infrastrutture di sicurezza;
- esperienza di configurazione, personalizzazione e "fine 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);
- certificazione ISO 27001 – LEAD AUDITOR o equivalenti.

Con riferimento allo standard e-CF (European e-Competence Framework), il profilo professionale richiesto corrisponde all'ICT Security Specialist la cui descrizione è illustrata di seguito:

Titolo del profilo	ICT Security Specialist		
Descrizione sintetica	Assicura l'implementazione della politica di sicurezza aziendale		
Missione	Propone ed implementa I necessari aggiornamenti della sicurezza. Consiglia, supporta, informa e fornisce addestramento e consapevolezza sulla sicurezza. Conduce azioni dirette su tutta o parte di una rete o di un sistema.		
Deliverable	**Accountable**	**Responsible**	**Contributor**

	Base di conoscenza o informazione (Sicurezza)	Proposta integrazione nuove tecnologie (Sicurezza)	- Politica di gestione dei rischi - Piano gestione dei rischi - Politica sicurezza informazioni
Task principali	Assicura la sicurezza e l'uso appropriato delle risorse ICT - Valuta rischi, minacce e conseguenze - Fornisce addestramento e formazione sulla sicurezza - Provvede alla validazione tecnica dei tool di sicurezza - Contribuisce alla definizione degli standard di sicurezza - Controlla la vulnerabilità della sicurezza - Controlla gli sviluppi della sicurezza per assicurare la sicurezza fisica e dei dati delle risorse ICT		
e-competence (da e-CF)	C.2. Supporto al cambiamento		Livello 3
	C.3. Erogazione del servizio		Livello 3
	D.9. Sviluppo del Personale		Livello 3
	D.10. Gestione dell'Informazione e della Conoscenza		Livello 3
	E.8. Gestione della Sicurezza dell'Informazione		Livello 3-4
Area di applicazione dei KPI	Misure di Sicurezza adottate		

I servizi specialistici potranno essere richiesti dal *Committente* e dovranno essere erogati con le seguenti modalità:

- tempo di presa in carico: entro 1 (uno) giorno lavorativo dalla ricezione della richiesta di intervento da parte del *Committente* (mediante e-mail contenente gli obiettivi dell'attività, i requisiti da soddisfare, la tipologia di intervento, se diurno e/o notturno/festivo, gli eventuali deliverable attesi), l'*Impresa*, pena l'applicazione delle penali previste nel Contratto, deve rispondere inviando e-mail di presa in carico;
- tempo di risposta: entro 5 (cinque) giorni solari dalla presa in carico, l'*Impresa* dovrà, pena l'applicazione delle penali previste nel Contratto, consegnare per l'approvazione del *Committente*, il "Piano di Lavoro" riportante dettaglio delle

attività, tempi di esecuzione, risorse necessarie in termini di giornate, deliverable di progetto (qualora richiesti). Tale piano dovrà includere inoltre l'esplicita indicazione della data di avvio e conclusione dell'intervento. Entro il medesimo termine di 5 giorni solari, l'*Impresa* dovrà, pena l'applicazione delle penali previste nel Contratto, altresì allegare al "Piano di Lavoro" i curricula o comunque la documentazione necessaria a comprovare l'esistenza dei requisiti professionali richiesti;

- tempo di sostituzione risorsa: nel caso in cui la *Committente* riscontri che i profili professionali non rispettino le prescrizioni del presente Capitolato Tecnico, entro 3 (tre) giorni lavorativi dalla segnalazione, l'*Impresa* dovrà, pena l'applicazione delle penali previste nel Contratto, proporre (fornendo opportuna documentazione) nuovo personale ritenuto idoneo;
- tempo di esecuzione prestazione: tempo, espresso in giorni lavorativi, entro il cui l'*Impresa*, in accordo al "Piano di Lavoro" approvato dalla *Committente*, deve portare a termine le attività richieste pena l'applicazione delle penali previste nel Contratto.

5.1.1 Proof of Concept (PoC)

L'*Impresa*, nell'ambito della fase di analisi/individuazione di nuove soluzioni, dovrà erogare un servizio di supporto allo svolgimento delle PoC realizzate da *Sogei* con l'obiettivo di selezionare la soluzione più adatta a soddisfare specifiche necessità dell'*Amministrazione*. Tale esigenza prevede, a titolo esemplificativo, lo svolgimento delle seguenti attività:

- analisi preliminare dei requisiti tecnici/funzionali e dell'ambiente di riferimento dell'*Amministrazione*;
- predisposizione dei controlli oggetto di verifica;
- supporto alla predisposizione dell'ambiente di test da implementare;
- supporto alle fasi di test.

5.2 ADDESTRAMENTO

L'*Impresa*, nell'ambito delle soluzioni fornite, al fine di soddisfare le esigenze formative espresse dal *Committente*, dovrà erogare, su richiesta del *Committente*, un servizio di addestramento rivolto al personale tecnico coinvolto, o eventuale personale di società da queste designato.

Le attività di addestramento dovranno essere volte all'approfondimento di aspetti riguardanti l'utilizzo e la gestione dei prodotti oggetto di fornitura, le caratteristiche

e le funzionalità salienti, con particolare riferimento alle configurazioni hardware e software adottate nonché le comuni problematiche riscontrabili nell'implementazione della soluzione nell'ambiente applicativo dell'*Amministrazione*.

L'*Impresa* quindi dovrà erogare sessioni di addestramento di durata consona alla complessità e all'ampiezza del contesto interessato garantendo docenti certificati sui prodotti oggetto di addestramento e provvedendo inoltre alla fornitura della documentazione didattica su supporto cartaceo e su supporto elettronico. L'*Impresa* presenterà al *Committente* per accettazione una proposta che includa una pianificazione del numero delle giornate di addestramento, delle sessioni e degli argomenti.

L'*Impresa* dovrà comprovare, di volta in volta, l'esistenza della opportuna certificazione dei docenti.

Le sessioni saranno tenute presso un apposito locale, adeguatamente attrezzato, sito in Roma e messo a disposizione dall'*Impresa*. In alternativa, *Sogei* potrà scegliere, discrezionalmente, di mettere a disposizione dell'*Impresa* un locale situato in una delle sedi indicate al paragrafo 3.2.

Le sessioni di addestramento dovranno essere erogate, previo accordo con il *Committente*, entro un tempo massimo di 60 (sessanta) giorni solari dalla richiesta del *Committente* stesso.

La "Relazione delle attività svolte" di cui al paragrafo 5, per il servizio di addestramento, dovrà comprendere anche un questionario che consenta ai discenti di esprimere il livello di gradimento del corso, predisposto a cura dell'*Impresa* ed accettato dalla *Committente*.

6 ESECUZIONE DELLA FORNITURA

6.1 Referenti

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

Il *Responsabile della Fornitura* dovrà ricoprire il ruolo di responsabile unico all'interno dell'organizzazione operativa del *Fornitore* per quanto riguarda la fornitura ed operare quale interfaccia unica verso il *Direttore dell'esecuzione*.

6.2 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 *Sogei/Amministrazione*. Tali Manuali di Gestione dovranno essere consegnati contestualmente con il Piano di Collaudo e la loro approvazione costituirà parte integrante delle verifiche comprese nell'attività di Verifica di Conformità.

6.2.1 Ulteriore documentazione tecnica degli apparati

Allo scopo di consentire un eventuale adeguamento dell'ambiente in cui saranno ospitate le apparecchiature, l'*Impresa* dovrà fornire, almeno 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.

6.3 Requisiti di conformità

Ove richiesto dal *Committente*, l'*Impresa* dovrà dimostrare, producendo tutta la relativa documentazione (anche in autodichiarazione), la sussistenza dei requisiti per il rispetto delle seguenti normative riportate di seguito nonché di 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):

- D.Lgs. 9 aprile 2008 n. 81 in materia di tutela della salute e della sicurezza nei luoghi di lavoro;
- art. 64 del DPR. 19/03/1956 n. 303, Norme Generali per l'igiene del lavoro;
- DM n. 37 del 22/01/2008, in materia di installazione degli impianti all'interno degli edifici;
- DL n. 300 del 2006 convertito nella legge n. 17 del 26/02/2007;
- requisiti per i videoterminali indicati nella circolare della Presidenza del Consiglio dei Ministri n. 71911/100296;
- 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 n. 36 del 22 febbraio 2001, "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.

6.4 Indicatori di qualità

Il profilo di qualità richiesto dalla fornitura ed i relativi indicatori di qualità sono descritti nel seguito.

Tranne ove espressamente specificato, i valori dei parametri di qualità descritti nei paragrafi seguenti saranno misurati in riferimento alla seguente finestra temporale

di erogazione dei servizi: **Lunedì-Venerdì 9.00-18.00.**

Se non diversamente specificato, i termini temporali espressi in questo paragrafo e relativi sottoparagrafi, sono tutti da intendersi come lavorativi.

6.4.1 IQG01 Presenza di software dannoso

L'indicatore di qualità IQG01 misura il numero di prodotti software, consegnati e/o installati dall'Impresa, che presentano codice dannoso (virus, malware, ecc.).

Caratteristica	Funzionalità	*Sotto-caratteristica*	Conformità
Aspetto da valutare	Assenza di codice dannoso nel software consegnato ed installato		
Unità di misura	N. di prodotti software	*Fonte dati*	e-mail, lettere, verbali, documentazione relativa a codice dannoso
Periodo di riferimento	durata contrattuale	*Frequenza di misurazione*	ad evento
Dati da rilevare	NC =Componenti su cui si rileva presenza di codice dannoso		
Regole di campionamento	Vanno considerate tutte le occorrenze		
Formula	IQG01 = NC		
Regole di arrotondamento	Nessuna		
Valore di soglia	IQG01 = 0		
Azioni contrattuali	L'applicazione delle penali, come specificato nel Contratto		
Eccezioni	Nessuna		

6.4.2 IQG02 Rispetto delle tempistiche

L'indicatore di qualità IQG02 rileva il rispetto delle tempistiche previste. Le scadenze riguardano l'esecuzione di attività pianificate.

Caratteristica	Efficienza	*Sotto-caratteristica*	Efficienza temporale
Aspetto da valutare	Il rispetto di una scadenza stabilita dal contratto o concordata		
Unità di misura	Giorni	*Fonte dati*	Contratto, e-mail, lettere, verbali, documenti di pianificazione
Periodo di riferimento	Giorni solari che intercorrono tra l'inizio di una fornitura o di un servizio e la sua conclusione	*Frequenza di misurazione*	per ogni evento
Dati da rilevare	Data prevista di consegna/esecuzione (data_prev) Data effettiva di consegna/esecuzione (data_eff) Numero totale di scadenze relative al periodo di riferimento (Nscadenze)		
Regole di campionamento	Vanno considerate tutte le scadenze relative al periodo di riferimento		
Formula	$IQG02 = \sum_{j=1}^{Nscadenze} ritardo_j$ dove: $ritardo_i$ = 0 se $data\_eff_i \leq data\_prev_i$ $data\_effi_j - data\_prev_j$ se $data\_effi > data\_prev_i$		
Regole di arrotondamento	Nessuna		
Valore di soglia	IQG02 = 0 giorni		
Azioni contrattuali	L'applicazione delle penali, come specificato nel Contratto		
Eccezioni	Nessuna		

Le scadenze a cui si riferisce l'indicatore descritto previste nel Contratto sono sintetizzate nella tabella seguente:

evento	*Attività*	*decorrenza*	*termine* *data_prev*
Primo ordinativo	consegna fornitura	ricezione "comunicazione di attivazione"	25 giorni solari
Primo ordinativo	configurazione ed installazione fornitura	ricezione "comunicazione di attivazione"	45 giorni solari
Ordinativo successivo	consegna "Piano di lavoro"	ricezione e-mail Ordinativo	5 giorni solari
Ordinativo successivo	consegna fornitura	comunicazione approvazione "Piano di Lavoro"	30 giorni solari **(*)**
Ordinativo successivo	configurazione ed installazione fornitura	comunicazione approvazione "Piano di Lavoro"	40 giorni solari **(*)**
Primo	consegna Piano di collaudo	dalla "Data di	5 giorni

ordinativo/Ordinativi successivi		ultimazione della fornitura"	solari
Primo ordinativo/Ordinativi successivi/	Eliminazione vizi	data di verifica di conformità con esito negativo	5 giorni solari
Servizi di supporto specialistico	presa in carico	ricezione e-mail di richiesta di intervento	1 giorno lavorativo
Servizi di supporto specialistico	risposta / consegna Piano di Lavoro / consegna CV	presa in carico	5 giorni solari
Servizi di supporto specialistico	tempo di sostituzione risorsa	ricezione e-mail di richiesta di sostituzione	3 giorni lavorativi
Servizi di supporto specialistico	Mancato rispetto dei tempi indicati nel "Piano di Lavoro" per la conclusione delle prestazioni	approvazione "Piano di Lavoro"	secondo quanto previsto nel Piano di Lavoro
Servizi di supporto specialistico	Eliminazione vizi	data di verifica di conformità con esito negativo	5 giorni solari
Servizio di addestramento	tempo di esecuzione	ricezione e-mail di richiesta	60 giorni solari

(*) tali scadenze possono essere oggetto di diverso accordo con il *Committente*

6.4.3 IQG03 Turn-over del personale

L'indicatore IQG03 rileva il numero di sostituzioni del personale impegnato nelle attività relative ai servizi di supporto specialistico, effettuate dal Fornitore di propria iniziativa.

Caratteristica	**Efficienza**	*Sottocaratteristica*	**Utilizzazione delle risorse**
Aspetto da valutare	Turn over: numero di risorse sostituite su iniziativa del Fornitore sul servizio di supporto Specialistico		
Unità di misura	Risorse sostituite	*Fonte dati*	E-mail, lettere, verbali
Periodo di riferimento	Durata dell'intervento	*Frequenza di misurazione*	settimanale
Dati da rilevare	Numero risorse sostituite su iniziativa del Fornitore (Nrisorse sostituite)		
Regole di campionamento	Tutte le sostituzioni		
Formula	IQG03 = Nrisorse sostituite		
Regole di arrotondamento	Nessuna		

Valori di soglia	IQG03<= 1
Azioni contrattuali	Il mancato rispetto del valore di soglia comporterà l'applicazione delle penali, come specificato nel contratto
Eccezioni	Nessuna

6.4.4 IQM01 Efficienza degli interventi di manutenzione

L'indicatore IQM01 misura l'efficienza degli interventi di manutenzione attraverso il calcolo della percentuale di malfunzionamenti risolti entro il tempo stabilito per il livello di servizio correlato alla classe di severità.

I malfunzionamenti segnalati al Call center vengono classificati in due classi di severità in funzione della gravità del disservizio, a cui corrisponde un severity code come specificato di seguito:

- Severity code 1: guasto bloccante, che determina la non operatività delle funzionalità di base e/o maggiormente rilevanti; il ripristino della piena funzionalità deve avvenire entro 8 ore lavorative;
- Severity code 2: guasto non bloccante che, pur non interrompendo il funzionamento, determina un degrado delle funzionalità; il ripristino della piena funzionalità deve avvenire entro 16 ore lavorative.

Caratteristica	**Efficienza**	*Sottocaratteristica*	**Efficienza temporale**
Aspetto da valutare	Numero di segnalazioni di malfunzionamento di apparecchiature risolte con esito positivo e concluse nei tempi previsti		
Unità di misura	Ore lavorative	*Fonte dati*	Strumenti di rilevazione e registrazione delle richieste di intervento, e-mail, note di ripristino
Periodo di riferimento	ad evento	*Frequenza di misurazione*	ad evento
Dati elementari da rilevare	Data e Ora (hh/mm/ss) di segnalazione (**TS**) Data e Ora (hh/mm/ss) di risoluzione (**TR**)		
Regole di campionamento	Vanno considerate tutte le segnalazioni di malfunzionamento di apparecchiature		
Formule	IQM01= TR-TS > SCj J=1 (severity code 1) => SCj = 8 ore lavorative J=2 (severity code 1) => SCj = 16 ore lavorative		
Regole di arrotondamento	Non verrà considerata la frazione di ora		

Valore di soglia	IQM01 = 0
Azioni contrattuali	Il superamento del valore di soglia è sanzionato con l'applicazione delle penali, come specificato nel contratto
Eccezioni	ogni causa ostativa, non dipendente dal Fornitore, che impedisca il tempestivo ripristino del servizio

6.4.5 IQF01 Efficacia delle sessioni di addestramento

Caratteristica	**Efficacia**	*Sottocaratteristica*	**Efficacia**
Aspetto da valutare	Efficacia delle sessioni di addestramento		
Unità di misura	Punto percentuale	*Fonte dati*	Risposte ai questionari somministrati ai discenti
Periodo di riferimento	Ad evento	*Frequenza di misurazione*	Per ogni sessione di addestramento
Dati elementari da rilevare	Su una scala: ottimo; buono; discreto; sufficiente; scarso; insufficiente Numero di valutazioni non inferiori a "Buono" (**N_b**) Numero di valutazioni non inferiori a "Sufficiente" (**N_s**) Numero totale di discenti della sessione (**N**)		
Regole di campionamento	Vanno considerate tutte le valutazioni espresse dai discenti. Tutti i discenti devono esprimere la propria valutazione		
Formule	IQF01b= (N_b/N) *100 IQF01s= (N_s/N) *100		
Regole di arrotondamento	Il risultato della misura va arrotondato al punto percentuale: - per difetto se la parte decimale è <= 0,5 - per eccesso se la parte decimale è > 0,5		
Valore di soglia	IQF01b ≥ 20% e IQF01s ≥ 80%		
Azioni contrattuali	l mancato raggiungimento dei valori di soglia comporta la ripetizione della sessione di addestramento con un altro docente, a spese del Fornitore		
Eccezioni	Nessuna eccezione		

APPENDICE 2

Nell'ambito della gara in oggetto, il Dipartimento per gli Affari Generali del MEF ha condiviso con Sogei l'opportunità di realizzare l'evoluzione della piattaforma SkyBox per il System Life Cycle Management dell'infrastruttura di sicurezza. SkyBox è sostanzialmente una suite tecnologica, costituita da diversi moduli funzionali che concorrono alla ottimizzazione ed alla corretta gestione del ciclo di vita dei prodotti di sicurezza ed alla gestione del rischio a livello di infrastruttura IT.

A tal proposito, il DAG era stato promotore di una iniziativa, realizzata nel 2012, riguardante la implementazione di un modulo dedicato specificamente alla ottimizzazione delle regole e delle configurazioni dei firewall. Infatti, tali sistemi di sicurezza sono spesso utilizzati per gestire le comunicazioni a livello di rete e applicativo all'interno della rete di una organizzazione, con la assidua predisposizione di nuove regole ad hoc o la modifica di regole già implementate. Era pertanto necessario dotarsi di uno strumento che consentisse di normalizzare l'elenco delle regole presenti, andando per esempio ad individuare regole duplicate o non più necessarie, ma anche a suggerire lo spostamento di una regola rispetto ad un'altra per aumentare l'efficienza dell'elaborazione. All'interno della suite SkyBox, tali funzioni sono svolte dal modulo Firewall Assurance, che è l'unico attualmente implementato.

Il suddetto modulo è in grado di governare ed ottimizzare il ciclo di vita delle regole e delle configurazioni su sistemi firewall di differenti tecnologie, che includono tutte quelle presenti all'interno della infrastruttura di sicurezza del MEF, ovvero CheckPoint, Fortinet e Palo Alto Networks. Firewall Assurance, infine, consente di verificare la conformità delle regole rispetto alle *best practice* internazionali ed alle politiche di sicurezza dell'organizzazione.

In considerazione dei benefici gestionali e di *performance* ottenuti tramite l'utilizzo di Firewall Assurance e delle ulteriori esigenze di sicurezza emerse nel corso degli ultimi anni, il DAG ha incaricato Sogei di acquisire componenti in grado di integrare ed ampliare le funzionalità di controllo e gestione della sicurezza.

In virtù di ciò, nel Primo Ordinativo della gara in oggetto è prevista la fornitura di due ulteriori moduli appartenenti alla piattaforma SkyBox, ovvero:

Network Assurance: raccoglie ed analizza le configurazioni dei dispositivi di rete,

creando e mantenendo aggiornati un modello ed una mappa topologica dettagliata della rete stessa. In tal modo, il modulo Network Assurance è in grado di rilevare potenziali vulnerabilità causate da errori di configurazione ma anche di supportare le attività di *troubleshooting* nell'individuazione di possibili problemi di connettività e *routing*.

Vulnerability Control: indicato con il precedente nome di **Risk Control** all'interno della Nota Tecnica, questo modulo effettua la rilevazione delle vulnerabilità analizzando le informazioni presenti sulle piattaforme di asset management e le patch installate sui sistemi, valutando automaticamente gli impatti ed i relativi rischi e assegnando una priorità alle attività di *remediation* previste.

I suddetti moduli, così come avviene attualmente per Firewall Assurance, saranno installati su macchine virtuali ed andranno ad estendere "orizzontalmente" la piattaforma SkyBox, ottenendo, di fatto, il risultato di ampliare le attuali capacità di gestione del rischio.