ALLEGATO 4

CAPITOLATO TECNICO

INDICE

1. CONTESTO ORGANIZZATIVO E TECNOLOGICO

Architettura dell'ISTITUTO NAZIONALE PER L'ASSICURAZIONE CONTRO GLI INFORTUNI SUL LAVORO – I.N.A.I.L.

L'I.N.A.I.L. (nel resto del Capitolato tecnico, anche "Amministrazione") ha un modello funzionale che prevede strutture centrali e strutture decentrate su tutto il territorio nazionale.

L'insieme delle Unità Operative Centrali costituisce la Direzione Generale, avente funzioni di direzione, coordinamento, indirizzo operativo, programmazione e controllo.

A livello regionale operano le Direzioni Regionali con compiti di governo del territorio di competenza, supporto delle attività produttive, indirizzo e controllo a garanzia dell'omogeneità e della correttezza di funzionamento delle Sedi Locali. A livello sub-regionale operano le Sedi Locali cui sono affidate la produzione e l'erogazione sul territorio dei prodotti e servizi dell'I.N.A.I.L. e, pertanto, tutte le attività di gestione degli utenti esterni, con particolare riferimento agli assistiti, sono svolte a livello di Sedi periferiche.

Il sistema informatico dell'I.N.A.I.L. è costituito da più sistemi di elaborazione collocati presso la Direzione Centrale Servizi Informativi e Telecomunicazioni (DCSIT) di Roma (sistemi grandi e medi), da sistemi elaborativi dipartimentali (sistemi medi) siti presso le Direzioni Regionali e le Sedi Locali, e da un network di Agenzie e di Telelavoratori interconnessi mediante la rete geografica condivisa con altre pubbliche amministrazioni.

Sono presenti sistemi UNIX like (Sistemi Open Source) e Windows Server 2003/2008 per la realizzazione della architettura aperta che affiancano il sistema centralizzato basato essenzialmente su Mainframe.

Le procedure applicative in esercizio supportano tutte le attività istituzionali e gran parte delle esigenze strumentali e informative.

A partire dal 2011 è iniziato il processo di integrazione con ISPESL e IPSEMA, enti assorbiti dall'I.N.A.I.L..

Contesto tecnico

Il sistema informatico/informativo dell'I.N.A.I.L. è attualmente costituito da:

- sistemi di elaborazione centrali grandi (mainframe e Open Source) e intermedi (Open Source e virtuali) siti presso i 2 CED della Direzione Centrale Servizi Informativi e Telecomunicazioni di Roma (di cui uno dedicato alla business continuity);
- sistemi di elaborazione dipartimentali medi (Open Source) siti presso le Direzioni Regionali e le Sedi Locali per la gestione della produzione, della rete locale, del documentale, ecc., interconnessi mediante la rete geografica condivisa con altre pubbliche amministrazioni;
- postazioni di lavoro (PC e stampanti) ad uso del personale, postazioni di servizio, personal computer portatili, smart phone;

- server Farm presso la DCSIT per la gestione dei servizi di interoperabilità, dei servizi web e di cooperazione applicativa;
- rete geografica di interconnessione all'interno delle sedi I.N.A.I.L. e con le altre Pubbliche Amministrazioni;
- reti locali (presso le Sedi, le Direzioni Regionali, le Direzioni Centrali);
- rete fonia composta da centralini telefonici elettronici con funzionamento a programma, telefoni da tavolo, apparecchi di telefonia mobile assegnati, prevalentemente, a dirigenti, professionisti e personale direttivo e ispettivo;
- diverse tipologie di Software di base;
- patrimonio applicativo e informativo che supporta tutte le attività istituzionali e gran parte delle esigenze strumentali e informative (applicazioni istituzionali per la gestione delle attività di produzione dei servizi connessi alla "mission" aziendale, applicazioni strumentali a supporto dei processi e servizi connessi al funzionamento dell'Ente, applicazioni e banche dati volte a fornire gli strumenti per l'analisi dell'andamento dei processi aziendali e per il controllo di gestione).

Lo stato dell'arte

Attraverso una precedente fornitura della durata di 36 mesi, l'Amministrazione ha realizzato e messo in produzione una soluzione integrata e centralizzata basata sulle tecnologie McAfee per la Sicurezza Perimetrale e Interna a prevenzione delle intrusioni e delle attività malevole originate da codice maligno o da azioni non conformi alle politiche istituzionali.
Per mezzo di questo progetto, l'I.N.A.I.L. ha provveduto a realizzare le attività di adeguamento del sistema in esercizio attraverso:

1) la migrazione dalla suite AVD alla suite TOPs-TEA e l'aggiornamento del sistema ePolicy Orchestrator Server per il controllo e monitoraggio di tutti i software McAfee (Agente di controllo, modulo Antivirus, modulo Anti-intrusione, modulo di Crittografia e modulo per il controllo della Conformità), opportunamente e selettivamente distribuiti a bordo delle Postazioni di Lavoro e dei Server;
2) l'aggiornamento e l'integrazione del Sistema di filtraggio Anti-Malware dei Contenuti Web e URL Filtering, potenziando l'esistente architettura basata sulle piattaforme McAfee SCM WebShield con l'introduzione della soluzione McAfee Web Gateway, basato su Lame di scansione;
3) l'aggiornamento e l'integrazione del sistema di Rilevamento e Blocco delle Intrusioni a livello di Rete basato sul McAfee Network Security Platform, noto come IntruShield;
4) la messa in produzione del McAfee Vulnerability Manager, noto come FoundStone, un sistema di Gestione delle Vulnerabilità informatiche e dell'analisi del Rischio tecnologico correlato alla rilevanza della Vulnerabilità e alla valenza degli Asset istituzionali.

Gli obiettivi perseguiti dall'Amministrazione attraverso l'adeguamento ed il completamento della soluzione McAfee per la sicurezza perimetrale antivirus e antintrusione e la fornitura di servizi professionali, nell'arco dell'ultimo triennio 2009/2012, possono essere così sinteticamente riassunti:

1) mantenimento e miglioramento di un livello di sicurezza adeguato alle esigenze dell'Amministrazione contro le potenziali minacce informatiche provenienti dall'interno e dall'esterno della rete dell'I.N.A.I.L.;
2) garanzia dell'integrità dei dati, protezione del patrimonio applicativo, prevenzione dalla eventuale perdita di dati, protezione della riservatezza dei dati;
3) contrasto e rimedio alle vulnerabilità;
4) miglioramento dell'efficienza ed efficacia della gestione degli strumenti di sicurezza;
5) ottimizzazione dell'infrastruttura tecnologica. L'applicazione di strumenti automatizzati ha consentito la definizione e l'utilizzo di metriche appropriate per la misurazione dei costi, delle prestazioni e dei livelli di servizio.

Nell'ambito delle attività di rinnovo dei servizi di supporto e manutenzione delle licenze Software e alle componenti Hardware si provvederà, tra l'altro, all'adeguamento dei livelli tecnologici delle soluzioni McAfee per mantenere efficiente il sistema in esercizio attualmente presente in I.N.A.I.L..

Descrizione della politica di sicurezza ICT prevista

La sicurezza ICT ruota attorno al dal D. Lgs. 196/03 e alle linee guida ISO 27002. In particolare l'I.N.A.I.L. ha programmato una serie di interventi specifici nell'ambito della "Sicurezza logica".

L'intervento per il rinnovo dei servizi e per il consolidamento del sistema in esercizio per la sicurezza perimetrale antivirus e antintrusione risponde ai seguenti criteri:

a) **Attivazione delle politiche di sicurezza fondamentali.**

   Antivirus - Un virus è una porzione di dati che si trasmette e si moltiplica in un sistema informatico causando una diminuzione di efficienza o un danneggiamento del sistema stesso. Il sistema antivirus rappresenta una barriera contro i vari virus presenti in Rete. E' importante sottolineare come la riduzione dei rischi ai minimi livelli è possibile solamente con una strategia dove la postazione di lavoro deve essere l'ultima linea di difesa, non la prima o l'unica.

   Content management - Sistema per la gestione della sicurezza del "contenuto" delle informazioni, integrando la soluzione antivirus: infatti oggi la sicurezza non significa più soltanto protezione dai virus. I contenuti non desiderati quali lo spamming ed i file multimediali di grandi dimensioni possono abbassare la produttività dei dipendenti e degradare le prestazioni di sistema. I contenuti sconvenienti - quali i messaggi volgari e offensivi - possono comportare responsabilità civili e causare gravi danni alla reputazione di un'azienda.
   La perdita di informazioni riservate e della proprietà intellettuale possono generare danni.

   Antispam - Sistema di sicurezza per la posta elettronica per la protezione dagli attacchi mirati e non mirati connessi alle E-mail, che si interpone fra Internet e il sistema di posta elettronica attivando vari livelli di sicurezza perimetrale completi, ispeziona il traffico E-mail e protegge la rete aziendale da attacchi noti e non noti, come virus e attacchi di virus di nuova generazione, worm e cavalli di Troia. Questa operazione si sviluppa utilizzando un sistema antivirus e un sistema antispam/anti-phishing con tecnologia multipla.

Antispyware - La soluzione previene lo Spyware al gateway, prima che possa entrare all'interno della rete; blocca le fuoriuscite di informazioni non autorizzate e rende sicuro ogni ambiente dagli attacchi di hackers, spyware, worm e virus, controlla il P2P, impedendo che applicazioni non autorizzate si impadroniscano di protocolli legittimi per la distribuzione di malware, e offre funzionalità avanzate di log, archiviazione e protezione delle conversazioni IM e di altri contenuti condivisi per essere allineati alle regolamentazioni (compliance).

NAC – Il componente (già integrato nella suite TEA, oggetto della precedente acquisizione), permette l'adeguamento della sicurezza degli end point. La componente NAC completa una soluzione di sicurezza per l'infrastruttura di accesso e compliance, integrata con l'infrastruttura di rete dell'Amministrazione basata su tecnologia CISCO/ATI/ENTERASYS, per l'accesso in conformità alle policy in uso e per mezzo di autenticazione con il protocollo 802.1x. Si intende utilizzare tale soluzione anche per le postazioni non gestite dall'attuale infrastruttura (ad esempio le postazioni di consulenti esterni).

b) **Filtraggio dei Contenuti Internet** (URL Filtering), funziona come linea di difesa aggiuntiva contro il materiale non gradito. Questo consente di stabilire e imporre accettabili politiche di accesso a Internet in base alle specifiche esigenze. Il Filtraggio dei Contenuti integrato consente di bloccare alcune caratteristiche dei siti Web nonché di monitorare e controllare gli utenti che visitano siti Web impropri e non produttivi

c) **Controlli di sicurezza IP** - Il Vulnerability Assessment è un sistema di rilevazione delle vulnerabilità dei sistemi su IP che aiuta il sistemista di rete/sicurezza a tenersi aggiornato. Il servizio di Verifica delle Vulnerabilità rappresenta idealmente il primo passo da compiere sulla strada del percorso per la messa in sicurezza della propria rete da attacchi e/o tentativi di intrusione non autorizzati. E' una fase che deve avvenire in locale, in quanto presuppone un'indagine approfondita dell'architettura di rete, dei componenti della rete stessa e, soprattutto, della configurazione dei diversi computer presenti in rete e dei software installati su di essi.

d) **Rilevazione delle intrusioni** (Intrusion Detection System - IDS, Intrusion Prevention System – IPS)
E' un sistema di rilevazione delle intrusioni, sia interne che esterne, capace di individuare violazioni delle policy ed attuare dei sistemi di controllo e alerting. Riesce a rilevare attacchi che sono riusciti a passare un firewall ed avvertire gli amministratori dello stato in cui si trova il sistema attaccato.
E' la telecamera della rete e dei sistemi che contengono informazioni critiche.
Individua automaticamente, nel minor tempo possibile e con minor margine di errore, un tentativo di intrusione sia alla propria rete che ai propri sistemi. E' capace di mettere in atto sistemi di difesa contro l'attacco avvenuto.
Mantiene la tracciabilità di un attacco in modo da averne evidenza, anche giuridica, della dinamica dell'intrusione.

e) **Gestione dei dispositivi mobili** (Enterprise Mobility Management). L'evoluzione tecnologica del sistema informativo aziendale, che si sintetizza nello sviluppo di un nuovo moderno portale WEB 2.0, comprende funzionalità specificatamente indirizzate ai dispositivi mobili, inclusi Apple iPhone, iPad e Android. Si intende applicare ai dispositivi mobili lo stesso livello di sicurezza e controllo applicato dall'IT ai Desktop e ai Laptop, includendo la capacità di identificare, marcare e assegnare le policy a smartphone e tablet PC di proprietà dei dipendenti o dell'azienda.

f) **Gestione di ambienti Virtuali Ottimizzati** - Nell'ottica della modernizzazione della propria infrastruttura, I.N.A.I.L. sta costituendo una piattaforma di virtualizzazione che necessita di nuovi

strumenti per poter ottimizzare la sicurezza in ambiente virtuale, ottimizzando al contempo le performance dei sistemi virtuali.
Indipendentemente dal fatto che si utilizzino desktop virtuali o una virtualizzazione dei server ben avviata nel proprio data center, si intende risolvere in modo specifico i problemi che si incontrano comunemente negli ambienti virtualizzati con soluzioni antivirus tradizionali.

g) **Viruscan for Linux for Server -** Soluzione integrata dotata di una console unica (ePO), che permette di ridurre la complessità di gestione della sicurezza dei server Linux; in termini generali si intende perseguire la prevenzione completa dalle minacce antimalware e la gestione centralizzata ed il controllo dei sistemi server Linux.
L'Amministrazione, coerentemente con le indicazioni mirate a prendere in considerazione le soluzioni Open Source, ha realizzato ambienti anche critici basati sulla tecnologia Linux. I.N.A.I.L. ha necessità di acquisire una soluzione in grado di garantire la sicurezza di tali sistemi poiché, al momento, i server Linux non hanno copertura di sicurezza. In considerazione del tasso di crescita dell'ambiente open source occorre raggiungere la totale messa in sicurezza dai malware dei sistemi Linux.

h) **Risk Advisor** - Soluzione integrata con tutte le soluzioni McAfee e nella console unica (ePO), che permette di ridurre la complessità di gestione del rischio e della sicurezza dei sistemi gestiti. Grazie alla presenza di questi strumenti, Risk Advisor riesce a fornire una vista real time dell'indice di rischio delle componenti IT gestite I.N.A.I.L.. Sfruttando l'integrazione nativa con le componenti McAfee, la soluzione ArcSight è in grado di ottenere beneficio dalle informazioni analizzate da Risk Advisor. McAfee Risk Advisor ha la capacità di correlare le informazioni in modo proattivo; ad esempio il prodotto è in grado di correlare un'informazione sulla minaccia con la vulnerabilità e le informazioni sulle contromisure ad esso associate per evidenziare le risorse critiche a rischio, che richiedono un intervento immediato. Risk Advisor agevola nella determinazione delle contromisure necessarie: quali contromisure applicare e quando applicarle, permettendo di approntare azioni di difesa contro le minacce effettive, tra cui attacchi botnet, malware virale e altri pericoli emergenti.

i) **TDA** è una soluzione integrata dotata di una console unica, che permette all'I.N.A.I.L. di ridurre la complessità di gestione della sicurezza aziendale; in termini generali le funzionalità fornite permettono la cifratura del disco fisso, di file e cartelle, a richiesta per le chiavette USB, il controllo dei dispositivi hardware con eventuali esclusioni e controlli, il controllo della movimentazione di dati sensibili. Questa soluzione, già in parte acquisita, permette di non lasciare i dischi rigidi in chiaro e quindi esclude la necessità di ricorrere ad una rottamazione onerosa in caso di dismissione. L'estensione delle licenze è necessaria per avere la possibilità di cifrare e mettere in sicurezza i dati di tutti gli utenti I.N.A.I.L. insieme anche a quelli di ISPSEL e IPSEMA. L'agent è lo stesso che gestisce l'antivirus e le altre soluzioni di sicurezza per l'endpoint McAfee

j) **McAfee Deep SAFE**
Sicurezza hardware-assisted sfruttando un footprinting della sicurezza "più approfondito", per individuare, bloccare e rimediare agli attacchi nascosti avanzati;

k) **Servizio di Supporto Platinum Enterprise** (con Resident SAM e Assigned Product Specialist Support)
Il livello di Supporto McAfee Platinum Enterprise che l'I.N.A.I.L. ha adottato nel passato e che intende continuare ad utilizzare, è comprensivo di un Support Account Manager (disponibile h24 e residente negli orari di lavoro presso gli stabili dell'I.N.A.I.L.) e di vari Specialisti di Prodotto dedicati ad ogni linea di prodotto McAfee (sempre contattabili telefonicamente e via email); il

servizio rappresenta un valore aggiunto e un ritorno pratico considerevole sull'investimento economico in relazione a molteplici aspetti dell'assistenza specializzata su architetture avanzate di protezione dalle minacce informatiche come quelle McAfee, tra cui un unico e fidelizzato punto di contatto per la gestione delle Richieste di Supporto, un costante monitoraggio della postura di sicurezza dell'I.N.A.I.L. attraverso il controllo e la consulenza sull'efficiente utilizzo dei prodotti e delle soluzioni in esercizio, l'allerta sulle più recenti vulnerabilità e frodi telematiche correlate con lo stato di protezione dei sistemi istituzionali più rilevanti, la linea diretta con i Laboratori McAfee in caso di eventi di sicurezza particolarmente importanti e la costante disponibilità di una Squadra di tecnici altamente specializzati che possono fornire assistenza immediata su tematiche di Sicurezza Informatica, siano esse inerenti a nuove tecnologie, a comparazioni di soluzioni diverse che rispondano alle esigenze dell'I.N.A.I.L. o a presentazioni e formazione sui prodotti McAfee in collaudo ed esercizio.

2. OGGETTO DELL'APPALTO

L'ISTITUTO NAZIONALE PER L'ASSICURAZIONE CONTRO GLI INFORTUNI SUL LAVORO – I.N.A.I.L. stipulerà con l'aggiudicatario della procedura ad evidenza pubblica indetta da Consip S.p.A., oggetto della presente iniziativa, apposito contratto, con il quale verrà regolamentata "la fornitura dei seguenti prodotti" e "l'affidamento dei seguenti servizi":

- prodotti McAfee, in particolare: licenze software, apparecchiature hardware e servizi di supporto e manutenzione, come successivamente dettagliato;
- servizi professionali McAfee di supporto/assistenza sistemistica, per lo sviluppo, il deploy ed il supporto alle attività progettuali e servizi di formazione, come successivamente dettagliato.

Nel dettaglio l'Impresa dovrà fornire:

a) servizi di supporto e manutenzione relativi ai prodotti Software in licenza d'uso perpetua e alle apparecchiature Hardware già in possesso dell'Amministrazione per 36 mesi;
b) nuove licenze d'uso perpetue di Software e nuove apparecchiature hardware, fino al massimo previsto dal presente Capitolato Tecnico, e i relativi servizi di supporto e manutenzione connessi per la durata contrattuale della fornitura;
c) il Servizio di Supporto tecnico McAfee Enterprise Platinum (inclusi RSAM e Specialist) per 36 mesi;
d) i seguenti Servizi professionali connessi alla fornitura:
   - servizi di supporto/assistenza sistemistica fino ad un massimo di 571 giorni/persona;
   - erogazione di Corsi formazione.

Tutti i prodotti/servizi sopra indicati devono rispettare le caratteristiche minime stabilite nei successivi paragrafi, pena l'esclusione dalla procedura di gara.

2.1. SUPPORTO E MANUTENZIONE LICENZE SOFTWARE E APPARECCHIATURE HARDWARE - SISTEMA ESERCIZIO ATTUALE

La fornitura dovrà garantire, per 36 mesi :

- il supporto, la manutenzione e l'aggiornamento relativamente alle licenze d'uso perpetue dei prodotti software;
- il supporto e la manutenzione delle apparecchiature hardware;

che attualmente fanno parte del sistema di esercizio dell'I.N.A.I.L. e precisamente :

Cross grade TEA→EPA

- N. 500 licenze del Client HIDS – Host IPS Server;
- N. 4.000 licenze Client TDA;

Codice prodotto	Prodotto	Tipologia	Quantità
HISYFM-AB	MFE HIP for Svrs 1Yr GL [P+]	Support	500
TDAYFM-AA	MFE Total Protection Data 1yr Gold [P+]	Support	4.000

Sistema di Content Management e URL Filtering, in configurazione Disaster Recovery per i due siti I.N.A.I.L.

- N. 4 Content Security Management Blade;
- N. 8 Content Security Scanning Blade;
- N. 1 Content Security Blade Server M7 Chassis
- N. 1 Content Security Blade Server M7 Chassis

Codice prodotto	Prodotto	Tipologia	Quantità
RFMGMTMXX	MFE MCS-MGMT-MXX 1Yr GL Sppt & NBDHWSppt	Support	4
RFBLDE1XX	MFE MCS-BLDE-1XX 1Yr CNSppt&NBDHWSppt	Support	8
RFCH1PM71	MFE MCS-CH1P-M71 M7 1Phase 1YrNBDHWSppt	Support	1
RFCH1PM72	MFE MCS-CH1P-M72 M7 1Phase 1YrNBDHWSppt	Support	1

Sistema di Intrusion & Prevention System

- N. 2 IPS-I-4010 e accessori :
  - N. 12 MM Opt Gigabit FO;
  - N. 4 Copper Gigabit FailOpen;
  - N. 2 Redundant Power Supply;
- N. 2 IPS-M-8000 e accessori :
  - N. 26 SM Opt Gigabit FO;
  - N. 4 Copper Gigabit FailOpen;
  - N. 2 Redundt PowerSupply 8000;
- N. 1 Global Manager;
- N. 1 Global Manager FO;

Codice prodotto	Prodotto	Tipologia	Quantità
IYVS41KADM	MFE Network Sec 4010 Sensor 1Yr GL+RMA	Support	2
REMMF13PTA	MM Opt Gigabit FO Kit 1Yr RMA	Support	12
RBCGFOKT2A	Copper Gigabit FailOpen Kit 1Yr RMA	Support	4
RBAP01PS2	Optional Redundant Power Supply 1Yr RMA	Support	2
IYVM80KADM	MFE Net Sec M-8000 Standard 1yr Gold+RM	Support	2
RESMF13PTA	SM Opt Gigabit FO Kit 1Yr RMA	Support	26
RBCGFOKT2A	Copper Gigabit FailOpen Kit 1Yr RMA	Support	4
RBRPM8PS2	MFE NetSec Redundt PwrSupply 8000 1YrRMA	Support	2
IYVGLBLADM	MFE Network Sec Glbl Mngr App 1YrGL+NBD	Support	1

IYVSTGLADM	MFE Network Sec Appl FO 1Yr GL+NBD	Support	1

Risk Asdvisor & Vulnerability Manager - Foundstone

- N. 3 Appliance MFE Vulnerability Mngr 3000;
- N. 2.500 licenze perpetue MFE Vulnerability Mngr;

Codice prodotto	Prodotto	Tipologia	Quantità
VYV3000ADM	MFE VulnrbiltyMgr MVM3000Appl 1Yr GL+NBD	Support	3
FSWYCM-AA	MFE Vulnerability Mngr EN SW 1YrGL	Support	2.500

2.2. ACQUISIZIONE NUOVE LICENZE SOFTWARE E NUOVE APPARECCHIATURE HARDWARE E RELATIVI SERVIZI DI SUPPORTO E MANUTENZIONE

L'Amministrazione, sulla base delle proprie esigenze, prevede di acquisire, i prodotti e le quantità di seguito indicate:

Cross grade TEA→EPA

- N. 16.150 licenze d'uso perpetue EPA in cross-grade rispetto alle 16.150 licenze d'uso perpetue di TEA attualmente presenti nel sistema di esercizio compreso il servizio di supporto e manutenzione;
- N. 2.350 nuove licenze d'uso perpetue della suite McAfee EPA compreso il servizio di supporto e manutenzione;
- N. 1.000 nuove licenze d'uso perpetue del Client HIDS – Host IPS Server compreso il servizio di supporto e manutenzione;
- N. 800 nuove licenze d'uso perpetue per la Protezione dei Server LINUX compreso il servizio di supporto e manutenzione;
- N. 14.500 nuove licenze d'uso perpetue Client TDA compreso il servizio di supporto e manutenzione;
- N. 1.000 nuove licenze d'uso perpetue Deep Defender compreso il servizio di supporto e manutenzione;

Codice prodotto	Prodotto	Tipologia	Quantità
EPACDE-DA	MFE Endpoint Prxtn - Adv UPGD [P+]:1YrGL	Perpetual License	16.150
EPACDE-AA	MFE Endpoint Protection - Adv P:1 GL[P+]	Perpetual License	2.350
EPAYFM-AA	MFE Endpoint Protection - Adv 1YrGL[P+]	Support	18.500
HISCDE-AB	MFE HIP for Svrs P:1 GL [P+]	Perpetual License	1.000

HISYFM-AB	MFE HIP for Svrs 1Yr GL [P+]	Support	1.000
LXSCKE-AB	MFE VirusScan Ent for Linux P:1 GL	Perpetual License	800
LXSYCM-AB	MFE VirusScan Ent for Linux 1Yr GL	Support	800
TDACDE-AA	MFE Total Protection Data P:1Gold [P+]	Perpetual License	14.500
TDAYFM-AA	MFE Total Protection Data 1yr Gold [P+]	Support	14.500
SDFCDE-AA	MFE Deep Defender P:1 GL [P+]	Perpetual License	1.000
SDFYFM-AA	MFE Deep Defender 1Yr GL [P+]	Support	1.000

Messa in sicurezza e gestione centralizzata dei dispositivi mobili, Smartphone e tablet

- N. 1.400 nuove licenze d'uso perpetue Client EMM, compreso servizio di supporto e manutenzione;

Codice prodotto	Prodotto	Tipologia	Quantità
EMMCDE-AA	MFE Ent Mobility Management P:1Gold	Perpetual License	1.400
EMMYFM-AA	MFE Ent Mobility Management 1YR GL	Support	1.400

Sistema di Content Management e URL Filtering, in configurazione Disaster Recovery per i due siti I.N.A.I.L.

- N. 12.500 Sottoscrizione licenza d'uso perpetue WEB Protection Suite per 36 mesi;
- N. 4 nuovi Content Security Scanning Blade, compreso servizio di supporto e manutenzione;

Codice prodotto	Prodotto	Tipologia	Quantità
WPSECE-AA	MFE Web Protection Suite 1:1 GL	Subscription	12.500
MCS-BLDE-1XX	MFE MCS-BLDE-1XX Blade	Hardware	4
RFBLDE1XX	MFE MCS-BLDE-1XX 1Yr CNSppt&NBDHWSppt	Support	4

Sistema di Network Access Control

- N. 10 NetSec N-550 Appliance, compreso servizio di supporto e manutenzione;
- N. 10 Net Sec Redundant PwrSupply 6050, compreso servizio di supporto e manutenzione;

Codice prodotto	Prodotto	Tipologia	Quantità
IAP-N550-NAC	MFE Net Sec N-550 Appliance	Hardware	10
IAPN550ARMA	MFE Net Sec Appl N-550 1Yr GL+ARMA	Support	10
IAC-RPMS-PS2	MFE Net Sec Redundant PwrSupply 6050	Hardware	10
RBRPMSPS2	MFE NetSec Redundt	Support	10

	PwrSupply 6050 1YrRMA		

Risk Asdvisor & Vulnerability Manager - Foundstone

- N. 22.500 nuove licenze d'uso perpetue MFE Vulnerability Mngr, compreso servizio di supporto e manutenzione;
- N. 25.000 licenze d'uso perpetue MFE Risk Advisor, compreso servizio di supporto e manutenzione;

Codice prodotto	Prodotto	Tipologia	Quantità
FSWCKE-AA	MFE Vulnerability Mngr EN SW P:1 GL	Perpetual License	22.500
FSWYCM-AA	MFE Vulnerability Mngr EN SW 1YrGL	Support	22.500
ERACDE-AA	MFE Risk Advisor P:1Gold [P+]	Perpetual License	25.000
ERAYFM-AA	MFE Risk Advisor P:1Gold [P+]	Support	25.000

Antivirus per Desktop e Server virtuali (MOVE)

- N. 4 nuove licenze d'uso perpetue per Server Virtuali, compreso servizio di supporto e manutenzione;
- N. 500 nuove licenze d'uso perpetue per Desktop Virtuali, compreso servizio di supporto e manutenzione;
- N. 20 nuove licenze d'uso perpetue Total Protection per server, compreso servizio di supporto e manutenzione;

Codice prodotto	Prodotto	Tipologia	Quantità
MOVCKE-AB	MFE MOVE AV for Virtual Servers P:1 GL	Perpetual License	4
MOVYCM-AB	MFE MOVE AV for Virtual Servers 1Yr GL	Support	4
MOVCDE-AA	MFE MOVE AV for Virtual DsktopsP:1GL[P+]	Perpetual License	500
MOVYFM-AA	MFE MOVE AV for Virtual Dsktops1YrGL[P+]	Support	500
TSRCDE-AA	MFE Total Protection for ServerP:1GL[P+]	Perpetual License	20
TSRYFM-AA	MFE Total Protection for Server1YrGL[P+]	Support	20

Il servizio di supporto, manutenzione e aggiornamento software in garanzia, relativo alle licenze d'uso perpetue di nuova acquisizione sarà della durata di 12 mesi a partire dalla data di consegna delle licenze d'uso e dovrà essere erogato a propria cura e spese e senza alcun onere aggiuntivo per l'Amministrazione, intendendosi ricompreso nel corrispettivo per l'acquisto delle licenze d'uso perpetue.

L'Impresa fornirà le licenze d'uso software e le apparecchiature hardware sopra elencati, previa richiesta dell'Amministrazione, che avverrà secondo le modalità descritte al successivo capitolo 3.

L'Amministrazione per ciascuno dei prodotti si riserva di richiedere in tutto o in parte le licenze d'uso software e le apparecchiature hardware sopra elencate. Si evidenzia comunque, che le quantità indicate rappresentano la stima delle attuali esigenze dell'Amministrazione.
Fermo quanto sopra l'amministrazione si impegna comunque a richiedere, entro il termine di tre mesi decorrente dalla "data di avvio della fornitura" come definita nel contratto, un quantitativo di nuove licenze d'uso software e nuove apparecchiature hardware per un importo almeno pari al 20% del corrispettivo relativo alla fornitura delle dette licenze d'uso e apparecchiature hardware.

2.3. SERVIZIO SUPPORTO TECNICO PLATINUM ENTERPRISE

Il livello di Supporto McAfee Platinum Enterprise che l'Istituto ha adottato nel passato e che intende continuare ad utilizzare, è comprensivo di un Support Account Manager (disponibile h24 e residente negli orari di lavoro presso gli stabili dell'Istituto) e di vari Specialisti di Prodotto dedicati ad ogni linea di prodotto McAfee (sempre contattabili telefonicamente e via email); il servizio rappresenta un valore aggiunto in relazione a molteplici aspetti, tra cui un unico e fidelizzato punto di contatto per la gestione delle Richieste di Supporto, un costante monitoraggio della postura di sicurezza dell'Istituto attraverso il controllo e la consulenza sull'efficiente utilizzo dei prodotti e delle soluzioni in esercizio, l'allerta sulle più recenti vulnerabilità e frodi telematiche correlate con lo stato di protezione dei sistemi istituzionali più rilevanti, la linea diretta con i Laboratori McAfee in caso di eventi di sicurezza particolarmente importanti e la costante disponibilità di una Squadra di tecnici altamente specializzati che possono fornire assistenza immediata su tematiche di Sicurezza Informatica, siano esse inerenti a nuove tecnologie, a comparazioni di soluzioni diverse che rispondano alle esigenze dell'Istituto o a presentazioni e formazione sui prodotti McAfee in collaudo ed esercizio.

L'oggetto di fornitura richiesto è la **Sottoscrizione Platinum Resident SAM Enterprise e Assigned Product Specialist Support per i 36 mesi previsti dalla fornitura.**

Codice prodotto	Prodotto	Tipologia	Quantità
PRSYDM-A	MFE Plat Resident SAM Enterprise Support	Support	1
PSAYDM-AT	MFE Assigned Product Specialist 1 Yr PL	Support	1

Si precisa che per l'erogazione del Servizio di Supporto Platinum Enterprise con Resident SAM e Assigned Product Specialist Support devono essere utilizzate esclusivamente risorse del produttore McAfee.

2.4. SERVIZI PROFESSIONALI DI SUPPORTO/ASSISTENZA SISTEMISTICA E SERVIZI DI FORMAZIONE

La tabella che segue contiene l'elenco delle singole iniziative progettuali, con una breve descrizione delle funzionalità/attività di sicurezza implementate, per le quali si intende richiedere il servizio professionale

di supporto e assistenza sistemistica. Per ogni iniziativa progettuale è indicata anche una stima di massima dei giorni/persona richiesti.

Iniziativa progettuale	Funzione/Attività	Giorni/persona stimati			
		1° anno	2° anno	3° anno	Totale
Progetto Design	Fase di analisi e stesura architettura	40	-	-	40
Progetto NAC	È il componente per il controllo degli accessi in rete dei sistemi, evita rischi di accessi in rete indesiderati	85	10	10	105
Progetto Risk Advisor	Il sistema di analisi del rischio centralizzato, analizzando le informazioni e le vulnerabilità ricavate dalle singole componenti di sicurezza mcAfee.	57	10	10	77
Progetto sicurezza ambienti Linux	Il progetto intende estendere le componenti di sicurezza anche per gli ambienti open source linux	50	10	10	70
Progetto sicurezza ambienti virtuali (MOVE)	In questa fase saranno implementate le feature di sicurezza appositamente create e studiate per gli ambienti virtuali.	52	8	8	68
Progetto cifratura sistemi end point	Il progetto prevede la cifratura dei file system dei sistemi end point.	62	10	10	82
Progetto DeepSafe	Il progetto prevede l'integrazione della soluzione DeepSafe, nata dalla sinergia di McAfee e Intel, utile a sfruttare dalla console McAfee le feature di sicurezza del processore Intel.	30	10	10	50
Progetto integrazione MVM e Risk Advisor ed ePO con le componenti già attive	Integrazione e sinergia tra le componenti di sicurezza McAfee, permettendo l'ottimizzazione e l'innalzamento complessivo del livello di sicurezza.	35	-	-	35
Progetto sicurezza per la gestione dei dispositivi mobili (EMM)	Questo progetto permette di gestire i dispositivi mobili di I.N.A.I.L. e la loro sicurezza in maniera centralizzata	40	2	2	44
Totale giorni		**451**	**60**	**60**	**571**

Per lo svolgimento delle attività legate alla presente iniziativa (analisi, progettazione, project management, ecc..) sono previsti servizi specialistici che dovranno necessariamente essere erogati dalle seguenti due figure professionali:

Security Architect - Project Leader (SSC) codice MD-SA-SECC-Z1
Ricopre il ruolo di interfaccia di alto livello con il cliente e soprattutto di gestione dei team di progetto che lavorano in parallelo sul cliente. Ha la responsabilità di coordinare ed integrare le informazioni delle singole pianificazioni dei progetti, stabilire le priorità, in accordo col cliente

e definire le macro schedulazioni con i Project Leader a vantaggio delle sinergie evitando sovrapposizioni di uso di risorse non condivisibili. Diventa il gestore delle Escalation e delle Change Request.
Security Consultant Product - Specialist (SCPS) codice MD-CONSULT-DY-Z1
Corrisponde alla figura tecnica del senior consultant sulla soluzione specifica. Il suo ruolo nel progetto consiste nel guidare le parti operative di implementazione nell'interfacciarsi con la parte tecnica del cliente per la normale operatività ed analisi dei requisiti tecnici, oltre ad essere di supporto in tutte le fasi di approfondimento tecnico.

Di seguito, per ogni figura professionale, è indicata la stima del numero di giorni persona massimi previsti.

Figura professionale	Totale giorni/persona
Security Architect – Project Leader	161
Security Consultant – Product Specialist	410

Si precisa che per l'erogazione del servizio di supporto/assistenza sistemistica devono essere utilizzate esclusivamente risorse McAfee.

L'Impresa si obbliga a prestare i servizi professionali di supporto specialistico sopra elencati, previa richiesta dell'Amministrazione, che avverrà secondo le modalità descritte al successivo capitolo 3.

L'Amministrazione si riserva di richiedere in tutto o in parte il le giornate/persona previste per il servizio si supporto/assistenza sistemistica, sulla base delle esigenze che emergeranno in corso di vigenza contrattuale.

Infine l'Amministrazione ha esigenza di formare proprio personale, pertanto richiede che la fornitura preveda l'erogazione dei seguenti corsi di formazione McAfee :

Corso Ufficiale McAfee	Giorni	SKU McAfee (codice)
Corso NAC	4	TRN-SITE4-Z1A
Corso Risk Advisor	3	TRN-SITE3-Z1A
Corso MOVE	2	TRN-SITE2-Z1A
Corso su Antimalware per Linux	2	TRN-SITE2-Z1A
Corso Encryption	4	TRN-SITE4-Z1A
Corso EMM	2	TRN-SITE2-Z1A
Corso DeepSafe	4	TRN-SITE4-Z1A

I corsi sono da svolgersi in aula, il numero di partecipanti sarà concordato tra l'Impresa e l'Amministrazione.
L'Impresa rilascerà documentazione ufficiale del corso ad ogni partecipante.

L'Impresa si obbliga a erogare i corsi di formazione sopra elencati, previa richiesta dell'Amministrazione, che avverrà secondo le modalità descritte al successivo capitolo 3.

L'Amministrazione si riserva di richiedere in tutto o in parte l'erogazione dei corsi di formazione previsti, sulla base delle esigenze che emergeranno in corso di vigenza contrattuale.

3. MODALITÀ DI ESECUZIONE DELLA FORNITURA

Nel presente capitolo sono descritte le modalità di erogazione per ogni oggetto di fornitura previsto dal presente contratto.

Fornitura di licenze d'uso Software e apparecchiature Hardware

La consegna degli oggetti di fornitura dovrà essere eseguita dall'Impresa entro il termine di 30 (trenta) giorni solari decorrenti da una richiesta formale dell'Amministrazione che avverrà a mezzo comunicazione scritta.
Tale comunicazione conterrà :

1. l'elenco dei prodotti software e corrispondenti quantità, relativo alle nuove licenze d'uso perpetue che l'Amministrazione intende acquisire;
2. l'elenco delle apparecchiature hardware e corrispondenti quantità, che l'Amministrazione intende acquisire.

I prodotti software e le apparecchiature hardware, e le relative quantità, contenuti in tali elenchi saranno compresi tra gli oggetti di fornitura previsti al precedente paragrafo 2.2 del presente Capitolato Tecnico.

La consegna della fornitura dovrà avvenire presso la Direzione Centrale per i Servizi Informativi e Telecomunicazioni - Via Santuario Regina degli Apostoli, 33 00145 Roma -, a cura e spese a totale carico del Fornitore.

Ultimate le operazione di consegna, l'Impresa dovrà redigere un "Rapporto di Consegna" recante almeno le seguenti indicazioni: data di consegna, tipo, modello e numero seriale delle versione dei prodotti, nonché la dichiarazione di rispondenza dei prodotti forniti alle specifiche del presente Capitolato Tecnico. A tal fine, l'Impresa comunicherà all'Amministrazione il nominativo del Responsabile della Fornitura, il quale assume il ruolo di referente per tutte le attività previste dalla fornitura.
Il "Rapporto di Consegna" dovrà essere espressamente approvato dall'Amministrazione.

Per quanto riguarda le apparecchiature hardware, ultimate le operazioni di consegna, l'Amministrazione procederà alla verifica della fornitura secondo le modalità previste al capitolo 4 del presente Capitolato Tecnico.

Servizi di supporto e manutenzione relativi ai prodotti Software e alle apparecchiature Hardware

L'Impresa, per tutto il periodo contrattuale della fornitura dovrà fornire:

- supporto, manutenzione e aggiornamento software per ciascuna delle licenze perpetue e delle apparecchiature hardware già in possesso dell'Amministrazione elencate al paragrafo 2.1 del presente Capitolato Tecnico a partire dalla data di avvio della fornitura;

- supporto, manutenzione e aggiornamento software per ciascuna delle licenze perpetue e delle apparecchiature hardware acquisite nel corso della presente fornitura a partire dal termine del previsto periodo di garanzia;

Il servizio di supporto, manutenzione e aggiornamento software in garanzia, relativo alle licenze d'uso perpetue di nuova acquisizione sarà della durata di 12 mesi a partire dalla data di consegna delle licenze d'uso e dovrà essere erogato a propria cura e spese e senza alcun onere aggiuntivo per l'Amministrazione, intendendosi ricompreso nel corrispettivo per l'acquisto delle licenze d'uso perpetue.

La manutenzione comprende ogni prestazione necessaria all'eliminazione dei malfunzionamenti. Si precisa che per malfunzionamento si intende qualsiasi anomalia funzionale che, direttamente o indirettamente, provochi l'interruzione o la non completa disponibilità del servizio all'utenza e, in ogni caso, ogni difformità dei prodotti in esecuzione dalla relativa documentazione tecnica e manualistica d'uso.

Relativamente al software, il servizio di supporto e manutenzione comprende, a titolo esemplificativo e non esaustivo: invio delle migliorie (correzioni, aggiornamenti e miglioramenti) dei Prodotti e relativa documentazione; invio delle riparazioni e aggiornamenti che l'Impresa mette a disposizione dei propri clienti; consegna di ogni nuovo aggiornamento dei Prodotti; peraltro, l'Amministrazione avrà facoltà di utilizzare le nuove versioni e/o di continuare ad usare le precedenti.
Per aggiornamento si intende sia nuove release che nuove versioni dei Prodotti.

L'Impresa comunicherà al Responsabile designato dalla Amministrazione, il Grant Number per effettuare l'apertura della richiesta di intervento direttamente al produttore McAfee e comunque dovrà fornire alla Amministrazione anche la possibilità di aprire l'intervento attraverso chiamata telefonica e/o fax e/o via web, anche presso la propria struttura di assistenza, secondo le modalità seguenti :

- l'Amministrazione comunicherà all'Impresa i malfunzionamenti, mediante strumento telematico confermandolo via fax;
- l'Impresa confermerà la presa in carico del problema mediante comunicazione via mail o via fax all'Amministrazione.

Per i prodotti software, in presenza di errori bloccanti, anche dovuti al rilascio di aggiornamenti che provochino disservizio alle apparecchiature dell'Istituto siano esse Server, Personal Computer o appliance, tale blocco deve essere rimosso ed il servizio ripristinato entro 4 ore lavorative dalla chiamata.

Per le apparecchiature Hardware, ritenute critiche per il buon funzionamento del Sistema Informativo dell'Istituto, si richiedono tempi di intervento e di ripristino entro le 6 ore lavorative successive alla chiamata.

Le richieste di intervento dovranno essere gestite dall'Impresa tramite un tecnico specializzato.
Ai fini del rispetto dei precedenti termini è ammessa anche una fix temporanea, una circumvention o un bypass, purché seguito dalla correzione definitiva del malfunzionamento.

Per le apparecchiature hardware il servizio di supporto e manutenzione deve essere erogato in modalità "on-site", su chiamata, dal lunedì al venerdì, escluso i festivi, dalle ore 8:00 alle ore 18:00.

Le parti di ricambio hardware - che dovranno essere identiche alle parti sostituite - verranno fornite dalla Impresa senza alcun onere aggiuntivo per l'Amministrazione; le parti sostituite verranno ritirate dalla Impresa stessa che ne acquisisce la proprietà. Le parti fornite - salvo diverso accordo - dovranno essere nuove, restando l'Impresa impegnata a quanto previsto contrattualmente in termini di garanzia.

L'Impresa potrà apportare le modifiche ed i miglioramenti tecnici ritenuti opportuni al fine di elevare il grado di affidabilità delle apparecchiature e/o di semplificare la manutenzione provvedendo a proprie spese alle relative installazioni.

Ove l'eliminazione del malfunzionamento e/o del fermo richieda un tempo superiore a quello stabilito o comporti il trasferimento delle apparecchiature in luogo diverso dai locali dell'Amministrazione, l'Impresa, previa comunicazione all'Amministrazione, dovrà provvedere alla sostituzione delle apparecchiature stesse con altre aventi le medesime caratteristiche tecniche e funzionali, sino al momento della sostituzione delle apparecchiature. L'Impresa dovrà adoperarsi, per quanto possibile, al recupero degli archivi presenti sulle apparecchiature da sostituire.
Il ritiro delle apparecchiature da sostituire e di quelle fornite in loro sostituzione, nonché la consegna delle apparecchiature in sostituzione e di quelle ripristinate dovranno essere effettuati a cura e spese dell'Impresa con le modalità e nei termini che verranno concordati con l'Amministrazione.
Per ogni intervento di manutenzione dovrà essere redatta da un incaricato dell'Amministrazione e da un incaricato della Impresa una 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.

Infine, l'Impresa si impegna a rendere disponibile alla Amministrazione, per i 36 mesi della fornitura, il servizio di supporto McAfee denominato:

- Platinum Enterprise Support con Resident SAM Enterprise e Assigned Product Specialist Support le cui caratteristiche sono indicate al precedente paragrafo 2.3.

Si precisa che per l'erogazione di tale servizio devono essere utilizzate esclusivamente risorse McAfee.

Servizi professionali specialistici

Servizi di Supporto/Assistenza Sistemistica
L'Amministrazione richiederà all'Impresa l'erogazione dei servizi di Supporto/Assistenza Sistemistica, previsti al paragrafo 2.4 del presente Capitolato Tecnico, mediante apposita comunicazione scritta all'Impresa contenente le attività richieste ed il periodo in cui prevede che tale attività debbano essere effettuate.

L'Impresa entro 5 giorni lavorativi dall'invio della richiesta dell'Amministrazione dovrà fornire un **Piano di lavoro** comprendente almeno :

- la descrizione dettagliata delle attività che verranno eseguite;
- la documentazione tecnica a supporto delle attività;
- la stima dell'impegno in giorni/persona previsto per l'esecuzione delle attività suddiviso per le figure professionali previste al precedente paragrafo 2.4 del Capitolato Tecnico;
- i nominativi e i Curriculum vitae delle risorse che intende utilizzare;

- le date ovvero il periodo in cui le attività verranno eseguite;
- la necessità di supporto da parte dell'Amministrazione.

Il Piano di lavoro sarà sottoposto ad approvazione da parte dell'Amministrazione.
In caso di mancata approvazione, l'Amministrazione comunicherà all'Impresa i motivi del dissenso che l'Impresa recepirà aggiornando il Piano e consegnandolo all'Amministrazione entro 5 giorni lavorativi.

Una volta terminata l'attività descritta nel suddetto Piano, l'Amministrazione procederà alla valutazione dell'intervento relativo al servizio richiesto attraverso attività di Verifica secondo le modalità previste al capitolo 4 del presente Capitolato Tecnico.

Il servizio di Supporto/Assistenza Sistemistica dovrà essere svolto presso la Direzione Centrale per i Servizi Informativi e Telecomunicazioni - Via Santuario Regina degli Apostoli, 33 - 00145 Roma dal lunedì al venerdì, esclusi i festivi, durante il normale orario lavorativo compreso dalle 8:00 alle 20:00.
Si precisa che per l'erogazione di tale servizio devono essere utilizzate esclusivamente risorse McAfee.

Corsi di formazione
Per quanto riguarda l'erogazione dei corsi di formazione previsti al paragrafo 2.4 del presente Capitolato Tecnico, l'Amministrazione ne richiederà all'Impresa l'erogazione mediante apposita comunicazione scritta contenente l'indicazione dei corsi richiesti e la data o il periodo in cui richiede che tali corsi vengano erogati.

L'Impresa entro 5 giorni lavorativi dall'invio della richiesta dell'Amministrazione dovrà fornire un Piano di lavoro comprendente le date in cui propone l'erogazione dei corsi richiesti

Il Piano di lavoro sarà sottoposto ad approvazione da parte dell'Amministrazione.
In caso di mancata approvazione, l'Amministrazione comunicherà all'Impresa i motivi del dissenso che l'Impresa recepirà aggiornando il Piano e consegnandolo all'Amministrazione entro 5 giorni lavorativi.

I corsi di formazione dovranno essere tenuti dall'Impresa dal lunedì al venerdì, escluso i festivi, all'interno dell'orario 9:00-18:00, e potranno svolgersi su richiesta dell'Amministrazione presso la Direzione Centrale per i Servizi Informativi e Telecomunicazioni - Via Santuario Regina degli Apostoli, 33 00145 Roma - ovvero presso una sede messa a disposizione dell'Impresa comunque ubicata in Roma.

4. VERIFICHE

Verifiche su apparecchiature hardware

Ultimata la consegna delle apparecchiature hardware, queste saranno sottoposte a verifica di conformità entro 30 giorni solari decorrenti dalla data di consegna contenuta nel rapporto di consegna.
A tal fine, contestualmente al "Rapporto di Consegna", l'Impresa dovrà consegnare un "Piano di collaudo", contenente l'articolazione delle prove proposte per la Verifica di conformità dei prodotti oggetto della fornitura.

A tal fine, l'Impresa dovrà:

- accettare che la verifica di conformità comprenda, come parte integrante, anche prove aggiuntive indicate dall' Amministrazione;
- fornire supporto durante il Collaudo.

Il Collaudo si svolgerà sia sulle singole componenti che sull'infrastruttura nel suo complesso.

Delle operazioni di Verifica di conformità verrà redatto apposito verbale. La Verifica di conformità delle apparecchiature si intende positivamente superato solo se tutte le componenti hardware risultino funzionare correttamente, singolarmente e integrate tra loro, secondo le specifiche indicate nella documentazione tecnica e d'uso fornita dall'Impresa.
Nel caso di esito positivo della verifica di conformità la data del verbale verrà considerata quale "Data di accettazione della fornitura".
Nel caso di esito negativo della verifica di conformità, l'Impresa dovrà eliminare i vizi accertati entro il termine massimo di 5 giorni solari. In tale ipotesi la verifica di conformità verrà ripetuta.

In sede di verifica di conformità, l'Impresa dovrà fornire all'Amministrazione tutta la documentazione tecnica ed i dati necessari al fine di consentire alla medesima di provvedere direttamente o tramite terzi alla manutenzione delle apparecchiature e alla presa in carico del bene da parte dell'Amministrazione.

Verifiche su servizi professionali

Una volta terminate le attività previste nel **Piano di lavoro**, l'Amministrazione, entro 30 giorni lavorativi, procederà alla verifica dell'intervento e alla certificazione di corretta esecuzione dello stesso. Nel caso di non approvazione dell'intervento, l'Impresa dovrà adoperarsi al fine di raggiungere quanto previsto nel piano di lavoro, pena il mancato riconoscimento dell'impegno stimato. L'eventuale impegno aggiuntivo non sarà riconosciuto economicamente, se non diversamente comunicato dall'Amministrazione.