ALLEGATO 4
CAPITOLATO TECNICO

INDICE

1. CONTESTO ORGANIZZATIVO E TECNOLOGICO

Architettura dell'ISTITUTO NAZIONALE PER L'ASSICURAZIONE CONTRO GLI INFORTUNI SUL LAVORO – INAIL

L'INAIL (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'INAIL 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'INAIL 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'INAIL.

Contesto tecnico

Il sistema informatico/informativo dell'INAIL 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, smartphone;
- 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 INAIL 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 rinnovato e consolidato la propria soluzione di sicurezza integrata e centralizzata McAfee, ottenendo i seguenti risultati:

- miglioramento del livello di protezione contro le potenziali minacce informatiche provenienti dall'interno e dall'esterno della rete dell'INAIL;
- garanzia dell'integrità dei dati, protezione del patrimonio applicativo, prevenzione dalla eventuale perdita di dati, protezione della riservatezza dei dati;
- contrasto e rimedio alle vulnerabilità;
- miglioramento dell'efficienza ed efficacia della gestione degli strumenti di sicurezza;
- 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.

Per mezzo di questo progetto, l'INAIL ha provveduto a realizzare le attività di adeguamento tecnologico ed ampliamento del sistema in esercizio attraverso:

1) la migrazione dalla suite TOPs-TEA alla suite EPA (McAfee® Endpoint Protection Advanced), che dispone di una piattaforma di gestione unificata, McAfee® ePolicy Orchestrator®, per la sicurezza degli endpoint e la gestione della conformità, e della soluzione McAfee® RealTime ePO, che consente alle aziende di interrogare le risorse aziendali, identificare i problemi potenziali e mitigare il rischio in maniera tempestiva;
2) l'acquisizione di ulteriori licenze TDA (MCAfee® Total Protection for Data), per avere la possibilità di cifrare e mettere in sicurezza i dati di tutti gli utenti INAIL insieme a quelli ISPSEL E IPSEMA;
3) l'acquisizione di ulteriori licenze HIPS (Host Intrusion Prevention Server), che protegge tempestivamente i server dalle minacce note e dai nuovi attacchi zero-day;
4) il rinnovo del servizio di supporto e manutenzione della soluzione McAfee® Intrushield (Network Security Platform), in grado di scoprire e bloccare le minacce più sofisticate presenti nella rete. L'approccio Security Connected alla gestione della sicurezza ottimizza le operazioni di sicurezza unendo i feed in tempo reale di McAfee Global Threat Intelligence™ (McAfee GTI™) a dati contestuali completi riferiti a utenti, dispositivi e applicazioni, per una risposta rapida e accurata agli attacchi che si sviluppano sulle reti;
5) l'aggiornamento del sistema di filtraggio anti-malware dei contenuti web e URL filtering, mediante l'implementazione della soluzione basata su due sistemi McAfee Content Security Blade Server, situati rispettivamente nella sede CED principale e nel sito di disaster recovery di INAIL;
6) la messa in sicurezza e gestione centralizzata dei dispositivi mobili, smartphone e tablet mediante software McAfee® Enterprise Mobility Managament, che applica ai dispositivi mobili lo stesso livello di sicurezza e controllo applicato dall'IT ai Desktop e ai Laptop, includendo la capacità di indentificare, marcare e assegnare le policy a smartphone e tablet PC di proprietà dei dipendenti o dell'azienda;
7) l'adozione della soluzione McAfee DeepSAFE, per la sicurezza hardware-assisted sfruttando un footprinting della sicurezza "più approfondito". La tecnologia McAfee DeepSAFE risiede al di sotto del sistema operativo, per fornire il monitoraggio kernel in tempo reale con cui rilevare e bloccare minacce nascoste avanzate come i rootkit nascosti e le APT;
8) l'acquisizione di ulteriori licenze McAfee Vulnerability Manager e delle licenze McAfee Risk Advisor, un sistema di gestione delle vulnerabilità informatiche e dell'analisi del rischio tecnologico correlato alla rilevanza della vulnerabilità e alla valenza degli Asset istituzionali;
9) la protezione antivirus per desktop e server virtuali;
10) la protezione dei server Linux e Windows.

Descrizione della politica di sicurezza ICT prevista

L'esigenza dell'Amministrazione consiste nell'intraprendere un piano di azioni per far fronte alle nuove minacce emergenti nell'ambito della sicurezza, derivanti in particolar modo dalla ingegnerizzazione e diffusione di massa, attraverso la rete, delle tecniche di danneggiamento e sfruttamento illecito delle risorse altrui.
La sempre crescente quantità di servizi e di risorse disponibili in rete, ha reso la navigazione Internet uno strumento essenziale per migliorare i processi aziendali, ma deve essere accuratamente controllata, al pari di qualsiasi altra risorsa aziendale, per evitare che i benefici che ne derivano siano parzialmente o totalmente annullati da un utilizzo non regolamentato.
Allo stato attuale, la sicurezza dei sistemi assume un carattere di assoluta priorità. Occorre pertanto predisporre una solida "barriera" contro le penetrazioni di virus da Internet, fornendo una protezione antivirus sui sistemi controllabile a livello centrale.
La presenza di una soluzione unica, centralizzata, di protezione delle risorse critiche dell'organizzazione, siano risorse di elaborazione che asset strategici, consente di ottimizzare tali risorse nel lavoro quotidiano sfruttando un meccanismo di controllo preventivo del sistema.

Gli obiettivi perseguiti dall'I.N.A.I.L, attraverso il rinnovo, il consolidamento e l'ottimizzazione dell'infrastruttura di sicurezza McAfee già esistente, possono essere così riassunti:

1. Protezione in tempo reale dalle minacce informatiche, su ogni vettore (file, web, e-mail, rete), per tutti i dispositivi, server e macchine virtuali fino a PC e dispositivi mobili;
2. Protezione immediata in presenza di nuovi attacchi scoperti a livello globale (malware zero-day);
3. Prevenzione delle minacce informatiche, attraverso lo scambio e l'utilizzo collettivo delle informazioni ad esse associate fra tutti gli strumenti di sicurezza, al fine di ridurre il più possibile il ritardo fra l'individuazione ed il contenimento delle stesse;
4. Garanzia dell'integrità dei dati, protezione del patrimonio applicativo, prevenzione dalla eventuale perdita di dati, protezione della riservatezza dei dati;
5. Contrasto e rimedio alle vulnerabilità;
6. Gestione del rischio e delle vulnerabilità;
7. Gestione unificata e semplificata di tutti gli strumenti di prevenzione e protezione.

Il rinnovo, consolidamento ed ottimizzazione dell'infrastruttura di sicurezza, si basano sui componenti McAfee di seguito elencati:

Componente	Funzione/Attività
Complete Endpoint Protection Suite (CEE)	Suite di protezione antimalware per gli endpoint, con piattaforma di gestione unificata. Questa suite, include i seguenti componenti: • VirusScan Enterprise; • VirusScan Command Line; • Endpoint Protection for MAC; • Host Intrusion Prevention for Desktops; • Desktop Firewall; • Deep Defender; • SiteAdvisor Enterprise with Web Filtering; • Application Control for PCs, • Device Control; • VirusScan for Linux; • Enterprise Mobility management; • McAfee Security for Email Servers with Anti-Spam; • Endpoint Intelligence Agent. Sarà effettuato il cross grade dall'attuale piattaforma EPA alla piattaforma CEE.
Server Security Suite – Advanced (DTS, DataCenter Suite)	Suite per la completa protezione e gestione dei server fisici, virtuali e nel cloud. Questa suite consente l'ampliamento, in termini di funzionalità e potenzialità, di soluzioni tecnologiche McAfee già in essere, includendo sia componenti già presenti nell'attuale infrastruttura di sicurezza INAIL, che componenti aggiuntivi: • VirusScan Enterprise for Linux and Windows (lato server. Componenti già presenti); • MOVE Anti-Virus for Servers (componente già presente. Comprende Multi-hypervisor, agentless, MOVE scheduler e offline scanning); • MOVE Firewall; • Host Intrusion Prevention for Servers (componente già presente); • DataCenter Connectors per: VMware vSphere, Amazon AWS, Microsoft Azure, OpenStack; • Application Control for Servers; • Change Control for Servers; • Deep Defender.
Complete Data Protection - CDA	Nuovo nome della Suite TDA, per la cifratura e messa in sicurezza dei dati degli utenti, sulla quale sarà

	erogato il servizio di supporto e manutenzione.
Secure Content Management	Sistema Gateway di rilevamento di virus, spam, malware e controllo e gestione spam e URL Filtering. Sarà effettuata la sostituzione degli attuali Content Security Blade Server, poiché in end of life.
Intrushield (Network Security Platform)	Sistema di Network Intrusion Detection. Sarà effettuata la sostituzione dei Global Manager, poichè in end of life.
TIE – Threat Intelligence Exchange	Cloud privato intelligente che mette in sicurezza e in comunicazione soluzioni Mcafee Host e Network. Tale componente costituisce l'evoluzione tecnologica del GTI.
ATD – Advance Threat Defense	Sistema di analisi completo del malware attraverso le sandbox.
MVM- McAfee Vulnerability Management	Sistema (agentless) di risk and Vulnerability Management. Sarà effettuata la sostituzione dei Vulnerability Manager, poichè in end of life. Le componenti Web Application Assessment ed Asset Manager, per l'identificazione delle vulnerabilità delle applicazioni web, degli assets dell'organizzazione e delle minacce verso questi ultimi, completeranno la soluzione. L'attuale componente Risk Advisor sarà sostituito con il componente Event Reporter, che ne rappresenta l'upgrade tecnologico.
Next Generation Firewall (NGFW)	Next Generation Firewall McAfee, che integra delle soluzioni per la gestione della banda delle VPN e degli accessi privilegiati alla rete.

2. OGGETTO DELL'APPALTO

INAIL 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 (ovvero appliance) 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 addestramento, come successivamente dettagliato.

Nel dettaglio l'Impresa dovrà fornire:

a) servizi di supporto e manutenzione relativi ai prodotti software in licenza d'uso perpetua ed 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 ed i relativi servizi di supporto e manutenzione 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 519 giorni/persona;
   - erogazione di sessioni di addestramento.

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

2.1. SUPPORTO E MANUTENZIONE LICENZE SOFTWARE E APPARECCHIATURE HARDWARE - SISTEMA IN 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'INAIL e precisamente:

Sezione Endpoint

- N. 15.000 licenze Client CDA (Complete Data Protection Advanced), nuovo nome della suite TDA;

- N. 500 licenze antivirus per Desktop Virtuali.

Codice prodotto	Prodotto	Tipologia	Quantità
CDAYFM-AA	MFE CompleteDataPrtxn Adv 1yr Gold [P+]	Support	15.000
MOVYFM-AA	MFE MOVE AV for Virtual Dsktops1YrGL[P+]	Support	500

Sistema di Intrusion & Prevention System (Network Security Platform)

- N. 2 IPS - M-8000 e accessori:
  - N. 26 SM Opt Gigabit FO kit;
  - N. 2 Redundant PowerSupply 8000;
  - N. 6 Opt (850nm) 10 Gigabit AFO Kit;
  - N. 24 XFPGbic 850nm 8K/6050;
- Servizio di supporto e manutenzione sugli accessori relativi all'unità di spare IPS – M-8000:
  - N. 12 MM Opt Gigabit FO Kit;
  - N. 8 Copper Gigabit FailOpen Kit;

- N.2 IPS – NS9300 e accessori:
  - N. 8 8port I/O Mod 10/1GigE
  - N. 32 Opt (850nm) 10 Gigabit AFO Kit
  - N. 16 Opt 62.5 Gigabit AFO Kit
  - N. 64 XFPGbic 850nm 8K/6050
- Servizio di supporto e manutenzione sugli accessori relativi a N.1 IPS – NS9300 di spare:
  - N.4 8 port I/O Mod 10/1 GigE.

Codice prodotto	Prodotto	Tipologia	Quantità
REMMF13PTA	MM Opt Gigabit FO Kit 1Yr RMA	Support	12
RBCGFOKT2A	Copper Gigabit FailOpen Kit 1Yr RMA	Support	8
IYVM80KADM	MFE Net Sec M-8000 Standard 1yr Gold+RM	Support	2
RBRPM8PS2	MFE NetSec Redundt PwrSupply 8000 1YrRMA	Support	2
RESMF13PTA	SM Opt Gigabit FO Kit 1Yr RMA	Support	26
RB10AFO85	Opt (850nm) 10	Support	6

	Gigabit AFO Kit 1Yr RMA		
RBX850CG1	MFE NetSec XFPGbic 850nm 8K/6050 1Yr RMA	Support	24
IPSNS9300NBD	MFE Net Sec IPS-NS9300 Appl 1Yr GL+NBD	Support	2
RBIAC8P10NETMOD	MFE Net Sec 8port I/O Mod 10/1GigE1YrRMA	Support	8
RB10AFO85	Opt (850nm) 10 Gigabit AFO Kit 1Yr RMA	Support	32
RB62F1KT7	Opt 62.5 Gigabit AFO Kit 1Yr RMA	Support	16
RBX850CG1	MFE NetSec XFPGbic 850nm 8K6050 1Yr	Support	64
RBIAC8P10NETMOD	MFE Net Sec 8port I/O Mod 10/1GigE1YrRMA	Support	4

McAfee Vulnerability Management -MVM

- N. 25.000 licenze perpetue MFE Vulnerability Manager.

Codice prodotto	Prodotto	Tipologia	Quantità
FSWYCM-AA	MFE Vulnerability Mngr EN SW 1YrGL	Support	25.000

2.2. UPGRADE TECNOLOGICO

Per attuare l'upgrade tecnologico delle soluzioni McAfee già in essere, l'Amministrazione acquisirà i prodotti e le quantità di seguito elencate:

Cross grade EPA→CEE

- N. 15.000 licenze d'uso perpetue CEE in cross-grade rispetto alle licenze d'uso perpetue EPA attualmente presenti nel sistema di esercizio, compreso il servizio di supporto e manutenzione.

Codice prodotto	Prodotto	Tipologia	Quantità
CEECDE-DA	MFE Complete EP Ent UPGD P:1 GL [P+]	Perpetual License	15.000
CEEYFM-AA	MFE Complete EP Protect Ent 1Yr GL [P+]	Support	15.000

McAfee Vulnerability Management -MVM

- N. 2 Appliance Event Reporter 5600, che sostituiscono l'attuale componente Risk Advisor, compreso il servizio di supporto e manutenzione.

Codice prodotto	Prodotto	Tipologia	Quantità
EVR-5600	MFE Event Reporter 5600 Appl	Hardware	2
EVR5600ARMA	MFE Event Reporter 5600 1YrGL+ARMA	Support	2

2.3. REFRESH TECNOLOGICO

Il refresh tecnologico prevede principalmente la sostituzione delle appliance hardware che risultano in end of life ed il completamento della piattaforma MVM, con l'introduzione del Web Application Assessment e dell'Asset Manager.

Sistema di Content Management e URL Filtering, in configurazione Disaster Recovery per i due siti INAIL

- N. 12.500 Sottoscrizione licenza d'uso perpetue WEB Protection Suite per 36 mesi;
- N. 2 Content Security Blade Server, compreso il servizio di supporto e manutenzione;
- N. 32 Content Security Scanning Blade, compreso il servizio di supporto e manutenzione;
- N.2 Content Security PDU da 32 A.

Codice prodotto	Prodotto	Tipologia	Quantità
MCS-CH1P-M72	MFE MCS-CH1P-M72 M7 1Phase power	Hardware	1
RFCH1PM72	MFE MCS-CH1P-M72 M7 1Phase 1YrNBDHWSppt	Support	1
MCS-BLDE-1XH	MFE MCS-BLDE-1XXHW Blade	Hardware	16
RFBLDE1XH	MFE MCS-BLDE-1XXHW 1Yr NBDHWSppt	Support	16
MCS-CH1P-M72	MFE MCS-CH1P-M72 M7 1Phase power	Hardware	1
RFCH1PM72	MFE MCS-CH1P-M72 M7 1Phase 1YrNBDHWSppt	Support	1
MCS-BLDE-1XH	MFE MCS-BLDE-1XXHW Blade	Hardware	16
RFBLDE1XH	MFE MCS-BLDE-	Support	16

	1XXHW 1Yr NBDHWSppt		
MCS-PDUI-32A	MFE Content Security 32AMP PDU for INTL	Hardware	2
WPSECE-AA	MFE Web Protection Suite 1:1 GL	Subscription	12500

Sistema di Intrusion & Prevention System (Network Security Platform)

- N. 1 Global Manager Appliance, compreso il servizio di supporto e manutenzione;
- N. 1 Global Manager FO Appliance, compreso il servizio di supporto e manutenzione.

Codice prodotto	Prodotto	Tipologia	Quantità
NSM-GLBL-NG	MFE Network Sec Glbl ManagerAppl-NG	Hardware	1
NYVGLBLNGARMA	MFE Net Sec Glbl Mngr Appl-NG 1YrGL+ARMA	Support	1
NSM-STND-NG-FO	MFE Network Sec Glbl Mngr App 1YrGL+NBD	Hardware	1
NYFSTNDNGARMA	MFE Network Sec FO Appl-NG 1Yr GL+ARMA	Support	1

McAfee Vulnerability Management -MVM

- N. 6 Appliance McAfee Vulnerability Manager 3200, compreso il servizio di supporto e manutenzione;
- N.1 licenza d'uso perpetua McAfee Web Application Assessment Module, compreso il servizio di supporto e manutenzione;
- N. 25.000 licenze d'uso perpetue McAfee Asset Manager, compreso il servizio di supporto e manutenzione.

Codice prodotto	Prodotto	Tipologia	Quantità
VAP-3200-MVM	MFE Vulnerability Mgr MVM3200 Appl	Hardware	6
MVM3200ARMA	MFE VulnrbiltyMgr MVM3200Appl 1YrGL+ARMA	Support	6
WAACKE-AD	MFE Web Application Assessmnt ModP:1Gold	Perpetual License	1
WAAYCM-AD	MFE Web Application Assessmnt	Support	1

	Mod1YrGold		
MAMCDE-AA	MFE Asset Manager P:1 GL [P+]	Perpetual License	25.000
MAMYFM-AA	MFE Asset Manager 1Yr GL [P+]	Support	25.000

2.4. AMPLIAMENTO TECNOLOGICO

L'ampliamento tecnologico, in termini di funzionalità e potenzialità, prevede il passaggio ad un'unica suite di protezione lato server, denominata DTS (DataCenter Suite), che ingloba licenze sw, prima acquistate separatamente (VirusScan, MOVE, HIPS) e funzionalità aggiuntive.

- N. 2.000 nuove licenze d'uso perpetue della suite DTS, compreso il servizio di supporto e manutenzione.

Codice prodotto	Prodotto	Tipologia	Quantità
DTSCDE-AB	MFE Server Security Suite Adv P:1GL[P+]	Perpetual License	2000
DTSYFM-AB	MFE Server Security Suite Adv 1YrGL[P+]	Support	2000

2.5. EVOLUZIONE TECNOLOGICA E COMPLETAMENTO DELL'INFRASTRUTTURA DI SICUREZZA

Per completare la propria infrastruttura di sicurezza e sfruttare i vantaggi offerti dall'evoluzione tecnologica della piattaforma McAfee, l'Amministrazione acquisirà le seguenti licenze software ed appliance hardware:

TIE – Threat Intelligence Exchange

- N. 15.000 licenze d'uso perpetue McAfee Threat Intel Exchange, compreso il servizio di supporto e manutenzione.

Codice prodotto	Prodotto	Tipologia	Quantità
TIECDE-AA	MFE Threat Intel Exchange P:1 GL [P+]	Perpetual License	15.000
TIEYFM-AA	MFE Threat Intel Exchange 1Yr GL [P+]	Support	15.000

Next Generation Firewall

- N. 1 licenza d'uso perpetua McAfee Security Management Center, compreso il servizio di supporto e manutenzione;
- N.2 Appliance Next Generation Firewall NGF 1401-C1, compreso il servizio di supporto e manutenzione.

Codice prodotto	Prodotto	Tipologia	Quantità
SM1CKE-2	MFE SMC 2 P:1 GL	Perpetual License	1
SM1YCM-2	MFE SMC 2 1Yr GL	Support	1
NGF-1401C1	MFE NGF 1401-C1 Appliance	Appliance	2
NGF1401C1RMA	MFE NGF 1401-C1 1Yr GL+RMA	Support	2

L'Amministrazione si riserva, inoltre, la possibilità di acquisire anche le seguenti appliance hardware:

ATD – Advance Threat Defense

- N.2 Appliance Advanced Threat Defense 6000, compreso il servizio di supporto e manutenzione.

Codice prodotto	Prodotto	Tipologia	Quantità
ATD-6000	MFE Adv Threat Def 6000 Standard HW	Hardware	2
ATD6000ADM	MFE Adv Threat Def 6000 Stand 1yrGL+RMA	Support	2

***

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 elencate, previa richiesta dell'Amministrazione, che avverrà secondo le modalità descritte al successivo paragrafo 3.

INAIL si impegna comunque a richiedere, entro il termine di tre mesi decorrente dalla "data di avvio della fornitura", la fornitura di nuove licenze d'uso di prodotti software e apparecchiature hardware, ad eccezione dell'appliance hardware ATD, sulla quale si riserva la possibilità di effettuare o meno l'acquisto.

2.6. 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 o incidenti 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 addestramento 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. I servizi saranno erogati su base annuale.**

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.

2.7. SERVIZI PROFESSIONALI DI SUPPORTO/ASSISTENZA SISTEMISTICA E SESSIONI DI ADDESTRAMENTO

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, suddivisi per figura professionale preposta all'erogazione del servizio, cioè:

- **Security Senior Consultant (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 macroschedulazioni 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 ruolo di Senior si acquisisce tramite la partecipazione a numerosi progetti di cui si è parte tecnica e in base alle certificazioni conseguite. Il suo ruolo nel progetto consiste nel guidare le parti operative di implementazione supportato dallo Junior Specialist, nell'interfacciarsi con la parte tecnica del cliente per la normale operatività ed analisi dei requisiti tecnici in cooperazione col PL e nel riportare al PL il risultato delle fasi operative, oltre ad essere di supporto in tutte le fasi di approfondimento tecnico.

Iniziativa progettuale	Funzione/Attività	Giorni/persona stimati							
		1° anno		2° anno		3° anno		Totale	
		SSC	SCPS	SSC	SCPS	SSC	SCPS	SSC	SCPS
Project Design	Fase di analisi e stesura architettura	15	15	-		-		15	15
TIE (Threat Intelligence Exchange)	É il componente per lo scambio di informazioni e interfaccia GTI per la rilevazione di nuovi malware. Componente di collegamento per la condivisione delle informazioni tra soluzioni di sicurezza di rete e sicurezza end point già esistente.	12	30					12	30
ATD (Advance Threat Defence)	Sistema di analisi delle nuove vulnerabilità non ancora scoperte, basato su un sistema di sandboxes; tale componente dialoga con i sistemi di network security ed end point già in produzione presso l'Istituto.	20	27					20	27
Refresh tecnologico Secure Content Management	L'attività prevede l'aggiornamento della componente hardware e software alle ultime release disponibili.	10	27					10	27
Refresh tecnologico Network Security Platform	In questa fase saranno aggiornate le componenti hardware e software dell'architettura Network Security Manager esistente.	15	18					15	18
Upgrade tecnologico Risk advisor	Il progetto prevede l'aggiornamento e la migrazione della	20	25					20	25

Iniziativa progettuale	Funzione/Attività	Giorni/persona stimati							
		1° anno		2° anno		3° anno		Totale	
		SSC	SCPS	SSC	SCPS	SSC	SCPS	SSC	SCPS
con l'introduzione di Event Reporter	componente Risk Advisor alla nuova tecnologia Event Reporter che sostituisce Risk Advisor.								
Refresh tecnologico di MVM (McAfee Vulnerability Manager)	Il progetto prevede l'aggiornamento tecnologico della componente MVM.	9	16					9	16
Next generation Firewall	Il progetto prevede l'applicazione della tecnologia Next Generation Firewall, per la protezione perimetrale.	8	12					8	12
Supporto Specialistico all'intera infrastruttura di sicurezza coinvolta nel progetto.	Supporto Specialistico per tutte le attività di verifica, aggiornamenti, tuning e personalizzazioni che si rendono necessarie durante il periodo di produzione delle componenti di sicurezza implementate.			10	110	10	110	20	220
Totale giorni/persona		**109**	**170**	**10**	**110**	**10**	**110**	**129**	**390**
Totale giorni persona [SSC+SCPS]								**519**	

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 paragrafo 3.

L'Amministrazione si riserva di richiedere in tutto o in parte i giorni/persona previsti per il servizio di 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 delle seguenti sessioni di addestramento McAfee:

Sessione di addestramento McAfee	Giorni	Codice Prodotto
Sessione TIE - Threat Intelligence Exchange	3	TRN-SITE3-Z1
Sessione ATD - Advanced Threat Defense	3	TRN-SITE3-Z1
Sessione MVM - WAA Web Application Assessment Module	2	TRN-SITE2-Z1
Sessione MVM - MAM Asset Manager	2	TRN-SITE2-Z1
Sessione Event reporter	4	TRN-SITE4-Z1
Sessione NGFW – Next Generation Firewall	4	TRN-SITE4-Z1

Le sessioni di addestramento sono da svolgersi in aula, il numero di partecipanti sarà concordato tra l'Impresa e l'Amministrazione.

L'Impresa rilascerà documentazione ufficiale della sessione di addestramento per ogni partecipante.

L'Impresa si obbliga a erogare le sessioni di addestramento sopra elencate, previa richiesta dell'Amministrazione, che avverrà secondo le modalità descritte al successivo paragrafo 3.

L'Amministrazione si riserva di richiedere in tutto o in parte l'erogazione delle sessioni di addestramento previste, 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.

3.1. FORNITURA DI LICENZE D'USO SOFTWARE E APPARECCHIATURE HARDWARE

La consegna della 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:

a) l'elenco dei prodotti software e delle corrispondenti quantità, relativo alle nuove licenze d'uso perpetue che l'Amministrazione intende acquisire;

b) l'elenco delle apparecchiature hardware e delle 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 del presente Capitolato Tecnico.

La consegna della fornitura dovrà avvenire presso la Direzione Centrale per l'Organizzazione Digitale - Via Santuario Regina degli Apostoli, 33 00145 Roma -, a cura e spese a totale carico del Fornitore.

L'impresa dovrà concludere il processo di installazione, configurazione e personalizzazione dei prodotti, nonché renderli operativi, entro il termine indicato nel Piano di lavoro, approvato dall'Amministrazione, relativo ai servizi professionali specialistici (vedi paragrafo 3.3) e, comunque, non oltre 30 giorni solari decorrenti dalla data di consegna della fornitura.

Ultimate le operazioni di installazione, configurazione e personalizzazione, l'Impresa dovrà consegnare all'Amministrazione un "Rapporto di Fine Installazione" recante le seguenti indicazioni: tipo, modello e numero seriale delle versione dei prodotti software installati, nonché la dichiarazione di rispondenza dei prodotti software forniti alle specifiche del Capitolato Tecnico e le articolazioni delle prove proposte per la Verifica di conformità, di cui al successivo paragrafo 4.

3.2. SERVIZI DI SUPPORTO E MANUTENZIONE RELATIVI AI PRODOTTI SOFTWARE E ALLE APPARECCHIATURE HARDWARE

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

- servizi di supporto e manutenzione per ciascuna delle licenze perpetue e delle apparecchiature hardware già in possesso dell'Amministrazione elencate al

paragrafo 2.1del presente Capitolato Tecnico a partire dalla data di avvio della fornitura;

- servizi di supporto e manutenzione, per ciascuna delle licenze perpetue, acquisite nel corso della presente fornitura, a partire dal termine del previsto periodo di garanzia;
- Servizi di supporto e manutenzione, per ciascuna delle apparecchiature hardware, acquisite nel corso della presente fornitura, a partire dalla data di accettazione della fornitura.

Il servizio di supporto e manutenzione in garanzia, relativo alle licenze d'uso perpetue di nuova acquisizione, sarà della durata di 12 mesi decorrenti dalla data di accettazione della fornitura 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 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 update dei prodotti; peraltro, l'Amministrazione avrà facoltà di utilizzare le nuove versioni e/o di continuare ad usare le precedenti. Per update si intende sia nuove release che nuove versioni dei Prodotti.

L'Impresa comunicherà al Responsabile del Procedimento 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, secondo le modalità seguenti:

- l'Amministrazione comunicherà all'Impresa i malfunzionamenti, mediante strumento telematico, confermandolo via fax. Si precisa che i termini per l'eliminazione dei malfunzionamenti decorrono dalla conferma 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 richiesta d'intervento, formalizzata secondo le

modalità sopra descritte. In presenza di errori non bloccanti sui prodotti software, l'Impresa dovrà ripristinare il servizio entro 24 ore lavorative dalla richiesta di intervento, formalizzata secondo le modalità sopra descritte.

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 richiesta d'intervento, formalizzata secondo le modalità sopra descritte.

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 2.6.

3.3. SERVIZI PROFESSIONALI SPECIALISTICI

Servizi di Supporto/Assistenza Sistemistica

L'Amministrazione richiederà all'Impresa l'erogazione dei servizi di Supporto/Assistenza Sistemistica, previsti al paragrafo 2.7 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 2.7 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 l'Organizzazione Digitale- 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.

Sessioni di addestramento

Per quanto riguarda l'erogazione delle sessioni di addestramento previste al paragrafo 2.7 del presente Capitolato Tecnico, l'Amministrazione ne richiederà all'Impresa l'erogazione mediante apposita comunicazione scritta contenente l'indicazione delle sessioni richieste e la data o il periodo in cui richiede che tali sessioni vengano erogate.

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 delle sessioni richieste.

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.

Le sessioni di addestramento dovranno essere tenute 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 l'Organizzazione Digitale - 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 software e hardware di nuova fornitura

Entro il termine di 20 (venti) giorni decorrente dalla data del "Rapporto di Fine Installazione", le componenti hardware e software di nuova fornitura, saranno sottoposte a Verifica di conformità da parte dell'Amministrazione.
A tal fine, contestualmente al "Rapporto di fine installazione", di cui al precedente paragrafo 3, l'Impresa dovrà, altresì, consegnare un "Piano di collaudo", contenente la proposta relativa alle operazioni e funzionalità che saranno oggetto di 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 processo verbale. La Verifica di conformità si intende positivamente superata solo in caso le prestazioni contrattuali siano state eseguite a regola d'arte sotto il profilo tecnico e funzionale, in conformità e nel rispetto delle condizioni, modalità, termini e prescrizioni espresse nel presente Capitolato tecnico.
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 che sarà concesso dall'Amministrazione in sede di verbale verifica di conformità, fatto salvo quanto previsto nei prescritti livelli di servizio. In tale ipotesi la verifica di conformità verrà ripetuta, fermo restando l'applicazione delle penali di cui allo SCHEMA SPECIALE DI CONTRATTO. Tutti gli oneri che l'Amministrazione dovrà sostenere saranno posti a carico dell'Impresa.
In sede di verifica di conformità, l'Impresa si impegna a 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.
L'impresa, in sede di verifica di conformità, si impegna, altresì, a fornire all'Amministrazione tutte le informazioni di dettaglio sul bene necessarie per la presa in carico del bene da parte dell'Amministrazione.
L'Amministrazione nel caso di particolari caratteristiche dell'oggetto contrattuale che non consentono la verifica di conformità per la totalità delle prestazioni contrattuali, si riserva la possibilità di effettuare controlli a campione o in forma semplificata con modalità comunque idonee a garantire la verifica dell'esecuzione contrattuale.
Tutti gli oneri derivanti dalla verifica di conformità si intendono a carico dell'Impresa.

Verifiche sui servizi di supporto e manutenzione e professionali

La verifica di conformità verrà avviata:
-con riferimento ai servizi di supporto e manutenzione su software e hardware già in uso o di nuovo fornitura, entro il mese successivo al trimestre di riferimento. Per quanto concerne il software di nuova fornitura, in garanzia per 12 mesi dalla data di accettazione della fornitura, i servizi di supporto e manutenzione, sui quali effettuare la verifica di conformità, potranno essere avviati alla scadenza di tale periodo;
- con riferimento al servizio di supporto tecnico Platinum Enterprise, entro il mese successivo al trimestre di riferimento;
- con riferimento ai servizi professionali di supporto/assistenza sistemistica e addestramento, entro il mese successivo al trimestre di riferimento.
Delle operazioni di Verifica di Conformità verrà redatto apposito processo verbale. La Verifica di conformità si intende positivamente superata solo in caso le prestazioni contrattuali siano state eseguite a regola d'arte sotto il profilo tecnico e funzionale, in conformità e nel rispetto delle condizioni, modalità, termini e prescrizioni espresse nel presente Capitolato tecnico.
Nel caso di esito positivo della verifica di conformità la data del verbale verrà considerata quale "Data di accettazione del Servizio", da parte dell'Amministrazione.
Nel caso di esito negativo della verifica di conformità, l'Impresa dovrà eliminare i vizi accertati entro il termine massimo che sarà concesso dall'Amministrazione in sede di verbale verifica di conformità, fatto salvo quanto previsto nei prescritti livelli di servizio. In tale ipotesi la verifica di conformità verrà ripetuta, fermo restando l'applicazione delle penali di cui allo SCHEMA SPECIALE DI CONTRATTO. Tutti gli oneri che l'Amministrazione dovrà sostenere saranno posti a carico dell'Impresa.
L'Amministrazione nel caso di particolari caratteristiche dell'oggetto contrattuale che non consentono la verifica di conformità per la totalità delle prestazioni contrattuali, si riserva la possibilità di effettuare controlli a campione o in forma semplificata con modalità comunque idonee a garantire la verifica dell'esecuzione contrattuale.
Tutti gli oneri derivanti dalla verifica di conformità si intendono a carico dell'Impresa.