

AS SDAPA PER L'AFFIDAMENTO DEI SERVIZI DI MANUTENZIONE ED EVOLUZIONE DELLA PIATTAFORMA TRELLIX (EX MCAFEE) DI INAIL ED. 3 – ID 2853

ALLEGATO 2 CAPITOLATO TECNICO

INDICE

Sommario

1. INTRODUZIONE	5
2. CONTESTO TECNOLOGICO	5
3. FABBISOGNO	10
4. OGGETTO, DURATA E AMBITO DELLA FORNITURA	11
4.1. Durata	17
4.2. Manutenzione dei prodotti software e delle apparecchiature hardware (di cui ai punti c) ed h) del precedente paragrafo 4)	17
4.3. Servizio di Supporto Sistemistico Trellix Thrive – SKU THRIVE-ELITEA	19
4.4. Servizio di supporto sistemistico Resident Program Manager – SKU CUSTOM SKU 20	20
4.5. Servizio di Supporto Sistemistico Skyhigh Enterprise Care – SKU SS-ENT-CARE	21
4.6. Servizio di Training (formazione) per il personale INAIL – SKU TRN-IL-PRI-1D	21
4.7. Servizi professionali di assistenza specialistica (a consumo)	22
4.8. Fornitura di nuovi prodotti software in sottoscrizione o in licenza d'uso perpetua e nuove apparecchiature hardware	32
4.9. Garanzia	32
4.10. Requisiti tecnici	33
4.10.1. Compatibilità'	33
4.10.2. Accessibilità'	33
4.10.3. Supporto alla verifica di conformità dell'hardware e del software	33
4.10.4. Consegna in gestione	33
4.10.5. Supporto passaggio in esercizio	34
4.11. Requisiti organizzativi	34
4.12. Ruoli richiesti	35
4.12.1. Responsabile della fornitura	35
4.13. Riservatezza	36
4.14. Adempimenti per la sicurezza	36
5. ESECUZIONE DELLA FORNITURA	36
5.1. Modalità di esecuzione della fornitura	37
5.1.1. Modalità di erogazione continuativa	37
5.2. Pianificazione	37
5.3. Attivazione dei servizi	38
5.4. Luogo di lavoro	38

5.5.	Impiego e stabilità delle risorse	39
5.6.	Verifica di conformità	39
5.7.	Azioni contrattuali	40
5.8.	Penali	41
6.	REQUISITI DI QUALIFICAZIONE DEI SERVIZI CLOUD	41
7.	CERTIFICAZIONI	41

GLOSSARIO, ACRONIMI E TERMINOLOGIA

Amministrazione o Committente	L'Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro (INAIL), di seguito anche Istituto, che usufruisce dei servizi e dei prodotti descritti nel presente Capitolato tecnico.
Consip	La società che, in qualità di stazione appaltante della presente fornitura, affida la fornitura oggetto del presente Capitolato.
Impresa o Fornitore	La società affidataria della presente procedura negoziata.
Contratto	Il contratto che verrà stipulato tra INAIL e l'Impresa aggiudicataria, recante le clausole che disciplineranno i rapporti giuridici tra le parti (INAIL e Impresa) nell'esecuzione del Servizio.
Fornitura	Le attività descritte nel presente documento tecnico.
Servizi	Il complesso dei servizi e delle attività oggetto del presente Capitolato tecnico.
Malfunzionamento	Qualsiasi anomalia funzionale del software e, in ogni caso, ogni difformità del prodotto in esecuzione rispetto alla relativa documentazione tecnica e manualistica d'uso.
Responsabile della Fornitura	La persona individuata dall'Impresa come interlocutore dell'Amministrazione e responsabile di tutte le attività contrattuali.
Piattaforma	La Piattaforma software per l'erogazione dei Servizi.
Giorni e Ore	Nella documentazione per giorno e ora si intendono rispettivamente giorno lavorativo e ora lavorativa; l'orario previsto per la fornitura è dalle 9,00 alle 18,00 dal lunedì al venerdì.
RUP e DEC	Rispettivamente il Responsabile Unico del Procedimento e il Direttore dell'Esecuzione del Contratto che svolgono ruoli e funzioni definiti all'art.31 del D.Lgs. n. 50/2016 e s.m.i.

1. INTRODUZIONE

Il presente capitolato è parte integrante della documentazione della presente procedura e definisce le caratteristiche e i requisiti richiesti per l'affidamento dei servizi di manutenzione ed evoluzione della piattaforma TRELLIX (ex McAfee) di INAIL ed. 3.

Le condizioni di cui al presente documento, gli atti e i documenti ivi richiamati, ancorché non materialmente allegati, costituiscono parte integrante e sostanziale del Contratto.

Le prescrizioni del presente capitolato rappresentano i requisiti minimi dell'affidamento.

2. CONTESTO TECNOLOGICO

Design Architettuale Esecutivo

L'I.N.A.I.L. ha concluso il progetto di "Data Center Transformation", al termine di un percorso di trasformazione e rinnovamento complessivo dal punto di vista tecnologico, impiantistico, gestionale e organizzativo.

Il progetto, di durata pluriennale, ha portato alla costruzione di una infrastruttura tecnologica su due Data Center di Tier 3+ come definito da TEIA-942 e Uptime Institute e ha consentito all'Istituto di dotarsi di un'infrastruttura moderna ed efficiente tale da potersi candidare a consolidatore delle dotazioni tecnologiche della Pubblica Amministrazione.

L'Istituto, infatti, riveste un ruolo fondamentale nel sistema del welfare pubblico in ragione della molteplicità di attività istituzionali che è chiamato a presidiare.

Politiche sanitarie, di prevenzione, ricerca e assicurative non costituiscono direttrici separate dell'azione pubblica ma convergono, in un sistema integrato e improntato alla interfunzionalità e alla multidisciplinarietà.

Il programma ha inoltre portato all'ammodernamento di oltre l'80% dell'hardware e la sostanziale rivoluzione dell'infrastruttura fisica che coinvolge tutte le sue componenti e i suoi livelli operativi.

La recente introduzione di piattaforme Cloud ha inoltre rinsaldato e ampliato le funzionalità dei Data Center, rendendo disponibili funzionalità ibride in termini di stack architeturali e applicativi.

La virtualizzazione dei server ha consentito di diminuire il numero dei server fisici del 25%, riducendo in tempo reale consumi e costi di gestione, aumentando efficienza, affidabilità e disponibilità della potenza di calcolo.

È stato quindi possibile consolidare l'infrastruttura di Storage e Backup, riducendo allo stesso tempo il footprint del Data Center dell'Istituto, passando da oltre 1.000 metri quadrati a circa 300, incidendo sulla potenza elettrica necessaria e il relativo raffreddamento per circa il 75%.

In questo modo, le infrastrutture necessarie a garantire la continuità di tutti i servizi I.N.A.I.L. presenti e futuri sono state dapprima ospitate nel Data Center che in precedenza era il sito Secondario e che in questa fase è diventato il sito Primario. Il vecchio sito Primario (DCOD

Santuario Regina Degli Apostoli) ha subito una radicale ristrutturazione della durata di più un anno, al termine del quale è stato “rieletto” a sito Primario e da cui sono, in condizioni normali, erogati i servizi della DCOD.

Dal punto di vista tecnologico i passi fatti sono tanti e sostanziali. Sono stati unificati SAN e LAN, semplificando la connettività e riducendo del 90% i cavi, con un utilizzo pressoché totale di fibre in sostituzione delle connessioni in rame, obsolete e meno funzionali.

I server sono stati raggruppati in “POD” omogenei composti da più rack, che sono stati soggetti a una lineare standardizzazione e si configurano come la struttura atomica da replicare in caso di espansione. I server stessi sono stati tutti aggiornati, portati allo stadio tecnologico di ultima generazione e, in futuro, saranno gestiti e sostituiti, come il resto dell’infrastruttura, secondo i cicli di vita previsti dai produttori, in modo da evitare i pericoli dell’obsolescenza che inducono oneri di gestione e limitano le possibilità evolutive e l’efficienza dell’organizzazione.

Attualmente, quindi, il sistema informatico dell’Istituto è costituito da più sistemi di elaborazione siti presso il DC Primario e Secondario e da sistemi elaborativi al servizio del territorio siti presso le Direzioni Regionali e le Sedi Locali, interconnessi mediante la rete geografica SPC (Sistema Pubblico di Connettività).

Il DC Secondario coopera all’erogazione dei servizi con il DC primario. Tra i due DC è attiva una soluzione di Business Continuity, per la maggior parte dei servizi in modalità active-active, per alcuni in modalità active-passive.

È prevista la realizzazione di un terzo sito (Casamassima) di DR per I.N.A.I.L. e per le altre PA che lo richiedano.

L’istituto è candidato come PSN e ospita già altre PA, in modalità Housing (ISTAT, CONSAP, AGID, altri) e Hosting (Ministero della Salute).

Parco Tecnologico

Il sistema informativo dell’I.N.A.I.L. è, in estrema sintesi, costituito dai seguenti componenti:

- ✓ sistemi di elaborazione centrali di grandi dimensioni e intermedi (open) siti presso i Data Center della Direzione Centrale Organizzazione Digitale (DCOD) e di Acilia, per la gestione dei servizi di interoperabilità, dei servizi web e di cooperazione applicativa in alta affidabilità ridondati per gli ambienti di sviluppo, test e produzione;
- ✓ piattaforme Cloud per l’erogazione e l’utilizzo di servizi IAAS, PAAS e SAAS;
- ✓ sistemi di elaborazione centrali di medie dimensioni situati presso il CED del Centro Protesi di Vigorso di Budrio;
- ✓ sistemi di elaborazione periferici di medie dimensioni situati presso le Sedi territoriali;
- ✓ postazioni di lavoro (PC e stampanti) ad uso del personale, postazioni di servizio, personal computer portatili, tablet, dispositivi di fonia mobile;

- ✓ rete geografica che interconnette le sedi I.N.A.I.L. tra loro (contesto Intranet), con le altre Pubbliche Amministrazioni (contesto Infranet) e verso la rete pubblica (contesto Internet);
- ✓ reti locali (LAN) presso le Sedi Locali, le Direzioni Regionali e le Direzioni Centrali (ivi compresi il Centro Protesi di Vigorso di Budrio e il CRM di Volterra);
- ✓ rete fonia VoIP (Voice over IP);
- ✓ diverse tipologie di software di base.

Progetti Realizzati e Innovazione

Negli ultimi anni, gli interventi progettuali hanno consentito all'Istituto di traghettare gli obiettivi strategici attesi e di registrare un passo in avanti nel percorso di efficientamento e digitalizzazione dei propri modelli operativi e di business.

- ✓ Scenario Post-Pandemico.

La pandemia COVID-19 è stato uno degli eventi di grande impatto che ha indotto l'Istituto verso un processo di evoluzione trasformando da un lato la sfera tecnologica e dall'altro sviluppando e rafforzando la sicurezza dei sistemi informatici appartenenti all'I.N.A.I.L..

Ciò ha messo in luce anche nuovi e rinnovati bisogni dei cittadini, rispetto ai quali l'Istituto si è trovato a rispondere.

La gestione di questo cambiamento ha introdotto e sviluppato nuovi servizi, uno tra i più rivoluzionari il concetto di "New Normal" che ha modificato il contesto ordinario di lavoro ripensato in ottica agile tramite piattaforme di **Digital Workspace**, ovvero spazi di lavoro digitale che permettono alle persone di accedere ai dati e alle informazioni di lavoro indipendentemente dal luogo in cui si trovano. L'Istituto ha quindi dovuto definire pratiche organizzative per gestire l'avvento dello smart working seguendo specifiche linee guida relative alla gestione e alla sicurezza.

Il contesto di "New Normal" ha permesso di individuare la digitalizzazione come motore di ripresa e di sviluppo soprattutto per il mondo delle PPAA ed in particolare per l'I.N.A.I.L., in modo da potersi adattare gestendo al meglio le opportunità e fattori critici.

- ✓ Soluzioni innovative.

Nell'ottica di full digital, è stato ripensato il modello di organizzazione digitale che garantisce un miglioramento degli strumenti e dei processi digitali per il supporto agli utenti attraverso l'introduzione di chatbot, assistenze virtuali, utilizzo dello strumento Teams e delle tecnologie AI al fine di semplificare e rendere più efficienti le fasi di assistenza tecnico-amministrativa e di favorire una maggiore integrazione tra le sedi territoriali all'interno del processo.

Si è quindi formalizzata la nuova modalità di erogazione dei servizi: lo **Sportello Digitale** infatti sfrutta tutti questi strumenti appartenenti alla sfera del Digital Workplace.

Da questa necessità di considerare una struttura tecnico-organizzativa, l'Istituto si è impegnato nel consolidamento e nell'integrazione delle componenti tecnologiche in sinergia e in coerenza con le strategie del cloud nazionale.

✓ Sicurezza tecnologica.

I presupposti sopra evidenziati hanno condotto l'I.N.A.I.L. verso lo sviluppo di una nuova strategia in ottica di protezione dei dati personali ponendola come una vera e propria scelta etica.

Grazie all'introduzione di sicurezza e compliance al GDPR il dato è stato individuato come elemento fondamentale da proteggere andando a impattare vari ambienti come **l'estensione dell'Autenticazione Multi Fattore a tutto il perimetro dell'Istituto** (*portale istituzionale, Office 365, VDI e VPN*), l'adozione di parametri biometrici in fase di autenticazione alla postazione di lavoro, la dismissione dell'obbligatorietà di accesso ai servizi dell'Istituto tramite username e password a favore dell'utilizzo di **SPID**, l'ulteriore estensione della piattaforma di **Log Management** e la **Correlazione** alla collezione di eventi provenienti dai sistemi in cloud.

È stato infine introdotto un **Gateway di Sicurezza** per l'accesso ai servizi erogati da diversi fornitori di servizi cloud e consolidate le attività per l'estensione della certificazione del sistema di gestione per la sicurezza delle informazioni.

La Sicurezza tramite piattaforma Trellix (ex McAfee) – Obiettivi conseguiti

La piattaforma di sicurezza Trellix è utilizzata dall'Istituto da diversi anni ed è stata oggetto di numerose evoluzioni. Attraverso le precedenti forniture e alla stipula del contratto attualmente in corso, I.N.A.I.L. ha provveduto a garantire continuità e adeguamento alle soluzioni Trellix in esercizio, profondamente integrate con le infrastrutture ICT dell'Istituto gestite dal personale interno del presidio, e ad avviare un processo di ampliamento ed evoluzione dei servizi, per assicurare l'alto livello di sicurezza richiesto dai progetti strategici di I.N.A.I.L..

Di seguito alcuni degli interventi realizzati e obiettivi assicurati con le soluzioni e i servizi Trellix nell'ultimo triennio:

- ✓ il consolidamento di un unico punto di raccordo per il governo delle attività operative e delle politiche inerenti a tutte le soluzioni Trellix, ovvero la singola console della piattaforma di gestione unificata ePO (ePolicy Orchestrator Server);
- ✓ la distribuzione a bordo di tutti gli endpoint gestiti della suite MV6 (MVISION Protect Plus and EDR for Endpoint) per garantire il riconoscimento di attacchi complessi sui sistemi di INAIL grazie all'introduzione di un modulo EDR, completamente integrato con i moduli già presenti a bordo dei sistemi di anti virus e anti intrusione. La coesistenza di questi moduli ha potenziato le capacità di contenimento e rilevamento di minacce sconosciute, sulla base di meccanismi di analisi avanzata basati su machine learning e contenimento dinamico;

- ✓ consolidamento sugli endpoint gestiti dell'utilizzo del modulo TIE (Threat Intelligence Exchange) al fine di rilevare e reagire immediatamente alle minacce denominate "zero-day", rendendo operative le informazioni relative ad un nuovo file compromesso e non ancora noto come malevolo su tutte le altre soluzioni di sicurezza Trellix, grazie alla combinazione tra le informazioni sui vettori di infezioni a livello mondiale e quelle acquisite a livello locale, riducendo il ritardo fra individuazione e contenimento;
- ✓ la distribuzione a bordo dei sistemi della suite Cloud Workload Security Detect and Respond per la protezione degli host fisici e virtuali (Windows e Linux, server e client) e per il riconoscimento e risposta a minacce complesse su tali sistemi, indipendentemente dalla natura delle piattaforme e dei sistemi operativi in uso nei Data Center;
- ✓ il consolidamento dell'uso della tecnologia Trellix Open Data Exchange Layer (DXL), grazie alla quale sono state predisposte una serie di integrazioni a valore aggiunto con soluzioni infrastrutturali di terze parti, già acquisite dall'Istituto, quali Fortinet Fortigate e CheckPoint per i Firewall perimetrali, Cisco ISE per il controllo degli accessi sulle reti multivendor cablate e wireless e le connessioni VPN remote, InfoBlox per la gestione del DHCP;
- ✓ il consolidamento ed upgrade della soluzione IPS Network Security Platform per la copertura in monitoraggio attivo antintrusione su entrambi i Data Center di I.N.A.I.L. di tutti i segmenti di Rete istituzionali di esercizio, con lo scopo di ottimizzare l'operatività nella gestione dei flussi di rete, anche in situazioni critiche;
- ✓ il consolidamento ed upgrade della soluzione Advanced Threat Defense (ATD), attiva e ridondata su entrambi i Data Center di I.N.A.I.L., per l'analisi dinamica e comportamentale in ambiente isolato (SandBox) di artefatti potenzialmente malevoli, non ancora categorizzati come pericolosi. A fronte di quanto riportato in premessa in merito alla fusione McAfee-FireEye nel brand Trellix, si evidenzia come beneficio a costo zero la messa in produzione del potenziamento della soluzione ATD (attualmente denominata "Intelligent Virtual Execution", IVX) , risultanza delle integrazioni citate, sulle medesime piattaforme hardware acquistate con la precedente fornitura;
- ✓ il consolidamento ed upgrade della tecnologia SIEM (Enterprise Security Manager, ESM), un concentratore dedicato alle soluzioni di sicurezza Trellix e di terze parti, atto alla raccolta dei log di tutti i sistemi istituzionali (nel rispetto delle normative del Garante) e alla correlazione intelligente e azionabile di eventi di sicurezza provenienti da sorgenti e apparati eterogenei, aumentando la capacità di storage e ammodernando le componenti relative alla storicizzazione e ricerca dei dati (Enterprise Log Search, ELM);
- ✓ il consolidamento ed upgrade del sistema di controllo sulla Navigazione Internet per quanto riguarda potenziali malware e contenuti WEB non desiderati, mediante adeguamento della soluzione Web Gateway, attiva, ridondata e con connettività in fibra a 10Gbps su entrambi i Data Center di I.N.A.I.L. e la conseguente espansione dei

suddetti criteri di protezione della navigazione anche ai dispositivi connessi a Internet al di fuori della rete interna e/o in Smart Working, mediante la progressiva attivazione del modulo Client Proxy;

- ✓ il consolidamento e l'ottimizzazione della piattaforma di protezione CASB inserita nelle suite Unified Cloud Edge (UCE) e Cloud Workload Protection (CWP), per mettere in sicurezza e monitorare sistemi, dati e comportamenti degli utenti sui servizi Cloud di varia natura, piattaforme IaaS, PaaS, SaaS e per visibilità e controllo sull'utilizzo di sistemi cloud non autorizzati;
- ✓ il consolidamento, per tutte le soluzioni Trellix sopra elencate, dell'integrazione nativa con i feed del Global Threat Intelligence (GTI) di Trellix, che, grazie alle informazioni condivise da milioni di sensori in tutto il mondo attraverso il Cloud, arricchite dalle ricerche degli analisti dei Trellix Advanced Research Center, rende possibile una protezione accurata contro vettori malevoli ancora sconosciuti, grazie alla valorizzazione per rischio di parametri che tengono conto della diffusione e della reputazione di una minaccia.
- ✓ il consolidamento, in ottica evolutiva, del Servizio di supporto denominato "Premier Success Plan", inclusivo di risorse dedicate esclusivamente all'Istituto (tra cui il Resident Customer Success Manager) e di prestazioni aggiuntive volte al miglioramento della postura di sicurezza dell'Istituto (di seguito le principali: Health Watch per la verifica della salute di tutte le piattaforme Trellix e delle loro configurazioni allo scopo di effettuare gli opportuni miglioramenti, Technical Support Engineer dedicati e la piattaforma di e-Learning tecnico);
- ✓ l'Erogazione di Servizi Professionali per un continuo miglioramento dell'efficienza ed efficacia della gestione degli strumenti di sicurezza Trellix, corredata da una dettagliata pianificazione delle singole iniziative progettuali concordate così come per la formazione al personale dell'Istituto.

Tutte le attività operative e le politiche inerenti alle soluzioni citate sono governate da un unico punto di raccordo e si interfacciano in tempo reale con i feed del Global Threat Intelligence di Trellix, che sfrutta l'attività di milioni di sensori in tutto il mondo e le ricerche di un ampio gruppo di analisti dei Trellix Advanced Research Center, rendendo disponibili le informazioni sulle minacce. Questo servizio, basato sul cloud e sempre attivo, rende possibile una protezione accurata contro le minacce note e in rapida emersione, grazie a dei parametri che tengono conto della diffusione e della reputazione di una minaccia.

3. FABBISOGNO

La fornitura richiesta è costituita da Prodotti/Servizi ascrivibili alle seguenti 3 macro Aree:

1. Rinnovo e Upgrade dell'attuale parco installato (hardware, software e servizi cloud), di cui ai successivi punti a), b), c);
2. Professional Services e Supporto, di cui ai successivi punti d), e), f);

Classificazione del documento: Consip Public

AS SDAPA, per l'affidamento dei servizi di manutenzione ed evoluzione della piattaforma TRELLIX (ex McAfee) di

INAIL ed. 3 – ID 2853 –

Allegato 2 - Capitolato Tecnico

3. Prodotti Opzionali, di cui ai successivi punti g), h).

4. OGGETTO, DURATA E AMBITO DELLA FORNITURA

La fornitura prevede le seguenti componenti:

➤ **Fornitura Base**

- a) Rinnovo del servizio di manutenzione dei prodotti software in licenza d'uso perpetua, rinnovo del servizio di manutenzione delle apparecchiature hardware (appliance) già in possesso dell'Istituto e rinnovo delle sottoscrizioni dei prodotti software già in possesso dell'Istituto;
- b) Upgrade tecnologico dei prodotti software in licenza d'uso perpetua e delle apparecchiature hardware (appliance) già in possesso dell'Istituto;
- c) Servizio di manutenzione dei prodotti di cui al precedente punto b);
- d) Servizi di supporto sistemistico: Trellix Thrive Elite, Resident Program Manager, Skyhigh Enterprise Care, erogati da casa madre;
- e) Servizio di Training (formazione a consumo G/P) per il personale INAIL, erogato da casa madre;
- f) Servizi professionali di assistenza specialistica (a consumo G/P, erogati da casa madre).

➤ **Fornitura Opzionale**

- g) Nuovi prodotti software;
- h) Servizio di manutenzione dei prodotti di cui al precedente punto g).

In particolare, INAIL ha l'esigenza di acquisire i seguenti oggetti di fornitura.

	<i>Oggetto di fornitura</i>	<i>Sottocategoria</i>
a)	Rinnovo del servizio di manutenzione dei prodotti software in licenza d'uso perpetua, rinnovo del servizio di manutenzione delle apparecchiature hardware (appliance) già in possesso dell'Istituto, e	Rinnovo ATD Advance Threat Defense
		Rinnovo SIEM (ESM)
		Rinnovo IPS (Network Security Platform)

Classificazione del documento: Consip Public

AS SDAPA, per l'affidamento dei servizi di manutenzione ed evoluzione della piattaforma TRELLIX (ex McAfee) di

INAIL ed. 3 – ID 2853 –

Allegato 2 - Capitolato Tecnico

	rinnovo delle sottoscrizioni dei prodotti software già in possesso dell'Istituto	Rinnovo End Point and Server Security
		Rinnovo cloud
		Rinnovo Secure Content Management
b)	Upgrade tecnologico dei prodotti software in licenza d'uso perpetua e delle apparecchiature hardware (appliance) già in possesso dell'Istituto inclusive del relativo servizio di manutenzione	Upgrade SIEM
		Upgrade IPS (Network Security Platform)
		Upgrade Sandbox
		Upgrade Secure Content Management
c)	Servizio di manutenzione dei prodotti di cui al precedente punto b)	
d)	Servizi di supporto sistemistico: Trellix Thrive Elite (ex McAfee Premier Success Plan - PSP), Resident Program Manager, Skyhigh Enterprise Care, erogati da casa madre	
e)	Servizio di Training (formazione a consumo G/P) per il personale INAIL, erogato da casa madre	
f)	Servizi professionali di assistenza specialistica (a consumo G/P, erogati da casa madre)	
g)	Nuovi prodotti software (Componenti opzionali)	
h)	Servizio di manutenzione dei prodotti di cui al precedente punto g) (Componenti opzionali)	

La tabella seguente contiene il dettaglio della parte di prodotti, di cui al precedente punto a), per i quali è previsto il **rinnovo**:

Product Name	Charge Type	Trellix/SH SKU	Quantità	anni	Start Date	End Date
Rinnovo ATD						
Thrive Essential & Onsite Next Business Day Hardware Support Trellix Intelligent Sandbox 6200	Support Fee	ATD6200NBD	8	3	24/06/2025	23/06/2028
Rinnovo SIEM						
Thrive Essential Trellix Virtual Enterprise Log Search VM 4 Core Add-On	Support Fee	ELS4YE-AA	6	3	30/05/2025	29/05/2028
Thrive Essential & Onsite Next Business Day Hardware Support Trellix Enterprise Security Manager, Log Manager and Event Receiver Combination 6075	Support Fee	ENMELM6075NBD	2	1	24/06/2025	23/06/2026
Trellix Global Threat Intelligence (Module for ESM) - ETM X10 Appliance	Subscription Fee	GTEETMX10GIEAD	2	3	22/05/2025	21/05/2028
Thrive Essential Trellix Virtual Enterprise Log Search VM 8 Cores	Support Fee	ELSVYE-AA	2	3	30/05/2025	29/05/2028
Trellix Enterprise Security, Enterprise Log Manager and	Support Fee	ELU4YE-AA	6	3	22/05/2025	21/05/2028

Classificazione del documento: Consip Public

AS SDAPA, per l'affidamento dei servizi di manutenzione ed evoluzione della piattaforma TRELLIX (ex McAfee) di

INAIL ed. 3 – ID 2853 –

Allegato 2 - Capitolato Tecnico

Enterprise Receiver VM (4 Core Add-On)						
Trellix Virtual Enterprise Security Manager, Log Manager and Event Receiver Combination VM 8 Cores	Support Fee	ELUVYE-AA	2	3	22/05/2025	21/05/2028
Thrive Essential & Onsite Next Business Day Hardware Support Trellix Enterprise Log Search 6075	Support Fee	ELS6075NBD	2	1	24/06/2025	23/06/2026
Onsite Next Business Day Hardware Support Trellix Direct Attached Storage 250	Support Fee	RBDAS250NBD	6	3	24/06/2025	23/06/2028
Thrive Essential & Onsite Next Business Day Hardware Support Event Receiver 4700	Support Fee	ERC4700NBD	8	2	30/05/2025	30/06/2027
Rinnovo IPS (Network Security Platform)						
Advanced RMA (next business day ship) Hardware Support Trellix Network Security Active 1/10G Fail-Open Chassis	Support Fee	RBAFOCHKT2	4	3	30/05/2025	29/05/2028
Onsite Next Business Day Hardware Support Trellix Network Security Manager Next Generation Appliance-Only for Standard, Global, Failover and Central manager	Support Fee	NYVMAPLNGNBD	2	3	30/05/2025	29/05/2028
Advanced RMA (next business day ship) Hardware Support Trellix Network Security 1600W AC Spare Power Supply for NS9x00	Support Fee	RBIAC1600ACPS	4	3	30/05/2025	29/05/2028
Trellix Network Security Manager Software Subscription Global Edition	Subscription Fee	NMGECE-AA	1	3	21/05/2025	29/05/2028
Trellix IPS NS9500 - 30Gbps Software license (Throughput based entitlement)	Subscription Fee	NS95X30ECE-AT	6	3	22/05/2025	21/05/2028
Advanced RMA (next business day ship) Hardware Support Trellix Network Security 8-Port 10/1 GigE SFP+/SFP Network I/O Expansion Module (without Built-In Fail-Open)	Support Fee	RBIAC8P10NETMOD	24	3	16/05/2025	15/05/2028
Trellix Network Security 8-Port 10/1 GigE SFP+/SFP Network I/O Expansion Module (without Built-In Fail-Open)	Support Fee	RBIAC8P10NETMOD	12	3	22/05/2025	21/05/2028
Advanced RMA (next business day ship) Hardware Support Trellix	Support Fee	RBAFOCH40KT2	8	3	22/05/2025	21/05/2028

Classificazione del documento: Consip Public

AS SDAPA, per l'affidamento dei servizi di manutenzione ed evoluzione della piattaforma TRELLIX (ex McAfee) di

INAIL ed. 3 – ID 2853 –

Allegato 2 - Capitolato Tecnico

Network Security Active 40G Fail-Open Chassis						
Advanced RMA (next business day ship) Hardware Support Trellix Network Security Active 40G Fail-Open Chassis	Support Fee	RBAFOCH40KT2	7	3	20/12/2025	18/12/2028
Advanced RMA (next business day ship) Hardware Support Trellix Network Security 1GigE 1000BASE-SX MM Active Fail-Open Module	Support Fee	RBAF85062KT1	16	3	24/06/2025	23/06/2028
Advanced RMA (next business day ship) Hardware Support Trellix Network Security Dual Segment 10GigE 10GBASE-SR MM Active Fail-Open Module	Support Fee	RBIAC4P10FOSRKIT	19	3	24/06/2025	23/06/2028
Advanced RMA (next business day ship) Hardware Support Trellix Network Security Dual Segment 10GigE 10GBASE-SR MM Active Fail-Open Module	Support Fee	RBIAC4P10FOSRKIT	24	3	22/05/2025	21/05/2028
Advanced RMA (next business day ship) Hardware Support	Support Fee	RBIAC4P1GMM62MOD	18	3	16/05/2025	21/05/2028
Trellix Network Security IPS NS9500 Appliance	Support Fee	RBIPSNS9500NBD	6	3	22/05/2025	21/05/2028
Trellix IPS NS9500 - 30Gbps Software license (Throughput based entitlement)	Subscription Fee	NS95X30ECE-AT	6	3	22/05/2025	21/05/2028
Rinnovo Endpoint and Server Security						
ProtectPLUS Thrive Essential Trellix MOVE AntiVirus for Virtual Desktops (VDI)	Support Fee	MOVYFM-AA	500	3	16/05/2025	15/05/2028
Trellix Mobile Security Advanced (Germany Data Center)	Subscription Fee	MV3DEE-AA	2000	3	12/05/2025	11/05/2028
Trellix Cloud Workload Security Detect and Respond (Germany Data Center)	Subscription Fee	CWRDEE-AA	2000	3	12/05/2025	11/05/2028
Trellix API	Subscription Fee	PL1ECE-AA	1	3	12/05/2025	11/05/2028
Trellix Protect Plus EDR for Endpoint - Upgrade (Germany Data Center)	Subscription Fee	MV6DEE-DA	15000	3	22/05/2025	21/05/2028
Rinnovo cloud						
Skyhigh CNAPP - CSPM Account Pooled (Germany Data Center)	Support Renewal	C42DEE-AA-AA	7	3	12/05/2025	11/05/2028

Classificazione del documento: Consip Public

AS SDAPA, per l'affidamento dei servizi di manutenzione ed evoluzione della piattaforma TRELLIX (ex McAfee) di

INAIL ed. 3 – ID 2853 –

Allegato 2 - Capitolato Tecnico

Skyhigh CNAPP - DLP and Malware Pooled (Germany Data Center)	Support Renewal	C43DEE-AA-AA	10	3	12/05/2025	11/05/2028
Skyhigh SSE Advanced (Germany Data Center)	Support Renewal	UCADEE-AA-FA	12500	3	12/05/2025	11/05/2028
Rinnovo Secure Content Management						
Onsite Next Business Day Hardware Support	Support Renewal	WBG5500E2NBDA	8	3	24/06/2025	23/06/2028
Advanced RMA (next business day ship) Hardware Support	Support Renewal	RB10G4SRFBREA	8	3	24/06/2025	23/06/2028

La tabella seguente contiene il dettaglio della parte di prodotti, di cui al precedente punto b), per i quali è previsto l'**upgrade**.

Product Name	Charge Type	Trellix/SH SKU	Quantità	Durata in anni
upgrade SIEM				
Trellix Enterprise Security Manager X10	Appliance/Hardware Fee	ETM-X10	2	1
Trellix Enterprise Security Manager X10	Support Fee	ETMX10NBD	2	3
Trellix Enterprise Log Manager 6100	Appliance/Hardware Fee	ELM-6100	2	1
Trellix Enterprise Log Manager 6100	Support Fee	ELM6100NBD	2	3
Trellix Event Receiver 4800	Appliance/Hardware Fee	ERC-4800	8	1
Trellix Event Receiver 4800	Support Fee	ERC4800NBD	8	3
Trellix Advanced Correlation Engine 4800	Appliance/Hardware Fee	ACE-4800	2	1
Trellix Advanced Correlation Engine 4800	Support Fee	ACE4800NBD	2	3
Trellix Virtual Enterprise Security Manager, Log Manager and Event Receiver Combination VM 8 Cores	License Fee	ELUVME-AA	2	1
Trellix Enterprise Security, Enterprise Log Manager and Enterprise Receiver VM (4 Core Add-On)	License Fee	ELU4AE-AA	6	1
Helix Connect (Germany Data Center)	Subscription Fee	XDRDEE-AA	15.000	3
Helix Connect Open XDR for External Data Add-on - 1 TB (Germany Data Center)	Subscription Fee	OX4DEE-AA	1	3
Helix Connect XDR Retention 10 Months Add-On - 1 TB (Germany Data Center)	Subscription Fee	XM4DEE-AA	1	3
Upgrade IPS (Network Security Platform)				
Trellix Network Security IPS NS9500 Appliance	Appliance/Hardware Fee	IPS-NS9500	6	1
Trellix Network Security IPS NS9500 Appliance	Support Fee	RBIPSNS9500NBD	6	3
Trellix Network Security Dual Segment 10GigE 10GBASE-SR MM Active Fail-Open Module	Appliance/Hardware Fee	IAC-4P10FOSR-KIT	5	1
Trellix Network Security Dual Segment 10GigE 10GBASE-SR MM Active Fail-Open Module	Support Fee	RBIAC4P10FOSRKIT	5	3

Classificazione del documento: Consip Public

AS SDAPA, per l'affidamento dei servizi di manutenzione ed evoluzione della piattaforma TRELLIX (ex McAfee) di

INAIL ed. 3 – ID 2853 –

Allegato 2 - Capitolato Tecnico

Trellix Network Security 8-Port 10/1 GigE SFP+/SFP Network I/O Expansion Module (without Built-In Fail-Open)	Appliance/Hardware Fee	IAC-8P10NET-MOD	2	1
Trellix Network Security 8-Port 10/1 GigE SFP+/SFP Network I/O Expansion Module (without Built-In Fail-Open)	Support Fee	RBIAC8P10NETMOD	2	3
Trellix Network Security 10GigE SFP+ 10GBASE-SR MM Transceiver	Appliance/Hardware Fee	IAC-SFTSR-FOT	96	1
Trellix Network Security Active 40G Fail-Open Chassis	Appliance/Hardware Fee	IAC-AFOCH40-KT2	9	1
Trellix Network Security Active 40G Fail-Open Chassis	Support Fee	RBAFOCH40KT2	9	3
Trellix Network Security Active 1/10G Fail-Open Chassis	Appliance/Hardware Fee	IAC-AFOCH-KT2	4	1
Trellix Network Security Active 1/10G Fail-Open Chassis	Support Fee	RBAFOCHK2	4	3
Trellix Network Security 1GigE 1000BASE-SX MM Active Fail-Open Module	Appliance/Hardware Fee	IAC-AF85062-KT1	16	1
Trellix Network Security 1GigE 1000BASE-SX MM Active Fail-Open Module	Support Fee	RBAF85062KT1	16	3
Trellix Network Security 1GigE SFP 1000BASE-SX MM Transceiver	Appliance/Hardware Fee	ITV-2KSG-NA-100	32	1
Network Detection and Response(T)	Subscription Fee	NDR2WECE-AA	1.000	3
Network Detection and Response(T)	License Fee	VNFIACXE-AT	1	1
Network Security NX Edition (Enterprise)(T)	Subscription Fee	NWNX2WECE-AT	2.000	3
Network Security NX Edition (Enterprise)(T)	License Fee	VNWSCXE-AT	2	3
Network Security NX Edition (Enterprise)(T)	License Fee	VCMCXE-AT	2	3
Forensics(T)	Subscription Fee	NFIAPXECE-AT	2.000	1
Forensics(T)	License Fee	VNFIACXE-AT	1	1
Forensics(T)	License Fee	VNFPXCXE-AT	2	3
upgrade Sandbox				
IVX Enterprise Cloud (Germany Data Center)	Subscription Fee	IVXDEE-AA	12.500	3
Network Security NX Edition (Enterprise)(T)	Appliance/Hardware Fee	VX-12600-T	6	1
Upgrade Secure Content Management				
Skyhigh SWG 5500F Appliance	Appliance/Hardware Fee	Skyhigh SWG 5500F	8	1
Skyhigh next business day support	Support Fee	Skyhigh WBG5500F NBD	8	3
Skyhigh 10 Gigabit Fiber OCP Card - F Model Appliances with Short Range Transceivers	Appliance/Hardware Fee	MAP-10G4SR-FBRFA	8	1
Advanced RMA (next business day ship) Hardware Support	Support Fee	RB10G4SRFBRFA	8	3

La tabella seguente contiene il dettaglio della parte di servizi, di cui ai precedenti punti d), e) ed f), per i quali è previsto l'acquisto dei **Servizi a pacchetto** e in modalità g/p (**Professional services e supporto specialistico**).

Tipologia	Trellix SKU	Prodotto	QT	Durata anni
Services	THRIVE-ELITEA	Trellix Thrive Elite, precedentemente denominato "McAfee Premier Success Plan	1	3
Services	CUSTOM-SKU	Resident Program Manager	1	3
Services	SS-ENT-CARE	Skyhigh Enterprise Care	1	3
Services	TRN-IL-PRI-1D	Training (Formazione) (gg/p)	24	3
Services	CONS-SA-DY-Z1	Security Architect Consulting Daily (gg/p)	399	3
Services	CONS-DY	Custom Consulting Daily (gg/p)	550	3

La tabella seguente contiene il dettaglio della parte di prodotti, di cui al precedente punto g), per i quali è previsto l'acquisto opzionale:

Product Name	Charge Type	Trellix/SH SKU	Quantità	Durata in anni
Trellix Endpoint Security Suite - Upgrade (Germany Data Center)	Subscription Fee	TRXE1DEE	15.000	2
Trellix Virtual Enterprise Log Search VM 4 Core Add-On	License Fee	ELS4AE-AA	8	1
Trellix Virtual Enterprise Log Search VM 4 Core Add-On	Support Fee	ELS4YE-AA	8	2
Trellix wise for EDR add on (Germany)	subscription Fee	EDRWDEE	15.000	2

Si precisa che i predetti prodotti opzionali potranno essere acquisiti da INAIL in tutto o in parte, anche per periodi minori di quelli previsti in tabella, senza alcuna garanzia di acquisizione, nei confronti del Fornitore.

4.1. Durata

La durata contrattuale prevista è pari a 36 (trentasei) mesi, a decorrere dalla “**Data di Accettazione della Fornitura**”, di cui al successivo paragrafo 5.6, lettera a). Nel corso del contratto, al Fornitore potranno essere richiesti i servizi professionali a consumo.

4.2. Manutenzione dei prodotti software e delle apparecchiature hardware (di cui ai punti c) ed h) del precedente paragrafo 4)

Per tutta la durata del contratto l'Impresa dovrà garantire:

- servizi di supporto e manutenzione per ciascuna delle licenze perpetue e delle apparecchiature hardware già in possesso dell'Amministrazione;
- servizi di supporto e manutenzione per ciascuna delle licenze perpetue acquisite nel corso della fornitura, a partire dal termine del previsto periodo di garanzia;
- servizi di supporto e manutenzione per ciascuno dei prodotti software in sottoscrizione e delle apparecchiature hardware acquisite nel corso della fornitura, a partire dalla data di accettazione della fornitura stessa.

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'Istituto, intendendosi ricompreso nel corrispettivo per l'acquisto delle licenze.

Il servizio di manutenzione, che dovrà essere prestato con le modalità indicate nel presente Capitolato Tecnico, comprende tutti gli oneri necessari per la perfetta e puntuale esecuzione del servizio stesso, nonché ogni altro onere per mantenere e/o riportare le apparecchiature hardware e i prodotti software in stato di funzionamento coerente con la documentazione, nonché le modifiche tecniche atte ad elevare il grado d'affidabilità, a migliorarne il funzionamento ed aumentarne la sicurezza.

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.

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.

L'Istituto comunicherà all'Impresa i malfunzionamenti per telefono, per e-mail o via web. In caso di comunicazione per telefono, si precisa che i termini per l'eliminazione dei malfunzionamenti decorrono dalla conferma per e-mail o via web. L'Impresa confermerà la presa in carico del problema via e-mail.

Ricevuta la comunicazione di cui sopra, l'Impresa si obbliga a confermare la presa in carico del problema mediante comunicazione via mail all'Istituto, entro 1 ora lavorativa.

L'Impresa si impegna ad attivarsi al fine di ripristinare la funzionalità delle apparecchiature e dei prodotti software entro i seguenti termini perentori:

- entro **4 ore lavorative** dalla presa in carico, nel caso di **problemi bloccanti** intervenuti su prodotti software, anche dovuti al rilascio di aggiornamenti che provochino disservizio alle apparecchiature dell'Istituto (siano esse Server, Personal Computer o Appliance);
- entro **24 ore lavorative** dalla presa in carico, nel caso di **problemi non bloccanti** intervenuti su prodotti software;
- entro **6 ore lavorative** dalla presa in carico, nel caso di **problemi bloccanti intervenuti su apparecchiature hardware ritenute critiche** per il buon funzionamento del sistema informativo dell'Istituto.

Ove la soluzione del malfunzionamento non intervenga entro il termine di cui al precedente comma, l'Istituto applicherà le penali previste all' articolo intitolato "Penali" del Contratto, salvo in ogni caso il risarcimento al maggior danno.

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 entro nuovi termini temporali da concordarsi tra le parti il cui rispetto sarà soggetto a verifica e ad eventuale applicazione di penali in caso di ritardo.

Le parti di ricambio hardware - che dovranno essere preferibilmente identiche o comunque equipollenti alle parti sostituite, purché con caratteristiche e funzionalità identiche o migliorative rispetto alle parti sostituite - verranno fornite dall'Impresa senza alcun onere aggiuntivo per l'Istituto; le parti sostituite verranno ritirate dall'Impresa stessa che ne riacquisirà pertanto la proprietà. Le parti fornite - salvo diverso accordo - dovranno essere nuove, restando l'Impresa impegnata a quanto previsto contrattualmente in termini di garanzie.

L'Impresa potrà apportare le modifiche e 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'Istituto, l'Impresa, previa comunicazione all'Istituto, dovrà provvedere alla sostituzione delle apparecchiature stesse con altre aventi le medesime caratteristiche tecniche e funzionali, ferma restando l'applicazione delle penali previste dal Contratto, sino al momento del ripristino definitivo o 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'Istituto.

Per ogni intervento di manutenzione dovrà essere redatta da un incaricato dell'Istituto e da un incaricato dell'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. Qualora il fermo o il malfunzionamento di una apparecchiatura comporti il mancato utilizzo di altre apparecchiature funzionalmente collegate, la Committente procederà all'applicazione delle penali anche per tali altre apparecchiature.

4.3. Servizio di Supporto Sistemistico Trellix Thrive – SKU THRIVE-ELITEA

Il livello di Supporto richiesto è il **Trellix Thrive Elite**, precedentemente denominato "McAfee Premier Success Plan", di cui al punto d) del precedente paragrafo 4.

Il Trellix Thrive Elite garantisce il massimo livello di assistenza del Vendor, in continuità migliorativa con il precedente piano.

Esso deve comprendere: un unico punto di contatto dedicato per la gestione delle richieste di supporto, un costante monitoraggio della postura di sicurezza dell'Istituto attraverso il controllo e la consulenza sull'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 Trellix 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 Trellix in collaudo ed esercizio.

Nel dettaglio, il "Trellix Thrive Elite", al fine di trarre il massimo valore dagli investimenti nelle soluzioni Trellix scelte da INAIL e ottimizzare le operazioni di sicurezza, deve prevedere una serie di risorse e di servizi integrati, tra cui:

1. un Resident Program Manager (RPM) assegnato e residente dedicato all'Istituto (precedentemente denominato Resident Customer Success Manager), per orchestrare tutte le soluzioni da implementare sia a breve che a lungo termine (configurazioni, distribuzioni, aggiornamenti, report sui casi aperti e sulla postura di sicurezza);
2. un contatto tecnico assegnato e remoto (Designated Support Engineer, DSE) per collaborare con l'RPM e INAIL per garantire una migliore esperienza nel supporto tecnico, affrontando proattivamente i problemi e gestendo le escalation;
3. L'accesso a tecnici senior del supporto tecnico (Customer Success Engineers, CSE) in tutto il mondo, che prendano in carico le richieste di supporto di INAIL con la massima priorità;
4. Il Trellix Health Watch, un servizio che fornisce un rapporto diagnostico approfondito e un riepilogo delle azioni di manutenzione consigliate e attuabili per garantire che le piattaforme Trellix siano completamente ottimizzate;
5. Servizi di consulenza avanzata sulla Cybersecurity e laboratori di prova e di studio sulle soluzioni Trellix.
6. Un Customer Success Manager remoto (CSM) e un Technical Account Manager remoto (TAM), risorse specifiche comprese nell' "Enterprise Care Plan" per le piattaforme Cloud.

4.4. Servizio di supporto sistemistico Resident Program Manager – SKU CUSTOM SKU

In particolare, con riferimento al Servizio di Resident Program Manager, di cui al punto d) del precedente paragrafo 4, si rende disponibile una risorsa specializzata e dedicata all'Istituto per tutta la durata del contratto. Risiede fisicamente presso la DCOD e lavora a stretto contatto con i referenti INAIL e con i consulenti esterni per le tematiche inerenti alla sicurezza informatica e alle tecnologie del fornitore utilizzate dall'Istituto. Tra le sue mansioni fondamentali, si occupa di coordinare, controllare e semplificare le attività delle risorse incluse nel "Trellix Thrive Elite" ai punti 2, 3, 4, 5 e 6 dell'elenco sopra descritto nel par. 4.3.

Il Resident Program Manager, inoltre, guida i task dei Servizi Professionali, d'accordo con i referenti INAIL, per agevolare la buona riuscita dei progetti di installazione, upgrade, migrazione e integrazione delle soluzioni Trellix scelte dall'Istituto, secondo le priorità e i tempi stabiliti.

In aggiunta, attingendo a quanto incluso nel "Trellix Thrive Elite", il Resident Program Manager:

1. Orchestra il Trellix Health Watch, un servizio che fornisce un rapporto diagnostico approfondito e un riepilogo delle azioni di manutenzione consigliate e attuabili per

garantire che le piattaforme Trellix siano utilizzate al meglio, secondo i più alti standard di sicurezza ed efficacia;

2. Si occupa del delivery di servizi di consulenza avanzata sulla Cybersecurity (ad esempio, con workshop mirati alla revisione dei processi interni di Gestione e Risposta agli Incidenti e di Protezione dei Dati, oppure coinvolgendo il Product Management in merito a richieste specifiche dell'Istituto sulle tecnologie in uso) e laboratori di collaudo e studio sulle soluzioni Trellix, tagliati sulle esigenze dei gruppi tecnici che ne abbiano bisogno.

Si faccia riferimento alla lista dei codici e quantità previste dal par. 4.3 per il livello di supporto richiesto nei 36 mesi.

L'obiettivo principale della consulenza specialistica Trellix è quello di ottenere il massimo dei benefici dalle installazioni Software e hardware implementate e da implementare presso la rete dell'Istituto, tali benefici devono rispondere a criteri di:

1. Gestione centralizzata delle soluzioni e monitoraggio totale del sistema;
2. Mantenimento di un elevato livello di sicurezza dell'infrastruttura nel tempo;
3. Capacità di adeguamento nel tempo alle nuove minacce;
4. Controllo e rendicontazione periodica sul livello di sicurezza del sistema informativo dell'Istituto attraverso analisi manuali e automatica, fornendo documenti dettagliati sia sull'AS IS e sia fornendo indicazioni sulle eventuali contromisure da implementare.
5. Integrazione nativa di tutte le componenti Trellix, sia quelle nuove e sia quelle già presenti presso l'Istituto.

Si precisa che per l'erogazione del Servizio devono essere utilizzate esclusivamente risorse del produttore Trellix.

4.5. Servizio di Supporto Sistemistico Skyhigh Enterprise Care – SKU SS-ENT-CARE

Il piano Skyhigh Enterprise Care avanzato, di cui al punto d) del precedente paragrafo 4, offre anche un Customer Success Manager (CSM) remoto e un Technical Account Manager (TAM) per supportare i programmi strategici dell'esperienza SSE. Questo piano prevede tempi di risposta rapidi (1 ora per SR di gravità 1 e 2 ore per SR di gravità 2), Health checks sono incluse.

4.6. Servizio di Training (formazione) per il personale INAIL – SKU TRN-IL-PRI-1D

La fornitura prevede l'erogazione di n° 6 training ufficiali Trellix, in aula per un **massimo di 6 persone a corso**, per un totale di **24 giorni**, al fine di garantire un aggiornamento delle competenze al personale dell'Istituto, di cui al punto d) del precedente paragrafo 4.

Corso Ufficiale Trellix	Giorni	SKU Trellix (codice)	Quantità
-------------------------	--------	----------------------	----------

Corso di aggiornamento della suite MV6 sulla componente EDR	2	TRN-IL-PRI-1D	2
Corso di aggiornamento Trellix Intelligent Virtual Execution (IVX)	2	TRN-IL-PRI-1D	2
Corso di aggiornamento Network IPS (NSP)	2	TRN-IL-PRI-1D	2
Corso di aggiornamento ENS/ATP	2	TRN-IL-PRI-1D	2
Corso di aggiornamento ESM	2	TRN-IL-PRI-1D	2
Corso di aggiornamento XDR	2	TRN-IL-PRI-1D	2

Per ogni corso dovrà essere rilasciata ad ogni partecipante documentazione ufficiale Trellix in relazione al completamento dello stesso.

L'Istituto 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.

L'Istituto richiederà all'Impresa l'erogazione delle suddette sessioni 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'Istituto 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'Istituto. In caso di mancata approvazione, l'Istituto comunicherà all'Impresa i motivi del dissenso che l'Impresa recepirà aggiornando il Piano e consegnandolo all'Istituto 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 ma comunque ubicata in Roma.

4.7. Servizi professionali di assistenza specialistica (a consumo)

La consulenza specialistica Trellix viene utilizzata per aggiornare e consolidare le soluzioni esistenti già installate e in produzione presso l'Istituto, di cui al punto e) del precedente paragrafo 4.

La tabella che segue descrive il profilo delle figure professionali dedicate alle attività.

Security Architect Consulting Daily - SKU MD-SA-SECC-Z1
<p>Il Security Architect è un ruolo di consulenza chiave che lavora con il cliente e con i clienti del settore pubblico e privato in generale per definire architetture e soluzioni di sicurezza che corrispondano ai requisiti e ai rischi aziendali. La sua figura consente di combinare la competenza del cliente in Cyber Security e architetture applicative/infrastrutturali con una consulenza aziendale adeguata a definire soluzioni sicure in alcuni degli ambienti più complessi. Inoltre ricopre il ruolo di interfaccia di alto livello con il cliente e si occupa del coordinamento dei team che lavorano in parallelo sui progetti di sicurezza del cliente. Ha anche la responsabilità di integrare, mediante analisi e proposte personali, le informazioni delle singole pianificazioni dei progetti, stabilire le fasi e le priorità dei singoli task di progetto in accordo col cliente. Si occupa anche di definire le macro schedulazioni con i Project Leader massimizzando l'impiego delle figure professionali coinvolte nello sviluppo dei progetti stessi. Diventa infine il gestore delle Escalation e delle Change Request.</p>
Custom Consulting Daily - SKU MD-CONSULT-DY-Z1
<p>Corrisponde alla figura tecnica del Senior Consultant su una o più soluzioni specifiche. Il Senior Consultant segue una formazione adeguata mediante la partecipazione a diversi progetti in cui è coinvolto dal punto di vista tecnologico anche superando con successo esami di certificazioni sulle tecnologie di cui si occupa più frequentemente. Il suo ruolo è focalizzato sulla gestione della delivery dei progetti Trellix al fine di implementare le soluzioni di sicurezza nell'infrastruttura del cliente. Si assume anche la responsabilità finale di comprendere la soluzione proposta per poi progettare e costruire un piano per implementarla e consegnarla con successo al cliente. Appartengono al suo ruolo anche le seguenti responsabilità:</p> <ul style="list-style-type: none"> ✓ collaborare a stretto contatto con i clienti e i team Trellix; ✓ consolidare la propria posizione di consulente strategico di fiducia con il cliente e promuovere il valore dei prodotti e servizi Trellix; ✓ interagire in modo proattivo con il cliente in ogni fase del loro percorso Trellix; ✓ identificare in modo proattivo i problemi e coordinarsi con i team Trellix per risolverli man mano che vengono identificati; ✓ fare da mentore ad altri consulenti junior.

L'ambito di intervento della consulenza Trellix è riconducibile **alle attività di configurazione, tuning, upgrade e refresh tecnologico** delle componenti Trellix elencate in tabella:

Componente	Funzione/Attività
Gestione attività e documentazione delle tecnologie Trellix	Fase di analisi dei requisiti e redazione della documentazione architeturale.
Rinnovo della suite Trellix Protect Plus EDR for Endpoint (MV6DEE-AA)	È la suite end point antimalware necessaria alla messa in sicurezza delle postazioni di lavoro e dei dispositivi mobili. Le attività prevedono l'analisi dello stato corrente delle tecnologie di sicurezza che appartengono a questa suite, l'implementazione di ottimizzazioni e miglioramenti evolutivi ed infine eventuali aggiornamenti nei contesti ove si ritenesse necessario.
Analisi e aggiornamento dell'architettura della tecnologia Skyhigh Secure Web Gateway	La tecnologia Skyhigh Secure Content Web Gateway è la componente di sicurezza Secure Web Gateway e protegge l'infrastruttura di rete aziendale dalle minacce provenienti dal web. Utilizzando diverse funzionalità in un processo complesso di integrazione di motori antimalware, filtra il traffico in uscita e in entrata quando gli utenti della rete aziendale accedono al web, consentendo o bloccando questo traffico in base alle regole della tua politica di sicurezza web. Questa attività prevede l'aggiornamento dell'architettura di

Classificazione del documento: Consip Public

AS SDAPA, per l'affidamento dei servizi di manutenzione ed evoluzione della piattaforma TRELLIX (ex McAfee) di

INAIL ed. 3 – ID 2853 –

Allegato 2 - Capitolato Tecnico

Componente	Funzione/Attività
	riferimento utilizzando delle appliance Skyhigh modello 5500-F (8 apparati).
Refresh tecnologico degli apparati Trellix Intrusion Prevention System	In questa fase saranno dismessi gli apparati a fine vita e saranno installati i nuovi sensori IPS Trellix Intrusion Prevention System con il relativo sistema di Management dei sensori stessi e alcuni componenti hardware come i Fail-Open Chassis and Module utilizzati nella configurazione corrente saranno integrati nella nuova.
Integrazione di Trellix Network Detection and Response	La tecnologia Trellix Network Detection and (NDR) ha il ruolo di mitigare qualsiasi tipologia di attacco evasivo a livello di rete. Il Trellix NDR verrà integrato nell'ecosistema IPS dell'Istituto come potenziamento dell'infrastruttura anti-intrusione attualmente in produzione.
Refresh tecnologico dell'architettura Trellix Enterprise Security Manager	L'attività prevede il refresh tecnologico dell'architettura hardware Trellix ESM, portando le componenti in produzione al livello software dell'ultima release disponibile ed integrando quelli presenti nella precedente architettura come gli Log Search e i Trellix Direct Attached Storage. L'attività prevede anche l'implementazione della soluzione XDR, che potenzia ed estende le funzionalità di raccolta, analisi, Hunting e risposta automatica fornite dal SIEM.
Aggiornamento tecnologico Sandbox Trellix	Il sistema di analisi di Trellix Virtual Execution 12600 consente di rilevare malware avanzati ed evasivi e convertire le informazioni sulle minacce in azioni e protezione immediate. Tali sistemi hanno anche funzionalità di ispezione aggiuntive che ampliano il rilevamento del malware e si basano su un sistema di sandboxes che interagisce con i sistemi di Network Security ed Endpoint Security già in produzione presso l'Istituto. Questa tecnologia sarà implementata ad integrazione dell'architettura Trellix ATD. Gli apparati Trellix ATD 6200 appartenenti all'architettura corrente saranno aggiornati a Trellix Intelligent Virtual Execution Server.
Integrazione nell'architettura di sandboxing di IVX Cloud	Trellix Intelligent Virtual Execution (IVX) Cloud sfrutta un motore di rilevamento Trellix IVX e più motori dinamici di apprendimento automatico, intelligenza artificiale e correlazione per raggiungere rapidamente una classificazione dei file inviati. IVX è un motore di analisi dinamico e senza firma che ispeziona anche il traffico di rete sospetto per identificare gli attacchi che eludono le difese tradizionali basate su firma e policy di sicurezza.
Aggiornamento Tecnologico Skyhigh SSE Advanced	La nuova suite Skyhigh SSE Advanced permette di unificare i servizi CASB, Data Protection e Web Gateway SAAS in un unico sistema con gestione centralizzata. L'attività prevede l'aggiornamento tecnologico con la nuova suite e l'attivazione delle nuove funzionalità.
Aggiornamento tecnologico di Trellix Cloud Workload Security Detect and Respond	È la suite per la sicurezza degli ambienti virtuali e server, sarà effettuato un aggiornamento tecnologico della piattaforma attualmente in produzione. Trellix Cloud Workload Security (CWS) automatizza la scoperta e la difesa da malware evoluti con lo scopo di eliminare i punti ciechi, fornire una difesa avanzata dalle minacce e semplificare la gestione multi-cloud.
Aggiornamento tecnologico della tecnologia Trellix MOVE AntiVirus for Virtual Desktops (VDI)	Trellix Management for Optimized Virtual Environments AntiVirus (Trellix MOVE AntiVirus) è la suite che offre una protezione antimalware avanzata e ottimizzata per i desktop

Classificazione del documento: Consip Public

AS SDAPA, per l'affidamento dei servizi di manutenzione ed evoluzione della piattaforma TRELLIX (ex McAfee) di

INAIL ed. 3 – ID 2853 –

Allegato 2 - Capitolato Tecnico

Componente	Funzione/Attività
	e server virtualizzati. Prevede anche un'opzione ottimizzata con agente e senza agente per VMware NSX. In entrambi i casi, implementa la massima sicurezza per il rilevamento e il contenimento delle minacce istantanee con un impatto minimo sulle prestazioni dei sistemi virtuali (VM). In questa fase si prevede l'aggiornamento software di questa tecnologia alle ultime versioni disponibili.

Piano attività

I servizi di assistenza specialistica dovranno essere svolti 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.

L'Amministrazione si riserva di richiedere in tutto o in parte i giorni/persona previsti, sulla base delle esigenze che emergeranno in corso di vigenza contrattuale. L'Istituto richiederà all'Impresa l'erogazione dei servizi mediante apposita comunicazione scritta 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'Istituto, dovrà fornire un Piano di lavoro contenente 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 nel presente Capitolato Tecnico;
- ✓ nominativi e 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'Istituto. In caso di mancata approvazione, l'Istituto comunicherà all'Impresa i motivi del dissenso che l'Impresa recepirà aggiornando il Piano e consegnandolo all'Istituto entro 5 giorni lavorativi. Una volta terminata l'attività descritta nel suddetto Piano, l'Istituto procederà alla Verifica di conformità secondo le modalità contrattualmente previste.

Per le attività di assistenza specialistica è prevista una rendicontazione su base mensile. La rendicontazione dovrà avvenire tramite invio di un rapporto dettagliato di intervento, realizzato su modulo Trellex "Timesheet", a cura del Responsabile della Fornitura. Per tutte le attività di assistenza specialistica l'erogazione e la rendicontazione sono previste in giorni/persona.

Gestione delle attività e documentazione

Classificazione del documento: Consip Public

AS SDAPA, per l'affidamento dei servizi di manutenzione ed evoluzione della piattaforma TRELLIX (ex McAfee) di

INAIL ed. 3 – ID 2853 –

Allegato 2 - Capitolato Tecnico

In questa fase sarà realizzata l'analisi iniziale e la documentazione di riferimento architetturale, l'integrazione, l'aggiornamento e il refresh tecnologico di tutte le seguenti componenti evolutive:

Analisi della suite Trellix Protect Plus EDR for Endpoint

Le attività prevedono l'analisi dello stato corrente delle tecnologie di sicurezza che appartengono a questa suite, l'implementazione di ottimizzazioni e miglioramenti evolutivi ed infine eventuali aggiornamenti nei contesti ove si ritenesse necessario. I task relativi a queste attività sono riportati nella tabella seguente:

Analisi della suite Trellix Protect Plus EDR for Endpoint	gg/uomo SKU MD-SA-SECC-Z1	gg/uomo SKU MD-CONSULT-DY-Z1
Analisi preliminare dell'architettura ePO e dei componenti integrati	8	3
Analisi preliminare delle tecnologie integrate in ePO	5	8
Aggiornamento dell'applicazione ePO all'ultima versione rilasciata ed integrazione degli aggiornamenti delle tecnologie di sicurezza integrate	6	8
Distribuzione degli aggiornamenti delle tecnologie di sicurezza Trellix sui sistemi gestiti da ePO	4	8
Valutazione di ottimizzazioni e miglioramenti evolutivi	6	6
Verifiche funzionali	3	5
Redazione della documentazione relativa alle procedure di collaudo	2	3
Supporto al collaudo	2	3
Totale gg/uomo per SKU	36	44
TOTALE giorni	80	

Analisi e aggiornamento dell'architettura della tecnologia Skyhigh Secure Web Gateway

La tecnologia Skyhigh Secure Content Web Gateway è la componente di sicurezza Secure Web Gateway e protegge l'infrastruttura di rete aziendale dalle minacce provenienti dal web. Questa attività prevede l'aggiornamento della architettura di riferimento utilizzando delle appliance Skyhigh modello 5500-F

Analisi e aggiornamento dell'architettura Skyhigh Secure Web Gateway	gg/uomo SKU MD-SA-SECC-Z1	gg/uomo SKU MD-CONSULT-DY-Z1
Assessment preliminare dell'architettura Skyhigh Secure Content Web Gateway	10	10
Installazione e configurazione dei nuovi appliance Skyhigh modello 5500-F	10	12

Migrazione dalla vecchia infrastruttura alla nuova aggiornata	10	12
Verifica delle configurazioni e delle policy di navigazione dei Skyhigh Secure Content Web Gateway	4	10
Verifiche funzionali e test di navigazione web	2	10
Redazione della documentazione relativa alle procedure di collaudo	4	5
Supporto al collaudo	2	2
Totale gg/uomo per SKU	42	61
TOTALE giorni	103	

Refresh tecnologico degli apparati Trellix Intrusion Prevention System

In questa fase saranno dismessi gli apparati a fine vita e saranno installati i nuovi sensori IPS Trellix Intrusion Prevention System con il relativo sistema di Management dei sensori stessi e alcuni componenti hardware come i Fail-Open Chassis and Module utilizzati nella configurazione corrente saranno integrati nella nuova.

Trellix Intrusion Prevention System – Refresh tecnologico	gg/uomo SKU MD-SA-SECC-Z1	gg/uomo SKU MD-CONSULT-DY-Z1
Studio e predisposizione dell'ambiente iniziale per il refresh tecnologico	10	10
Installazione e configurazione delle ultime release software rilasciate	10	12
Aggiornamento e integrazione dei nuovi componenti hardware	10	15
Integrazione dei componenti hardware presenti nella precedente architettura	6	12
Configurazione ed assessment delle policy	10	15
Configurazione ed analisi della reportistica	4	8
Test e verifiche funzionali	10	12
Redazione della documentazione relativa alle procedure di collaudo	2	3
Supporto al collaudo	5	8
Totale gg/uomo per SKU	67	95
TOTALE giorni	162	

Integrazione di Trellix Network Detection and Response

La tecnologia Trellix Network Detection and (NDR) ha il ruolo di mitigare qualsiasi tipologia di attacco evasivo a livello di rete. Il Trellix NDR verrà integrato nell'ecosistema IPS dell'Istituto come potenziamento dell'infrastruttura anti-intrusione attualmente in produzione.

Integrazione di Trellix Network Detection and Response	gg/uomo SKU MD-SA-SECC-Z1	gg/uomo SKU MD-CONSULT-DY-Z1
Studio e analisi iniziale della topologia di rete anche in funzione delle sonde IPS presenti nell'organizzazione aziendale	1	3
Installazione e configurazione del virtual appliance dedicato alla tecnologia Trellix Network Detection and Response all'ultima release software rilasciata	1	3
Integrazione dei flussi provenienti dalle sonde IPS	1	1
Analisi degli alert e delle detection	1	1
Prime analisi di asset inventory	1	1
Test e verifiche funzionali	1	2
Redazione della documentazione relativa alle procedure di collaudo	1	1
Supporto al collaudo	1	1
Totale gg/uomo per SKU	8	13
TOTALE giorni	21	

Refresh tecnologico dell'architettura Trellix Enterprise Security Manager

L'attività prevede il refresh tecnologico dell'architettura hardware Trellix Enterprise Security Manager e quella software di Trellix Enterprise Log Manager e Trellix Event Receiver a bordo di virtual appliance All-In-One. Tutte le componenti in produzione dei software saranno installate all'ultima release disponibile ed integrando quelli presenti nella precedente architettura come gli Log Search e i Trellix Direct Attached Storage. L'attività prevede anche l'implementazione della soluzione XDR, che potenzia ed estende le funzionalità di raccolta, analisi, Hunting e risposta automatica fornite dal SIEM.

Refresh tecnologico dell'architettura Trellix Enterprise Security Manager	gg/uomo SKU MD-SA-SECC-Z1	gg/uomo SKU MD-CONSULT-DY-Z1
Studio e predisposizione dell'ambiente iniziale per il refresh tecnologico	5	10
Installazione e configurazione dei nuovi apparati fisici Trellix Enterprise Security Manager aggiornati alle ultime release software rilasciate	10	15
Trellix Enterprise Log Manager e Trellix Event Receiver a bordo di virtual appliance All-In-One	5	6
Log Search e i Trellix Direct Attached Storage presenti nella precedente architettura	6	12
Integrazione del modulo GTI	3	8
Configurazione e porting della reportistica	4	10
Integrazione delle sorgenti On Premise con la piattaforma Trellix XDR	8	12
Integrazione delle sorgenti Cloud con la piattaforma Trellix XDR	4	12

Classificazione del documento: Consip Public

AS SDAPA, per l'affidamento dei servizi di manutenzione ed evoluzione della piattaforma TRELLIX (ex McAfee) di

INAIL ed. 3 – ID 2853 –

Allegato 2 - Capitolato Tecnico

Personalizzazione delle Dashboard della piattaforma Trellix XDR	8	10
Tuning e personalizzazione delle regole della piattaforma Trellix XDR	8	10
Implementazione e testing delle funzionalità di Risposta Automatica della piattaforma Trellix XDR	8	10
Test e verifiche funzionali	3	5
Redazione della documentazione relativa alle procedure di collaudo	2	2
Supporto al collaudo	2	3
Totale gg/uomo per SKU	76	125
TOTALE giorni	201	

Aggiornamento tecnologico Sandbox Trellix

Il sistema di analisi di Trellix Virtual Execution 12600 consente di rilevare malware avanzati ed evasivi e convertire le informazioni sulle minacce in azioni e protezione immediate. Tali sistemi hanno anche funzionalità di ispezione aggiuntive che ampliano il rilevamento del malware e si basano su un sistema di sandboxes che interagisce con i sistemi di Network Security ed Endpoint Security già in produzione presso l'Istituto. Questa tecnologia sarà implementata ad integrazione dell'architettura Trellix ATD. Gli apparati Trellix ATD 6200 appartenenti all'architettura corrente saranno aggiornati a Trellix Intelligent Virtual Execution Server.

Aggiornamento tecnologico Sandbox Trellix	gg/uomo SKU MD-SA-SECC-Z1	gg/uomo SKU MD-CONSULT-DY-Z1
Studio e analisi iniziale della configurazione ed architettura della tecnologia Trellix ATD	5	10
Analisi ed aggiornamento degli appliance Trellix ATD a Trellix Intelligent Virtual Execution Server	10	10
Preparazione dell'ambiente all'upgrade tecnologico realizzato mediante le nuove appliance fisiche Virtual Execution 12600	10	10
Migrazione delle configurazioni presenti nella precedente infrastruttura ove possibile	6	10
Valutazione di ottimizzazione e migliorie evolutive	3	5
Implementazione delle policy di sicurezza	3	3
Test e verifiche funzionali	2	3
Redazione della documentazione relativa alle procedure di collaudo	2	2
Supporto al collaudo	2	2
Totale gg/uomo per SKU	43	55
TOTALE giorni	98	

Integrazione nell'architettura di sandboxing di IVX Cloud

Classificazione del documento: Consip Public

AS SDAPA, per l'affidamento dei servizi di manutenzione ed evoluzione della piattaforma TRELLIX (ex McAfee) di

INAIL ed. 3 – ID 2853 –

Allegato 2 - Capitolato Tecnico

L'attività consiste nell'implementazione e integrazione della componente IVX Cloud con l'architettura dell'Istituto.

Integrazione nell'architettura di sandboxing di IVX Enterprise Cloud	gg/uomo SKU MD-SA-SECC-Z1	gg/uomo SKU MD-CONSULT-DY-Z1
Studio e analisi iniziale dell'architettura di sandboxing	10	12
Analisi del contesto di protezione e di implementazione (collaboration, spazi di archiviazione di dati aziendali in cloud, app di messaggistica e di sharing di file, ecc.)	10	10
Integrazione della componente IVX Cloud con le componenti Trellix e di terze parti in produzione.	10	12
Test e verifiche funzionali	10	12
Redazione della documentazione relativa alle procedure di collaudo	2	2
Supporto al collaudo	2	2
Totale gg/uomo per SKU	44	50
TOTALE giorni	94	

Aggiornamento Tecnologico Skyhigh SSE Advanced

La nuova suite Skyhigh SSE Advanced permette di unificare i servizi CASB, Data Protection e Web Gateway SAAS in un unico sistema con gestione centralizzata. L'attività prevede l'aggiornamento tecnologico con la nuova suite e la valutazione dell'attivazione delle nuove funzionalità.

Aggiornamento Tecnologico Skyhigh SSE Advanced	gg/uomo SKU MD-SA-SECC-Z1	gg/uomo SKU MD-CONSULT-DY-Z1
Studio e analisi iniziale dell'architettura esistente	8	12
Aggiornamento tecnologico alla nuova suite Skyhigh SSE Advanced	12	15
Configurazione delle policy e valutazione di miglievie evolutive	15	15
Test e verifiche funzionali	8	8
Redazione della documentazione relativa alle procedure di collaudo	4	4
Supporto al collaudo	2	3
Totale gg/uomo per SKU	49	57
TOTALE giorni	106	

Aggiornamento tecnologico di Trellix Cloud Workload Security Detect and Respond

L'attività prevede l'aggiornamento in produzione alla nuova piattaforma Trellix Cloud Workload Security (CWS).

Aggiornamento tecnologico di Trellix Cloud Workload Security Detect and Respond	gg/uomo SKU MD-SA-SECC-Z1	gg/uomo SKU MD-CONSULT-DY-Z1
--	----------------------------------	-------------------------------------

Studio e analisi iniziale dell'architettura esistente	5	8
Valutazione di aggiornamenti di nuove versioni	5	8
Configurazione e ottimizzazione delle policy e valutazione di migliorie evolutive	5	8
Test e verifiche funzionali	2	3
Redazione della documentazione relativa alle procedure di collaudo	1	1
Supporto al collaudo	2	3
Totale gg/uomo per SKU	20	31
TOTALE giorni	51	

Aggiornamento tecnologico della tecnologia Trellix MOVE AntiVirus for Virtual Desktops (VDI)

L'attività prevede l'aggiornamento in produzione all'ultima release rilasciata della tecnologia Trellix MOVE AntiVirus for Virtual Desktops (VDI).

Aggiornamento tecnologico della tecnologia Trellix MOVE AntiVirus for Virtual Desktops (VDI)	gg/uomo SKU MD-SA-SECC-Z1	gg/uomo SKU MD-CONSULT-DY-Z1
Studio e analisi iniziale dell'architettura esistente	2	3
Integrazione in ePO delle ultime release di Trellix MOVE Antivirus for Virtual Desktop	3	5
Configurazione e ottimizzazione delle policy e valutazione di eventuali migliorie evolutive	3	3
Installazione in aggiornamento del prodotto sui sistemi gestiti da ePO	2	4
Test e verifiche funzionali	2	2
Redazione della documentazione relativa alle procedure di collaudo	1	1
Supporto al collaudo	1	1
Totale gg/uomo per SKU	14	19
TOTALE giorni	33	

Servizi di consulenza/assistenza sistemistica - Tabelle riepilogative

Nella seguente tabella si fornisce il riepilogo del totale giornate comprensivo di supporto sistemistico alla gestione per l'intero periodo di validità del contratto (36 mesi).

Figura professionale	SKU Trellix (codice)	Giorni uomo
Security Architect Consulting Daily	MD-CONSULT-DY-Z1	399
Custom Consulting Daily	MD-SA-SECC-Z1	550
TOTALE giorni		949

4.8. Fornitura di nuovi prodotti software in sottoscrizione o in licenza d'uso perpetua e nuove apparecchiature hardware

La consegna di nuovi prodotti software in sottoscrizione o in licenza d'uso perpetua e nuove apparecchiature hardware 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 l'elenco dei prodotti software e delle corrispondenti quantità, l'elenco delle apparecchiature hardware e delle corrispondenti quantità, che l'Istituto intende acquisire. I prodotti software e le apparecchiature hardware, nonché le relative quantità, saranno compresi tra gli oggetti di fornitura previsti dal presente Capitolato Tecnico.

Le consegne dovranno avvenire presso la Direzione Centrale per l'Organizzazione Digitale - Via Santuario Regina degli Apostoli, 33 00145 Roma - 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 operativo approvato dall'Istituto e, comunque, non oltre **60 giorni solari decorrenti dalla data di consegna**.

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

4.9. Garanzia

Ogni prodotto software e apparecchiatura hardware deve essere pienamente rispondente ai requisiti funzionali espressi, alle normative vigenti, ai requisiti non funzionali (sicurezza, usabilità, prestazionalità, manutenibilità, ecc.), nonché agli standard, linee guida e miglior prassi disponibile per lo sviluppo software.

Ne discende che eventuali anomalie e difettosità non intercettate durante le fasi di test del Fornitore e di verifica di conformità (collaudo) della Committente, riscontrabili sulle funzionalità abilitate e/o modificate durante l'intera fornitura devono essere rimosse, come parte integrante dei servizi che li hanno realizzati, a totale carico del Fornitore. Pertanto, l'Impresa dovrà garantire la tempestiva rimozione dei difetti dell'hardware e del software nuovo e/o modificato nonché la correzione e/o il ripristino delle basi dati deteriorate come ripercussione dei difetti.

Si precisa che gli interventi correttivi dovranno riguardare anche la documentazione a corredo.

Per tutto l'hardware e il software rilasciato, inoltre, il Fornitore deve produrre/aggiornare la relativa documentazione. La documentazione deve rispondere a requisiti di accuratezza, comprensibilità e più in generale usabilità.

Pertanto deve essere garantita la correzione gratuita dei difetti riguardanti:

- ✓ gli oggetti hardware e software nuovi e/o modificati;
- ✓ le basi dati deteriorate come ripercussione dei difetti;

- ✓ la documentazione a corredo al software.

La garanzia opera per 36 mesi relativamente a tutto l'hardware e software della piattaforma Trellix installato e configurato ad inizio fornitura, a partire dalla "Data di accettazione della fornitura" delle licenze software, di cui al successivo paragrafo 5.6, lettera a).

La suddetta garanzia deve essere prestata in proprio dall'Impresa anche per il fatto del terzo, intendendo l'Amministrazione restare estranea ai rapporti tra l'Impresa e le ditte fornitrici.

4.10. Requisiti tecnici

Di seguito si specificano i principali requisiti tecnici previsti per la fornitura.

4.10.1. Compatibilità'

Tutto il l'hardware e software installato dovrà essere compatibile con la release/il livello effettivo degli ambienti di collaudo/esercizio attivi al momento in cui l'hardware e il software saranno utilizzati.

Si rappresenta che i prodotti hardware e software, citati nel presente capitolato, nel corso della fornitura potranno subire variazioni di release/livello o potranno essere oggetto di sostituzione con altri prodotti.

4.10.2. Accessibilità'

I prodotti resi disponibili dal Fornitore devono essere conformi ai requisiti di accessibilità stabiliti dal decreto del Ministro per l'innovazione e le tecnologie dell'8 luglio 2005 e successive modifiche. In altre parole deve essere garantito il diritto di accesso ai servizi informatici e telematici della Pubblica Amministrazione da parte di soggetti disabili e/o svantaggiati.

4.10.3. Supporto alla verifica di conformità dell'hardware e del software

Nel corso della verifica di conformità dell'hardware e del software da parte della Committente sull'ambiente di collaudo, il Fornitore deve garantire, senza alcun onere aggiuntivo, il supporto richiesto.

In particolare dovrà garantire:

- ✓ passaggio di conoscenza sulle funzionalità della soluzione alla Committente o a terzi indicati dalla Committente;
- ✓ training-on-the-job durante i primi giorni di avviamento in collaudo;
- ✓ presenza on site, su chiamata, entro 1 giorno lavorativo delle figure professionali competenti;
- ✓ supporto all'esecuzione dei test;
- ✓ altre eventuali attività richieste dalla Committente per ottimizzare la verifica di conformità (collaudo) ed il successivo rilascio in esercizio.

4.10.4. Consegna in gestione

È compresa nella fornitura la consegna in gestione del nuovo hardware e software installato e

configurato, al fine di assicurare un appropriato passaggio di consegne ai team dedicati ai servizi di gestione; l'attività deve essere formalizzata nel Piano Operativo; in particolare dovranno essere previste almeno le seguenti attività:

- ✓ illustrazione della documentazione prodotta nell'ambito del rilascio del software in esame;
- ✓ passaggio di conoscenza funzionale e tecnica.

Il Fornitore è tenuto, preliminarmente al passaggio del software in gestione, a fornire il proprio supporto a INAIL nell'esecuzione dei test di qualità e della certificazione del software, al fine di garantire omogeneità di comportamento e aderenza alle best practice internazionali in materia di sviluppo software.

4.10.5. Supporto passaggio in esercizio

È compreso nella fornitura il supporto ai gruppi di gestione, alle strutture della Committente e ad altre strutture dedicate, finalizzato alla predisposizione dell'ambiente di esercizio. Si precisa che la messa in esercizio potrà avvenire anche in un momento differito rispetto all'avvenuta verifica di conformità dell'hardware e del software.

4.11. Requisiti organizzativi

È richiesto al Fornitore che le risorse impiegate nella fornitura abbiano elevate capacità tecniche e professionali: prontezza, precisione, affidabilità, competenza e perfetta conoscenza della documentazione contrattuale.

È essenziale da parte del Fornitore un elevato grado di flessibilità nel rendere disponibili le risorse, nonché nel garantire le necessarie competenze.

In caso di sostituzione, le nuove risorse professionali devono avere attestati ed esperienze, in tipologia e durata, non inferiori alle risorse da sostituire.

Si precisa, inoltre, che i titoli e le certificazioni richiesti/offerti, dovranno essere posseduti per l'intera durata contrattuale.

In caso di sostituzione di risorse certificate le nuove risorse dovranno possedere le stesse certificazioni.

Si richiede che il Fornitore, nell'ambito dei diversi servizi, provveda alla verbalizzazione degli incontri con la Committente, al fine di condividere in tempi rapidi quanto deciso nel corso degli incontri.

Nel caso di indisponibilità dei referenti, ad esempio per ferie, malattia, il Fornitore deve garantire un'adeguata sostituzione al fine di assicurare il servizio richiesto dalla Committente.

I referenti dovranno dare piena visibilità alla Committente su tutte le attività di propria competenza.

Si sottolinea infine che, a prescindere dall'organizzazione che il Fornitore adotterà per l'erogazione dei servizi, è richiesto un alto grado di sinergia tra tutte le risorse impiegate nella fornitura, al fine di garantire un costante e adeguato grado di conoscenza e di attenzione

evitando discontinuità.

4.12. Ruoli richiesti

La Società dovrà fornire entro **10 (dieci) giorni** dalla data di stipula del contratto l'elenco delle risorse che utilizzerà nell'esecuzione della fornitura. Eventuali variazioni (in ingresso o in uscita) alla composizione dell'elenco del personale dichiarato dovranno essere comunicate anticipatamente e debitamente motivate.

La Società deve inoltre fornire, con un preavviso di cinque giorni, l'elenco delle ulteriori risorse che utilizza nell'esecuzione della fornitura per particolari esigenze tecniche o per picchi di lavoro.

La Committente si riserva la facoltà di esaminare le risorse messe a disposizione dalla Società, per verificarne sia i livelli di conoscenza sia la generale idoneità allo svolgimento delle attività richieste. Nel caso in cui la Committente non fornisca l'approvazione delle risorse proposte, il Fornitore si obbliga a procedere alla sostituzione delle risorse umane entro il termine di **10 (dieci) giorni solari** dalla comunicazione da parte dell'Amministrazione e a garantire la continuità del team di lavoro.

Qualora la sostituzione fosse fatta in ritardo o la nuova risorsa fosse ancora inadeguata e si dovesse ricorrere a un'ulteriore sostituzione, verranno applicate le penali del caso, secondo le modalità previste dallo schema di contratto.

Le risorse assegnate non possono essere sostituite dalla Società durante l'esecuzione delle attività; qualora intervenissero eventi non dipendenti dalla Società (per esempio dimissioni) che costringessero alla sostituzione di una risorsa, la Società dovrà farsi carico del periodo di affiancamento/istruzione necessario per rendere la nuova risorsa autonoma per il servizio.

La Società dovrà curare l'aggiornamento professionale delle proprie risorse, per garantire il pieno svolgimento delle attività di supporto per l'evoluzione tecnologica e di attuazione dell'eventuale adeguamento dell'applicazione a nuove versioni.

La Società dovrà mettere a disposizione le risorse in conformità con la tipologia richiesta, con la quantità richiesta e con le date previste per l'inizio delle singole attività.

4.12.1. Responsabile della fornitura

Entro **5 (cinque) giorni** lavorativi dalla stipula del contratto, l'Impresa dovrà comunicare all'Amministrazione il nominativo del proprio rappresentante designato quale **Responsabile della fornitura** (o Responsabile della Società per le attività contrattuali). In particolare, tale responsabile sarà, per gli aspetti amministrativi e contrattuali, l'interlocutore unico di INAIL.

Sarà cura del Responsabile della fornitura verificare il rispetto di tutti gli adempimenti contrattuali.

Tale referente non dovrà comportare alcun onere aggiuntivo per la Committente.

Il Responsabile della fornitura non farà parte di alcuno dei gruppi di lavoro relativi ai servizi oggetto della fornitura.

Il Responsabile della fornitura dovrà in particolare:

Classificazione del documento: Consip Public

AS SDAPA, per l'affidamento dei servizi di manutenzione ed evoluzione della piattaforma TRELLIX (ex McAfee) di

INAIL ed. 3 – ID 2853 –

Allegato 2 - Capitolato Tecnico

- ✓ predisporre ed aggiornare il piano operativo, in assenza di figure specifiche di maggiore e più puntuale preparazione tecnica specifica;
- ✓ monitorare i livelli di servizio sulle attività oggetto della fornitura ed intraprendere eventuali azioni correttive a fronte del mancato rispetto delle soglie previste e/o a fronte di rilievi;
- ✓ fornire i risultati sugli indicatori di qualità;
- ✓ riferire ed intervenire su problematiche relative ad eventuale mancata aderenza delle risorse impiegate rispetto ai profili professionali richiesti.

4.13. Riservatezza

La Società, al di fuori delle attività oggetto del presente capitolato, non potrà utilizzare, a nessun titolo, i moduli software forniti dalla INAIL nell'ambito dei servizi della fornitura, la documentazione e qualunque informazione della Committente di cui dovesse venire al corrente o entrare in possesso.

4.14. Adempimenti per la sicurezza

L'Impresa s'impegna a porre in essere quanto necessario a garantire l'esecuzione dei servizi in piena aderenza con le disposizioni del D. Lgs. 81/2008 "*Testo Unico sulla sicurezza durante il lavoro*", cooperando e coordinandosi, in particolare, con i referenti della Committente ai fini degli adempimenti di cui al comma 2 dell'art. 26 del citato decreto.

5. ESECUZIONE DELLA FORNITURA

Al Fornitore è richiesto in tutte le attività della fornitura il rispetto dei processi, degli standard e delle linee guida adottate dalla Committente; il Fornitore deve farsi carico di conoscere e diffondere al proprio interno tali conoscenze, di applicarle proattivamente, e di recepirne tempestivamente eventuali variazioni.

La tipologia delle attività da svolgere e la delicatezza della materia trattata richiedono che tutte le attività dell'Impresa siano improntate a un'assoluta attenzione alla riservatezza. È inoltre fatto divieto all'Impresa di utilizzare il presente affidamento quale riferimento per altri incarichi, salvo esplicita autorizzazione da parte dell'Amministrazione.

Il corrispettivo complessivo offerto dall'Impresa si intende comprensivo di tutte le attività richieste e necessarie per l'esecuzione della fornitura. Tale corrispettivo non potrà subire aumenti neanche al variare della pianificazione effettiva rispetto a quanto inizialmente previsto.

L'Impresa dovrà indicare, entro **5 (cinque) giorni** lavorativi dalla stipula del contratto, il **Responsabile della Fornitura** che, assumendo la piena responsabilità dei rapporti con la Committente, sarà il riferimento per gli aspetti generali e per ogni problema riguardante la fornitura stessa.

Tutte le attività dovranno essere svolte in collaborazione con i referenti dell'Amministrazione, secondo modalità che saranno opportunamente concordate in fase di avvio.

L'amministrazione si riserva di modificare le modalità di esecuzione descritte e di introdurre

nuove modalità, anche in corso d'opera, dandone congruo preavviso all'Impresa. In aggiunta, tali modalità di esecuzione potranno essere congiuntamente riviste, su proposta dell'Impresa, e potranno essere concordate opportune semplificazioni o variazioni in funzione delle specificità dei singoli interventi.

INAIL si riserva di avvalersi di terzi per il supporto allo svolgimento di attività di propria competenza, ferma restando la responsabilità globale di INAIL nello svolgimento di tali attività.

5.1. Modalità di esecuzione della fornitura

Le attività correlate alla fornitura/installazione dei prodotti, alla manutenzione dei prodotti installati e al supporto specialistico avranno luogo presso la sede INAIL di Via S. Regina Degli Apostoli 33, 00145 Roma (RM).

Eventuali interventi presso altre sedi, site nel comune di Roma, potranno essere comunque richiesti dalla Committente al Fornitore del servizio.

Le attività di manutenzione, secondo modalità da concordare con la Committente, potranno essere svolte anche presso le sedi del Fornitore.

5.1.1. Modalità di erogazione continuativa

Il servizio da erogare in modalità continuativa è quello di Manutenzione dei prodotti software e delle apparecchiature hardware Trellix in esercizio presso i sistemi dell'Amministrazione.

L'attivazione è prevista a partire dalla data di avvio delle attività e l'erogazione è senza soluzione di continuità fino alla data di fine delle attività, salva ed impregiudicata la facoltà della Committente di sospendere, ridurre e/o interrompere il servizio.

In particolare, il servizio di Manutenzione Correttiva, anche se attivato su uno specifico evento, è erogato in modalità continuativa in quanto lo specifico evento non è pianificabile.

Dal momento in cui una richiesta per malfunzionamento è registrata nel sistema della Committente, o nel sistema del Fornitore in assenza dello stesso, decorrono i tempi relativi ai livelli di servizio definiti nel presente capitolato tecnico.

Il Fornitore ha la responsabilità della esecuzione dell'attività di risoluzione del malfunzionamento ed è tenuto ad aggiornare le informazioni di propria competenza sul sistema fino alla soluzione del malfunzionamento stesso motivato con la opportuna e dettagliata diagnosi.

Per la Manutenzione Adeguativa, il Fornitore dovrà presentare un piano di attività da sottoporre alla valutazione della Committente, al fine di garantire gli obiettivi prefissati (upgrade di release, installazione patch, ecc.).

Il piano dovrà includere la fase di collaudo (verifica di conformità) necessaria per l'accettazione dell'intervento stesso.

5.2. Pianificazione

Le modalità di gestione della pianificazione riportate di seguito si riferiscono a tutte le attività previste nella Fornitura.

PIANIFICAZIONE

Dovrà essere predisposto e mantenuto costantemente aggiornato il **Piano Operativo** contenente attività, tempi e impegno dei diversi servizi, contenente il piano iniziale relativo all'installazione e configurazione della soluzione di Trellix, il piano dei servizi continuativi nonché il piano riepilogativo per le attività relative al servizio di supporto specialistico.

Il Fornitore è tenuto a comunicare proattivamente e con la massima tempestività qualsiasi criticità, ritardo o impedimento che modifichi il piano concordato e ad inviare una ripianificazione delle attività, aggiornando e riconsegnando alla Committente il Piano operativo.

A fronte di ripianificazioni autorizzate dalla Committente, dovrà essere predisposta una nuova versione del Piano operativo.

In nessun caso potrà essere rivisto il Piano operativo per inadempimenti da parte del Fornitore.

Il Piano operativo e le sue modifiche, come formalizzate nei verbali/email, certificano ai fini contrattuali gli obblighi formalmente assunti dal Fornitore e accettati dalla Committente, su stime e tempi di esecuzione delle attività e sulle relative date di consegna dei prodotti (scadenze).

L'Impresa si impegna, pertanto, a tenere costantemente aggiornato il Piano operativo in modo da riflettere, in ogni momento, lo stato dell'arte delle singole attività.

STATO AVANZAMENTO LAVORI

Il Fornitore dovrà mantenere aggiornata la sezione di stato di avanzamento prevista nel piano operativo, fornendo tempestivamente indicazioni sulle attività concluse ed in corso, esplicitandone la percentuale di avanzamento, descrivendo eventuali criticità/ritardi e le relative azioni di recupero.

5.3. Attivazione dei servizi

L'Impresa, entro 5 (cinque) giorni solari dalla stipula del Contratto, dovrà sottoporre a INAIL un "**Piano Operativo**" contenente le modalità di attivazione dei servizi individuando, per ciascuna attività, personale, mezzi e tempi di esecuzione. Tale Piano Operativo dovrà essere approvato da INAIL entro 15 (quindici) giorni dall'avvenuta consegna dello stesso.

Fatto salvo eventuali modifiche richieste dalla Committente sui termini proposti nel *Piano operativo*, i termini previsti nel piano approvato debbano intendersi inderogabili, pena l'applicazione delle penali.

L'allestimento dei servizi da parte del Fornitore deve avvenire secondo quanto disposto dal presente Capitolato, nonché come eventualmente migliorato nell'offerta tecnica, in termini di logistica, organizzazione, sicurezza, documentazione e quanto altro necessario.

5.4. Luogo di lavoro

Le attività oggetto dei servizi della fornitura sono svolte, salvo diversa indicazione della Committente, presso la sede INAIL già specificata nel par. 5.1.

Resta inteso che i costi di trasferimento e soggiorno del personale che svolge le attività presso

la Committente sono comunque a carico della Società.

Il Fornitore dovrà garantire la presenza presso l'Amministrazione per l'erogazione dei servizi e/o per riunioni e/o per qualsiasi esigenza connessa alla fornitura, senza oneri aggiuntivi rispetto a quanto offerto.

Le attività di correzione di eventuali malfunzioni potranno essere svolte presso le sedi del Fornitore.

Gli ambienti messi a disposizione saranno disponibili nel normale orario di lavoro e comunque potranno essere congiuntamente definiti diversi orari per esigenze straordinarie.

Per le attività della fornitura, in particolare per il servizio di manutenzione, il gruppo di lavoro dovrà garantire una copertura tra le 8:00 e le 18:00 nei giorni dal lunedì al venerdì, secondo una distribuzione delle presenze da concordare con la Committente.

Altre necessità di presenza di risorse in orari e/o giorni diversi, verranno pianificate e concordate tra le parti.

5.5. Impiego e stabilità delle risorse

L'Impresa garantisce che tutte le risorse che impiegherà per l'erogazione dei servizi oggetto della fornitura, sia in fase di attivazione dei servizi sia durante l'affidamento stesso, in caso di integrazioni e/o sostituzioni, rispondono ai requisiti minimi espressi dal presente capitolato.

L'Amministrazione si riserva comunque la possibilità di procedere a colloqui di approfondimento per verificare la corrispondenza dei profili proposti rispetto alle specifiche esigenze progettuali.

Per il personale ritenuto inadeguato, qualunque sia il ruolo ed il servizio impiegato, la Committente procederà alla richiesta formale di sostituzione.

Si evidenzia che le eventuali sostituzioni di personale durante l'esecuzione della fornitura ovvero all'inizio della stessa dovranno essere preventivamente concordate con il referente dell'Amministrazione e la sostituzione dovrà prevedere un adeguato periodo di affiancamento per la risorsa entrante.

5.6. Verifica di conformità

All'avvio della fornitura e in corso di contratto l'Amministrazione effettuerà le verifiche di conformità delle prestazioni, volta a certificare che le prestazioni contrattuali siano eseguite a regola d'arte sotto il profilo tecnico-funzionale.

A tal fine, il Fornitore dovrà 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.

Delle operazioni di verifica di conformità verrà redatto apposito verbale. La Verifica di conformità si intende positivamente superata solo nel caso in cui le prestazioni risultino eseguite a regola d'arte, sotto il profilo tecnico-funzionale, ed in conformità e nel rispetto delle condizioni, modalità, termini e prescrizioni espresse nel presente documento. La Verifica di conformità si intende altresì positivamente superata se il valore economico delle Sottoscrizioni

acquisite annualmente risulterà conforme ai valori economici annuali previsti da INAIL.

L'Impresa è tenuta a prestare all'Amministrazione, a propria cura e spese, l'assistenza tecnica necessaria e a mettere a disposizione della Amministrazione le attrezzature eventualmente occorrenti alle operazioni di verifica di conformità.

La verifica di conformità verrà effettuata, a seconda della complessità dell'oggetto contrattuale e verrà conclusa:

- con riferimento alla fornitura di cui al paragrafo 4, lett. b) (e, se esercitata l'opzione, lettera g)) entro il termine di 30 giorni con decorrenza dalla consegna del Rapporto di Fine Installazione;
- con riferimento al servizio di cui al paragrafo lett. a), c), d) (e se esercitata l'opzione, anche al servizio di cui alla lettera h)) entro il mese successivo al trimestre di riferimento;
- con riferimento ai servizi di cui al paragrafo lett. e) e f), entro il mese successivo al completamento dell'attività.

Nel caso di esito positivo della verifica di conformità la data del verbale verrà considerata quale:

- a) **“Data di Accettazione della Fornitura”** con riferimento alla fornitura di cui al paragrafo 4 lett. b) (e se esercitata l'opzione, lett. g)),
- b) **“Data di accettazione del Servizio”** con riferimento ai servizi di cui al paragrafo 4, lett. a), c), d), e), f) (e se esercitata l'opzione, anche al servizio di cui alla lettera h)), relativamente alle attività verificate da parte della Committente.

In caso di esito negativo della verifica di conformità, l'Impresa dovrà provvedere, a propria cura e spese, ad eliminare i vizi accertati entro il termine massimo che le verrà comunicato dalla Amministrazione. In tale ipotesi, la verifica di conformità verrà ripetuta, con le modalità precedentemente descritte.

Nel caso in cui anche la seconda verifica di conformità dia esito negativo, l'Amministrazione, ferma l'applicazione delle penali, avrà facoltà di risolvere il contratto e di fare eseguire in tutto o in parte le prestazioni a terzi in danno dell'Impresa.

Tutti gli oneri derivanti dalla verifica di conformità si intendono a carico dell'Impresa.

Le verifiche saranno ripetute in corso di esecuzione del contratto per le prestazioni continuative.

Nel caso in cui, durante la verifica, venissero rilevate anomalie in ragione dei livelli di servizio richiesti, sarà emessa una penale in funzione degli indicatori applicabili ai casi riscontrati.

5.7. Azioni contrattuali

Ogni inadempimento contrattuale darà origine ad un'azione commisurata alla criticità della violazione.

Pertanto, il mancato rispetto dei requisiti minimi richiesti determina azioni contrattuali

conseguenti che possono consistere in una o più delle seguenti azioni:

- ✓ coinvolgimento di un livello più elevato di interlocutori, sia del Fornitore che della Committente, allo scopo di prendere le decisioni necessarie al ripristino delle situazioni fuori soglia o fuori controllo (attivazione di una procedura di escalation);
- ✓ ripetizione da parte del Fornitore dell'erogazione di una prestazione, rifacimento di una attività, riconsegna di un prodotto (chiusura di una non conformità);
- ✓ azione di intervento sui processi produttivi del Fornitore per evitare il ripetersi di sistematiche non conformità (esecuzione di una azione correttiva);
- ✓ applicazione di penali;
- ✓ azioni aggiuntive (richiesta danni, risoluzione anticipata del contratto, ecc.) laddove previsto contrattualmente.

Segue un approfondimento degli istituti a tutela della qualità dell'erogazione della fornitura.

5.8. Penali

Lo scopo delle penali è quello di riequilibrare il servizio effettivamente ricevuto (di minore qualità, e/o generando disservizi e/o ritardi e/o inducendo un danno all'utilizzatore) dalla Amministrazione al corrispettivo da erogarsi che è stabilito per prestazioni effettuate a regola d'arte.

Le penali da adottare sono individuate contrattualmente e normalmente sono organizzate in modo progressivo, in relazione alla gravità o al ripetersi della mancata soddisfazione degli adempimenti richiesti.

Per il dettaglio del processo di contestazione ed applicazione delle penali, si rinvia a quanto puntualmente disciplinato nel contratto.

6. REQUISITI DI QUALIFICAZIONE DEI SERVIZI CLOUD

I servizi cloud oggetto della presente iniziativa dovranno essere erogati nel rispetto dei requisiti descritti dall'ACN, in tema di qualificazione dei servizi e delle infrastrutture cloud. Il contratto verrà stipulato previa verifica sul Catalogo ACN di cui al Regolamento ACN n. 21007/2024 del 27/06/2024 del possesso del livello di qualificazione dei servizi cloud e/o del livello di adeguatezza dell'infrastruttura richiesto.

Ciò premesso, nell'ambito del regime transitorio in essere, **il livello di qualificazione minimo da possedere per i servizi oggetto della presente acquisizione è il QC1.**

Si precisa che la qualificazione è condizione essenziale ai fini della stipula del contratto e dovrà essere mantenuta per tutta la durata dello stesso, secondo la disciplina di cui agli articoli 4 S – Bis e 4 S – Ter delle Condizioni speciali di contratto.

7. CERTIFICAZIONI

Per l'esecuzione dei servizi oggetto del presente appalto è richiesto che l'impresa

aggiudicataria disponga di almeno una delle seguenti certificazioni **Trellix**:

- ✓ **Platinum;**
- ✓ **Gold;**
- ✓ **Silver.**

In sede di esecuzione, e quindi di stipula contrattuale, è richiesto che l'aggiudicataria sia in grado di comprovare il possesso di almeno una delle precedenti certificazioni, in quanto tale requisito **è condizione essenziale ai fini della stipula del contratto da parte dell'aggiudicatario della procedura.**