CLASSIFICAZIONE DEL DOCUMENTO: CONSIP PUBLIC

ALLEGATO 2

CAPITOLATO TECNICO - PARTE SPECIALE

ID 2367 - GARA A PROCEDURA APERTA PER L'AFFIDAMENTO DI UN ACCORDO QUADRO AI SENSI DELL'ART. 54 COMMA 3 DEL D. LGS 50/2016 PER LA FORNITURA DI PRODOTTI PER LA SICUREZZA PERIMETRALE, PROTEZIONE DEGLI ENDPOINT E ANTI-APT ED EROGAZIONE DI SERVIZI CONNESSI PER LE PUBBLICHE AMMINISTRAZIONI – LOTTI 1, 2, 3

Principali modifiche intervenute dalla pubblicazione del documento "ID 2367 - Condizioni di Fornitura - parte Speciale" relativo all'avviso di preinformazione pubblicato sulla GUUE n. S-147 del 02/08/2021

Paragrafi	Ambito
1.1	Modifica inerente l'entrata in vigore della L. n. 109/2021
3.1	Inserimento di ulteriori requisiti di sicurezza sui prodotti
3.1	Precisazione sui requisiti di commerciabilità dei prodotti hardware e software
3.1.3	Aggiornamento del requisito minimo relativo alla Funzionalità di Sandboxing
3.1.5	Aggiornamento del requisito migliorativo relativo alla Funzionalità di Sandboxing
3.1.6	Aggiornamento del requisito migliorativo relativo alla Funzionalità di Sandboxing
3.2	Modifica al requisito migliorativo ID 12.5 in seguito all'entrata in vigore della L. 108/2021
4.3.1	Esplicitazione delle modalità di produzione della reportistica
4.3.2	Esplicitazione delle modalità di produzione della reportistica
6	Inserimento della colonna "Valorizzazione della penale" nelle tabelle del paragrafo

SOMMARIO

Indice delle Tabelle

1 PREMESSA

Il presente Capitolato Tecnico, parte speciale, ha l'obiettivo di descrivere i requisiti minimi e le caratteristiche migliorative dei prodotti per la **sicurezza perimetrale, protezione degli endpoint, anti-APT e dei relativi servizi connessi**, che riguardano i lotti 1-3 della presente procedura di gara.

Se non diversamente specificato, i termini temporali espressi nel presente Capitolato sono tutti da intendersi come solari (di calendario).

Il fornitore si impegna, **pena l'esclusione dalla gara**, ad offrire prodotti e servizi che posseggano almeno i requisiti minimi come esposti nella documentazione di gara nel suo complesso.

Saranno oggetto di valutazione esclusivamente le caratteristiche migliorative indicate e per le quali è previsto nel Capitolato d'Oneri il relativo punteggio premiante.

1.1 Definizioni

Per agevolare la lettura viene di seguito riportato il glossario dei termini più frequentemente utilizzati e relativa definizione nell'ambito del presente documento:

- **Accordo Quadro (AQ)**: Accordo Quadro con un solo operatore economico, ai sensi dell'art. 54, comma 3 del D. Lgs. n. 50/2016;
- **AD:** Active Directory;
- **Aggiudicatario** o **Fornitore**: le imprese, i Raggruppamenti Temporanei di Imprese o i Consorzi che risultano Aggiudicatari dei singoli Lotti 1-3;
- **Amministrazione Aggiudicatrice**: Consip S.p.A.;
- **Amministrazione Contraente/Amministrazione/i**: le Amministrazioni Pubbliche legittimate all'utilizzo dell'Accodo Quadro, secondo quanto previsto nell'"Allegato 1 Capitolato Tecnico – Parte Generale" in base al lotto;
- **Anti – APT:** anti-Advanced Persistent Threat;
- **API:** application programming interface;
- **ATT&CK:** Adversarial Tactics, Techniques & Common Knowledge, elenco strutturato di tattiche e tecniche di attacco cyber elaborato dall'organizzazione MITRE;
- **BEC:** business email compromise;
- **BOT/BOTNET:** malware utilizzato per assumere il controllo remoto di un computer/ rete di computer infettati da malware in modo da essere controllati da remoto;
- **Brand/Vendor:** produttore della specifica tecnologia offerta;
- **BYOD:** bring your own device;
- **Capitolato Tecnico – Parte Speciale (o semplicemente Capitolato Tecnico)**: il presente documento;
- **CASB:** cloud access security broker;
- **C&C:** command & control;
- **CERT:** Computer Emergency Response Team;
- **CSIRT:** Computer Security Incident Response Team;

- **CNTI:** Canale Nazionale di Trasmissione IoC;
- **Concorrente** o **Offerente**: l'Impresa o il Raggruppamento Temporaneo di Imprese o il Consorzio che partecipano alla presente gara;
- **Contratto Esecutivo**: il contratto stipulato dall'Amministrazione con il Fornitore, che si perfeziona con l'invio dell'OdF;
- **CV:** centri di valutazione del Ministero dell'interno e del Ministero della difesa;
- **CVCN:** Centro di Valutazione e Certificazione nazionale, istituito presso il Ministero dello sviluppo economico e trasferito dal D.L. 82/2021 (convertito con L. n. 109/2021) presso l'Agenzia per la cybersicurezza nazionale;
- **DHCP:** Dynamic Host Configuration Protocol;
- **DLP:** data loss prevention;
- **DOS/DDOS:** Denial of Service/ Distributed Denail of Service;
- **EAP-TLS:** Extensible Authentication Protocol – Transport Layer Security;
- **EDR**: endpoint detection and response;
- **EPP**: endpoint protection platform;
- **FIX:** protocollo Financial Information eXchange;
- **FTP/FTPS:** file transfer protocol/ FTP Secure;
- **Gbps:** gigabit per secondo;
- **GE:** gigabit ethernet**;**
- **Giorno lavorativo**: da lunedì a venerdì, esclusi sabato e festivi;
- **HTTP/HTTPS:** HyperText Transfer Protocol/ HTTP Secure;
- **ICT/IT:** Information and Communications Technology/Information Technology;
- **IDS:** intrusion detection system;
- **IoC:** indicatori di compromissione;
- **IOT:** internet of things;
- **IP:** internet protocol;
- **IPS:** intrusion prevention system;
- **IPSEC:** Internet protocol security;
- **IPV4/V6:** Internet protocol versione 4/versione 6;
- **KB:** kilobyte;
- **JSON:** formato per lo scambio di dati JavaScript Object Notation;
- **LDAP:** Lightweight Directory Access Protocol;
- **Listino di fornitura**: corrispettivi risultanti dall'Offerta economica presentata dall'Aggiudicatario in sede di Gara per tutti i prodotti e servizi previsti e descritti nel Capitolato tecnico;
- **MAC:** Media Access Control;
- **Mbps:** megabit per secondo;
- **MISP:** Malware Information Sharing Platform;
- **MS-CHAP v2:** Microsoft Challenge Handshake Authentication Protocol;
- **MSSQL:** Microsoft Structured Query Language;
- **NAC**: network access control;
- **NGFW**: next generation firewall;
- **NTLM:** New Technology Lan Manager, protocollo di autenticazione Microsoft;

- **Offerta Tecnica**: il documento redatto dal Concorrente in risposta alla gara alla quale il presente Capitolato fa riferimento;
- **Ordinativo di fornitura (OdF)**: il documento con il quale le Amministrazioni Contraenti, eventualmente anche attraverso le Unità Ordinanti, manifestano la loro volontà di acquistare i sistemi oggetto dell'AQ, impegnando il Concorrente alla relativa fornitura e prestazione dei servizi;
- **OUI:** Organizationally Unique Identifier;
- **PAC file:** proxy auto configuration file;ù
- Portale della Fornitura: il Portale implementato dal Fornitore Aggiudicatario, secondo le specifiche tecniche descritte nel Capitolato Tecnico Parte Generale par. 4.1;
- **QoS:** quality of service;
- **QSFP+:** porta in grado di ospitare un transceiver Quad Small Form-factor Pluggable +**;**
- **RCA:** root cause analysis;
- **RDP:** remote desktop protocol;
- **Responsabile dell'Amministrazione:** la persona indicata dall'Amministrazione nell'OdF e individuata come interlocutore tecnico con il Fornitore per tutte le attività contrattuali.
- **Responsabile del Fornitore:** la persona indicata dal Fornitore, nell'ambito di ciascun contratto esecutivo, come referente operativo per le attività di fornitura ed erogazione dei relativi servizi connessi, i cui requisiti professionali e compiti sono descritti al par. 2.4.1.2 del Capitolato Tecnico Generale;
- **RUAC:** responsabile unico delle attività contrattuali, cioè il referente del Fornitore nei confronti di Consip S.p.A. per tutte le attività di gestione relative all'AQ, dotato di appositi poteri di firma tali da impegnare in maniera esecutiva il Fornitore nei confronti delle Amministrazioni, i cui requisiti professionali e compiti sono descritti al par. 2.4.1.1 del Capitolato Tecnico Generale;
- **SDK:** software development kit;
- **SFP/SFP+:** porta in grado di ospitare un transceiver small form factor pluggable/SFP +;
- **SEG:** secure email gateway;
- **SIEM:** security information & event management;
- **SIP:** session initiation protocol;
- **SLA:** service level agreement, livelli di servizio;
- **SMB:** protocollo server message block;
- **SMTP:** Simple Mail Transfer Protocol;
- **SNMP:** Simple Network Management Protocol;
- **SOC:** security operations center;
- **SPP**: server protection platform;
- **SSL:** protocollo secure sockets layer;
- **STIX:** Structured Threat Information eXpression;
- **SWG**: secure web gateway;
- **Sistema telematico (o semplicemente "Sistema")**: indica la piattaforma telematica attraverso cui saranno gestite le fasi di adesione all'AQ e invio degli OdF;
- **TAXII:** Trusted Automated eXchange of Indicator Information**;**
- **TCP:** transmission control protocol
- **TLS:** protocollo transport layer security;

- **UDP:** user datagram protocol;
- **Unità Ordinante/i**: gli Uffici e le persone fisiche delle Amministrazioni Contraenti abilitati ad effettuare gli OdF;
- **URL:** Uniform Resource Locator**;**
- **VPN:** virtual private network;
- **WAF**: web application firewall;
- **WCCP:** Web Cache Communication Protocol;
- **XML:** linguaggio di programmazione eXtensible Markup Language.

1.2 Oggetto

I prodotti richiesti sono:

- Next Generation Firewall (NGFW);
- Network Access Control (NAC);
- Endpoint Protection Platform (EPP)/Endpoint Detection & Response (EDR);
- Server Protection Platform (SPP);
- Protezione Anti-Advanced Persistent Threat (Anti-APT).

I servizi connessi alla loro fornitura richiesti sono:

- installazione e configurazione (inclusi nella fornitura);
- formazione e affiancamento;
- manutenzione;
- Contact Center ed help desk (inclusi nel complesso dei corrispettivi previsti);
- hardening su client;
- supporto specialistico.

Si precisa che:

- per tutti gli ambiti di prodotto è richiesta **l'offerta obbligatoria** di un numero fissato di tecnologie ("brand") su tutte le fasce dimensionali/prestazionali richieste (offerta completa).
- in relazione ai servizi connessi, è richiesta una quotazione economica specifica unicamente per:
    - formazione e affiancamento;
    - manutenzione;
    - hardening su client;
    - supporto specialistico.

  I costi relativi ai servizi di installazione, configurazione e aggiornamenti software/firmware (compresi nella fornitura) **si intendono invece inclusi nei corrispettivi offerti per i prodotti**.

1.3 Condizioni di utilizzo dell'Accordo Quadro

Le Amministrazioni Contraenti potranno utilizzare l'AQ attraverso l'emissione di Ordinativi di Fornitura (OdF).

È onere dell'Aggiudicatario: ***(i)*** verificare che l'Ordinativo di fornitura emesso nei suoi confronti dall'Amministrazione Contraente sia stato da quest'ultima correttamente emesso nel rispetto di tutti i vincoli dell'AQ, ***(ii)*** chiarire alle Amministrazioni le condizioni di utilizzo dell'AQ, ***(iii)*** dare seguito agli OdF nei termini e modalità espresse nello schema di Accordo Quadro.

1.4 Durata

La durata temporale dell'AQ è fissata in 24 mesi dalla data di attivazione. Entro tale termine le Amministrazioni Contraenti potranno emettere Ordinativi di Fornitura all'Aggiudicatario.

I servizi di manutenzione potranno avere durata di 12/24 mesi, in base alle richieste dell'Amministrazione Contraente, mentre il servizio di supporto specialistico potrà essere erogato fino ad un massimo di 24 mesi dalla data accettazione del relativo OdF.

I singoli Contratti di Fornitura, che si perfezionano con l'accettazione da parte dell'Aggiudicatario degli Ordinativi di Fornitura, potranno avere quindi una durata massima di 24 mesi.

2 MODALITÀ DI ATTIVAZIONE DELLA FORNITURA

L'Aggiudicatario dovrà impegnarsi a garantire il rispetto delle fasi operative del processo di fornitura secondo quanto indicato nel presente paragrafo e riassunto nello schema seguente.
L'Amministrazione gestirà direttamente con l'Aggiudicatario le fasi procedurali necessarie all'emissione dell'Ordinativo di Fornitura.

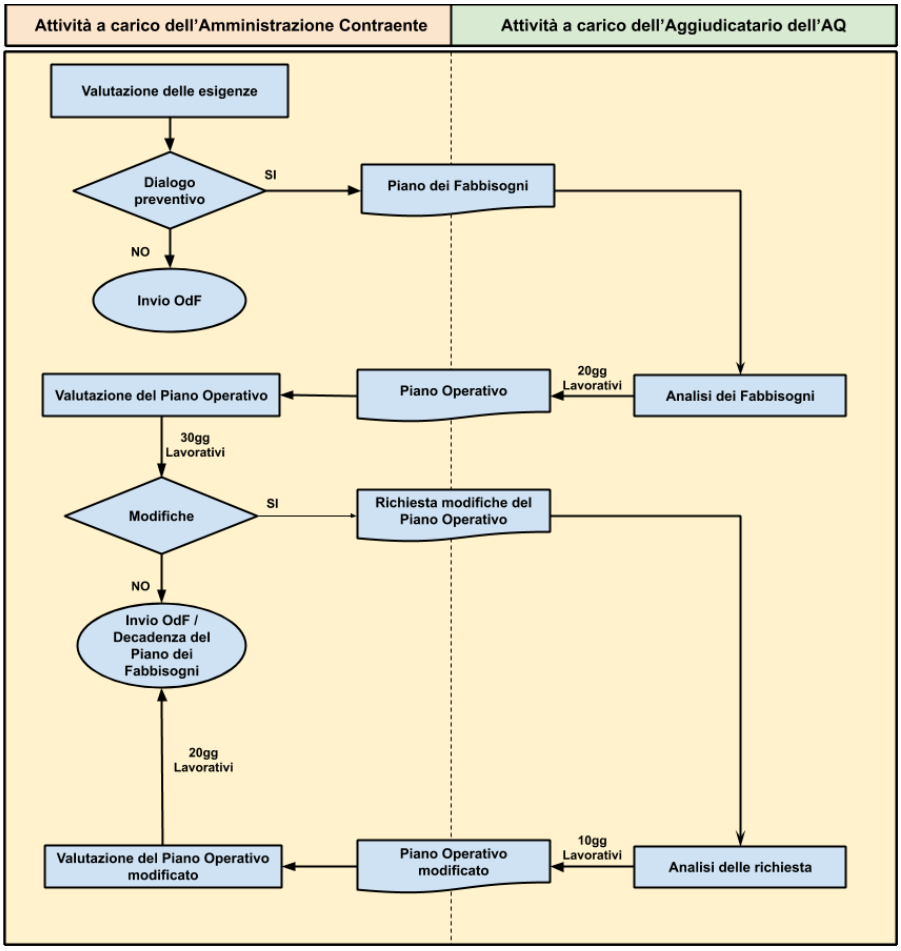

Figura 1: Modalità di adesione all'AQ

Il modello di fornitura e di erogazione dei servizi prevede l'iter procedurale di seguito descritto:

- l'Amministrazione, per utilizzare l'AQ e acquistare i prodotti e servizi in essa previsti, dovrà valutare preventivamente la necessità di effettuare un dialogo preventivo alla realizzazione dell'ordinativo con il Fornitore in modo da comprendere al meglio, in base alle proprie specifiche peculiarità, quali siano i prodotti e servizi maggiormente indicati a rispondere alle proprie esigenze, individuando in tal modo la relativa stima dei costi affrontati sulla base delle condizioni (economiche e tecnico-prestazionali) stabilite nell'Accordo Quadro:
    - qualora dalla valutazione preliminare effettuata dall'Amministrazione, questa dovesse determinare che non vi è necessità alcuna di dialogo preventivo con il Fornitore, potrà procedere all'acquisto diretto dei prodotti e dei servizi emettendo, attraverso il Sistema, un OdF, secondo i vincoli previsti nel successivo paragrafo 2.1;
    - qualora dalla valutazione preliminare effettuata dall'Amministrazione, questa dovesse determinare che vi è necessità di dialogo preventivo con il Fornitore, invierà un "*Piano dei Fabbisogni*" che dia indicazione delle proprie necessità, secondo quanto previsto nel paragrafo 2.1. **Il Fornitore dovrà assicurare, in ogni caso, il necessario supporto all'Amministrazione, propedeutico all'invio del suddetto piano;**

- il Fornitore, nel caso di invio del "*Piano dei Fabbisogni*" da parte dell'Amministrazione, **dovrà innanzitutto effettuare un'analisi del piano inviato e dovrà redigere un "*Piano Operativo*"**, che dovrà essere fornito all'Amministrazione Contraente secondo quanto previsto nel paragrafo 2.2;
- l'Amministrazione valuterà il suddetto documento, contenente l'esatta definizione tecnica ed economica del perimetro delle forniture e dei servizi e potrà procedere con:
    - l'approvazione del documento e l'emissione dell'OdF;
    - la richiesta di eventuali modifiche;
    - la non approvazione, qualora l'Amministrazione decida di non proseguire con l'emissione dell'OdF. In tale eventualità il relativo "*Piano dei Fabbisogni*" si intenderà decaduto;
- in caso di variazioni richieste da parte dell'Amministrazione, il Fornitore procederà alla modifica del "*Piano Operativo",* in accordo con le indicazioni/informazioni supplementari fornite dall'Amministrazione, provvedendo alla successiva ritrasmissione dello stesso all'Amministrazione;
- l'Amministrazione valuterà il "*Piano Operativo"* integrato e potrà procedere con:
    - l'approvazione del documento e l'emissione dell'OdF
    - la non approvazione, qualora l'Amministrazione decida di non proseguire con l'emissione dell'OdF. In tale eventualità il relativo "*Piano dei Fabbisogni*" si intenderà decaduto.

Successivamente alla ricezione dell'OdF, l'Aggiudicatario provvederà all'esecuzione delle attività richieste e concordate nel "*Piano Operativo"*.

2.1 Valutazione delle esigenze e Piano dei Fabbisogni

L'Amministrazione contraente valuterà preliminarmente la necessità di dover ricorrere al preventivo dialogo con il Fornitore sulla base delle sue esigenze.
Laddove ritenga che tale dialogo non sia richiesto, l'Amministrazione potrà procedere a effettuare direttamente un OdF a Sistema, nei limiti di quanto nel seguito specificato, stipulando il Contratto Esecutivo con il Fornitore.
I prodotti e i servizi che l'Amministrazione Contraente potrà acquisire direttamente tramite la piattaforma, senza la necessità di emettere il Piano dei Fabbisogni, sono:

- **tutti i prodotti previsti**. Si precisa che potranno essere acquistati anche solamente delle "componenti" che fanno riferimento ai prodotti richiesti, in ogni caso rientranti nel listino di fornitura (a titolo esemplificativo l'Amministrazione potrà procedere ad acquisire unicamente una specifica licenza connessa ad uno dei prodotti di cui al paragrafo 1.2). Si precisa che l'acquisto dei prodotti prevede obbligatoriamente le relative attività di installazione e configurazione (cfr. paragrafo 3.2.1), il cui costo si intende incluso nei corrispettivi offerti per i relativi prodotti. Quindi, in caso di ordine diretto, è onere dell'Amministrazione fornire al Fornitore tutte le specifiche di installazione e configurazione e garantire che tutte le attività propedeutiche alle stesse siano state correttamente eseguite. Nel prezzo dei prodotti è altresì **incluso l'aggiornamento dei software/firmware /subscription necessarie per la durata di due anni;**
- **il servizio di manutenzione** (contestualmente ai prodotti da manutenere).

Gli ulteriori servizi opzionali acquistabili (servizio di supporto specialistico, hardening su client e formazione e affiancamento) saranno ordinabili a Sistema solo a seguito dell'approvazione del Piano Operativo.
Nell'OdF l'Amministrazione riporterà inoltre il nominativo e i riferimenti del "*Responsabile dell'Amministrazione*", che sarà responsabile dei contatti con il Fornitore e l'indicazione del/i luogo/ghi di esecuzione dei servizi. In tale caso il Fornitore, entro due giorni lavorativi dalla data di accettazione dell'OdF, dovrà obbligatoriamente inviare al *Responsabile dell'Amministrazione* il nominativo e i riferimenti del proprio *Responsabile del Fornitore* (cfr. par. 2.4.1.2 del Capitolato Tecnico Generale)

Al contrario, laddove l'Amministrazione ritenga che un dialogo preventivo con il Fornitore sia necessario, l'Amministrazione procederà ad inviare il suo "*Piano dei Fabbisogni*" in cui si specificano i prodotti e le quantità stimate, con eventuali indicazioni relative all'infrastruttura esistente, alle modalità tecniche ed operative per l'erogazione dei servizi connessi e i corrispettivi unitari da applicare, in funzione di quelli previsti nell'Accordo Quadro, nonché tutte le informazioni tecniche, funzionali ed economiche che l'Amministrazione ritenga utile indicare.

Il "*Piano dei Fabbisogni*" dell'Amministrazione conterrà il nominativo e i riferimenti del "*Responsabile dell'Amministrazione*" e potrà, a titolo esemplificativo, ricomprendere le seguenti informazioni:

- il contesto in cui si inserisce la fornitura;
- gli obiettivi che la fornitura si propone di soddisfare;
- l'importo contrattuale e le quantità previste per i prodotti e i servizi oggetto del Contratto Esecutivo;
- indicazione se il contratto esecutivo è finanziato, in tutto o in parte, con le risorse previste dal Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021 e dal Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, nonché' dal PNC;
- le tempistiche richieste per la realizzazione della fornitura, con descrizione di eventuali vincoli e/o criticità;
- l'indicazione del/i luogo/ghi di interesse della fornitura;
- la durata del Contratto Esecutivo;
- informazioni tecniche quali schemi di rete, piani di indirizzamento, apparati già in essere, utili a meglio comprendere il perimetro di interesse e indirizzare la migliore soluzione tecnologica;
- le modalità con cui il Fornitore, che si sia riservato la possibilità di ricorrere al subappalto, debba indicare, nel **Piano Operativo**, le prestazioni da subappaltare;
- ogni altra informazione che l'Amministrazione ritenga utile condividere, quali la categorizzazione degli interventi e il/gli indicatori di digitalizzazione di cui al Capitolato Tecnico – Parte Generale.

L'Amministrazione dovrà inoltre identificare nel "*Piano dei Fabbisogni*" il "*Responsabile dell'Amministrazione*" con i relativi riferimenti.

Su richiesta dell'Amministrazione il Fornitore dovrà fornire eventuale supporto nella predisposizione del "*Piano dei fabbisogni*", fornendo all'Amministrazione tutte le informazioni, procedurali e tecnico/economiche, inerenti l'Accordo Quadro.

Si precisa che dalla trasmissione del "***Piano dei fabbisogni*"** da parte dell'Amministrazione verso il Fornitore selezionato non scaturisce obbligo per l'Amministrazione di procedere alla stipula del Contratto Esecutivo con il Fornitore.

2.2 Emissione del Piano Operativo

Il Fornitore - entro **20 giorni lavorativi** dalla ricezione del "*Piano dei Fabbisogni*" pena l'applicazione della penale di cui al par. 6 - dovrà predisporre e inviare all'Amministrazione un "*Piano Operativo*" nel quale raccogliere e dettagliare le richieste dell'Amministrazione, contenute nel "*Piano dei Fabbisogni*", e formulare una proposta tecnico/economica secondo le modalità tecniche ed operative ed i corrispettivi unitari previsti nell'Accordo Quadro.

Ai fini della redazione del documento il Fornitore potrà richiedere all'Amministrazione di effettuare dei sopralluoghi e/o incontri con il personale dell'Amministrazione per meglio verificare l'infrastruttura tecnica e le modalità di erogazione dei servizi, secondo quanto richiesto dall'Amministrazione nel "*Piano dei fabbisogni*". In tale eventualità il Fornitore deve approntare il calendario dei sopralluoghi necessari e deve indicare, per ciascuna sede oggetto di sopralluogo, il nominativo dell'incaricato dal fornitore che effettuerà il sopralluogo, con gli estremi di un documento di riconoscimento e l'elenco delle verifiche da effettuare. Il calendario viene sottoposto all'approvazione dell'Amministrazione interessata. Di ogni sopralluogo eseguito dovrà essere redatto specifico verbale attestante luogo, data, ora e attività di massima espletate.

Nel "*Piano Operativo*" il Fornitore dovrà riportare, a titolo esemplificativo e non esaustivo, almeno i seguenti aspetti, in coerenza con quanto espresso dall'Amministrazione nel suo "*Piano dei fabbisogni*":

- l'importo contrattuale complessivo e per ciascuna voce oggetto di quotazione economica, con il dettaglio dei prodotti e dei servizi oggetto del contratto esecutivo, anche in base alle indicazioni riportate nei rispettivi paragrafi relativi ai prodotti e ai servizi previsti
- la durata del Contratto Esecutivo
- informazione tecniche quali:
    - informazioni riguardanti l'Hardware di ogni apparato. L'Aggiudicatario dovrà riportare, per ogni tipologia di apparato, il codice prodotto e la descrizione di ogni elemento costituente;
    - informazioni riguardanti il Software di ogni apparato. L'Aggiudicatario dovrà riportare, per ogni tipologia di apparato, la release software configurata e l'elenco di tutte le patch correttive installate
    - configurazioni previste;
    - regole di nomenclatura individuate per i vari elementi. L'Aggiudicatario dovrà proporre delle regole di nomenclatura, che dovranno in ogni caso essere conformi a quanto già eventualmente realizzato dall'Amministrazione Contraente e con quest'ultima condivise
    - schemi logici dell'architettura
    - schemi di indirizzamento, policy di sicurezza ed ogni altra informazione di configurazione necessaria per l'introduzione dei nuovi apparati, stabiliti in accordo all'Amministrazione Contraente conformemente a quanto già implementato

- ogni altra informazione utile a consentire alle Amministrazioni rientranti nel perimetro di sicurezza cibernetica la redazione della comunicazione da trasmettere al CVCN o ai CV;
- indicazione dei prerequisiti necessari all'installazione degli elementi di fornitura e delle necessarie attività in carico all'Amministrazione Contraente

- indicazione delle verifiche funzionali da effettuare, descrivendo i casi di test identificati ed i risultati attesi e delle modalità di effettuazione di tali verifiche
- l'elenco di eventuali deliverable di fornitura
- il cronoprogramma, riportante i tempi previsti per l'esecuzione delle attività e dei servizi richiesti in accordo con l'Amministrazione Contraente, evidenziando anche le tempistiche legate a eventuali attività propedeutiche a carico dell'Amministrazione. I tempi che saranno concordati, una volta approvati, dovranno essere rispettati pena l'applicazione delle penali riportate al par. 6. Si precisa che è facoltà dell'Amministrazione concordare con il Fornitore la possibilità di effettuare rilasci successivi in caso di forniture di particolare complessità, o in base a esigenze manifestate dall'Amministrazione
- l'indicazione del/i luogo/ghi e delle sedi di esecuzione dei servizi
- l'impegno in giorni persona dei singoli profili professionali coinvolti, previsto per l'erogazione di ciascun servizio di fornitura
- i CV delle risorse professionali da impiegare con le relative certificazioni
- le prestazioni che si intende subappaltare, nel rispetto delle previsioni dell'Accordo Quadro e di quanto indicato nel Piano dei fabbisogni;
- le informazioni relative alla categorizzazione degli interventi e utili all'Amministrazione ai fini del calcolo degli indicatori di digitalizzazione, così come indicati dall'Amministrazione stessa in fase di Piano dei Fabbisogni.

Dovrà inoltre essere indicato nel suddetto documento il modello organizzativo impiegato per l'esecuzione delle attività ed in particolare le persone di riferimento che saranno coinvolte nel processo, che comprendono almeno:

- il "*Responsabile dell'Amministrazione*" (già identificato nel "*Piano dei Fabbisogni*");
- il "*Responsabile del Fornitore*" (cfr. par. 2.4.1.2 del Capitolato Tecnico Generale).

Si precisa che dalla trasmissione del "*Piano Operativo*" da parte del Fornitore verso l'Amministrazione **non scaturisce l'obbligo per l'Amministrazione** di procedere alla stipula del Contratto Esecutivo con il Fornitore. Le Amministrazioni saranno tenute a comunicare in forma scritta alla Consip S.p.A. tutte le ipotesi di mancato rispetto da parte del Fornitore del termine per la trasmissione del "*Piano Operativo*", ai fini dell'applicazione da parte dell'Amministrazione aggiudicatrice della penale di cui al par. 6.

2.3 Contratto Esecutivo

L'Amministrazione, entro **30 giorni lavorativi** dalla ricezione, ha la facoltà di approvare il "*Piano Operativo*", o di comunicare la richiesta di eventuali modifiche e/o integrazioni, in coerenza con il "*Piano dei fabbisogni*". In tal caso l'aggiudicatario dovrà apportare al documento presentato le modifiche necessarie, in accordo con quanto richiesto. Laddove l'Amministrazione, trascorso il summenzionato termine, non abbia proceduto né all'emissione dell'OdF né alla richiesta di modifiche, il relativo "***Piano dei fabbisogni***" si intenderà decaduto.

A seguito dell'eventuale richiesta di modifiche da parte dell'Amministrazione, il Fornitore dovrà inviare la versione definitiva del Piano Operativo **entro 10 giorni lavorativi** dalla comunicazione di richiesta dell'Amministrazione contraente, pena l'applicazione, da parte dell'Amministrazione aggiudicatrice su segnalazione dell'Amministrazione contraente, della penale di cui al par. 6.

Qualora, decorsi **20 giorni lavorativi** dalla ricezione del "*Piano Operativo*" modificato l'Amministrazione non lo abbia approvato, il relativo "*Piano dei fabbisogni*" si intenderà decaduto.

Contestualmente all'approvazione del "*Piano Operativo*", l'Amministrazione provvederà all'invio a Sistema dell'OdF, mediante il quale stipulerà il Contratto Esecutivo con il Fornitore.

Si precisa che in tutti i casi in cui, a seguito delle interlocuzioni tra l'Amministrazione contraente e il Fornitore, la medesima Amministrazione stabilisse, come in precedenza descritto, di non procedere con la stipula del Contratto Esecutivo, il "*Piano Operativo*" rimarrà di proprietà intellettuale del Fornitore, fatta ovviamente eccezione per tutti i dati comunicati dall'Amministrazione o comunque relativi alla propria dotazione tecnica e struttura tecnico/organizzativa.

In tutti i casi, il Fornitore inoltre dovrà produrre, **entro 10 giorni lavorativi** dall'invio dell'OdF, il **Piano di lavoro generale**, riportante **la pianificazione di dettaglio** di tutte le attività, in accordo con le modalità operative e i livelli di servizio previsti e in conformità con il Piano Operativo ad esso allegato.

Nel caso in cui l'Amministrazione non abbia fatto ricorso al preventivo dialogo con il Fornitore e, pertanto, non sia stato precedentemente redatto e approvato il Piano Operativo, il Piano di lavoro generale dovrà comprendere, oltre alla pianificazione di dettaglio di tutte le attività, a titolo esemplificativo e non esaustivo, almeno i seguenti aspetti:

- informazione tecniche quali:
  - informazioni riguardanti l'Hardware di ogni apparato. L'Aggiudicatario dovrà riportare, per ogni tipologia di apparato, il codice prodotto e la descrizione di ogni elemento costituente;
  - informazioni riguardanti il Software di ogni apparato. L'Aggiudicatario dovrà riportare, per ogni tipologia di apparato, la release software configurata e l'elenco di tutte le patch correttive installate;
  - configurazioni previste;
  - regole di nomenclatura individuate per i vari elementi. L'Aggiudicatario dovrà proporre delle regole di nomenclatura, che dovranno in ogni caso essere conformi a quanto già eventualmente realizzato dall'Amministrazione Contraente e con quest'ultima condivise
  - schemi logici dell'architettura
  - schemi di indirizzamento, policy di sicurezza ed ogni altra informazione di configurazione necessaria per l'introduzione dei nuovi apparati, stabiliti in accordo all'Amministrazione Contraente conformemente a quanto già implementato
- indicazione dei prerequisiti necessari all'installazione degli elementi di fornitura e delle necessarie attività in carico all'Amministrazione Contraente
- indicazione delle verifiche funzionali da effettuare, descrivendo i casi di test identificati ed i risultati attesi e delle modalità di effettuazione di tali verifiche
- l'elenco di eventuali deliverable di fornitura
- l'impegno in giorni persona dei singoli profili professionali coinvolti, previsto per l'erogazione di ciascun servizio di fornitura
- i CV delle risorse professionali da impiegare con le relative certificazioni

- le prestazioni che si intende subappaltare, nel rispetto delle previsioni dell'Accordo Quadro e di quanto indicato nel Piano dei fabbisogni;
- il modello organizzativo impiegato per l'esecuzione delle attività ed in particolare le persone di riferimento che saranno coinvolte nel processo, che comprendono almeno il "*Responsabile del Fornitore" e il "Responsabile dell'Amministrazione";*
- le informazioni relative alla categorizzazione degli interventi e utili all'Amministrazione ai fini del calcolo degli indicatori di digitalizzazione, così come indicati dall'Amministrazione stessa in fase di Ordinativo;
- il ricorso alle risorse previste dal Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021 e dal Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, nonché' dal PNC, così come indicato dall'Amministrazione stessa nel Piano dei Fabbisogni e/o nell'Ordinativo di Fornitura.

Solo nel caso in cui l'Amministrazione non abbia fatto ricorso al "Piano dei Fabbisogni" inviando direttamente l'OdF a Sistema, questa potrà richiedere eventuali modifiche al Piano di lavoro generale entro 10 giorni lavorativi dalla sua ricezione, altrimenti il Piano si intende approvato. Le modifiche richieste dall'Amministrazione dovranno essere recepite dal Fornitore entro il termine di 5 giorni lavorativi, pena l'applicazione delle penali.

Nel corso dell'esecuzione del Contratto Esecutivo, l'Amministrazione potrà richiedere aggiornamenti del "*Piano dei fabbisogni*" e del relativo "*Piano di Lavoro Generale*" e dei suoi allegati *("Piano Operativo"*) ogni qualvolta lo ritenga necessario, nel rispetto delle previsioni di cui all'art. 106 co.1 lett. b) e c) e nei limiti previsti dall' art. 106 co. 7 del D.Lgs. 50/2016, nonché nel rispetto dei massimali dell'Accordo Quadro.
Il Fornitore sarà tenuto ad effettuare le forniture e i servizi connessi in conformità ai processi, alle procedure e alle responsabilità attribuite secondo le direttive dell'Amministrazione, che saranno definite e condivise nella fase di avvio di della fornitura e, sulla base delle peculiarità dell'oggetto dell'ordinativo, eventualmente aggiornate durante il corso del contratto esecutivo in funzione di potenziali cambiamenti.

Si precisa che l'invio del "*Piano dei Fabbisogni*" non garantisce all'Amministrazione l'emissione dell'OdF in quanto potrebbe verificarsi che, nelle more del completamento dell'iter procedurale in precedenza descritto, il massimale previsto dall'AQ si sia esaurito. Il Fornitore è pertanto tenuto ad effettuare un costante monitoraggio della disponibilità economica residua dell'AQ, dandone evidenza alle Amministrazioni nelle varie fasi di attivazione in modo da consentire alle stesse un'attenta pianificazione delle attività di richiesta/approvazione della documentazione eventualmente propedeutica all'emissione dell'OdF.

In tutti i casi in cui l'Amministrazione procederà all'emissione di un Ordinativo di Fornitura (direttamente o in seguito alla fase preliminare sopra descritta) ad esso dovrà essere allegato il DUVRI o, in caso non sia necessario in base a quanto previsto nell'art. 26 del D.Lgs. 81/2008, il documento attestante la valutazione preliminare dell'assenza dei rischi da interferenza.

Si ribadisce che è onere dell'Aggiudicatario verificare che l'Ordinativo di fornitura emesso nei propri confronti dall'Amministrazione Contraente sia stato da quest'ultima correttamente emesso nel rispetto dei vincoli su

riportati, non dando seguito agli OdF erroneamente emessi, previa immediata comunicazione per iscritto all'Amministrazione Contraente che dia evidenza dell'errore in cui quest'ultima è incorsa.

In seguito all'emissione dell'OdF e/o all'approvazione del *"Piano di lavoro generale"*, l'Aggiudicatario dovrà provvedere, con mezzi, materiali e personale specializzato, a:

- consegnare direttamente presso le sedi interessate tutti i materiali costituenti la fornitura
- installare integralmente gli apparati oggetto di fornitura secondo quanto previsto nel "*Piano Operativo*"
- garantire tutte le attività di configurazione previste
- procedere alla verifica funzionale di tutti gli apparati e funzionalità oggetto di fornitura
- minimizzare gli eventuali disservizi, che impattino sulla continuità e funzionalità di eventuali sistemi preesistenti, nel periodo di installazione delle nuove componenti, prevedendo se possibile anche l'installazione di elementi provvisori a supporto delle attività;
- garantire che, qualora un'operazione di attivazione dei prodotti dovesse costituire causa di disservizio, dovrà essere possibile un ripristino immediato della condizione preesistente;
- garantire che qualora gli interventi comportino una completa interruzione dell'attività lavorativa, gli stessi siano effettuati in orario non coincidente con il periodo di operatività dell'Amministrazione e comunque concordati preventivamente con l'Amministrazione;
- svolgere tutte le precedenti attività nel rispetto della vigente normativa in materia di sicurezza (D.Lgs. n. 81/2008 e s.m.i.) a tutela sia dei propri dipendenti, sia del personale dell'Amministrazione Contraente e di chiunque altro si trovi nei locali dell'Amministrazione stessa
- garantire che gli interventi vengano effettuati nel rispetto delle normative vigenti
- attivare il personale ai fini dell'erogazione degli eventuali servizi connessi richiesti.

A conclusione della fornitura l'Aggiudicatario dovrà rilasciare un documento, denominato *"Verbale di Fornitura"*, comprovante l'avvenuta esecuzione di tutte le attività inerenti la fornitura, l'installazione e la verifica funzionale (cfr. par. 3.2.2). Tale documento dovrà riportare la data di completamento della fornitura e tutte le informazioni di dettaglio qualificanti l'oggetto della fornitura stessa (ad esempio, a titolo esemplificativo e non esaustivo: l'elenco di prodotti e servizi forniti, il luogo di fornitura, il codice di riferimento dell'Ordinativo di fornitura, ecc.) e l'elenco dei test ed i relativi risultati, effettuati al fine di verificare che quanto fornito dall'Aggiudicatario sia conforme ai requisiti indicati nel presente Capitolato Tecnico. Si precisa che i "*Verbali di Fornitura*" potranno essere anche più di uno, in considerazione del fatto che, come in precedenza indicato, l'Amministrazione potrà richiedere la possibilità di effettuare rilasci successivi in caso di forniture di particolare complessità, o in base a manifestate esigenze.

3 DESCRIZIONE DELLA FORNITURA

Nel presente capitolo si riportano le specifiche di dettaglio dei prodotti e le modalità di erogazione dei servizi oggetto dei lotti 1-3 della presente iniziativa.

Al Concorrente è richiesta un'offerta su tutte le tipologie di prodotti e servizi elencati nel presente capitolato. Si ribadisce che, come evidenziato nel precedente paragrafo 1.2, i costi relativi ai servizi di installazione e configurazione **si intendono inclusi nei corrispettivi offerti per i prodotti**.

3.1 Prodotti

Il Concorrente dovrà, per ogni "*brand*" richiesto, indicare in offerta la marca, il modello e il codice identificativo univoco di ogni prodotto.

Qualora il Concorrente intenda offrire prodotti che possiedano caratteristiche migliorative, dovrà prevedere e includere nella fornitura tutto quanto necessario alla corretta installazione, configurazione e/o utilizzo delle caratteristiche migliorative stesse, a meno di specifiche indicazioni riportate nel presente documento.

Il prezzo offerto per i prodotti **dovrà includere** le relative attività di installazione e configurazione e, inoltre, gli **aggiornamenti di firmare/software per la durata di due anni**, **decorrenti dalla data di accettazione dei prodotti**. Dovranno quindi essere incluse tutte le eventuali nuove minor release e le licenze/subscription che garantiscano il corretto funzionamento del prodotto per due anni dalla "*Data di accettazione*" della fornitura, di cui al successivo paragrafo 3.2.2. L'Aggiudicatario si impegna a monitorare costantemente il rilascio di aggiornamenti (o correzioni di eventuali bug) del software/firmware e a provvedere al deployment del nuovo software/firmware sui sistemi interessati.

Tutti i prodotti costituiti da un apparato HW devono essere forniti con gli alimentatori/Power Supply Unit necessari alla loro corretta alimentazione e con il necessario corredo di cavi e relativi accessori per permettere una corretta posa in opera ed installazione.

Tutti i prodotti offerti devono essere, **a pena di esclusione**, necessariamente già commercializzati o commercializzabili alla data di presentazione delle offerte, possedendo tutte le caratteristiche minime e migliorative eventualmente offerte. La commerciabilità dei prodotti hardware deve risultare dalla dichiarazione di conformità UE che attesti la conformità alle direttive UE necessarie per l'apposizione della marcatura CE.
La commerciabilità dei prodotti software deve risultare dalla dichiarazione resa dal produttore in fase di verifica tecnica (vedi par. 21 bis del Capitolato d'Oneri) che attesti fra l'altro che il Fornitore ha pieno titolo a commercializzare i suddetti prodotti.

Inoltre tutti i prodotti offerti:

- non dovranno prevedere servizi e funzionalità, che non siano esplicitamente documentati dal Produttore, in grado di comunicare verso reti esterne e/o interne;
- dovranno prevedere la possibilità di disabilitare, da parte dell'Amministratore di sistema, qualsiasi servizio o funzionalità, documentato dal Produttore, in grado di comunicare verso reti esterne e/o interne anche per funzioni gestionali e/o di aggiornamento/manutenzione.

Tali requisiti dovranno attestati mediante la dichiarazione resa dal produttore in fase di verifica tecnica (vedi par. 21 bis del Capitolato d'Oneri). In ogni caso Consip si riserva di richiedere, come ulteriore documentazione a comprova dei requisiti sopra indicati, la presentazione da parte del Fornitore, di un Security Assessment (inclusivo di Penetration Test), eseguito sull'ultimo aggiornamento disponibile del software/firmware dei dispositivi, eventualmente elaborato da una terza parte qualificata ed operante, preferibilmente, nell'Unione Europea, in cui si attesti il soddisfacimento dei requisiti tecnici di sicurezza elencati.

3.1.1 Requisiti di conformità

Consip, in qualità di centrale di Committenza, ha redatto il presente documento con lo scopo di perseguire le indicazioni applicabili all'oggetto dell'appalto e al suo ruolo di Centrale di Committenza, contenute nelle "Linee Guida relative alla Sicurezza nel Procurement ICT".

Analogamente il Fornitore si impegna a rispettare le indicazioni contenute nelle predette Linee Guida, limitatamente a quelle al medesimo applicabili in relazione all'oggetto dell'appalto in fase di esecuzione:

- Tabella 10 delle Linee Guida di Sicurezza nel Procurement ICT "Requisiti Specifici per forniture di oggetti connessi in rete";
- Tabella 8 delle Linee Guida di Sicurezza nel Procurement ICT "Requisiti Generali" n. R1, R6, R11, R12 R13, R15, R16, R17, R18, R19;
- Tabella 9 delle Linee Guida di Sicurezza nel Procurement ICT " Requisiti specifici per forniture di servizi di sviluppo applicativo" (laddove applicabili nel caso di servizi di supporto specialistico o di hardening su client).

Tutte le apparecchiature fornite dovranno essere conformi alla normativa vigente che regolamenta la loro produzione, commercializzazione ed utilizzazione. Inoltre dovranno rispettare, ciascuna per le singole specifiche caratteristiche, le seguenti prescrizioni:

- Decreto Legislativo del 19 maggio 2016 n. 86 e ss.m.i., "attuazione della direttiva 2014/35/UE concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato del materiale elettrico destinato ad essere adoperato entro taluni limiti di tensione";
- D. Lgs. 4 marzo 2014, n. 27 e s.m.i., "attuazione della direttiva 2011/65/UE sulla restrizione dell'uso di determinate sostanze pericolose nelle apparecchiature elettriche ed elettroniche";
- D. Lgs. 18 maggio 2016, n. 80 e s.m.i., "modifiche al decreto legislativo 6 novembre 2007, n. 194, di attuazione della direttiva 2014/30/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014,

concernente l'armonizzazione delle legislazioni degli Stati membri relative alla compatibilità elettromagnetica";

- D. Lgs, n. 49/2014 così come modificato da ultimo dal D.Lgs. n. 11 del 3 settembre 2020 e s.m.i., "Attuazione degli articoli 2 e 3 della direttiva (UE) 2018/849 relativa a pile e accumulatori e ai rifiuti di pile e accumulatori e sui rifiuti di apparecchiature elettriche ed elettroniche.

Inoltre, tutti i prodotti hardware forniti dovranno essere:

1. nuovi di fabbrica e non ricondizionati, per cui il numero di matricola, corrispondente ai dispositivi forniti, non dovrà mai essere stato precedentemente oggetto di fatturazione verso un cliente;
2. provvisti di regolare marcatura "CE".

3.1.2 Requisiti del multibrand

Per tutti gli ambiti di prodotto è richiesta l'offerta **obbligatoria** del numero fissato di tecnologie ("*brand*") su tutte le fasce dimensionali/prestazionali previste (**offerta completa**) riportato in tabella:

Multi brand
Requisiti minimi
NGFW - Offerta di 4 brand completi su tutte le fasce richieste
NAC - Offerta di 2 brand completi su tutte le fasce richieste
EPP/EDR - Offerta di 4 brand completi su tutte le fasce richieste
SP- Offerta di 2 brand completi su tutte le fasce richieste
Anti-APT - Offerta di 2 brand completi su tutte le fasce richieste

Tabella 1 - Requisiti minimi multi brand

3.1.3 Requisiti dei Next Generation Firewall (NGFW)

Nel presente paragrafo sono descritti i **requisiti minimi** e migliorativi relativi ai **NGFW**.
I NGFW sono apparati che consentono l'ispezione dei pacchetti di rete e si differenziano dai firewall "tradizionali" in quanto non si occupano solamente di analizzare e filtrare i pacchetti dati sulla base della porta e/o protocollo ma consentono di eseguire l'ispezione a livello applicativo, fornendo inoltre funzionalità di prevenzione dalle intrusioni, analisi e rilevamento dei malware e capacità di utilizzo di sorgenti esterne a supporto della propria attività di protezione.

Per i NGFW sono richieste sei fasce dimensionali.
Nelle tabelle seguenti si riportano i requisiti minimi e migliorativi di tipo dimensionale **per ogni fascia richiesta**.

NGFW - Fascia 1
Requisiti dimensionali minimi
Throughput NGFW [Mbps]: almeno 250
Numero di sessioni TCP contemporanee: almeno 48.000
Numero di nuove sessioni TCP/secondo: almeno 3.000
Porte 1000Base-T: almeno 6

Tabella 2 - Requisiti dimensionali minimi NGFW_1

NGFW - Fascia 1	
Requisiti dimensionali migliorativi	
ID	Caratteristica
1.1	Throughput NGFW [Mbps]: valore compreso tra 250 e 325
1.2	Porte 1000Base-T: almeno 8

Tabella 3 - Requisiti dimensionali migliorativi NGFW_1

NGFW - Fascia 2
Requisiti dimensionali minimi
Throughput NGFW [Gbps]: almeno 2
Numero di sessioni TCP contemporanee: almeno 300.000
Numero di nuove sessioni TCP/secondo: almeno 16.000
Porte 1000Base-T: almeno 8
Porte 1 GE SFP: almeno 4

Tabella 4 - Requisiti dimensionali minimi NGFW_2

NGFW - Fascia 2	
Requisiti dimensionali migliorativi	
ID	Caratteristica
2.1	Throughput NGFW [Gbps]: valore compreso tra 2 e 2,6
2.2	Porte 1000Base-T: almeno 10
2.3	Porte 1 GE SFP: almeno 6

Tabella 5 - Requisiti dimensionali migliorativi NGFW_2

NGFW - Fascia 3
Requisiti dimensionali minimi
Throughput NGFW [Gbps]: almeno 4
Numero di sessioni TCP contemporanee: almeno 1.500.000
Numero di nuove sessioni TCP/secondo: almeno 20.000
Porte 1000Base-T: almeno 8

Porte 10 GE SFP+: almeno 2

Tabella 6 - Requisiti dimensionali minimi NGFW_3

NGFW - Fascia 3	
Requisiti dimensionali migliorativi	
ID	Caratteristica
3.1	Throughput NGFW [Gbps]: valore compreso tra 4 e 5,2
3.2	Porte 1000Base-T: almeno 10
3.3	Porte 10 GE SFP+: almeno 4

Tabella 7 - Requisiti dimensionali migliorativi NGFW_3

NGFW - Fascia 4
Requisiti dimensionali minimi
Throughput NGFW [Gbps]: almeno 7
Numero di sessioni TCP contemporanee: almeno 2.200.000
Numero di nuove sessioni TCP/secondo: almeno 43.000
Porte 1000Base-T o 1 GE SFP: almeno 10
Porte 10 GE SFP+: almeno 4

Tabella 8 - Requisiti dimensionali minimi NGFW_4

NGFW - Fascia 4	
Requisiti dimensionali migliorativi	
ID	Caratteristica
4.1	Throughput NGFW [Gbps]: valore compreso tra 7 e 9,1
4.2	Porte 1000Base-T o 1 GE SFP: almeno 12
4.3	Porte 10 GE SFP+: almeno 6

Tabella 9 - Requisiti dimensionali migliorativi NGFW_4

NGFW - Fascia 5
Requisiti dimensionali minimi
Throughput NGFW [Gbps]: almeno 15
Numero di sessioni TCP contemporanee: almeno 6.000.000
Numero di nuove sessioni TCP/secondo: almeno 150.000
Porte 1000Base-T o 1 GE SFP: almeno 10
Porte 10 GE SFP+: almeno 6

Tabella 10 - Requisiti dimensionali minimi NGFW_5

NGFW - Fascia 5

Requisiti dimensionali migliorativi	
ID	Caratteristica
5.1	Throughput NGFW [Gbps]: valore compreso tra 15 e 19,5
5.2	Porte 1000Base-T o 1 GE SFP: almeno 12
5.3	Porte 10 GE SFP+: almeno 8

Tabella 11 - Requisiti dimensionali migliorativi NGFW_5

NGFW - Fascia 6
Requisiti dimensionali minimi
Throughput NGFW [Gbps]: almeno 30
Numero di sessioni TCP contemporanee: almeno 18.500.000
Numero di nuove sessioni TCP/secondo: almeno 200.000
Porte 10 GE SFP+: almeno 8
Porte 40 GE QSFP+: almeno 2

Tabella 12 - Requisiti dimensionali minimi NGFW_6

NGFW - Fascia 6	
Requisiti dimensionali migliorativi	
ID	Caratteristica
6.1	Throughput NGFW [Gbps]: valore compreso tra 30 e 39
6.2	Porte 100 GE QSFP28: almeno 2

Tabella 13 - Requisiti dimensionali migliorativi NGFW_6

Si precisa che:

- l'acquisto di eventuali transceiver da alloggiare nelle porte dei NGFW è a cura dell'Amministrazione;
- per *Throughput NGFW* si intende il troughput ottenuto con le funzionalità di ispezione *stateful* (*stateful inspection*), riconoscimento applicativo (*application awareness*) e prevenzione delle intrusioni (*intrusion prevention - IPS*) **contemporaneamente attive**.
- i valori di NGFW *Throughput* dovranno essere misurati prendendo a riferimento un profilo di traffico iMIX (Internet Mix);
- il numero di sessioni TCP contemporanee è misurato nelle condizioni in cui non vi siano dati che transitano attraverso le sessioni, mentre il numero di sessioni TCP al secondo è misurato nelle condizioni in cui un byte di dati transiti attraverso le sessioni.

Nelle tabelle seguenti si riportano i requisiti minimi e migliorativi di tipo funzionale **comuni a tutte le fasce richieste**.

NGFW - Tutte le fasce
Requisiti funzionali minimi
Funzionalità di Firewalling

Funzionalità di Intrusion Prevention System
Funzionalità di Application Control
Funzionalità Antimalware di tipo Signature Based
Supporto VPN IPSEC
Funzionalità di URL Filtering
Funzionalità di Antimalware Avanzate: detection, blocco e tracciamento di IP, URL, domini, file malevoli con il supporto di feed di threat intelligence del Produttore
Funzionalità di sandboxing su infrastruttura remota del Produttore, ubicata almeno in UE
Supporto del protocollo IPV6
Supporto per configurazione in alta affidabilità

Tabella 14 - Requisiti funzionali minimi per tutte le fasce di NGFW

NGFW - Tutte le fasce	
Requisiti funzionali migliorativi	
ID	Caratteristica
7.1	Supporto VPN TLS
7.2	Funzionalità di SSL/TLS Inspection - a livello software oppure - a livello hardware su chipset dedicato
7.3	Integrazione con almeno una piattaforma di threat intelligence (MISP e/o Minemeld e/o Cabby e/o CNTI)
7.4	Supporto dei protocolli standard STIX/TAXII
7.5	Funzionalità di traffic shaping (gestione della QoS)
7.6	Presenza di almeno 10 contesti virtuali
7.7	Piattaforma SW di Management in grado di gestire fino a 10 NGFW per: configurazione degli apparati, monitoraggio del corretto funzionamento, configurazione degli aggiornamenti sw, gestione delle policy di sicurezza, gestione degli eventi associati alle policy di sicurezza, analisi di file e malware

Tabella 15 - Requisiti funzionali migliorativi per tutte le fasce di NGFW

Si precisa che, per tutte le fasce, è richiesta l'offerta di un apparato fisico (*HW corredato dal relativo SW necessario*). Non sono quindi ammesse offerte che contemplino soluzioni puramente software.

3.1.4 Requisiti dei Network Access Control (NAC)

Nel presente paragrafo sono descritti i **requisiti minimi** e migliorativi relativi ai **NAC**.

Il NAC consente l'implementazione di regole per il controllo degli accessi all'infrastruttura aziendale da parte degli utenti, siano essi "umani" (attraverso personal computer, apparati mobili, …) oppure "cose"

(elementi in ambito *IoT*). Le regole possono basarsi su più modalità quali l'autenticazione degli utenti, la configurazione degli apparati che accedono alla rete, il ruolo degli utenti. Per mezzo del NAC è inoltre possibile applicare regole successive alla connessione degli utenti, in base ad eventi che possono provenire da altri elementi di sicurezza.

Per i NAC sono richieste sei fasce dimensionali/prestazionali:

- NAC_1 (fascia 1): **fino a 100 Endpoint concorrenti**
- NAC_2 (fascia 2): **fino a 500 Endpoint concorrenti**
- NAC_3 (fascia 3): **fino a 1.000 Endpoint concorrenti**
- NAC_4 (fascia 4): **fino a 10.000 Endpoint concorrenti**
- NAC_5 (fascia 5): **fino a 25.000 Endpoint concorrenti**
- NAC_6 (fascia 6): **fino a 50.000 Endpoint concorrenti**.

Nelle tabelle seguenti si riportano i requisiti minimi e migliorativi **comuni a tutte le fasce richieste**.

NAC - Tutte le fasce
Requisiti minimi
Discovery degli endpoint connessi alle reti wired, wireless, tramite VPN
Controllo degli accessi in base alle policy di sicurezza
Gestione accessi Guest
Profilatura degli endpoint di rete indipendentemente dalla modalità di accesso alla rete
Supporto standard 802.1x, MAC Authentication, Web Authentication
Integrazione con sistemi di Identity Management esterni: Radius/LDAP/Active Directory
Assegnazione dinamica della VLAN in base a parametri di autenticazione o profilatura
Isolamento di endpoint di rete non autorizzati
Gestione delle regole e policy da una dashboard centralizzata
Funzionalità di BYOD (Bring Your Own Device) almeno per endpoint Android e iOS
Funzionalità di check compliance con agent su endpoint Windows, Mac OS (almeno versioni Windows e Mac OS commercializzate alla data di presentazione dell'offerta) e Linux (almeno una fra le distribuzioni più diffuse tra CentOS, Debian, Fedora, Linux Mint, Ubuntu), con possibilità di verifica della presenza di software installati e/o file sul sistema operativo e/o software antivirus
Visibilità dispositivi IoT
Funzionalità di reportistica che consentano: - il monitor in real-time attraverso dashboard - la realizzazione di report attraverso template predefiniti - la possibilità di esportare i report
Supporto del protocollo IPv6
Supporto per configurazione in alta affidabilità

Tabella 16 - Requisiti funzionali minimi per tutte le fasce di NAC

NAC - Tutte le fasce	
Requisiti migliorativi	
ID	Caratteristica
8.1	Supporto dei seguenti metodi di autenticazione MS-CHAPv2, EAP-TLS
8.2	Funzionalità Radius Server
8.3	Profilatura degli endpoint basata su tecniche agent-less: Mac-OUI e/o Dhcp fingerprinting e/o snmp e/o http user-agent e/o nmap
8.4	Funzionalità di remediation ai fini dell'ottenimento della compliance degli endpoint alle policy di sicurezza -manuale oppure -automatica
8.5	Integrazione con la soluzione di NGFW: -Integrazione con 1 brand di NGFW (tutte le fasce) oppure -Integrazione con 2 brand di NGFW (tutte le fasce) L'integrazione deve consentire lo scambio di informazioni tra NAC e NGFW sia per l'implementazione dinamica di policy di sicurezza sia per consentire di segnalare endpoint/utenti da isolare.
8.6	Integrazione/integrabilità dei brand offerti con ulteriori soluzioni di sicurezza (ulteriori brand di NGFW, soluzioni MDM, soluzioni SIEM, soluzioni di Single-Sign-On, soluzioni antivirus,etc). Sarà premiata: - la varietà, per i differenti brand offerti, di soluzioni di sicurezza con le quali risultano già realizzate le integrazioni e la relativa numerosità per specifico ambito tecnologico - la disponibilità e fruibilità, per i differenti brand offerti, di Software Development Kit e API per future integrazioni

Tabella 17 - Requisiti funzionali migliorativi per tutte le fasce di NAC

Il requisito migliorativo 8.6, come si evince chiaramente dalla sua declinazione, si intende anche riferito ai differenti brand offerti richiesti dal requisito multibrand. La valutazione discrezionale della Commissione pertanto terrà conto di quanto offerto dal Concorrente relativamente ai differenti brand richiesti.
Si precisa che, per tutte le fasce, è richiesta l'offerta di un apparato fisico (*HW*). Non sono quindi ammesse offerte che contemplino soluzioni puramente software (*virtual appliance*).

3.1.5 Requisiti dell'Endpoint Protection Platform (EPP)/Endpoint Detection & Response (EDR)

Nel presente paragrafo sono descritti i **requisiti minimi** e migliorativi relativi all'**EPP/EDR**.

Una soluzione EPP/EDR consente di proteggere gli endpoint di tipo client da minacce quali virus, trojan, worm, etc, bloccando le attività di applicazioni che risultano potenzialmente dannose, fornendo inoltre funzionalità utili all'investigazione e al ripristino in seguito a violazioni di sicurezza.

Per l'EPP/EDR sono richieste quattro fasce dimensionali:

- EPP_EDR_1 (fascia 1): **fino a 500 client**
- EPP_EDR_2 (fascia 2): **fino a 1000 client**
- EPP_EDR_3 (fascia 3): **fino a 5000 client**
- EPP_EDR_4 (fascia 4): **oltre 5000 client**

Si precisa che la soluzione offerta potrà essere composta da:

i. un unico agent che soddisfi tutti i requisiti minimi richiesti e i migliorativi eventualmente offerti
ii. due agent integrati che complessivamente soddisfino tutti i requisiti minimi richiesti e i migliorativi eventualmente offerti.

Nel caso di soluzione composta da due agent (punto ii) uno degli agent dovrà obbligatoriamente soddisfare i requisiti minimi richiesti e i migliorativi eventualmente offerti identificati nelle successive tabelle come di tipo "EPP" e, ai fini del multibrand (vedi paragrafo 3.1.2), affinché due brand siano considerati differenti, è sufficiente che siano differenti gli agent che soddisfano i requisiti minimi richiesti e i migliorativi eventualmente offerti di tipo "EPP".

Pertanto, a mero titolo esemplificativo e non esaustivo, ai fini del multibrand:

- un'offerta in cui un Concorrente presenti:
  - Per un brand: Agent A (Brand X) e Agent B (Brand Y)
  - Per un altro brand: Agent C (Brand Z) e Agent B (Brand Y)

  dove:
  - Agent A del Brand X soddisfa tutti i requisiti minimi di tipo EPP e gli eventuali requisiti migliorativi di tipo EPP offerti
  - Agent C del Brand Z soddisfa tutti i requisiti minimi di tipo EPP e gli eventuali requisiti migliorativi di tipo EPP offerti
  - Agent B del Brand Y soddisfa tutti i requisiti minimi di tipo EDR e gli eventuali requisiti migliorativi di tipo EDR offerti;

<u>darà luogo al conteggio di due differenti brand;</u>

- un'offerta in cui un Concorrente presenti:
  - Per un brand: Agent A (Brand X) e Agent B (Brand Y)
  - Per un altro brand: Agent C (Brand Z) e Agent D (Brand W)

  dove:
  - Agent A del Brand X soddisfa tutti i requisiti minimi di tipo EPP e gli eventuali requisiti migliorativi di tipo EPP offerti;
  - Agent B del Brand Y soddisfa tutti i requisiti minimi di tipo EDR e gli eventuali requisiti migliorativi di tipo EDR offerti;
  - Agent C del Brand Z soddisfa tutti i requisiti minimi di tipo EPP e gli eventuali requisiti migliorativi di tipo EPP offerti;
  - Agent D del Brand W soddisfa tutti i requisiti minimi di tipo EDR e gli eventuali requisiti migliorativi di tipo EDR offerti;

<u>darà luogo al conteggio di due differenti brand.</u>

- un'offerta in cui un Concorrente presenti:
  - Per un brand: Agent A (Brand X) e Agent B (Brand Y)
  - Per un altro brand: Agent C (Brand Z) e Agent D (Brand Z)

  dove:

- Agent A del Brand X soddisfa tutti i requisiti minimi di tipo EPP e gli eventuali requisiti migliorativi di tipo EPP offerti
- Agent B del Brand Y soddisfa tutti i requisiti minimi di tipo EDR e gli eventuali requisiti migliorativi di tipo EDR offerti;
- Agent C del Brand Z soddisfa tutti i requisiti minimi di tipo EPP e gli eventuali requisiti migliorativi di tipo EPP offerti;
- Agent D del Brand Z soddisfa tutti i requisiti minimi di tipo EDR e gli eventuali requisiti migliorativi di tipo EDR offerti;

darà luogo al conteggio di due differenti brand.

L'offerta di una soluzione che preveda un unico agent (punto i) sarà premiata secondo quanto nel seguito previsto.
Nelle tabelle seguenti si riportano i requisiti minimi e migliorativi **comuni a tutte le fasce richieste**.

EPP/EDR - Tutte le fasce
Requisiti minimi - EPP
Supporto degli endpoint con S.O. Windows (almeno Windows 8 e Windows 10)
Funzionalità Antimalware signature based
Aggiornamento delle signature in maniera automatica
Possibilità di effettuare: - il blocco di azioni dannose - la gestione della quarantena dei file - la pulizia dell'endpoint in seguito al rilevamento di malware
Protezione del traffico in entrata e in uscita dagli endpoint, comprensivo di controllo delle applicazioni, delle porte e dei protocolli utilizzati al fine di prevenire attacchi e intrusioni contro gli endpoint
Protezione dell'endpoint dai malware attraverso il monitoraggio degli eventi che accadono sull'endpoint e l'analisi comportamentale, controllando le principali modifiche (controllo/interruzione di programmi, modifica chiavi di registro, installazione impropria di device o driver, accesso anomalo alla memoria) apportate sull'endpoint. In caso di tentativo di modifica, è richiesto il blocco della modifica e l'avviso all'utente.
Protezione dai ransomware
Protezione anti-exploit
Possibilità di impostare regole per limitare o bloccare l'accesso a supporti removibili collegati all'endpoint.
Disponibilità di strumenti che consentano, durante la navigazione, di verificare se un sito web è considerato sicuro o meno con impostazione di eventuali policy di sicurezza associate (ad esempio blocco di siti considerati non sicuri).
Possibilità di definire policy di sicurezza attraverso le quali sia consentita l'esecuzione dei soli programmi autorizzati.

Possibilità di effettuare delle scansioni in modalità: - real time - manuale - programmata
La soluzione deve avere funzionalità di reportistica e logging che consentano: - il monitor in real-time attraverso dashboard - la realizzazione di report attraverso template predefiniti - la possibilità di esportare i report
Supporto del protocollo IPv6
Requisiti minimi - EDR
Supporto degli endpoint con S.O. Windows (almeno Windows 8 e Windows 10)
Possibilità di effettuare la Root Cause Analysis
Possibilità di effettuare detection di malware attraverso sorgenti IoC
Disponibilità di strumenti di investigazione sulla base di records storici per analizzare la timeline di un attacco e sulla base di system snapshot per analizzare lo stato attuale dell'endpoint
Possibilità di registrare dati di telemetria degli endpoint (almeno connessioni di rete, esecuzione di file, modifiche di file, modifiche di registro)
La soluzione deve avere funzionalità di reportistica e logging che consentano: - il monitor in real-time attraverso dashboard - la realizzazione di report attraverso template predefiniti - la possibilità di esportare i report

Tabella 18 - Requisiti funzionali minimi per tutte le fasce di EPP/EDR

EPP/EDR - Tutte le fasce	
ID	Caratteristica
Requisiti migliorativi comuni tra EPP e EDR	
9.1	Unico agent per le funzionalità di EPP e di EDR
9.2	Integrazione con la soluzione di anti-APT: -Integrazione con 1 brand di anti-APT (tutte le fasce) oppure -Integrazione con 2 brand di anti-APT (tutte le fasce)
9.3	Supporto degli endpoint con ulteriori S.O. Sarà premiata la numerosità dei sistemi operativi supportati (MacOS X, Linux, etc.) e la completezza della funzionalità EPP ed EDR supportate dagli ulteriori S.O ed offerte per ciascuno dei 4 brand richiesti , anche con particolare riguardo al supporto di sistemi operativi legacy.
9.4	Integrazione con soluzioni di NGFW: - Integrazione con 1 brand di NGFW (tutte le fasce) oppure - Integrazione con 2 brand di NGFW (tutte le fasce)
Requisiti migliorativi - EPP	
9.5	Monitoraggio delle connessioni a server di Command & Control
9.6	Funzionalità di sandboxing su infrastruttura remota del Produttore, ubicata almeno in UE

9.7	Funzionalità di Data Loss Prevention
9.8	Qualità e Innovatività, nei brand offerti, delle tecniche di protezione da malware non identificato e attacchi zero day mediante motori di machine learning, al fine di rilevare un'ampia varietà di malware e attacchi, su un'ampia varietà di file, script, processi, riducendo allo stesso tempo i falsi positivi
Requisiti migliorativi - EDR	
9.9	Possibilità di effettuare detection di malware attraverso ulteriori sorgenti (YARA Rule, feed di terze parti)
9.10	Possibilità di mappare gli alert di sicurezza con il framework MITRE ATT&CK
9.11	Funzionalità avanzate di Contenimento e Bonifica, nei brand offerti (roll back, terminazione processi, disinstallazione/cancellazione applicazioni/file, installazione applicazioni, esecuzione script, dump di memoria, etc.) Sarà valutata la numerosità e varietà delle funzionalità di contenimento e bonifica messe a disposizione dalle soluzioni dei brand offerti.

Tabella 19 - Requisiti funzionali migliorativi per tutte le fasce di EPP/EDR

Si precisa che, nel caso sia offerta una soluzione composta da due agent (precedente punto ii), dovrà essere garantito per entrambi gli agent:

- il supporto dei sistemi operativi previsti come minimi;
- le funzionalità di reportistica e logging;

I requisiti migliorativi sull'integrazione con le soluzioni di anti-APT e NGFW (req. n. 9.2 e 9.4) offerte dovranno essere soddisfatti da entrambi gli agent per i medesimi brand.

Si precisa inoltre che i requisiti migliorativi 9.3, 9.8 e 9.11, come si evince chiaramente dalla loro declinazione, si intendono anche riferiti ai differenti brand offerti richiesti dal requisito multibrand. La valutazione discrezionale della Commissione pertanto terrà conto di quanto offerto dal Concorrente relativamente ai differenti brand richiesti.

3.1.6 Requisiti della Server Protection Platform (SPP)

Nel presente paragrafo sono descritti i **requisiti minimi** e migliorativi relativi alla **SPP**.

Una soluzione SPP consente di proteggere gli endpoint di tipo server da minacce quali virus, trojan, worm, malware, bloccando le attività di applicazioni che risultano potenzialmente dannose, fornendo inoltre funzionalità utili all'investigazione e al ripristino in seguito a violazioni di sicurezza.

Per la SPP sono richieste quattro fasce dimensionali:

- SPP_1 (fascia 1): **fino a 50 server**
- SPP_2 (fascia 2): **fino a 100 server**
- SPP_3 (fascia 3): **fino a 500 server**
- SPP_4 (fascia 4): **oltre 500 server**

Si precisa che la soluzione offerta dovrà essere composta da un unico agent che soddisfi tutti i requisiti minimi richiesti e i migliorativi eventualmente offerti, ad eccezione del **requisito migliorativo 10.5 sulle "funzionalità EDR"** che, laddove offerto, potrà essere implementato attraverso un ulteriore agent integrato con il primo.

Nelle tabelle seguenti si riportano i requisiti minimi e migliorativi **comuni a tutte le fasce richieste**.

Server Protection - Tutte le fasce
Requisiti minimi
Supporto dei server con S.O. Windows Server (almeno Windows Server 2016 e 2019)
Supporto dei server con S.O. Linux (il Fornitore dovrà indicare in offerta l'elenco delle distribuzioni supportate)
Supporto sui seguenti ambienti di virtualizzazione (per tutti gli ambienti richiesti, il Fornitore dovrà indicare in offerta l'elenco delle versioni supportate): - VMWare - Citrix Hypervisor - Microsof Hyper-V
Funzionalità Antimalware signature based
Possibilità di effettuare delle scansioni in modalità: - real time - manuale - programmata
Aggiornamento delle signature in maniera automatica
Protezione da attacchi botnet e di tipo Denial of Service
Funzionalità di Firewall Stateful
Funzionalità Antimalware tramite sistemi di analisi comportamentale
Attivazione delle protezioni firewall e prevenzione delle intrusioni già in fase di avvio dei server
Possibilità di autorizzare l'esecuzione di SW sulla base di: - whitelist dinamiche - classificazione del SW attraverso analisi della reputazione del SW in base alla Threat Intellligence del Vendor
Funzionalità di messaggistica tramite pop-up che informino gli utenti per delle ragioni per cui non è concesso l'accesso alle applicazioni non autorizzate
Possibilità di approvare automaticamente l'esecuzione di applicazioni per utenti che godono di specifici privilegi
Funzionalità di monitoraggio dell'integrità dei file di sistema critici e delle chiavi di registro
Funzionalità di protezione dei file di sistema critici e delle chiavi di registro da manomissioni, autorizzando le modifiche solo in accordo alle policy definite
La soluzione deve avere funzionalità di reportistica e logging che consentano: - il monitor in real-time attraverso dashboard - la realizzazione di report attraverso template predefiniti - la possibilità di esportare i report
Supporto del protocollo IPv6

Tabella 20 - Requisiti funzionali minimi per tutte le fasce di SPP

Server Protection - Tutte le fasce	
Requisiti migliorativi	
ID	Caratteristica
10.1	Protezione da attacchi di buffer overflow della memoria che sfruttano le applicazioni inserite in whitelist
10.2	Possibilità di effettuare attività sui client in push per ricercare file malevoli tramite stringhe identificative (hash)
10.3	Monitoraggio delle connessioni a server di Command & Control
10.4	Funzionalità di sandboxing su infrastruttura remota del Produttore, ubicata almeno in UE
10.5	Varietà e numerosità delle funzioni di EDR offerte dalle soluzioni dei brand offerti, al fine di accelerare e semplificare la fase di investigazione e di ripristino in seguito a violazioni di sicurezza .
10.6	Integrazione con la soluzione di anti-APT: -Integrazione con 1 brand di anti-APT (tutte le fasce) oppure -Integrazione con 2 brand di anti-APT (tutte le fasce)
10.7	Integrazione con soluzioni di NGFW: - Integrazione con 1 brand di NGFW (tutte le fasce) oppure - Integrazione con 2 brand di NGFW (tutte le fasce)

Tabella 21 - Requisiti funzionali migliorativi per tutte le fasce di SPP

Si precisa che il requisito migliorativo 10.5, come si evince chiaramente dalla sua declinazione, si intende anche riferito ai differenti brand offerti richiesti dal requisito multibrand. La valutazione discrezionale della Commissione pertanto terrà conto di quanto offerto dal Concorrente relativamente ai differenti brand richiesti.

3.1.7 Requisiti dell'Anti-Advanced Persistent Threat (Anti-APT)

Nel presente paragrafo sono descritti i **requisiti minimi** e migliorativi relativi all'**Anti-APT**.

La soluzione di Anti-APT consente l'analisi di file che possono essere inviati all'elemento da altri dispositivi di sicurezza o direttamente dal personale che si occupa di sicurezza. All'interno dell'ambiente protetto (sandbox) è quindi possibile, attraverso varie tecniche, esaminare i file e i loro comportamenti per determinare se questi siano o meno malevoli, assegnando loro un grado di severità.

Per l'Anti-APT sono richieste due fasce dimensionali/prestazionali:

- Anti_APT_1 (fascia 1): **fino a 450 file/ora**
- Anti_APT_2 (fascia 2): **fino a 1000 file/ora**

Nelle tabelle seguenti si riportano i requisiti minimi e migliorativi **comuni a tutte le fasce richieste**.

Anti-APT - Tutte le fasce
Requisiti minimi
Supporto di ambienti con S.O. Windows (almeno Windows 8, Windows 10), Mac OS e Linux
Rilevazione, mediante analisi comportamentale in ambiente sandbox di malware, minacce zero-day e APT.
Possibilità di verificare file attraverso la corrispondenza delle firme di malware in precedenza già analizzati.
Supporto di almeno le seguenti tipologie di file: .zip, .gz, .bz2, .exe, .dll, .bat, .pdf, .jar, .doc, .docx, .xls, .xlsx, .ppt, .pptx., .iso, .img
Identificazione, mediante analisi del traffico di rete in ambiente sandbox, di minacce quali: comunicazione C&C, botnet e worm
Funzionalità in ambiente sandbox che consentano di rilevare tecniche di elusione utilizzate dai malware quali: cifratura, compressione e offuscamento del codice
Possibilità di creare regole di rilevazione personalizzate attraverso YARA
Ricezione, attraverso almeno un feed di threat intelligence, di informazioni su nuovi malware rilevati
Possibilità di creare macchine virtuali personalizzate per l'analisi dei malware nello specifico contesto dell'Amministrazione
La soluzione deve avere funzionalità di reportistica che consentano: - il monitor in real-time attraverso dashboard - la realizzazione di report attraverso template predefiniti - la possibilità di esportare i report
Supporto del protocollo IPv6
Supporto a configurazione in alta affidabilità

Tabella 22 - Requisiti funzionali minimi per tutte le fasce di Anti-APT

Anti-APT - Tutte le fasce	
Requisiti migliorativi	
ID	Caratteristica
11.1	Funzionalità di analisi dell'intero ciclo di vita di un malware, consentendo e tracciando l'eventuale connessione a reti esterne
11.2	Integrazione con una piattaforma di analisi su infrastruttura remota del Produttore per verificare, in modo rapido, se l'analisi su particolari file o minacce sia già stata effettuata
11.3	Presenza di tecniche di anti evasione che siano in grado di trattare malware progettati per riconoscere l'esecuzione in ambiente di sandboxing (ad esempio rimanendo latenti fino a quando non siano effettuate operazioni che indichino l'effettiva presenza di un utente reale come l'esecuzione di un click del mouse)
11.4	Funzionalità di sniffing del traffico di rete

11.5	Integrazione con la soluzione di NGFW: -Integrazione con 1 brand di NGFW (tutte le fasce) oppure -Integrazione con 2 brand di NGFW (tutte le fasce)

Tabella 23 - Requisiti funzionali migliorativi per tutte le fasce di Anti-APT

Si precisa che, per tutte le fasce, è richiesta l'offerta di un apparato fisico (*HW corredato dal relativo SW necessario*). Non sono quindi ammesse offerte che contemplino soluzioni puramente software.

3.1.8 Garanzia dei prodotti

Tutti i prodotti offerti dovranno prevedere una garanzia di 12 mesi dalla "*Data di accettazione*" della fornitura come definita nel par.3.2.2.
Tale garanzia prevede la sostituzione del prodotto, ovvero la correzione di bachi software, nel caso di vizi del prodotto, di produzione o di conformità, già presenti al momento della consegna o che si manifestino, anche in seguito, durante il periodo di garanzia. In aggiunta a tale garanzia, l'Amministrazione potrà richiedere il servizio di manutenzione secondo quanto previsto nel successivo paragrafo 3.2.3.

3.1.9 Mappatura dei prodotti con le misure minime di sicurezza AGID

Al fine di agevolare le Amministrazioni Contraenti nell'individuazione delle soluzioni tecnologiche più idonee a garantire la sicurezza dei propri sistemi, è riportata di seguito in tabella una mappatura tra le tipologie di prodotti acquistabili e le misure minime di sicurezza AGID (*Circolare 18 aprile 2017, n. 2/2017, Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni»* e successive modifiche e integrazioni) ad esse associabili. Tali misure, pertanto, potrebbero essere implementate, in tutto o in parte, mediante l'adozione di una o più specifiche tipologie merceologiche.

La mappatura rappresenta una linea guida per le Amministrazioni Contraenti, che possa essere loro di supporto nella fase precedente l'emissione dell'Ordinativo di Fornitura e/o che consenta loro di effettuare una verifica ad alto livello circa la rispondenza, alle proprie esigenze di sicurezza, del Piano Operativo proposto dal Fornitore.

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI					
ABSC_ID			Livello	Descrizione	Ambito Merceologico
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	NAC
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	NAC
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati	NAC

				dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	NAC
ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI					
ABSC_ID			Livello	Descrizione	Ambito Merceologico
2	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	EPP/Server Protection
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	Server Protection/EPP
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	EPP/Server Protection
ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER					
ABSC_ID			Livello	Descrizione	Ambito Merceologico
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Servizio di hardening
3	1	2	S	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	Servizio di hardening
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	Server Protection/EPP/EDR
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	Server Protection/EPP/EDR
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE					
ABSC_ID			Livello	Descrizione	Ambito Merceologico
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Servizi di supporto specialistico

5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Servizi di supporto specialistico
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Servizi di supporto specialistico
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Servizi di supporto specialistico
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Servizi di supporto specialistico
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Servizi di supporto specialistico
ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE					
ABSC_ID			Livello	Descrizione	Ambito Merceologico
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	EPP/EDR/SERVER PROTECTION
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	EPP/SERVER PROTECTION
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	EPP/EDR/SERVER PROTECTION
8	2	2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	EPP/EDR/SERVER PROTECTION
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	EPP/EDR/SERVER PROTECTION/Anti-APT/NGFW
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	EPP
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	Servizio di hardening
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	Servizio di hardening
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	NGFW
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	Anti -APT

8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	NGFW/Anti-APT
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	EPP
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Servizio di hardening
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Servizio di hardening
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Servizio di hardening
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	EPP
8	9	2	M	Filtrare il contenuto del traffico web.	NGFW
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	NGFW/EPP/EDR/Server Protection
8	11	1	S	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	EPP/EDR/SERVER PROTECTION
ABSC 13 (CSC 13): PROTEZIONE DEI DATI					
ABSC_ID			Livello	Descrizione	Ambito Merceologico
13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	NGFW
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	EPP
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	EPP/SERVER PROTECTION
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	NGFW
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	NGFW

3.2 Servizi

L'Aggiudicatario dovrà garantire che tutti i servizi prestati siano espletati da personale qualificato, che abbia le idonee competenze in base alle particolari attività richieste e tecnologie utilizzate.

La struttura organizzativa e le modalità impiegate per l'erogazione dei servizi connessi alla fornitura saranno oggetto di valutazione secondo quanto previsto nella seguente tabella.

Struttura organizzativa e modalità impiegate per l'esecuzione dei contratti esecutivi/erogazione dei servizi connessi alla fornitura	
Requisiti migliorativi	
ID	Caratteristica
12.1	Qualità dei Centri di Competenza nel settore della Sicurezza ICT, in termini di: - varietà e specificità delle competenze del personale impiegato, acquisite sia in ambito nazionale che internazionale; - tipologie, modalità e frequenza degli aggiornamenti formativi; - numerosità e continuità delle collaborazioni con università, enti di ricerca, start up, produttori di tecnologia; - presenza di laboratori presso i quali analizzare o testare le soluzioni tecnologiche da inserire nel proprio portfolio di offerta. Per Centro di Competenza nel settore della Sicurezza ICT si intende una struttura del Fornitore che consenta di: - presidiare il mercato della sicurezza ICT effettuando uno scouting degli ultimi trend evolutivi tecnologici nonché dei prodotti di mercato, al fine di assicurare una proposizione di soluzioni e servizi in grado di proteggere i sistemi della PA dalle minacce cibernetiche in costante evoluzione; - sviluppare e consolidare le competenze necessarie per progettare, realizzare e gestire soluzioni e servizi nell'ambito della sicurezza ICT.
	Capacità di ottimizzare le attività di aggiornamento (12.2) e l'erogazione dei servizi di manutenzione (12.3) e hardening su client (12.4) anche ai fini di dimostrare il soddisfacimento dei livelli di servizio offerti dal Concorrente descritti al paragrafo 3.2.3 del Capitolato Tecnico in base ai seguenti elementi:
12.2	- modalità operative e strumenti adottati per una diagnosi proattiva e/o tempestiva di eventuali anomalie SW e HW, che potrebbero compromettere e/o che compromettono la sicurezza dei sistemi dell'Amministrazione; - modalità di rilascio e deployment degli aggiornamenti sw, al fine di assicurare la continuità operativa dei sistemi dell'Amministrazione e al contempo la loro sicurezza.
12.3	- modello organizzativo e strumenti adottati dalle strutture di supporto qualificato e per la logistica, per le attività di ripristino/riparazione dei prodotti software e hardware oggetto della fornitura (es. strutture di coordinamento, di assistenza tecnica hardware e software, magazzini di parti di ricambio, etc.); - modalità e tempistiche di approvvigionamento e gestione delle parti di ricambio.

12.4	Modalità operative e strumenti adottati per il servizio di hardening al fine di semplificare le fasi di progettazione e/o distribuzione degli adeguamenti sw sugli elementi di un cluster omogeneo e su più cluster in parallelo, anche ottimizzando i tempi di rilascio dei deliverable
12.5	Rispetto al complesso delle assunzioni necessarie per ogni contratto esecutivo finanziato, in tutto o in parte, con le risorse previste dal Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021 e dal Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, nonché dal PNC, l'offerente si impegna, fermo restando il rispetto del requisito minimo di cui al par. 2.4 del Capitolato Tecnico parte Generale, ad assumere persone disabili, giovani di qualsiasi genere, con età inferiore a trentasei anni, e donne per l'esecuzione di ciascun contratto esecutivo o per la realizzazione di attività ad esso connesse o strumentali, nella misura di: - nessuno miglioramento del requisito minimo - >30% e ≤35% - >35% secondo le modalità indicate nel Capitolato d'Oneri.

Tabella 24 - Requisiti migliorativi relativi alla struttura organizzativa e alle modalità impiegate per l'esecuzione dei contratti esecutivi/erogazione dei servizi connessi alla fornitura.

3.2.1 Servizio di installazione e configurazione

Il servizio di installazione e configurazione è obbligatorio ed il relativo costo è da intendersi compreso nei corrispettivi previsti per i prodotti offerti. Il servizio deve essere prestato dall'Aggiudicatario nel rispetto degli SLA previsti (cfr. par 5.1.2), pena l'applicazione delle penali indicate al par.6.

Il servizio comprende tutto quello che è necessario per le attività di installazione e configurazione degli elementi acquistati dall'Amministrazione Contraente, inclusi eventuali elementi offerti come migliorativi dal Fornitore Aggiudicatario in sede di gara.

Si precisa che tutte le eventuali attività propedeutiche all'installazione degli apparati sono a carico dell'Amministrazione Contraente (predisposizione delle linee di alimentazione, linee dati, rack, supporti etc…). Inoltre come specificato nel paragrafo 2.1, laddove l'Amministrazione proceda ad acquistare un prodotto tramite ordine diretto (cioè senza la preventiva fase di dialogo con il Fornitore, descritta nel paragrafo 2), la medesima dovrà fornire all'Aggiudicatario tutte le specifiche di installazione.

In linea generale dovranno essere previste almeno le seguenti attività:

- alloggiamento ed eventuale fissaggio sullo specifico supporto che sarà messo a disposizione dall'Amministrazione Contraente (rack, ripiano, …) in relazione alla tipologia apparato;
- collegamento alla rete di alimentazione, presso il punto di presenza della rete indicato dall'Amministrazione. I cavi di alimentazione si intendono inclusi nell'offerta;
- collegamento alla rete dati, presso il punto di presenza della rete indicato dall'Amministrazione Contraente. I cavi per i collegamenti dati si intendono inclusi nell'offerta (fino ad una lunghezza massima di tre metri);

- configurazione dell'elemento per il suo corretto riconoscimento e funzionamento, quali:
    - configurazione dell'indirizzamento IP;
    - assegnazione del nome di rete;
    - configurazione delle policy di sicurezza;
    - creazione di utenze e profili definiti;
    - installazione del software, configurazione e attivazione delle eventuali licenze necessarie;
    - la configurazione delle specifiche funzionalità previste in base alla tipologia di elemento installato e alla complessità del sistema nel suo complesso.

È richiesto che al termine delle attività il Fornitore aggiorni il "Piano di lavoro generale " e il relativo "Piano Operativo" (laddove previsto) con eventuali informazioni aggiornate (ad esempio specifiche configurazioni software realizzate in fase di installazione e non inizialmente previste).

Il servizio dovrà inoltre prevedere, in caso il prodotto sia acquistato in sostituzione di un prodotto già presente presso l'Amministrazione, l'analisi delle impostazioni/policy/configurazioni in precedenza previste e la loro migrazione, con le specificità dovute alla nuova tecnologia acquistata, sul nuovo prodotto.

Nell'ambito del servizio, l'Aggiudicatario dovrà garantire, laddove applicabile, il rispetto della normativa in materia di:

- rifiuti da apparecchiature elettriche ed elettroniche (Direttiva 2012/19/UE sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE) recepita con D.Lgs. 14-3-2014 n. 49 e s.m.i.);
- sostanze pericolose nelle apparecchiature fornite (direttiva 2011/65/UE, anche nota come "Restriction of Hazardous Substances" (RoHS), recepita dalla legislazione italiana con D.Lgs. 4-3-2014 n. 27 e ss.m.i.).

L'Aggiudicatario dovrà prestare l'attività di ritiro, se richiesto dall'Amministrazione, ai fini del corretto conferimento dei materiali e delle apparecchiature sostituite, già in possesso dell'Amministrazione Contraente e dichiarate non più utilizzabili, presso i Centri di Trattamento competenti. L'attività è limitata ai materiali e alle apparecchiature dismesse nell'ambito del perimetro di intervento relativo all'installazione delle nuove apparecchiature, sebbene tale vincolo non implichi una corrispondenza unitaria tra un apparato nuovo e un apparato da dismettere.

Non si potrà procedere alla verifica di conformità dei nuovi prodotti installati finché l'Aggiudicatario non abbia provveduto a rimuovere dai locali dell'Amministrazione Contraente tutto il materiale che è stato sostituito.

3.2.2 Servizio di supporto alla verifica di conformità

Ai sensi di quanto previsto all'art. 1, comma 6 lett. a) del D.L. 105/2019, si precisa innanzitutto che il Fornitore dovrà fornire pieno supporto alle Amministrazioni chiamate a collaborare con il CVCN o i CV all'effettuazione di verifiche preliminari e condizioni e test hardware e software su forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui all'art 1 comma 2 lett. b legge 133/2019.

In aggiunta, è previsto un servizio di supporto alla verifica di conformità, da intendersi quale assistenza del Fornitore all'Amministrazione nella fase di verifica di quanto fornito e realizzato, obbligatorio ed il cui relativo costo è da intendersi compreso nei corrispettivi previsti per i prodotti offerti.

L'Aggiudicatario procederà, con propri mezzi e risorse, alla verifica funzionale di tutti gli elementi oggetto di Fornitura; tali prove dovranno consistere in test volti a verificare che quanto installato sia conforme ai requisiti offerti e si intenderanno positivamente superati solo se tutti gli apparati installati risulteranno funzionare correttamente, sia singolarmente che interconnessi tra loro in modo che il complesso dei prodotti implementati e/o delle attività eseguite sia in linea con i requisiti espressi dall'Amministrazione riportati nel "Piano di lavoro generale " e nel relativo "*Piano Operativo*" (laddove previsto) o nella "*Richiesta di attivazione del servizio di supporto*" nel caso del servizio di supporto specialistico.

Al termine di tale verifica, l'Aggiudicatario consegnerà all'Amministrazione Contraente il "*Verbale di Fornitura*" nel rispetto dei termini stabiliti nel paragrafo 5.1.2, o il "*Rapporto di Fine Intervento*" nel rispetto dei termini stabiliti nel paragrafo 5.1.5, pena l'applicazione delle relative penali.

Il Fornitore inoltre, in sede e al termine della verifica, dovrà fornire all'Amministrazione tutte le informazioni di dettaglio necessarie per la presa in carico dei beni da parte della stessa.

L'Amministrazione Contraente procederà alla verifica di conformità dei prodotti e dei servizi oggetto di Fornitura, anche in corso di esecuzione, e potrà a suo insindacabile giudizio:

- eventualmente avvalersi della documentazione di autocertificazione rilasciata dall'Aggiudicatario, mediante accettazione del "*Verbale di Fornitura*" o del "*Rapporto di Fine Intervento*". In questo caso l'Amministrazione Contraente sottoscriverà, entro **15 giorni** dalla data di sottoscrizione del "*Verbale di Fornitura*" o del "*Rapporto di Fine Intervento*", un "*Verbale di Verifica di conformità*", la cui data sarà ritenuta quale "*Data di Accettazione*" della fornitura;
- provvedere alla nomina di una propria Commissione di Verifica di Conformità. In questo caso l'Amministrazione stessa dovrà nominare la Commissione di Verifica di Conformità entro **15 giorni** dalla data riportata sul "*Verbale di Fornitura*" o sul "*Rapporto di Fine Intervento*". L'Aggiudicatario dovrà collaborare, con mezzi, materiali e personale specializzato proprio, al supporto dei lavori della Commissione di Verifica di Conformità. In particolare, l'Aggiudicatario dovrà supportare l'esecuzione dei test ed il rilascio in esercizio dell'hardware e del software. I lavori della Commissione dovranno concludersi nei **15 giorni** successivi alla costituzione della Commissione di Verifica di Conformità.

In caso di esito negativo della Verifica di Conformità, l'Aggiudicatario dovrà procedere ad ogni attività necessaria all'eliminazione dei malfunzionamenti e sostituzioni di parti e comunicare la disponibilità ad una seconda verifica entro il termine perentorio di **15 giorni** decorrenti dalla data della prima Verifica di Conformità negativa, pena l'applicazione delle penali di cui al paragrafo 6.

Qualora anche la seconda Verifica di Conformità abbia esito negativo verranno applicate le penali di cui al paragrafo 6. È facoltà dell'Amministrazione procedere ad ulteriori Verifiche di Conformità ovvero dichiarare

risolto di diritto il Contratto di fornitura, in tutto o in parte. Nel caso in cui anche le ulteriori Verifiche di Conformità avessero esito negativo verranno applicate le penali di cui al paragrafo 6, fatta salva la facoltà dell'Amministrazione di dichiarare risolto il Contratto di fornitura, in tutto o in parte.

Tutte le attività di verifica dovranno concludersi con la stesura di un "*Verbale di Verifica di Conformità*". Nel caso di esito positivo, la data del "*Verbale di Verifica di Conformità*" positivo avrà valore di "*Data di accettazione*" della fornitura.

L'Aggiudicatario dovrà supportare, fornendo la strumentazione e il personale necessario per la realizzazione delle prove, l'Amministrazione Contraente nell'esecuzione di tutte le verifiche funzionali previste dalle procedure che saranno concordate con l'Amministrazione stessa e definite nel "*Piano Operativo*" approvato (cfr. par. 2.2). A tal fine potrà essere previsto anche l'utilizzo di un "test-bed" da realizzarsi presso l'Amministrazione o presso locali messi a disposizione del Fornitore (su richiesta ed approvazione dell'Amministrazione).

3.2.3 Servizio di manutenzione

Il servizio di manutenzione è opzionale (sebbene oggetto di quotazione) e quindi dovrà essere prestato, a pagamento, dall'Aggiudicatario soltanto se espressamente richiesto dall'Amministrazione.

Il servizio di manutenzione deve essere prestato dall'Aggiudicatario nel rispetto degli SLA previsti (cfr. par 5.1.4), anche con interventi da effettuarsi presso i siti dell'Amministrazione Contraente, pena l'applicazione delle penali indicate al par.6.

La manutenzione comprende le attività volte a garantire una pronta correzione dei malfunzionamenti e il ripristino delle funzionalità, anche attraverso attività di supporto on-site.

Sarà facoltà dell'Amministrazione Contraente richiedere a pagamento il servizio manutenzione in base al profilo di qualità richiesto per i servizi erogati, *Low Profile* (*Business Day*) o *High Profile* (*H24*), a cui sono associati i relativi SLA di cui al par. 5.1.4.

Resta inteso che, indipendentemente dalla finestra di erogazione associata al profilo selezionato, qualora gli interventi di manutenzione dovessero comportare una completa interruzione dell'attività lavorativa, gli interventi stessi dovranno essere effettuati in orario non coincidente con il periodo di operatività dell'Amministrazione. Tutti gli interventi di manutenzione dovranno in ogni caso essere concordati preventivamente con l'Amministrazione.

L'Aggiudicatario sarà tenuto ad offrire il servizio di manutenzione per annualità, quindi per 12 mesi o massimo 24 mesi.

Nell'esecuzione delle attività richieste l'Aggiudicatario avrà la facoltà, in accordo con l'Amministrazione, di predisporre un accesso remoto sicuro (utilizzando account VPN personali configurati e abilitati

opportunamente, con tracciatura degli accessi per eventuali successivi audit, accessi che comunque dovranno essere limitati al tempo strettamente necessario all'esecuzione dell'attività, ad esempio mediante utenze token create all'occorrenza) a supporto delle stesse (ad. es. effettuazione di diagnosi attraverso i propri sistemi di gestione e di management per analisi di problematiche e malfunzionamenti segnalati dall'Amministrazione). Tale possibilità dovrà essere riportata nel *"Piano di lavoro generale*" e nel relativo "*Piano Operativo*" (laddove previsto)

La possibilità di predisporre tale accesso remoto sarà concordata con l'Amministrazione Contraente in sede di attivazione della fornitura, descritta nel "*Piano di lavoro generale*" e nel relativo "*Piano Operativo*" (laddove previsto) e dovrà garantire le Amministrazioni sul rispetto delle prassi e delle norme sulla sicurezza dei dati e rispetto della normativa della privacy, anche in accordo con le policy di sicurezza definite dalle singole Amministrazioni.

In fase di offerta economica al concorrente sarà richiesto di esprimere due valori percentuali in base al profilo di qualità richiesto per i servizi erogati, *Low Profile* (*Business Day*) o *High Profile* (*H24*). Ogni valore espresso rappresenta la percentuale del prezzo di fornitura degli elementi offerti in Accordo Quadro relativa al canone di manutenzione annuale (ad esempio: se il prezzo dell'elemento di fornitura "X" offerto dal concorrente è pari a 10€ e la percentuale relativa alla manutenzione per il profilo *Low Profile* offerta dal concorrente è pari al 10% il corrispondente canone annuale della manutenzione con profilo *Low Profile* dell'elemento di fornitura "X" è pari a 10€ x 10% = 1€).

Le attività di manutenzione potranno essere richieste dalle Amministrazioni Contraenti sui soli elementi di fornitura acquistati nell'ambito del presente AQ e potranno essere acquistati solo contestualmente alla fornitura oggetto del servizio, con avvio dalla "*Data di accettazione*" definita nel paragrafo 3.2.2.

Le attività di manutenzione possono riassumersi in:

- ricezione della chiamata di assistenza da parte dell'Amministrazione e assegnazione del Severity Code (cfr. par. 3.2.6)
- risoluzione del problema tramite supporto telefonico all'utente (ove possibile) e/o eventuale intervento/i remoto/i;
- risoluzione della causa del guasto tramite, ove necessario:
    - intervento presso la sede/luogo interessato
    - ripristino del servizio/funzionalità sui livelli preesistenti al guasto/anomalia, secondo gli SLA contrattualizzati, anche attraverso sostituzioni di elementi danneggiati
    - verifica funzionale del sistema per assicurare l'eliminazione della causa del guasto.

Ogni intervento di manutenzione dovrà prevedere la redazione del relativo "*verbale di intervento*" e l'eventuale aggiornamento della documentazione di progetto.

Gli interventi dovranno concludersi con l'attività di verifica del corretto funzionamento delle apparecchiature sostituite o riparate e del sistema nella sua globalità; tale verifica sarà a cura dell'Aggiudicatario, ma è lasciata libertà all'Amministrazione Contraente di coinvolgere proprio personale e/o

personale di terzi. L'Aggiudicatario è tenuto al rispetto delle modalità operative richieste dall'Amministrazione.

Tutte le attività previste (interventi del Fornitore presso l'Amministrazione, rimozione degli elementi, riparazione degli elementi guasti, successiva installazione) sono da intendersi **incluse nel costo del servizio**.

Il servizio dovrà inoltre comprendere l'attivazione, sui prodotti manutenuti, di tutte le eventuali *Major release* successive a quella installata sui prodotti acquisiti emesse dal produttore nel periodo di validità del servizio.

Si precisa infine che, in caso di malfunzionamenti inerenti la componente software/firmware, il Fornitore dovrà farsi carico di informare tempestivamente le Amministrazioni che hanno acquisito i medesimi prodotti provvedendo a tutte le attività volte all'aggiornamento della componente software/firmware soggetta al malfunzionamento. Tale attività dovrà essere svolta sia nel caso il malfunzionamento sia identificato proattivamente dal Fornitore o dal produttore sia nel caso esso sia identificato da un'Amministrazione Contraente. Dovrà essere prestata particolare attenzione a quanto attiene **bug o problematiche che possano compromettere le funzionalità di sicurezza cui i prodotti acquistati sono destinati**, rendendo di fatto, sia loro sia i sistemi da loro protetti, **vulnerabili a *exploit***. In tale eventualità il Fornitore dovrà, oltre ad attivarsi tempestivamente per procedere alla risoluzione della problematica e all'aggiornamento dei sistemi, fornire eventuali *work-around* (documentati e inviati all'Amministrazione) che consentano di eliminare o quanto meno attenuare il rischio di sfruttamento delle falle identificate da parte di soggetti non autorizzati.

3.2.4 Servizio di supporto specialistico

Il servizio supporto specialistico è opzionale (sebbene oggetto di quotazione), quindi dovrà essere prestato, a pagamento, dall'Aggiudicatario soltanto se espressamente richiesto dall'Amministrazione.

Tale servizio consente alle Amministrazioni Contraenti di richiedere del personale specializzato con l'obiettivo di essere supportata in varie attività inerenti sia la fornitura specifica acquistata in AQ sia, in maniera più generale, la propria infrastruttura di sicurezza informatica. Il servizio riguarderà esclusivamente le attività riportate nel seguito:

a) la realizzazione di specifiche integrazioni tra i prodotti acquistati e prodotti già presenti presso l'Amministrazione al fine di massimizzare l'efficacia dei prodotti acquisiti e garantire la sicurezza del sistema nel suo complesso
b) l'effettuazione, nelle fasi successive all'implementazione dei prodotti, di attività di analisi specifiche che consentano di stabilire le policy di sicurezza maggiormente adeguate da implementare nel complesso dei sistemi dell'Amministrazione
c) il supporto operativo al personale dell'Amministrazione nella gestione della sua infrastruttura, fornendo competenze specifiche in ambito di sicurezza informatica. Tale supporto potrà essere sia in modalità "a chiamata" sia in modalità "presidio" laddove l'Amministrazione, in ragione della complessità della propria infrastruttura, ravveda la necessità di avere del personale del Fornitore presso la propria sede in maniera continuativa

d) il supporto operativo al personale dell'Amministrazione nella gestione del suo centro operativo dedicato alla sicurezza (SOC), fornendo competenze specifiche in tale ambito.

Tale servizio potrà essere acquistato dalle Amministrazioni Contraenti unicamente in maniera contestuale ai prodotti e avere durata massima pari a 24 mesi dalla "*Data di accettazione*" della fornitura. La descrizione delle attività previste e il relativo effort saranno quindi riportate nel "*Piano Operativo*" (laddove previsto).

Il servizio potrà essere prestato secondo le seguenti modalità:

i. in fase iniziale - lett. a) del precedente elenco;
ii. in modalità "*spot*" - lett. b) e lett c) (limitatamente alla modalità "a chiamata") del precedente elenco
iii. con periodicità definita - lett. c) (limitatamente alla modalità "presidio") e d) del precedente elenco.

In particolare, in caso di necessità di attivazione della modalità "*spot*" in corso di vigenza di contratto esecutivo, l'Amministrazione invierà una "*Richiesta di attivazione del servizio di supporto*" all'Aggiudicatario tramite uno dei canali messi a disposizione con la descrizione dell'attività richiesta, dichiarando le tempistiche richieste per l'erogazione del servizio. L'Amministrazione potrà inoltre preventivamente contattare l'Aggiudicatario per meglio delimitare il perimetro dell'intervento richiesto ed il relativo effort. Entro 2 giorni lavorativi dalla ricezione della "*Richiesta di attivazione del servizio di supporto*", l'Aggiudicatario sarà tenuto a inviare una "*Lettera di presa in carico del servizio di supporto*" nella quale dovrà indicare il numero identificativo della lavorazione, l'effort e le tempistiche richieste dall'Amministrazione nella richiesta effettuata o successivamente concordate con l'Amministrazione stessa, inclusa la data di completamento dell'intervento. Il mancato rispetto dei tempi concordati è oggetto di penale secondo quanto previsto al par. 6. Al termine delle attività l'Aggiudicatario dovrà fornire un documento di "*Rapporto di Fine Intervento*" che specifichi la data di avvio dell'intervento, le attività eseguite, la durata dell'intervento, la data di completamento e attesti la disponibilità alla verifica di conformità.

Il servizio di supporto specialistico sarà soggetto a Verifica di Conformità eseguita dall'Amministrazione, in base alle summenzionate modalità:

i. in tale caso la verifica è parte di quella effettuata a seguito del completamento dell'installazione dei prodotti acquistati e alla ricezione del "*Verbale di Fornitura*" (cfr. paragrafo 3.2.2)
ii. in tale caso la verifica avverrà a valle del "*Rapporto di Fine Intervento*" consegnato all'Amministrazione
iii. in tale caso la verifica sarà effettuata entro il quindicesimo giorno del mese *N* con riferimento alle attività eseguite nel mese *N-1*.

Pe l'effettuazione del complesso di attività previste per il supporto specialistico il Fornitore dovrà prevedere le figure professionali riportate nel seguito. Si precisa che, fatto salvo il possesso del diploma di scuola media superiore, i requisiti accademici richiesti per ogni figura (titoli di studio) possono essere utilmente soddisfatti attraverso il possesso di una cultura equivalente, maturata attraverso lo svolgimento di esperienze lavorativo-professionali, pari a:

- **5 (cinque) anni aggiuntivi nel settore ICT** nel caso di laurea specialistica
- **3 (tre) anni aggiuntivi nel settore ICT** nel caso di laurea triennale.

Quindi, ad esempio, per la figura di Security Principal sarà accettata una risorsa in possesso di diploma ma con esperienza lavorativa di almeno 15 anni (di cui almeno 5 anni di provata esperienza nella specifica funzione).

Figura professionale	Security Principal
Titolo di studio	Laurea specialistica in discipline scientifiche
Anzianità lavorativa	anzianità lavorativa di almeno 10 (dieci) anni nel settore ICT, da computarsi successivamente alla data di conseguimento della laurea, di cui almeno 5 (cinque) anni di provata esperienza nella specifica funzione
Competenze ed esperienze richieste	- conoscenza della metodologia di Project Management; - esperienza di Project Management in progetti analoghi; - conoscenza approfondita dei processi di Security Governance e Security Management; - conoscenza approfondita delle metodologie di vulnerability assessment, penetration test, compliance management e security audit; - esperienza nel disegno e nella valutazione dei sistemi per la gestione della sicurezza delle informazioni; - conoscenza delle metodologie e degli strumenti operativi richiesti in progetti di IT Security; - conoscenza dei processi e delle procedure operative IT; - conoscenza delle tecnologie principali per la sicurezza IT.

Tabella 25 – Supporto specialistico "Security Principal"

Figura professionale	Security Solution Architect
Titolo di studio	Laurea triennale in discipline scientifiche
Anzianità lavorativa	anzianità lavorativa di almeno 8 (otto) anni nel settore ICT, da computarsi successivamente alla data di conseguimento del diploma di laurea, di cui almeno 4 (quattro) anni di provata esperienza nella specifica funzione
Competenze ed esperienze richieste	- capacità di comprendere l'infrastruttura sotto analisi e le relazioni tra i differenti sistemi e componenti infrastrutturali; - esperienza nell'analisi e nella valutazione delle configurazioni e delle regole tecniche delle principali soluzioni di sicurezza utilizzate per proteggere l'infrastruttura e i servizi (reti TCP/IP, Firewall, IPS/IDS, SIEM, soluzioni anti-malware, Web Application Firewall, Database Monitoring, servizi Anti-DDoS, servizi cloud oriented per la sicurezza, ecc.); - esperienza nell'analisi di un'infrastruttura IT complessa volta all'individuazione di problematiche architetturali che ne potrebbero compromettere la sicurezza;

	- esperienza nella verifica dell'efficacia delle misure tecniche ed organizzative preposte alla sicurezza di un'infrastruttura IT complessa; - consolidata esperienza nella progettazione della sicurezza ICT maturata in contesti analoghi; - conoscenza approfondita delle problematiche di sicurezza delle infrastrutture IT; - conoscenza delle metodologie e degli strumenti operativi richiesti per verificare l'efficacia delle contromisure di sicurezza poste a salvaguardia delle infrastrutture IT; - esperienza nell'identificazione di soluzioni tecnologiche ed organizzative da porre in essere per ottimizzare e migliorare le configurazioni e le politiche e per traguardare la piena adozione delle contromisure previste; - conoscenza delle tecnologie principali per la sicurezza IT, soprattutto in ambito sicurezza cloud, sicurezza minacce di nuova generazione, modalità di contenimento, ecc.; - ottima conoscenza sistemi di correlazione eventi, progettazione regole di correlazione e tuning sistemi di analisi eventi con esperienza di integrazione in contesti analoghi; - buona conoscenza sistemi di autenticazione, specialmente sistemi di Identity & Access Management con esperienza di integrazione su ambienti analoghi; - conoscenza delle tecnologie in uso nel contesto di riferimento, con esperienza nella configurazione e nell'inserimento in rete delle stesse, in funzione delle minacce riscontrate.

Tabella 26 – Supporto specialistico "Senior Security Architect"

Figura professionale	**Senior Security Tester**
Titolo di studio	Laurea triennale in discipline scientifiche
Anzianità lavorativa	anzianità lavorativa di almeno 6 (sei) anni nel settore ICT, da computarsi successivamente alla data di conseguimento del diploma di laurea, di cui almeno (quattro) anni di esperienza nella specifica funzione
Competenze ed esperienze richieste	○ analisi dinamica delle vulnerabilità e penetration testing sia in ambito applicativo che sulle infrastrutture di sistema e middleware; ○ analisi statica del codice sorgente o delle configurazioni di sistema; ○ disegno e valutazione dei sistemi di gestione per la sicurezza; ○ gestione processo di hardening di sistemi e piattaforme middleware; ○ validazione pattern di sviluppo sicuro del codice; - capacità di comprendere l'infrastruttura sotto analisi e le relazioni tra i differenti sistemi;

Figura professionale	Senior Security Tester
	- conoscenza approfondita delle diverse tipologie di attacco informatico, delle tecniche di penetration test, degli strumenti software utilizzati e dei più importanti tool ed exploit disponibili pubblicamente; - esperienza nell'analisi delle vulnerabilità di sistemi e reti in esercizio senza impattare sull'operatività ed il funzionamento degli stessi; - conoscenza complessiva delle problematiche di sicurezza dei dati e delle informazioni.

Tabella 27 – Supporto specialistico "Senior Security Tester"

Figura professionale	Senior Security Analyst
Titolo di studio	Laurea triennale in discipline scientifiche
Anzianità lavorativa	anzianità lavorativa di almeno 6 (sei) anni nel settore ICT, da computarsi successivamente alla data di conseguimento del diploma di laurea, di cui almeno 4 (quattro) anni di esperienza nella specifica funzione
Competenze ed esperienze richieste	- capacità di coordinamento dei Consulenti Junior; - conoscenza dei processi e delle procedure operative IT; - conoscenza approfondita dei processi di Incident Handling ed Escalation per la gestione degli incidenti di sicurezza informatica; - conoscenza approfondita dei processi di analisi forense, acquisizione degli elementi probatori e conservazione degli stessi; - conoscenza approfondita dei sistemi di rilevazione e analisi degli allarmi; - esperienza consolidata nell'analisi tecnica di incidenti all'interno di strutture SOC o CERT nell'ambito della Pubblica Amministrazione o Clienti Privati; - esperienza consolidata nella gestione delle attività di supporto agli organi di Polizia Giudiziaria in caso di illeciti informatici; - esperienza consolidata nella definizione proattiva di configurazioni e analisi di sicurezza; - esperienza nella definizione di regole di correlazione e nel tuning delle stesse; - conoscenza dei processi di reverse engineering dei malware ed esperienza consolidata nella analisi forense di malware mediante strumenti di analisi e attività di reverse; - conoscenza approfondita dei protocolli di rete e della tipologia di traffico all'interno di un contesto complesso con esperienza consolidata nell'analisi forense del traffico di rete e nell'identificazione di anomalie o elementi a supporto per la corretta gestione degli incidenti di sicurezza.

Tabella 28 – Supporto specialistico "Senior Security Analyst"

Figura professionale	Junior Security Analyst
Titolo di studio	Laurea triennale in discipline scientifiche
Anzianità lavorativa	anzianità lavorativa di almeno 4 (quattro) anni nel settore ICT, da computarsi successivamente alla data di conseguimento del diploma di laurea, di cui almeno 2 (due) anni di esperienza nella specifica funzione
Competenze ed esperienze richieste	- conoscenza dei processi e delle procedure operative IT; - conoscenza dei processi di Incident Handling ed Escalation per la gestione degli incidenti di sicurezza informatica; - conoscenza dei sistemi di rilevazione e analisi degli allarmi; - esperienza nell'analisi tecnica di incidenti; - conoscenza della modalità di intervento sulle postazioni client e sui server in caso di diffusione di malware di nuova generazione; - conoscenza dei protocolli di rete e della tipologia di traffico all'interno di un contesto IT.

Tabella 29 – Supporto specialistico "Junior Security Analyst"

In fase di offerta è richiesto al Concorrente di esprimere un prezzo per giorno/persona per ogni figura professionale prevista. I prezzi espressi saranno riferiti rispettivamente a:

- 8 ore lavorative complessive nella fascia oraria feriale Lun-Sab 8.00-20.00 (fascia standard).
- 8 ore lavorative complessive nella fascia oraria Lun-Sab 20.00-7.00 o la domenica o nei giorni festivi (fascia straordinaria).

Nell'erogazione del servizio l'Aggiudicatario dovrà rispettare i livelli di servizio descritti nel paragrafo 5.1.5, pena l'applicazione di apposite penali (cfr. par. 6).

Inoltre l'Aggiudicatario dovrà:

- in caso di servizio richiesto in fase iniziale o con periodicità definita - precedenti punti i) e iii): presentare all'Amministrazione Contraente, entro 20 giorni solari dalla data di stipula del contratto esecutivo, pena l'applicazione delle penali di cui al paragrafo 6, i CV delle risorse proposte per l'erogazione del servizio in cui dovranno essere anche inserite copie delle certificazioni possedute dalle risorse, in accordo con i requisiti minimi o i migliorativi eventualmente offerti;
- in caso di servizio richiesto in modalità "spot" – precedente punto ii): presentare all'Amministrazione Contraente, entro 5 giorni solari dalla data di invio della "*Lettera di presa in carico del servizio di supporto*", pena l'applicazione delle penali di cui al paragrafo 6, i CV delle risorse proposte per l'erogazione del servizio in cui dovranno essere anche inserite copie delle certificazioni possedute dalle risorse, in accordo con i requisiti minimi o i migliorativi eventualmente offerti.

Sulla base dei CV presentati l'Amministrazione procederà alla verifica che il personale proposto sia in linea con i requisiti minimi e gli eventuali requisiti migliorativi offerti, riservandosi la possibilità di procedere ad un colloquio di approfondimento per verificare la corrispondenza delle competenze elencate nel CV. Per il personale ritenuto inadeguato, qualunque sia il ruolo, l'Amministrazione Contraente procederà alla richiesta

formale di sostituzione inviando la "*Richiesta di sostituzione del personale per il servizio di supporto*" in cui indicherà puntualmente la risorsa che ritiene inadeguata e le relative motivazioni in riferimento ai requisiti minimi e/o migliorativi di gara. La presentazione del CV della nuova risorsa in sostituzione dovrà quindi avvenire secondo i tempi previsti nel paragrafo 5.1.5, pena l'applicazione di apposite penali (cfr. par. 6). La richiesta di sostituzione potrà avvenire anche successivamente all'avvio del servizio, laddove l'Amministrazione riscontri che il personale impiegato non sia adeguato ad effettuare le attività richieste.

Gli offerenti potranno offrire l'impiego, in fase di esecuzione, di personale in possesso di certificazioni in ambito *security* secondo quanto previsto nella seguente tabella.

Personale del servizio di supporto specialistico		
Requisiti migliorativi		
13.1	Security Principal	Percentuale di risorse offerte, nell'ambito di ciascun contratto esecutivo, in possesso della certificazione ISACA CISM (Certified Information Security Manager): almeno il 50%
13.2	Senior Security Architect	Percentuale di risorse offerte, nell'ambito di ciascun contratto esecutivo, in possesso della certificazione (ISC)^2 CISSP (Certified Information System Security Professional): almeno il 50%
13.3	Senior Security Tester	Percentuale di risorse offerte, nell'ambito di ciascun contratto esecutivo, in possesso di almeno una delle seguenti certificazioni: EC-Council CEH (Certified Etical Hacker) e/o GIAC Penetration Tester e/o Offensive Security Certified Professional e/o CompTIA Pentest+: almeno il 50%
13.4	Senior Security Analyst	Percentuale di risorse offerte, nell'ambito di ciascun contratto esecutivo, in possesso di almeno una delle seguenti certificazioni: EC-Council CSA (Certified SOC Analyst) e/o CompTIA CySA+ (Cyber Security Analyst) e/o GIAC Certified Intrusion Analyst: almeno il 50%
13.5	Junior Security Analyst	Percentuale di risorse offerte, nell'ambito di ciascun contratto esecutivo, in possesso di almeno una delle seguenti certificazioni: EC-Council CSA (Certified SOC Analyst) e/o CompTIA CySA+ (Cyber Security Analyst) e/o GIAC Certified Intrusion Analyst, e/o ISACA CSX-F (Cyber Security Fundamentals) e/o CompTIA Security+: almeno il 50%

Tabella 30 - Requisiti migliorativi relativo al personale del servizio di supporto specialistico

3.2.5 Servizio di hardening su client

Il servizio di hardening su client è opzionale (sebbene oggetto di quotazione) e quindi dovrà essere prestato, a pagamento, dall'Aggiudicatario soltanto se espressamente richiesto dall'Amministrazione.

Con tale servizio si vuole fornire all'Amministrazione il supporto operativo necessario per rendere sicuri i client utilizzati. Le attività effettuate dovranno essere aderenti a quanto previsto dalle "*Linee guida per adeguare la sicurezza del software di base*" rilasciate da AgID.

Le specifiche attività che dovranno essere eseguite sono dipendenti dagli specifici software utilizzati sui client, ma in linea generale possono essere riassunte in:

- eliminazione di programmi non necessari dalle postazioni utente. Potenzialmente ogni programma è una porta di accesso per soggetti non legittimati e dunque la loro diminuzione consente di limitare i rischi di intrusioni. Tutti i programmi che non sono stati autorizzati e controllati e che non sono strettamente utili all'esecuzione delle attività lavorative dovrebbero essere rimossi
- supporto ai sistemisti PA nelle fasi di monitoraggio e controllo che il sistema operativo e i programmi leciti siano aggiornati alle ultime versioni e agli ultimi "*service pack*" disponibili
- controllo che sui client siano abilitati i servizi autorizzati, ossia che non vi siano "*demoni*" in ascolto sulle porte di rete se non quelli strettamente necessari
- verifica che gli utenti abbiano i corretti privilegi in relazione al loro ruolo e che appartengono ai corretti gruppi utenti
- verifica della consistenza delle password richieste e della periodicità di cambio password richiesta agli utenti
- supporto ai sistemisti PA nella definizione di gruppi di policy che potranno essere applicati agli utenti sulla base dei loro ruoli
- verifica che gli eventi di sicurezza siano correttamente storicizzati (logging) ai fini del controllo e dell'audit
- supporto al personale dell'Amministrazione nella distribuzione delle azioni correttive individuate (ad es. installazione di eventuali *patch* mancanti, realizzazione e installazione di fix temporanee, etc..) siano esse relative al sistema operativo che ai programmi utilizzati

Il servizio dovrà essere effettuato sulle postazioni di tipo client e dovrà includere almeno i seguenti software:

- Sistemi operativi Windows Client
- Sistemi operativi macOS
- Sistemi operativi UNIX/Linux di tipo Client
- Principali Web Browser (Edge, Explorer, Firefox, Chrome)
- Principali applicativi software di produttività (Microsoft Office/OpenOffice, Pdf Readers, Outlook, …).

In fase di attivazione della fornitura l'Amministrazione e il Fornitore concorderanno, sulla base delle esigenze espresse dall'Amministrazione nel suo "*Piano dei fabbisogni*", la numerosità di elementi interessata dagli interventi, tempistiche e modalità di attuazione previste, che saranno riportate nel "*Piano Operativo*". In particolare nel "*Piano Operativo*" dovranno essere dettagliate le scadenze per le attività e/o i deliverable previsti, il cui mancato rispetto è soggetto, in caso di inadempienza, alle penali di cui al par. 6.

Per gli elementi e la loro relativa numerosità si dovrà procedere come segue:

- dovranno essere identificati il numero di *cluster* omogenei di elementi, considerando che l'identificazione delle azioni correttive di un elemento appartenente ad un insieme omogeneo possono essere facilmente ripetute su tutti gli elementi del medesimo insieme anche per mezzo di strumenti di *software distribution*. Si pensi ad esempio al caso in cui le postazioni client dell'Amministrazione siano tutte derivate da una medesima "immagine" SW, presentando quindi le medesime caratteristiche in termini di pacchetti installati e relativa configurazione, tranne che per le specificità legate al singolo utente (ad es. login/passwd)
- dovranno essere identificate nel dettaglio le attività che dovranno essere effettuate nella realizzazione del servizio. Ad esempio, laddove l'Amministrazione abbia già tutte le informazioni relative allo stato della propria infrastruttura interessata dall'attività, la fase di *assessment*, nel seguito descritta, potrà non essere effettuata
- dovranno essere identificati il numero di elementi appartenenti a ciascun cluster omogeneo
- dovrà essere calcolata, sulla base di tali elementi, la spesa del servizio in base al listino di fornitura.

In fase di esecuzione il servizio dovrà quindi prevedere (a meno che alcune fasi non siano state preventivamente escluse in accordo con l'Amministrazione):

- una fase di *assessment* per ogni *cluster* identificato, che consenta di raccogliere tutte le informazioni utili a definire il contesto e a progettare gli interventi specifici da effettuarsi sugli elementi del *cluster*
- la progettazione degli interventi per un elemento di ogni *cluster* identificato
- la realizzazione degli interventi su un elemento di ogni *cluster* identificato
- la verifica che le attività effettuate non abbiano avuto impatti sulla normale operatività prevista
- il supporto al personale preposto alle attività sistemistiche per la distribuzione di quanto realizzato su tutti gli elementi di ogni *cluster* identificato
- la redazione di *deliverable* che diano evidenza
    - dello stato iniziale di ogni elemento di ogni *cluster* omogeneo, come risultante dalle attività di *assessment*
    - delle azioni correttive previste per ogni elemento di ogni *cluster* omogeneo
    - dello stato finale di ogni elemento di ogni *cluster* omogeneo, come risultante dalle attività di *hardening* effettuate.

In fase di offerta è richiesto agli Offerenti di esprimere dei prezzi in relazione a:

a) la fase di assessment di un *cluster* omogeneo
b) la progettazione e la realizzazione dell'attività su un singolo elemento di un *cluster* omogeneo

c) il supporto al personale preposto alle attività sistemistiche per la distribuzione di quanto realizzato su tutti gli elementi di un *cluster* omogeneo (tre fasce in base alla numerosità complessiva degli elementi di un *cluster*)

Il servizio di hardening potrà essere acquistato solo contestualmente ai prodotti e avere durata massima di 24 mesi dalla "*Data di accettazione*" della fornitura.

3.2.6 Servizio di Contact Center ed help desk

Tale servizio è obbligatorio e i costi si intendono ricompresi nel complesso dei corrispettivi previsti. L'Aggiudicatario dovrà assicurare un servizio di assistenza da remoto, con accesso multicanale (telefono, fax, email, PEC), dedicato all'AQ che dovrà essere reso disponibile alla **data di attivazione dell'AQ**. Il servizio dovrà essere accessibile mediante un "Numero Verde" (gratuito) per le comunicazioni telefoniche. Le informazioni di contatto dovranno essere disponibili alla data di stipula dell'AQ.
Il servizio sarà utilizzato per:

a) Contact Center: per fornire alle Amministrazioni supporto informativo sulle modalità di utilizzo dello strumento e informazioni di carattere generale sui prodotti e servizi previsti, nonché per gli aspetti legati alla fatturazione e rendicontazione, utilizzo e segnalazioni di eventuali anomalie al Portale della Fornitura (cfr. par. 4.1 del Capitolato Tecnico parte Generale). Dovranno inoltre essere gestite le chiamate che interessano i prodotti acquistati dalle PA in caso di guasti che intervengano nel periodo di garanzia;
b) Help Desk: a completamento del servizio di manutenzione erogato. In tale caso le dovranno essere gestite le richieste di supporto a seguito di problematiche riscontrate dalle Amministrazioni.

Il servizio deve essere:

- attivo 24h 7x7 365 giorni all'anno, attraverso strumenti di interazione (IVR)
- attivo con operatore nella fascia oraria Lun-Ven 9.00 – 18.00 per quanto attiene le richieste di cui al precedente punto a)
- attivo con operatore nella fascia oraria relativa al profilo di servizio contrattualizzato dall'Amministrazione Contraente (cfr. paragrafo 5.1) per quanto attiene le richieste di cui al precedente punto b).

A titolo esemplificativo le attività che dovranno essere previste nell'ambito complessivo di tale servizio sono:

- fornire informazioni su tematiche legate all'adesione dell'AQ, in accordo con il processo di cui al paragrafo 2
- fornire informazioni sulle attività preliminari all'Ordinativo di fornitura
- il supporto alla compilazione degli Ordinativi di Fornitura
- fornire informazioni sullo stato di avanzamento degli ordini e sulla loro evasione
- la risoluzione di problematiche di carattere amministrativo
- la ricezione di segnalazione di guasti agli apparati acquistati dalle Amministrazioni;
- l'assistenza nella formulazione di diagnosi e/o di tentativi di risoluzione del guasto da parte del personale dell'Amministrazione;
- la ricezione di richieste di intervento per manutenzione;

- l'apertura e gestione del guasto, su segnalazione del personale dell'Amministrazione, attraverso apertura di Trouble Ticket e assegnazione del Severity Code. Il Severity Code dovrà essere assegnato in accordo con l'Amministrazione Contraente in base alla gravità della problematica riscontrata. Nel caso la gravità del Severity Code non sia di immediata determinazione, si dovrà comunque preferire l'assegnazione della gravità maggiore in maniera da minimizzare il disservizio.

Oltre ai canali di accesso summenzionati, l'accesso al servizio potrà essere basato sul canale WEB. In ogni caso tale modalità non sarà considerata sostitutiva delle modalità richieste in precedenza. Il servizio dovrà essere erogato per tutta la durata dell'AQ e dei contratti esecutivi.

Ogni comunicazione da parte dell'Aggiudicatario o dell'Amministrazione Contraente, avvenuta nell'ambito dell'utilizzo del servizio che abbia rilevanza ai fini della verifica del rispetto dei livelli di servizio, deve essere formalizzata tramite email.

In caso di assistenza per malfunzionamento l'Aggiudicatario dovrà assegnare, e quindi comunicare tramite mail all'Amministrazione, un numero progressivo di richiesta (identificativo della richiesta di intervento) contestualmente alla ricezione della segnalazione con l'indicazione della data ed ora di registrazione.

I termini di erogazione del servizio di manutenzione decorreranno dall'ora di registrazione della richiesta di intervento riportata nella email inviata all'Amministrazione a seguito della segnalazione effettuata.

Si precisa che tale servizio va inteso come servizio basato su punti di contatto e modalità di accesso dedicati all'AQ, mentre il personale dell'aggiudicatario adibito a tale servizio potrà essere condiviso con altri servizi/clienti, fermo restando il rispetto degli SLA richiesti di cui al par 5.1.4.

3.2.7 Servizio di formazione e affiancamento

Il servizio di formazione e affiancamento è opzionale (sebbene oggetto di quotazione), quindi dovrà essere prestato, a pagamento, dall'Aggiudicatario solo se espressamente richiesto dall'Amministrazione.

Il servizio consente la fruizione di sessioni formative impartite presso le sedi dell'Amministrazione Contraente che permettano di istruire i discenti sulle specifiche tecnologie acquistate nell'AQ, e deve avere l'obiettivo di:

- istruire i discenti sulle principali minacce che i prodotti acquistati si prefiggono di contrastare;
- descrivere gli apparati installati in termini di caratteristiche, configurazione e funzionalità, con particolare enfasi sulle componenti software
- mettere il personale designato dall'Amministrazione Contraente in grado di provvedere alla gestione delle componenti installate in maniera autonoma ed ottimale
- descrivere le eventuali attività di integrazione effettuate con altri prodotti acquistati o con prodotti già presenti presso l'Amministrazione e le relative finalità
- realizzare demo e/o attività di test che consentano ai discenti di apprendere le principali funzionalità dei prodotti attraverso l'esperienza diretta.

È richiesto che tali attività formative siano erogate in moduli da massimo 16 ore e che per ogni modulo siano previsti al massimo 10 discenti. Ogni modulo è composto da due sezioni indicativamente di 8 ore ciascuna:

- una sezione teorica, in cui sono descritti i sistemi interessati e le relative funzionalità previste
- una sezione pratica, in cui il personale dell'Amministrazione opererà attivamente sui sistemi, secondo una modalità *traning on the job*.

Il numero dei moduli e, conseguentemente, la durata complessiva del servizio sarà concordata con l'Amministrazione Contraente sulla base dei sistemi richiesti, del grado di conoscenza dei discenti e del loro numero.

Il servizio di addestramento dovrà essere svolto da personale dotato di conoscenza ed esperienza all'insegnamento dello specifico argomento e nel "*Piano Operativo*" ne dovranno essere dettagliati programma, sessioni e durata complessiva, nonché fornito il Curriculum vitae di ciascun docente previsto. L'organizzazione del corso sarà in ogni caso concordata con l'Amministrazione Contraente che avrà la facoltà di chiedere la sostituzione del docente in caso di non idoneità.

Sulla base della complessità dei sistemi forniti e sulla base del grado di preparazione e conoscenza dei sistemi medesimi da parte del personale dell'Amministrazione che parteciperà al corso e a valle della presentazione del programma di addestramento da parte dell'Aggiudicatario, l'Amministrazione Contraente potrà apportare opportune modifiche al programma di addestramento, presentato in fase preliminare, al fine di massimizzarne l'efficacia.

Sarà a carico dell'Aggiudicatario la predisposizione di una scheda di valutazione che rispecchi gli argomenti riportati nel programma del corso di addestramento specifico e preveda una valutazione del trattamento degli stessi da parte del personale dell'Amministrazione Contraente partecipante al corso con tre livelli di gradimento, di cui uno insufficiente. Al termine di ciascuna sessione l'Amministrazione Contraente valuterà le schede compilate dai partecipanti e, in caso di una valutazione negativa da parte di almeno il 30% dei partecipanti, dovrà essere ripetuta la sessione per gli argomenti che hanno avuto gradimento negativo.

In seguito alla valutazione positiva effettuata dall'Amministrazione, a conclusione del corso l'Aggiudicatario rilascerà all'Amministrazione Contraente un "*Verbale di erogazione del Corso*" attestante la data di effettiva erogazione del servizio, la durata effettiva, il programma effettivamente seguito ed eventuali criticità emerse.

Le date di erogazione del servizio in oggetto e il programma dovranno essere preventivamente previste e concordate nel "*Piano Operativo*" e il rispetto dei menzionati termini è monitorato e soggetto, in caso di inadempienza, alla specifica penale di cui al par. 6.

La fatturazione del servizio potrà essere effettuata dall'Aggiudicatario soltanto in seguito all'esito positivo della verifica e valutazione sull'andamento del corso sopra descritta, ossia dalla data riportata nel "*Verbale di erogazione del Corso*".

Il servizio potrà essere acquisito solo contestualmente ai prodotti. In fase di offerta è richiesto al Concorrente di esprimere un prezzo per modulo formativo come in precedenza descritto.

4 GESTIONE DELLA FORNITURA

4.1 Accordo Quadro

Ai fini della gestione dell'Accordo Quadro, ogni Aggiudicatario dovrà indicare un **Responsabile unico delle attività contrattuali (RUAC)**, i cui compiti e requisiti professionali sono descritti nel Capitolato Tecnico Generale.

4.2 Contratto Esecutivo

L'Amministrazione Contraente dovrà individuare nell'OdF o nel proprio *Piano dei Fabbisogni* un "*Responsabile dell'Amministrazione*" che sarà responsabile della direzione e del coordinamento delle attività.

Come riportato ai par.2.1 e 2.2, sarà definito il "*Responsabile del Fornitore*" che dovrà lavorare in accordo con il "*Responsabile dell'Amministrazione"* per tutte le attività legate alla pianificazione ed al controllo delle attività e i cui compiti e requisiti professionali sono descritti nel Capitolato Tecnico Generale.

4.3 Reporting per le Amministrazioni

4.3.1 Dati per l'Amministrazione Aggiudicatrice

Flusso dati relativi ai livelli di servizio
Su richiesta dell'Amministrazione Aggiudicatrice, l'Aggiudicatario dovrà rendere disponibili i dati di dettaglio relativi ai livelli di servizio effettivamente conseguiti per la fornitura e l'erogazione dei servizi contrattualizzati. L'Aggiudicatario dovrà presentare tale reportistica all'Amministrazione Aggiudicatrice entro 30 giorni solari dalla richiesta.
L'Aggiudicatario dovrà garantire elevati livelli di riservatezza nel trattamento delle informazioni documentali.

Reportistica sulla situazione del personale di cui al par. 2.4 del Capitolato Tecnico Parte Generale
Su richiesta dell'Amministrazione Aggiudicatrice, l'Aggiudicatario di ciascun lotto dovrà produrre, entro 6 mesi ed entro 18 mesi (in questo secondo caso, su richiesta scritta di Consip) dalla stipula dell'Accordo Quadro, un report specifico relativo ai contratti esecutivi stipulati alla data di effettuazione della richiesta e finanziati, in tutto o in parte, con le risorse previste dal Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021 e dal Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, nonché dal PNC, relativo alla situazione del personale impiegato, che dia evidenza almeno dei seguenti elementi:

- per ciascun contratto esecutivo finanziato:

- personale in forza impiegato nell'ambito di ciascun contratto, di genere maschile, femminile e di età inferiore ai 36 anni necessario per l'esecuzione del contratto esecutivo o per la realizzazione delle attività ad esso connesse o strumentali;
- nuove assunzioni di personale di età inferiore ai 36 anni e personale femminile necessarie per l'esecuzione del contratto esecutivo o per la realizzazione delle attività ad esso connesse o strumentali;
- quota delle nuove assunzioni, calcolata come il rapporto tra il personale neoassunto di genere femminile e il personale di età inferiore ai 36 anni rispetto al totale delle nuove assunzioni.

Qualora per l'esecuzione dei contratti esecutivi sopra indicati, l'Aggiudicatario faccia ricorso all'istituto del subappalto, la reportistica sopra descritta dovrà essere integrata anche con i dati relativi al personale del subappaltatore.

Tale reportistica dovrà essere firmata digitalmente dal Legale Rappresentante del Fornitore.

Per ciascun contratto esecutivo che presenti una percentuale di nuove assunzioni inferiore alla quota minima del 30% prescritta al par. 2.4 del Capitolato Tecnico Parte Generale, l'Amministrazione Aggiudicatrice applicherà la penale di cui al paragrafo 6.

4.3.2 Dati per le Amministrazioni Contraenti

Servizio di fatturazione e rendicontazione per le Amministrazioni Contraenti

La fatturazione dei servizi sarà generalmente indirizzata alle Unità Ordinanti, salvo diverse disposizioni da parte delle singole Amministrazioni.

La struttura della fattura dovrà recepire le specifiche esigenze dell'Amministrazione ordinante. L'Aggiudicatario dovrà per questo garantire la disponibilità di dati sia analitici che sintetici su supporto elettronico, nonché la possibilità di personalizzazioni.

In particolare i dati della fattura devono rappresentare la rendicontazione, per singola fornitura e/o servizio, relativamente a tutti i servizi prestati nell'ambito dell'Accordo Quadro.

Flusso dati relativi ai livelli di servizio

Su richiesta dell'Amministrazione Contraente, l'Aggiudicatario dovrà rendere disponibili i dati di dettaglio relativi ai livelli di servizio effettivamente conseguiti per la fornitura e l'erogazione dei servizi contrattualizzati. L'Aggiudicatario dovrà presentare tale reportistica all'Amministrazione entro 30 giorni solari dalla richiesta.

L'Aggiudicatario dovrà garantire elevati livelli di riservatezza nel trattamento delle informazioni documentali.

Reportistica sulla situazione del personale di cui al par. 2.4 del Capitolato Tecnico Parte Generale

Il Fornitore dovrà produrre all'Amministrazione Contraente, entro 10 giorni lavorativi dalla stipula del Contratto esecutivo, idonea reportistica volta a documentare il rispetto dell'impegno eventualmente assunto con riguardo al sub-criterio ID 12.5, che dia evidenza almeno dei seguenti elementi:

- personale in forza impiegato nell'ambito ciascun contratto, di genere maschile, femminile, di età inferiore ai 36 anni e persone disabili, necessario per l'esecuzione del contratto esecutivo o per la realizzazione delle attività ad esso connesse o strumentali;

- nuove assunzioni di persone disabili, personale di età inferiore ai 36 anni e personale femminile, necessarie per l'esecuzione del contratto esecutivo o per la realizzazione delle attività ad esso connesse o strumentali;
- quota delle nuove assunzioni, calcolata come il rapporto tra il personale neoassunto di genere femminile, di età inferiore ai 36 anni e di persone disabili, rispetto al totale delle nuove assunzioni.

Qualora per l'esecuzione del contratto esecutivo, l'Aggiudicatario faccia ricorso all'istituto del subappalto, la reportistica sopra descritta dovrà essere integrata anche con i dati relativi al personale del subappaltatore.
Tale reportistica dovrà essere firmata digitalmente dal Legale Rappresentante del Fornitore.
Per ogni contratto esecutivo che presenti una percentuale di nuove assunzioni inferiore alla quota migliorativa eventualmente offerta in fase di AQ, come previsto al par. 2.4 del Capitolato Tecnico Parte Generale e al Capitolato d'Oneri, l'Amministrazione Contraente applicherà la penale di cui al paragrafo 6.

5 LIVELLI DI SERVIZIO E QUALITÀ

5.1 Service Level Agreement

I **Service Level Agreement (SLA)** definiscono i parametri di qualità del servizio che devono essere rispettati dall'Aggiudicatario.
Tutti gli SLA descritti nel presente capitolo e le relative definizioni che li caratterizzano si applicano a tutti i Lotti di Fornitura. Per ciascuno di tali parametri è stabilita una **Soglia Richiesta (SR)**, al superamento della quale scatterà il meccanismo di applicazione delle relative penali descritte nel paragrafo 6.

Tranne ove espressamente specificato, i valori dei parametri di SLA descritti nei paragrafi seguenti saranno misurati in riferimento alla **finestra temporale di erogazione dei servizi** associata al profilo di qualità richiesto dall'Amministrazione Contraente di seguito riportata:

Low Profile = LP (Business Day)	High Profile = HP (H24)
Lun-Ven 9.00 - 18.00	H24, 7 giorni su 7

Tabella 31 - Finestra di erogazione dei servizi

Per l'esecuzione delle attività richieste nei tempi previsti, l'Amministrazione dovrà consentire l'accesso alle aree interessate agli interventi.
Relativamente ai servizi di manutenzione, i guasti segnalati al servizio di help desk fornito dall'Aggiudicatario saranno codificati secondo una classe di severità (**Severity Code**), in base alla gravità del problema riscontrato. L'assegnazione dello specifico Severity Code dovrà essere repentinamente segnalata e formalizzata tramite email. Sulla base del Severity Code assegnato l'operatore del servizio di assistenza da remoto dovrà fornire una stima dei tempi di ripristino e delle modalità di intervento nel rispetto dei parametri di SLA nel seguito definiti, eventualmente avvalendosi della possibilità di effettuare una prima diagnosi da remoto.

I Severity Code sono identificati nella Tabella seguente:

Severity Code	
Severity Code 1	Guasto Bloccante: le funzionalità di base e/o maggiormente rilevanti non sono più operative o fortemente compromesse.
Severity Code 2	Disservizio: le funzionalità di base sono operative ma il loro utilizzo non è soddisfacente.

Tabella 32 – Classificazione dei Severity Code

5.1.1 SLA per l'attivazione della fornitura

Le attività di progettazione saranno monitorate sulla base dei seguenti parametri di SLA:

- **Tempo di emissione del *"Piano Operativo"***: è definito come il tempo, misurato in giorni lavorativi, che intercorre tra la data di ricezione da parte dell'Aggiudicatario del "*Piano dei Fabbisogni*" (emesso dall'Amministrazione Contraente) e la data di ricezione da parte dell'Amministrazione Contraente del "*Piano Operativo*" (cfr. paragrafo 2.2);
- **Tempo di emissione del *"Piano Operativo"* modificato**: è definito come il tempo, misurato in giorni lavorativi, che intercorre tra la data di ricezione da parte dell'Aggiudicatario della richiesta di modifiche al "*Piano Operativo*" (emessa dall'Amministrazione Contraente) e la data di ricezione da parte dell'Amministrazione Contraente del "*Piano Operativo*" modificato (cfr. paragrafo 2.2);
- **Tempo di emissione del *"Piano di lavoro generale"***: è definito come il tempo, misurato in giorni lavorativi, che intercorre tra la data di invio dell'OdF e la data di ricezione da parte dell'Amministrazione Contraente del "*Piano di lavoro Generale*" (cfr. paragrafo 2.3);
- **Tempo di emissione del *"Piano di lavoro generale"* modificato**: è definito come il tempo, misurato in giorni lavorativi, che intercorre tra la data di ricezione da parte dell'Aggiudicatario della richiesta di modifiche al *"Piano di lavoro generale"* e la data di ricezione da parte dell'Amministrazione Contraente del "*Piano di lavoro Generale*" modificato (cfr. paragrafo 2.3);

Parametro	SR
Tempo di emissione del "*Piano Operativo*"	20 giorni lavorativi
Tempo di emissione del "*Piano Operativo*" modificato	10 giorni lavorativi
Tempo di emissione del "*Piano di lavoro generale*"	10 giorni lavorativi
Tempo di emissione del "*Piano di lavoro generale*" modificato	5 giorni lavorativi

Tabella 33 - SLA per l'attivazione della fornitura

5.1.2 SLA per la consegna, installazione, configurazione e verifica

Le attività di fornitura, installazione, configurazione e verifica effettuata dall'Aggiudicatario, saranno monitorate sulla base del seguente parametro di SLA:

- ***Tempo di consegna, installazione, configurazione e verifica***: è definito come il tempo, misurato in giorni solari, che intercorre tra la data stipula del contratto e la data riportata sul "*Verbale di Fornitura*" come definito al paragrafo 3.2.2

L'Aggiudicatario dovrà effettuare la fornitura, l'installazione e le verifiche funzionali degli apparati, hardware e software, entro i tempi massimi di seguito indicati, decorrenti dalla stipula del contratto.

Parametro	SR
Tempo di consegna, installazione, configurazione e verifica	60 giorni solari

Tabella 34 - SLA per la consegna, installazione e verifica.

5.1.3 SLA per le attività di supporto alla verifica di conformità

Le attività di supporto alla verifica di conformità (a carico dell'Aggiudicatario) effettuata dalla Commissione di Verifica di Conformità nominata dall'Amministrazione Contraente, saranno monitorate sulla base dei seguenti parametri di SLA:

- ***Predisposizione seconda verifica***: è definito come il tempo, misurato in giorni solari, che intercorre tra la data riportata sul "Verbale di Verifica di Conformità" relativa alla prima verifica negativa e la data della comunicazione della disponibilità all'effettuazione della seconda verifica;
- ***(Eventuale, ad esclusiva discrezione dell'Amministrazione Contraente) Predisposizione ulteriore verifica***: è definito come il tempo, misurato in giorni solari, che intercorre tra la data riportata sul "Verbale di Verifica di Conformità" relativa alla seconda verifica negativa e la data della comunicazione della disponibilità all'effettuazione di una ulteriore verifica.

Parametro	SR
Predisposizione seconda verifica	15 giorni solari
(Eventuale, ad esclusiva discrezione dell'Amministrazione Contraente) Predisposizione ulteriore verifica	10 giorni solari

Tabella 35 - SLA per le attività di supporto alla verifica di conformità

5.1.4 SLA per i servizi di manutenzione, Contact Center ed help desk

Di seguito sono elencati i Service Level Agreement che il Concorrente dovrà soddisfare relativamente ai servizi di assistenza e manutenzione del nuovo e dell'esistente.

- ***Tempestività di risposta al disservizio:*** è definita come la percentuale che misura lo scostamento tra il tempo misurato ed i valori target (in base al profilo) in relazione alla segnalazione del disservizio da parte dell'Amministrazione Contraente al servizio di Contact Center ed help desk e la comunicazione, da parte dell'operatore del servizio di assistenza da remoto, della diagnosi di massima del disservizio e previsione su modalità e tempistiche di intervento e ripristino (compreso il Severity Code).

  Il calcolo di tale parametro sarà pari a $[(T_{RD\_XX} – VT_{RD\_XX})/VT_{RD\_XX}] \times 100$ dove:

  - T_{RD_XX} = tempo di risposta al disservizio misurato in ore nell'ambito della finestra di erogazione del servizio per il profilo *XX* (LP, HP).
  - VT_{RD_XX} = tempo di risposta al disservizio target per il profilo *XX* (LP, HP), pari a:
    - LP: 4 ore;
    - HP: 2 ore.

- ***Tempestività del tempo di intervento:*** è definita come la percentuale che misura lo scostamento tra il tempo misurato ed i valori target (in base al profilo) in relazione alla segnalazione del disservizio

da parte dell'Amministrazione Contraente al servizio di Contact Center ed help desk e l'intervento, qualora necessario, presso la sede interessata a cura del personale tecnico messo a disposizione dall'Aggiudicatario.

Il calcolo di tale parametro sarà pari a $[(T_{I\_XX} – VT_{I\_XX})/VT_{I\_XX}] \times 100$ dove:

- T_{I_XX} = tempo di intervento misurato in ore nell'ambito della finestra di erogazione del servizio per il profilo *XX* (LP, HP);
- VT_{I_XX} = tempo di intervento target per il profilo *XX* (LP, HP), pari a:
  - LP: 8 ore;
  - HP: 4 ore.

- ***Tempestività del tempo di ripristino del servizio:*** è definita come la percentuale che misura lo scostamento tra il tempo misurato ed i valori target (in base al profilo) in relazione alla segnalazione del disservizio da parte dell'Amministrazione Contraente al servizio di Contact Center ed help desk e la risoluzione dello stesso.

  Il calcolo di tale parametro sarà pari a $[(T_{RS\_XX} – VT_{RS\_XX})/VT_{RS\_XX}] \times 100$ dove:

  - T_{RS_XX} = tempo di ripristino del servizio misurato in ore nell'ambito della finestra di erogazione del servizio per il profilo *XX* (LP, HP);
  - VT_{RS_XX} = tempo di ripristino del servizio target per il profilo *XX* (LP, HP), pari a:
    Severity Code 1:
    - LP: 14 ore;
    - HP: 6 ore;

    Severity Code 2:
    - LP: 18 ore;
    - HP: 10 ore.

Si precisa che per i suddetti indicatori la misurazione delle frazioni di ora avverrà secondo quanto di seguito indicato:

- **per la prima ora di ritardo**, per minuti compresi tra 1-59, sarà considerato il valore orario superiore (ad esempio se il valore misurato è pari a 20 minuti= 0,33 ore sarà considerato pari a 1 ora);
- **per le ore successive alla prima ora di ritardo:**
  - per minuti compresi tra 1-29 sarà considerato il valore orario inferiore (ad esempio se il valore misurato è pari a 132 minuti = 2,2 ore sarà considerato pari a 2 ore);
  - per minuti compresi tra 30 – 59 sarà considerato il valore orario superiore (ad esempio se il valore misurato è pari a 165 minuti = 2,75 ore sarà considerato pari a 3 ore).

- ***Attesa per il servizio di Contact Center ed help desk:*** è definita come la percentuale, consolidata su base mensile, di chiamate risposte entro i 120 secondi nell'ambito della finestra di erogazione del servizio con operatore, misurati tra l'inizio della chiamata al servizio di Contact Center ed help desk (o dalla eventuale selezione sul risponditore automatico dell'opzione per parlare con un operatore) e la risposta dell'operatore.

- ***Percentuale di chiamate perse per il servizio di Contact Center ed help desk*:** si definisce chiamata persa quella telefonata:
    - che non ottiene risposta da un operatore entro 120 secondi;
    - a cui segue il segnale di occupato;
    - che viene messa in diretto contatto con la segreteria telefonica (soluzione ammessa solo per chiamate fuori orario di servizio con operatore).

  Detto valore viene valutato considerando il numero delle chiamate consolidato su base mensile**.**

- ***Disponibilità del servizio di Contact Center ed help desk***: è definita come la data in cui il servizio deve essere reso disponibile.

- ***Disponibilità delle informazioni di contatto relative al servizio di Contact Center ed help desk***: è definita come la data in cui il Fornitore rende disponibili le informazioni di contatto relative al servizio.

Parametro		SR
Descrizione	Severity Code	
Tempestività di risposta al disservizio		Minore o uguale a 0%
Tempestività del tempo di intervento		Minore o uguale a 0%
Tempestività del tempo di ripristino del servizio	1	Minore o uguale a 0%
	2	Minore o uguale a 0%
Attesa per il servizio di Contact Center ed help desk		Maggiore o uguale al 95%
Percentuale di chiamate perse per il servizio di Contact Center ed help desk		inferiore al 4%
Disponibilità del servizio di Contact Center ed help desk		Alla data di attivazione dell'AQ
Disponibilità delle informazioni di contatto relative al servizio di Contact Center ed help desk		Alla data di stipula dell'AQ.

Tabella 36 - SLA per i servizi di assistenza e manutenzione

5.1.5 SLA per il servizio di supporto specialistico

Di seguito sono elencati i Service Level Agreement che il Concorrente dovrà soddisfare relativamente al servizio di supporto specialistico.

- ***Tempo di presa in carico del servizio di supporto*:** è definito come il tempo, misurato in giorni lavorativi, intercorrenti tra la ricezione della "*Richiesta di attivazione del servizio di supporto*", effettuata dall'Amministrazione Contraente e la risposta dell'Aggiudicatario formalizzata nella "*Lettera di presa in carico del servizio di supporto*".

- ***Data di completamento dell'intervento:*** è definito come il tempo, misurato in giorni lavorativi, intercorrenti tra la data concordata per il completamento dell'intervento relativo al servizio di supporto (servizio svolto in modalità "*spot*") riportata nella "*Lettera di presa in carico del servizio di supporto*" e la data di effettivo completamento.

- ***Tempo di consegna dei CV delle risorse del servizio di supporto*:** è definito come il tempo, misurato in giorni solari, intercorrenti tra la data di stipula del contratto esecutivo (servizio svolto in fase iniziale o con periodicità definita) o la data di invio della "*Lettera di presa in carico del servizio di supporto*" (servizio svolto in modalità "*spot*") e la data di invio dei CV delle risorse che erogheranno il servizio di supporto specialistico.

- ***Tempo di sostituzione del personale del servizio di supporto*:** è definito come il tempo, misurato in giorni lavorativi, intercorrenti tra la ricezione della "*Richiesta di sostituzione del personale per il servizio di supporto*", effettuata dall'Amministrazione Contraente e la presentazione da parte dell'Aggiudicatario del CV della nuova risorsa in sostituzione.

Parametro	SR
Tempo di presa in carico del servizio di supporto	2 giorni lavorativi
Data di completamento dell'intervento (servizio svolto in modalità "*spot*")	0 giorni lavorativi
Tempo di consegna dei CV delle risorse del servizio di supporto (servizio svolto in fase iniziale o con periodicità definita)	20 giorni solari
Tempo di consegna dei CV delle risorse del servizio di supporto (servizio svolto in modalità "*spot*")	5 giorni solari
Tempo di sostituzione del personale del servizio di supporto	5 giorni lavorativi

Tabella 37 - SLA per il servizio di supporto specialistico

5.1.6 SLA per il servizio di hardening su client

Di seguito sono elencati i Service Level Agreement che il Concorrente dovrà soddisfare relativamente al servizio di hardening su client.

- ***Slittamento di una scadenza per il servizio di hardening su client*:** è definito come il tempo, misurato in giorni lavorativi, che intercorre tra la data prevista per il completamento di un'attività e/o la consegna di un deliverable (come previsti nel "*Piano Operativo"*) e la data di effettivo completamento e/o di effettiva consegna.

Parametro	SR
Slittamento di una scadenza per il servizio di hardening su client	0 giorni lavorativi

Tabella 38 - SLA per il servizio di hardening su client

5.1.7 SLA per il servizio di formazione e affiancamento

Di seguito sono elencati i Service Level Agreement che il Concorrente dovrà soddisfare relativamente al servizio di formazione e affiancamento.

- ***Data di avvio del servizio di formazione e affiancamento:*** è definita come la data concordata per l'avvio del servizio di addestramento, riportata nel "*Piano Operativo*".

Parametro	SR
Data di avvio del servizio di formazione e affiancamento	Valore indicato nel *"Piano Operativo"*

Tabella 39 - SLA per il servizio di formazione e affiancamento

5.1.8 SLA per la gestione della fornitura

Di seguito è elencato il Service Level Agreement che il Concorrente dovrà soddisfare relativamente alla gestione della fornitura.

- ***Tempo di consegna dei dati relativi agli SLA*:** è definito come il tempo, misurato in giorni solari, intercorrente tra la richiesta effettuata dall'Amministrazione Contraente e/o dalla Consip S.p.A. e l'effettiva ricezione dei dati;
- ***Tempo di gestione delle richieste:*** è definito come il tempo, misurato in giorni lavorativi, intercorrente tra la segnalazione del disservizio/reclamo/segnalazioni da parte dell'Amministrazione Contraente e/o dalla Consip S.p.A. e l'invio delle relative deduzioni all'Amministrazione Contraente e/o alla Consip S.p.A. da parte dell'Aggiudicatario (cfr. par. 2.4.1.1 del Capitolato Tecnico parte Generale);
- **Disponibilità del Portale della Fornitura:** definita su base mensile, come il tempo in cui tutta la catena end to end di responsabilità del Fornitore risulta disponibile (nel quale quindi Portale è interamente fruibile) ed il tempo di misurazione (cfr par. 4.1 del Capitolato Tecnico Parte Generale). Per la quantificazione dell'effettiva disponibilità del Portale raggiunta nel mese, si calcoleranno i

tempi di indisponibilità risultanti dalle comunicazioni con il Contact Center relativamente alla segnalazione del guasto/malfunzionamento/disservizio e alla sua risoluzione. Si precisa a tal proposito che non saranno considerati ai fini del calcolo della disponibilità del Portale eventuali "ticket" riconducibili a malfunzionamenti imputabili all'utente o ad elementi della catena end-to-end al di fuori della responsabilità del Fornitore, quali la rete internet.

Parametro	SR
Tempo di gestione delle richieste	3 giorni lavorativi
Tempo di consegna dei dati relativi agli SLA	30 giorni solari
Disponibilità del Portale della Fornitura	100%

Tabella 40 - SLA per la gestione della fornitura

5.1.9 Miglioramento dei SLA

Gli Offerenti potranno proporre dei SLA migliorati in accordo con la seguente tabella.

SLA	
Requisiti migliorativi	
ID	Caratteristica
14.1	Tempo di emissione del "*Piano Operativo*": 15 giorni lavorativi
14.2	Tempo di emissione del "*Piano Operativo*" modificato: 7 giorni lavorativi
14.3	Tempo di consegna, installazione, configurazione e verifica: 50 giorni solari
	Tempestività del tempo di intervento
14.4	Profilo LP: 6 ore
14.5	Profilo HP: 3 ore
	Tempestività del tempo di ripristino del servizio
14.6	Profilo LP - Severity Code 1: 12 ore
14.7	Profilo LP - Severity Code 2: 16 ore
14.8	Profilo HP - Severity Code 1: 4 ore
14.9	Profilo HP - Severity Code 2: 8 ore

Tabella 41 - Requisiti migliorativi relativi ai SLA

5.2 Monitoraggio della qualità erogata

Consip/AGID e/o le Amministrazioni Contraenti potranno monitorare:

- la struttura e qualità del *Piano di lavoro generale* e/o del *Piano operativo*;
- la qualità della fornitura e dei servizi erogati;
- la conduzione della fornitura.

Il RUAC sarà responsabile del controllo e del coordinamento, per l'intera durata dell'AQ, per tutte le attività di monitoraggio della qualità erogata. Tale figura sarà il punto di riferimento dell'Amministrazione Aggiudicatrice e/o Amministrazioni Contraenti e parteciperà ad incontri regolari con i suoi rappresentanti per l'aggiornamento sullo stato di avanzamento dell'AQ ovvero del singolo OdF, per condividere ogni azione correttiva che si rendesse necessaria per il rispetto dei livelli di servizio contrattualizzati.

Al fine del monitoraggio dei livelli di servizio da parte di Consip/AGID, l'Aggiudicatario dovrà approntare il Portale della Fornitura, descritto al paragrafo 4.1 del Capitolato Tecnico Generale.

Nel corso dell'esercizio sarà effettuato, da parte dell'Amministrazione Aggiudicatrice o azienda esterna autorizzata da essa, un monitoraggio periodico o a campione delle modalità di progettazione e di erogazione dei servizi al fine di verificare il rispetto dei parametri prescritti. L'Aggiudicatario si impegna in ogni caso a risolvere quelle condizioni di ridotta qualità che possono creare problemi alle Amministrazioni Contraenti.

L'Aggiudicatario, nel prendere atto di quanto espresso, dovrà rendere disponibile tutta la necessaria collaborazione attraverso la fornitura tempestiva dei dati necessari (su supporto informatico). L'Amministrazione Aggiudicatrice si riserva di effettuare tutte le verifiche che riterrà opportune, addebitandone all'Aggiudicatario i relativi costi nel caso esse dimostrino la non completezza o correttezza dei dati ricevuti.

6 PENALI

In caso di mancato rispetto dei parametri di SLA richiesti nel presente Documento, l'Aggiudicatario sarà tenuto a corrispondere all'Amministrazione Contraente e/o a quella Aggiudicatrice (come indicato nella colonna *"Soggetto avente diritto alla penale"* delle Tabelle seguenti), le penali di seguito riepilogate fatto salvo, in ogni caso, il risarcimento del maggior danno subito.

Parametro	Valorizzazione della penale	Soggetto avente diritto alla penale
Tempo di emissione del "*Piano Operativo*" (par. 5.1.1) e Tempo di emissione del "*Piano Operativo*" modificato (par. 5.1.1)	Per entrambi i parametri, la penale sarà così valorizzata: In caso di mancata emissione dell'ordinativo di fornitura: 100 Euro per ogni giorno solare di ritardo ovvero In caso di emissione dell'ordinativo di fornitura: 0,5‰ del valore complessivo dell'ordinativo di	Amministrazione aggiudicatrice ovvero Amministrazione Contraente

	fornitura per ogni giorno solare di ritardo	
Tempo di emissione del "*Piano di lavoro generale*" (par. 5.1.1) e Tempo di emissione del "*Piano di lavoro generale*" modificato (par. 5.1.1)	Per entrambi i parametri, la penale sarà così valorizzata: 0,5‰ del valore complessivo dell'ordinativo di fornitura per ogni giorno solare di ritardo	Amministrazione Contraente

Tabella 42 - Penali relative all'attivazione della fornitura

Parametro	Valorizzazione della penale	Soggetto avente diritto alla penale
Tempo di consegna, installazione, configurazione e verifica (par. 5.1.2)	1‰ del valore complessivo dell'ordinativo di fornitura per ogni giorno solare di ritardo	Amministrazione Contraente

Tabella 43 - Penali relative alla consegna, installazione, configurazione e verifica

Parametro	Valorizzazione della penale	Soggetto avente diritto alla penale
Predisposizione seconda verifica (par. 5.1.3)	1‰ del valore complessivo dell'ordinativo di fornitura per ogni giorno solare di ritardo.	Amministrazione Contraente
Predisposizione ulteriore verifica collaudo (par. 5.1.3)	1‰ del valore complessivo dell'ordinativo di fornitura per ogni giorno solare di ritardo.	Amministrazione Contraente
Esito negativo seconda verifica (o successive) (par. 5.1.3)	500 Euro	Amministrazione Contraente

Tabella 44 - Penali relative alle attività di supporto alla verifica di conformità

Parametro	**Valorizzazione della penale**	**Soggetto avente diritto alla penale**
Tempestività di risposta al disservizio (par. 5.1.4)	20€ per ogni punto percentuale di scostamento rispetto al valore target.	Amministrazione Contraente

Tempestività di intervento (par. 5.1.4)	20€ per ogni punto percentuale di scostamento rispetto al valore target.	Amministrazione Contraente
Tempestività di ripristino del servizio - Severity Code 1 (par. 5.1.4)	50€ per ogni punto percentuale di scostamento rispetto al valore target.	Amministrazione Contraente
Tempestività di ripristino del servizio - Severity Code 2 (par. 5.1.4)	30€ per ogni punto percentuale di scostamento rispetto al valore target.	Amministrazione Contraente
Attesa per il servizio di Contact Center ed help desk (par. 5.1.4)	300,00 € per ogni punto percentuale in diminuzione rispetto al 95% dei campioni di misura del parametro, calcolato su un periodo di osservazione mensile	Amministrazione Aggiudicatrice
Percentuale di chiamate perse per il servizio di Contact Center ed help desk (par. 5.1.4)	1.000,00 euro per ogni punto percentuale in aumento rispetto al numero dei campioni di misura del parametro, calcolato su un periodo di osservazione mensile	Amministrazione Aggiudicatrice
Disponibilità del servizio di Contact Center ed help desk (par. 5.1.4)	200 Euro per ogni giorno solare di ritardo	Amministrazione Aggiudicatrice
Disponibilità delle informazioni di contatto relative al servizio di Contact Center ed help desk (par. 5.1.4)	100 Euro per ogni giorno solare di ritardo	Amministrazione Aggiudicatrice

Tabella 45 - SLA per i servizi di assistenza e manutenzione

Parametro	Valorizzazione della penale	Soggetto avente diritto alla penale
Tempo di presa in carico del servizio di supporto (cfr. 5.1.5)	1‰ del valore del servizio per ogni giorno lavorativo di ritardo	Amministrazione Contraente
Data di completamento dell'intervento (cfr. 5.1.5)	1‰ del valore del servizio per ogni giorno lavorativo di ritardo	Amministrazione Contraente
Tempo di consegna dei CV delle risorse del servizio di supporto (cfr. 5.1.5)	1‰ del valore del servizio per ogni giorno lavorativo di ritardo	Amministrazione Contraente
Tempo di sostituzione del personale del servizio di supporto (cfr. 5.1.5)	1‰ del valore del servizio per ogni giorno lavorativo di ritardo	Amministrazione Contraente

Tabella 46 - Penali relative al servizio di supporto specialistico

Parametro	Valorizzazione della penale	Soggetto avente diritto alla penale
Slittamento di una scadenza per il servizio di hardening su client (cfr. 5.1.6)	1‰ del valore del servizio per ogni giorno lavorativo di ritardo	Amministrazione Contraente

Tabella 47 - **Penali relative al servizio di hardening su client**

Parametro	Valorizzazione della penale	Soggetto avente diritto alla penale
Data di avvio del servizio di formazione e affiancamento (cfr.5.1.7)	100 € per ogni giorno lavorativo di ritardo	Amministrazione Contraente

Tabella 48 - **Penali relative al servizio di addestramento sulla fornitura**

Parametro	Valorizzazione della penale	Soggetto avente diritto alla penale
Tempo di gestione delle richieste (par. 5.1.8)	150 € per ogni giorno lavorativo di ritardo	Amministrazione Aggiudicatrice
	150 € per ogni giorno lavorativo di ritardo	Amministrazione Contraente
Tempo di consegna dei dati relativi agli SLA (par. 5.1.8)	100 € per ogni giorno solare di ritardo	Amministrazione Aggiudicatrice
	100 € per ogni giorno solare di ritardo	Amministrazione Contraente
Disponibilità del Portale della Fornitura	Euro 30,00 per ogni punto decimale (0,1 %) di scostamento tra il valore percentuale misurato ed il valore richiesto dal Capitolato Tecnico	Amministrazione Aggiudicatrice
Attivazione del Portale della Fornitura (par. 4.1 del Capitolato Tecnico parte Generale)	Euro 1.000,00 per ogni giorno solare di ritardo	Amministrazione Aggiudicatrice

Tabella 49 - Penali relative alla gestione della fornitura

Parametro	Valorizzazione della penale	Soggetto avente diritto alla penale
Reportistica sulla situazione del personale di cui al par. 2.4 del Capitolato Tecnico Parte Generale (Rispetto della quota minima del 30%)	Per ciascun contratto esecutivo finanziato, Euro 2000, per ogni giorno di ritardo dalla trasmissione del report che rilevi una quota percentuale inferiore a quella minima, fino al giorno di regolarizzazione della stessa. Il mancato invio del report comporterà l'applicazione della medesima penale	Amministrazione Aggiudicatrice
Reportistica sulla situazione del personale di cui al par. 2.4 del Capitolato Tecnico Parte Generale (Rispetto della quota migliorativa eventualmente offerta)	Per ciascun contratto esecutivo finanziato, Euro 2000, per ogni giorno di ritardo dalla trasmissione del report che rilevi una quota percentuale inferiore a quella migliorativa offerta, fino al giorno di regolarizzazione della stessa. Il mancato invio del report comporterà l'applicazione della medesima penale.	Amministrazione Contraente

Tabella 50 – Penale relativa alla situazione del personale di cui al par. 2.4 del Capitolato Tecnico Parte Generale