CONDIZIONI DI FORNITURA – PARTE SPECIALE

ID 2174 - GARA A PROCEDURA APERTA PER L'AFFIDAMENTO DI UN ACCORDO QUADRO IN UN UNICO LOTTO AI SENSI DELL'ART. 54 COMMA 4 LETT.C) PER LA FORNITURA DI PRODOTTI PER LA GESTIONE DEGLI EVENTI DI SICUREZZA E DEGLI ACCESSI, LA PROTEZIONE DEI CANALI EMAIL, WEB E DATI ED EROGAZIONE DI SERVIZI CONNESSI PER LE PUBBLICHE AMMINISTRAZIONI

SOMMARIO

Indice delle Tabelle

1 PREMESSA

Il presente documento ha l'obiettivo di descrivere i requisiti minimi e le caratteristiche migliorative dei prodotti per **l'orchestrazione e la correlazione degli eventi di sicurezza e per la protezione dei dati e degli accessi privilegiati e dei relativi servizi connessi**, che riguardano la presente procedura di gara.

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

Il fornitore si impegna, **pena l'esclusione dalla gara**, ad offrire beni e servizi che posseggano almeno i requisiti minimi come richiesti nella documentazione di gara nel suo complesso. Saranno oggetto di valutazione esclusivamente le caratteristiche migliorative indicate nelle Informazioni sulla procedura.

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 ai sensi dell'art. 54, comma 4 lett. c) del D. Lgs. n. 50/2016. La fase di identificazione dei vincitori dell'AQ (che potranno essere quindi gli assegnatari dei successivi Appalti Specifici) è anche denominata "prima fase";
- **Aggiudicatario** o **Fornitore**: le imprese, i Raggruppamenti Temporanei di Imprese o i Consorzi che risultano Aggiudicatari della gara (in riferimento alla prima fase) ovvero dei singoli AS (in riferimento alla seconda fase);
- **Amministrazione Aggiudicatrice**: Consip S.p.A.;
- **Amministrazione Contraente/Amministrazione/i**: le Amministrazioni Pubbliche legittimate all'utilizzo dell'Accodo Quadro;
- **API:** application programming interface;
- **Appalto Specifico (AS)**: Procedura di gara realizzata autonomamente dall'Amministrazione Contraente tra gli aggiudicatari dell'AQ e secondo le regole disciplinate nell'AQ stesso. La fase di identificazione dello specifico vincitore dell'AS è anche denominata "seconda fase";
- **Bene**: rappresenta un oggetto di fornitura richiesto in fase di AQ, caratterizzato da una descrizione funzionale e da caratteristiche minime obbligatorie e da caratteristiche migliorative che potranno essere eventualmente offerte;
- **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 dopo l'aggiudicazione dell'Appalto Specifico;
- **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;
- **Giorno lavorativo**: da lunedì a venerdì, esclusi sabato e festivi;

- **Meta-prodotto**: rappresenta l'offerta di riferimento per ogni bene richiesto in prima fase. Ogni meta-prodotto è caratterizzato dalla sua descrizione funzionale, da requisiti minimi, da eventuali requisiti migliorativi offerti in prima fase e da un prezzo di riferimento che non potrà essere superato in AS, **ma non da una specifica tecnologia** (marca, modello, release firmware/software);
- **Prodotto**: rappresenta uno specifico prodotto (marca, modello, release firmware/software) offerto in seconda fase come istanza del meta-prodotto offerto in prima fase. Lo specifico prodotto offerto avrà quindi descrizione funzionale, requisiti minimi, requisiti migliorativi del corrispondente meta-prodotto offerto in prima fase ed eventuali ulteriori requisiti migliorativi offerti in base alle richieste dell'Amministrazione Contraente. Il prezzo del prodotto non potrà superare quello del corrispondente meta-prodotto a meno di quanto espressamente previsto nelle Informazioni sulla procedura;
- **Offerta Tecnica**: il documento redatto dal Concorrente in risposta alla gara alla quale il presente documento fa riferimento;
- **Portale della fornitura**: il Portale implementato dal Fornitore aggiudicatario secondo le specifiche tecniche descritte nelle Condizioni di fornitura parte Generale al paragrafo 4.1
- **Servizi Base**: i servizi, a condizioni non tutte definite, che possono essere richiesti dalle Amministrazioni a completamento della fornitura richiesta in AS, ad eccezione dei servizi inclusi nella fornitura che dovranno essere obbligatoriamente erogati;
- **Servizi Aggiuntivi**: i servizi, a condizioni da definire da parte delle Amministrazioni, che possono essere richiesti a completamento della fornitura prevista in AS. L'Amministrazione potrà valorizzare i servizi accessori secondo le regole riportate nelle Informazioni sulla procedura;
- **Sistema telematico (o semplicemente "Sistema")**: indica la piattaforma telematica attraverso cui saranno gestiti gli Appalti Specifici;
- **Unità Ordinante/i**: gli Uffici e le persone fisiche delle Amministrazioni Contraenti abilitati a esperire gli Appalti Specifici;
- **Responsabile dell'Amministrazione:** la persona indicata dall'Amministrazione nel contratto esecutivo 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 nelle Condizioni di fornitura parte 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 nelle Condizioni di fornitura parte Generale;
- **Jflow/SFlow/Netflow:** protocolli per la raccolta di informazioni e per il monitoraggio del traffico IP;
- **STIX:** Structured Threat Information eXpression;
- **XML:** linguaggio di programmazione eXtensible Markup Language;
- **TAXII:** Trusted Automated eXchange of Indicator Information**;**
- **SNMP:** Simple Network Management Protocol;
- **SMTP:** Simple Mail Transfer Protocol;

- **SDK:** software development kit;
- **SSL:** protocollo secure sockets layer;
- **TLS:** protocollo transport layer security;
- **LDAP:** Lightweight Directory Access Protocol;
- **AD:** Active Directory;
- **URL:** Uniform Resource Locator**;**
- **MISP:** Malware Information Sharing Platform;
- **NTLM:** New Technology Lan Manager, protocollo di autenticazione Microsoft;
- **WCCP:** Web Cache Communication Protocol;
- **ICAP:** Internet content adaptation protocol;
- **UBA:** user behavior analytics;
- **SQL:** structured query language;
- **HSM:** hardware security module;
- **OCR:** optical character recognition;
- **FTP/FTPS:** file transfer protocol/ FTP Secure;
- **SFTP:** SSH file transfer protocol;
- **MDM:** mobile device management;
- **CASB:** cloud access security broker;
- **SSH:** secure shell;
- **MFA:** multi - factor authentication;
- **OWASP:** organizzazione "Open Web Application Security Project";
- **JSON:** formato per lo scambio di dati JavaScript Object Notation;
- **LDAP:** Lightweight Directory Access Protocol;
- **PCI/DSS:** Payment Card Industry Data Security Standard;
- **VPN:** virtual private network;
- **SIEM:** security information & event management;
- **SOAR:** Security Orchestration, Automation and Response
- **SEG:** secure email gateway;
- **SWG:** secure web gateway:
- **WAF**: web application firewall;
- **PAM:** privileged access management;
- **DLP:** data loss prevention;
- **SOC:** security operations center;
- **CERT:** Computer Emergency Response Team;
- **CSIRT:** Computer Security Incident Response Team;
- **EPS**: eventi per secondo;
- **Vendor/produttore:** si intende il produttore dello specifico bene.

1.2 Oggetto

I beni richiesti sono:

- Security Information and Event Management (SIEM)
- Security Orchestration, Automation and Response (SOAR)
- Secure Email Gateway (SEG)
- Secure Web Gateway (SWG)
- Database Security (DB Security)
- Data Loss Prevention (DLP)
- Privileged Access Management (PAM)
- Web Application Firewall (WAF).

I servizi base connessi alla fornitura richiesti sono:

- installazione e configurazione (inclusi nella fornitura)
- formazione e affiancamento
- manutenzione
- Contact Center ed Help Desk (incluso nel complesso dei corrispettivi previsti)
- hardening su client
- supporto specialistico

I servizi aggiuntivi connessi alla fornitura richiesti sono:

- hardening su altri sistemi
- Data Assessment
- Privileged Account Assessment
- servizi professionali erogati dal vendor
- servizio di incident response.

1.3 Durata

La durata temporale dell'AQ è fissata in 24 mesi dalla data di attivazione. Entro tale termine le Amministrazioni Contraenti potranno esperire i propri Appalti Specifici i quali, a loro volta, potranno avere durata massima pari a 24 mesi.

1.4 Modalità di offerta in AQ/AS

Si precisa che in prima fase (AQ) i Concorrenti dovranno offrire, per ogni bene richiesto, un **meta-prodotto**, come in precedenza definito. **Non è quindi richiesto ai Concorrenti di riportare, in relazione ai beni richiesti, alcuna specifica tecnologia (intesa come marca, modello, release firmware/software) che dovrà essere**

indicata unicamente in risposta ai vari Appalti Specifici e potrà, di volta in volta, essere differente anche in base alle eventuali personalizzazioni, funzionalità aggiuntive e requisiti migliorativi espressi dall'Amministrazione Contraente in seconda fase.
Rimane in ogni caso fermo che ogni aggiudicatario dell'AQ dovrà offrire in seconda fase dei **prodotti che dovranno possedere obbligatoriamente tutti i requisiti minimi richiesti nel presente documento e i requisiti migliorativi dei corrispondenti meta-prodotti offerti in prima fase**.

Gli Offerenti dovranno **offrire una quotazione economica per tutti i beni e le relative fasce dimensionali e/o prestazionali** richieste.

In relazione ai servizi base connessi, è richiesta una quotazione economica specifica unicamente per:

- manutenzione
- hardening su client
- supporto specialistico
- formazione e affiancamento.

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.
I prezzi offerti in tale prima fase saranno utilizzati dalle Amministrazioni Contraenti **per costruire la base d'asta dei propri AS,** in funzione delle proprie specifiche esigenze, **secondo i vincoli che sono puntualmente descritti nelle Informazioni sulla procedura.**
In fase di AS inoltre l'Amministrazione potrà:

- definire ulteriormente le proprie specifiche esigenze personalizzando i beni e/o i servizi richiesti nei limiti di quanto previsto all'interno del presente documento. Tali personalizzazioni **non prevedono alcun corrispettivo ulteriore** rispetto al prezzo previsto in prima fase e quindi ogni Aggiudicatario dell'AQ potrà offrire, per il relativo prodotto/servizio, un prezzo che è **al massimo pari** al prezzo offerto in prima fase;
- richiedere funzionalità/caratteristiche aggiuntive dei beni e/o servizi connessi aggiuntivi, nei limiti di quanto previsto nel presente documento, per le quali l'Amministrazione dovrà determinare la relativa sotto base d'asta **secondo i vincoli che sono puntualmente descritti nelle Informazioni sulla procedura.**

Si riporta di seguito una schematizzazione di quanto descritto.

AQ – Prima Fase		
Consip S.p.A.	**Offerente**	
	Elementi tecnici	**Elementi economici**
Richiede *Beni* con caratteristiche minime e migliorative	Per ogni *Bene* richiesto offre un ***meta-prodotto*** con caratteristiche	Per ogni ***meta-prodotto*** offre un prezzo di riferimento

	minime ed eventuali caratteristiche migliorative	
Richiede *Servizi Base* con caratteristiche minime e migliorative Descrive i *Servizi Aggiuntivi* che potranno essere puntualmente definiti in seconda fase	Per ogni *Servizio Base* richiesto descrive le modalità previste nella Relazione Tecnica di AQ, in accordo con i requisiti minimi e le eventuali caratteristiche migliorative.	Per ogni *Servizio Base* offre un prezzo di riferimento
AS – Seconda Fase		
Amministrazione Contraente	**Aggiudicatario dell'AQ**	
	Elementi tecnici	**Elementi economici**
Richiede, tra i *Beni* previsti in AQ, quelli peculiari al suo AS. Adatta la sua richiesta inserendo eventuali requisiti migliorativi e/o funzionalità e caratteristiche aggiuntive in accordo con quanto previsto nell'AQ	Per ogni *Bene* richiesto offre un ***prodotto*** specifico, indicando marca, modello, release firmware/software. Il prodotto offerto ha obbligatoriamente le caratteristiche minime e le caratteristiche migliorative del corrispondente meta-prodotto offerto in prima fase ed eventuali requisiti migliorativi e/o funzionalità e caratteristiche aggiuntive in accordo con la richiesta dell'Amministrazione Contraente.	Per ogni ***prodotto*** offre un prezzo che non potrà essere superiore al prezzo del corrispondente meta-prodotto offerto in prima fase, a meno che l'Amministrazione Contraente abbia richiesto delle funzionalità e delle caratteristiche aggiuntive associate, per le quali ne determina la corrispondente base d'asta, in accordo con quanto previsto nell'AQ.
Richiede, tra i *Servizi Base* previsti in AQ, quelli peculiari al suo AS. Adatta la sua richiesta prevedendo *Servizi Aggiuntivi* o eventuali personalizzazioni dei *Servizi Base* in accordo con quanto previsto nell'AQ	Per ogni *Servizio Base* richiesto descrive le modalità previste nella Relazione Tecnica di AS, in accordo con i requisiti minimi e migliorativi dei servizi offerti in prima fase e con le eventuali personalizzazioni richieste dall'Amministrazione Contraente. Per ogni *Servizio Aggiuntivo* richiesto descrive le modalità previste nella Relazione Tecnica di AS, in accordo con le richieste dall'Amministrazione Contraente	Per ogni *Servizio Base* richiesto offre un prezzo che non potrà essere superiore al prezzo del corrispondente servizio offerto in prima fase. Per ogni *Servizio Aggiuntivo* richiesto offre un prezzo che non potrà essere superiore al prezzo a base d'asta autonomamente determinato dall'Amministrazione Contraente in accordo con quanto previsto nell'AQ.

Tabella 1 - Modalità di offerta in AQ/AS

2 DESCRIZIONE DELLA FORNITURA

Nel presente capitolo si riportano le specifiche di dettaglio dei beni e le modalità di erogazione dei servizi base oggetto della presente iniziativa. Si riportano inoltre i servizi aggiuntivi che potranno essere richiesti e puntualmente definiti dall'Amministrazione Contraente nel proprio AS.

Al Concorrente è richiesta un'offerta su tutte le tipologie di beni e servizi base elencati nel presente documento.
Si ribadisce che, come evidenziato nel precedente paragrafo 1.4, in prima fase (AQ) **non è richiesto agli Offerenti di riportare, in relazione ai beni richiesti, alcuna specifica tecnologia**. Quindi **la tecnologia offerta (intesa come marca, modello, release firmware/software) dovrà essere indicata in risposta ai vari Appalti Specifici** e potrà, di volta in volta, essere differente anche in base agli eventuali requisiti migliorativi espressi dall'Amministrazione Contraente in seconda fase. Rimane in ogni caso fermo che **i prodotti puntualmente declinati in seconda fase dovranno possedere obbligatoriamente tutti i requisiti minimi richiesti nel presente documento e i migliorativi eventualmente offerti in prima fase.**

2.1 Beni

Qualora il Concorrente intenda offrire meta-prodotti che possiedano caratteristiche migliorative, dovrà prevedere e includere nella fornitura, che si perfezionerà nell'ambito degli AS, tutto quanto necessario alla corretta installazione e/o utilizzo delle caratteristiche migliorative stesse, a meno di specifiche indicazioni riportate nel presente documento.

Il prezzo che sarà offerto per i prodotti in fase di AS **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**. Nei prezzi offerti in AQ i Concorrenti dovranno quindi considerare sia le attività di installazione e configurazione sia 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 2.2.1.2. L'Aggiudicatario di ogni AS 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.

In fase di AS tutti i prodotti che saranno offerti dovranno:

- in caso essi siano costituiti da un apparato hardware, essere forniti con gli alimentatori/Power Supply Unit necessari alla loro corretta alimentazione e con il necessario corredo di cavi per permettere una corretta posa in opera ed installazione;
- essere, **a pena esclusione**, necessariamente già commercializzati o commercializzabili alla data di presentazione delle offerte tecniche ed economiche del singolo AS, implementando tutte le funzionalità minime e migliorative offerte in AQ ed eventualmente quelle ulteriori richieste dall'Amministrazione Contraente e offerte in fase di AS.

2.1.1 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 applicabili al Fornitore stesso 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).

Tutte le apparecchiature che saranno fornite in fase di AS 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 in materia di sicurezza:

- **Legge 1 marzo 1968, n. 186** "disposizioni concernenti la produzione di materiali, apparecchiature, macchinari, installazioni e impianti elettrici ed elettronici";
- **Decreto Legislativo del 19 maggio 2016 n. 86,** "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,** "attuazione della direttiva 2011/65/UE sulla restrizione dell'uso di determinate sostanze pericolose nelle apparecchiature elettriche ed elettroniche";
- **D. Lgs. 3 aprile 2006, n. 152**, "Norme in materia ambientale";
- **D. Lgs. 18 maggio 2016, n. 80,** "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 14 marzo 2014, n. 49 e s.m.i.,** "attuazione della direttiva 2012/19/UE sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE)".

Inoltre, tutti i prodotti forniti dovranno essere:

1. stati progettati, testati e controllati in termini di sicurezza prima di essere commercializzati;
2. 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;
3. provvisti di regolare marcatura "CE";
4. conformi alle normative CEI o ad altre disposizioni europee riconosciute e, in generale, alle vigenti norme legislative, regolamentari e tecniche disciplinanti i componenti e le modalità di impiego degli stessi anche nel rispetto dei requisiti in materia di sicurezza elettrica, emissioni/compatibilità elettromagnetica e sostanze pericolose. La conformità a standard non europei è considerata rispondente al requisito richiesto purché tali standard siano equivalenti o maggiormente stringenti di quelli EN. Tutte le estensioni degli standard di riferimento devono essere rispettate se pertinenti agli argomenti trattati nel presente documento. Dove non esplicitamente richiesto, si riterrà pertanto attuato il pieno rispetto degli standard qui indicati e nel caso di sovrapposizione nella materia trattata dovrà essere rispettato lo standard più restrittivo.

Le prescrizioni di cui ai bullet 2, 3 e 4 non si applicano ai prodotti puramente software.

2.1.2 Requisiti del Security Information and Event Management (SIEM)

Nel presente paragrafo sono descritti i **requisiti minimi** e migliorativi relativi al **SIEM**.
Il SIEM è l'elemento che consente di raccogliere, archiviare, monitorare log e correlare eventi con l'obiettivo di identificare attacchi o violazioni di dati. Esso fornisce un utile strumento a supporto delle attività di indagine (sia in real time sia storiche) in risposta a incidenti di sicurezza o a supporto dell'analisi forense o ancora a supporto della compliance a standard. Il SIEM consente di aggregare gli eventi che sono originati da una vasta gamma di elementi, tra cui apparati di sicurezza, apparati di rete, endpoint e applicazioni, tipicamente attraverso l'analisi dei log prodotti ma anche attraverso altre fonti, quali ad esempio il traffico di rete. I dati raccolti possono essere arricchiti con ulteriori dati di contesto, quali ad esempio utenti, asset, minacce conosciute e vulnerabilità riscontrate. Il SIEM effettua attività di normalizzazione delle informazioni raccolte dalle varie fonti, fornendo viste e report specifici che consentono di semplificare le attività di analisi della vasta mole di dati raccolta.

Per il SIEM (per il quale è richiesta la quotazione di una soluzione composta da Appliance fisica hardware e relativo software) sono richieste sei fasce dimensionali in funzione del numero di device ed eventi gestiti:

- SIEM_1 (fascia 1): fino a 50 device e massimo 300 eps;
- SIEM_2 (fascia 2): fino a 100 device e massimo 600 eps;
- SIEM_3 (fascia 3): fino a 200 device e massimo 1200 eps;
- SIEM_4 (fascia 4): fino a 500 device e massimo 3000 eps;

- SIEM_5 (fascia 5): fino a 1000 device e massimo 6000 eps;
- SIEM_6 (fascia 6): fino a 2500 device e massimo 15000 eps.

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

SIEM - Tutte le fasce
Requisiti minimi
Capacità di raccogliere i log/eventi generati dagli apparati, dai sistemi e dalle applicazioni attraverso l'utilizzo di agent e/o in modalità agent-less
Acquisizione dei log/eventi, tramite parser completi già disponibili nativamente nella soluzione, almeno dalle seguenti tipologie di sorgenti: o switch e router di almeno due dei seguenti Produttori: Cisco, Juniper, HPE, Huawei, Alcatel-Lucent; o sistemi operativi Microsoft Windows e Linux; o piattaforma di virtualizzazione VMWare; o database Oracle e Microsoft SQL Server; o web server Apache e Microsoft IIS; o application server WebLogic, WebSphere,TomCat, JBoss
Possibilità di sviluppare parser per acquisire e normalizzare i log/eventi ricevuti da ulteriori sorgenti non disponibili nativamente
Indicizzazione, compressione e memorizzazione dei log/eventi garantendone l'integrità e consentendo di impostarne la retention
Possibilità di effettuare ricerche personalizzate sui log/eventi e di esportarli almeno in CSV e/o XML
Correlazione delle informazioni di varia natura provenienti da differenti sorgenti
Possibilità di creare regole di correlazione personalizzate
Possibilità di creare utenti opportunamente profilati in modo tale da poter disporre solo di determinati diritti e solo limitatamente a determinate sorgenti o tipologie di log/eventi;
Possibilità di registrare le operazioni eseguite dagli utenti
Generazione allarmi e inoltro tramite e-mail, SMS, SNMP Traps
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 - la realizzazione di report personalizzati
Supporto Protocollo IPv6
Supporto per configurazione in alta affidabilità

Tabella 2 - Requisiti minimi SIEM

SIEM - Tutte le fasce	
Requisiti migliorativi di AQ	
ID	Caratteristica

	Acquisizione dei log/eventi, tramite parser completi già disponibili nella soluzione, anche dalle seguenti tipologie di sorgenti (1.1, 1.2, 1.3, 1.4):
1.1	o switch e router di ulteriori due Produttori (oltre ai due minimi richiesti) sempre tra i seguenti: Cisco, Juniper, HPE, Huawei, Alcatel-Lucent;
1.2	o sistema operativo Mac OS
1.3	o piattaforma di virtualizzazione KVM
1.4	o piattaforma di virtualizzazione Hyper-V
1.5	Filtraggio dei log/eventi ricevuti o prelevati dalle sorgenti per evitare che vengano elaborati e memorizzati
1.6	Possibilità di interrogare la base dati della soluzione tramite API
1.7	Possibilità di integrare piattaforme di threat intelligence tramite standard STIX/TAXII

Tabella 3 - Requisiti migliorativi di AQ SIEM

Si riportano di seguito le funzionalità aggiuntive relative alla seconda fase e i requisiti migliorativi richiedibili in fase di AS, secondo i vincoli previsti nelle Informazioni sulla procedura.

Funzionalità aggiuntive SIEM	
Funzionalità	Fase di AS Requisiti migliorativi associabili
Disponibilità della soluzione su cloud privato	N.A.
Ricezione informazioni di security threat intelligence attraverso un feed	AS.1.3
Cattura e analisi dei flussi di rete in formato NetFlow	AS.1.4 e/o AS.1.5
Analitiche per la rilevazione di potenziali minacce mediante l'esame del traffico di rete e del comportamento utente (UBA)	AS.1.6
Funzionalità che indirizzino e semplifichino la gestione della compliance al GDPR (ad. es. dashboard specifiche, etc)	AS.1.7
Configurazione in alta affidabilità	AS.1.8

Tabella 4 – Funzionalità aggiuntive SIEM

SIEM	
Requisiti migliorativi di AS	
ID	Caratteristica
AS.1.1	Acquisizione dei log/eventi, tramite parser completi già disponibili nella soluzione di specifiche sorgenti richieste dall'Amministrazione non comprese tra quelle minime e migliorative previste in AQ
AS.1.2	Integrazione con specifica piattaforma di vulnerability management richiesta dall'Amministrazione
AS.1.3	Qualità del feed di threat intelligence. Sarà premiata: - la numerosità e la varietà di fonti, fra cui fonti OSINT, utilizzate dal feed di threat intelligence; - la capacità di arricchimento degli indicatori di compromissione (threat actors, IP addresses, etc.) -l'innovatività e la capacità dei motori di machine learning di correlare le informazioni di sicurezza provenienti da varie fonti, al fine di rendere più rapida l'analisi di tali informazioni e il processo decisionale da parte degli operatori di sicurezza.

AS.1.4	Cattura e analisi dei flussi di rete anche in formato Jflow
AS.1.5	Cattura e analisi dei flussi di rete anche in formato Sflow
AS.1.6	Efficacia delle analitiche messe a disposizione per la rilevazione di potenziali minacce mediante l'analisi del traffico di rete e del comportamento utente (UBA), al fine di rilevare con accuratezza gli attacchi informatici e ridurre i tempi di indagine e i tempi di risposta associati alle minacce.
AS.1.7	Efficacia delle funzionalità che indirizzino e semplifichino la gestione della compliance al GDPR, in termini di: -semplicità e rapidità nella produzione di reportistica adeguata a comprovare lo stato di compliance su dati storici e in real time, provenienti da un'ampia varietà di sistemi IT dell'organizzazione; -semplificazione dell'attività di monitoraggio della compliance in real time; - capacità di individuare i dati associati al GDPR più a rischio.
AS.1.8	Configurazione della soluzione in alta affidabilità. Saranno valutate le modalità implementative proposte per la configurazione in alta affidabilità, in termini di disponibilità della soluzione e delle sue componenti in caso di guasto.

Tabella 5 - Requisiti migliorativi di AS SIEM

2.1.3 Requisiti del Security Orchestration, Automation and Response (SOAR)

Nel presente paragrafo sono descritti i **requisiti minimi** e migliorativi relativi al **SOAR**.
Il SOAR è l'elemento che consente di orchestrare le funzioni utili a garantire una risposta automatizzata agli incidenti di sicurezza. Il SOAR deve quindi consentire la realizzazione di workflow in seguito a determinati eventi garantendo l'integrazione con un'ampia varietà di sistemi e di applicazioni esterne con l'obiettivo di velocizzare ed efficientare le attività di gestione di risposta agli incidenti di sicurezza.

Per il SOAR (per il quale è richiesta la quotazione di una soluzione software) è richiesta la quotazione di due configurazioni così composte:

- SOAR_CT1: configurazione di tipo 1 che comprende una sottoscrizione biennale fino a 2 utenti
- SOAR_CT2: configurazione di tipo 2 che comprende una sottoscrizione biennale fino a 2 utenti e una sottoscrizione biennale per ulteriori 5 utenti aggiuntivi.

Nelle tabelle seguenti si riportano i requisiti minimi e migliorativi relativi al SOAR.

SOAR
Requisiti minimi
Orchestrazione del processo di risposta agli incidenti di sicurezza informatici attraverso l'impiego di playbook standardizzati e automatizzati.
Possibilità di mettere in relazione nuovi incidenti di sicurezza con incidenti già risolti, di identificare investigazioni duplicate, al fine di ridurre i tempi di indagine.
Possibilità di effettuare ricerche sulla base degli indicatori di compromissione
Documentazione automatica di tutti gli incidenti e delle indagini effettuate

Disponibilità di dashboard e reportistica per ricavare ed evidenziare le metriche/livelli di sevizio più significativi relativi alle procedure di incident response, misurare la loro efficacia e l'efficacia delle misure di sicurezza adottate. Possibilità di esportare la reportistica e di realizzare dei report personalizzati
Supporto protocollo IPv6

Tabella 6 - Requisiti minimi SOAR

SOAR	
Requisiti migliorativi di AQ	
ID	Caratteristica
2.1	Automazione di azioni basate su scripts
2.2	Possibilità di interrogare la base dati della soluzione tramite API
2.3	Integrabilità con piattaforme e sorgenti di eventi sicurezza tramite API e/o SDK

Tabella 7 - Requisiti migliorativi di AQ SOAR

Si riportano di seguito le funzionalità aggiuntive relative alla seconda fase e i requisiti migliorativi richiedibili in fase di AS, secondo i vincoli previsti nelle Informazioni sulla procedura.

Funzionalità aggiuntive SOAR	
Funzionalità	Fase di AS Requisiti migliorativi associabili
Ricezione di informazioni di security threat intelligence attraverso un feed	AS.2.3
Presenza di strumenti di comunicazione e collaborazione integrati che consentano la condivisione delle informazioni fra gli analisti di sicurezza	AS.2.4

Tabella 8 – Funzionalità aggiuntive SOAR

SOAR	
Requisiti migliorativi di AS	
ID	Caratteristica
AS.2.1	Varietà e numerosità delle integrazioni native con sorgenti di eventi di sicurezza (firewalls, endpoint protection, SIEM, threat intelligence, authentication, etc.) sia in fase di apertura dell'incidente informatico, sia per la raccolta di ulteriori informazioni per il triage e l'analisi degli incidenti che per la fase di remediation
AS.2.2	Integrazione con una specifica piattaforma di Service Management richiesta dall'Amministrazione
AS.2.3	Qualità del feed di threat intelligence. Sarà premiata: - la numerosità e la varietà di fonti, fra cui fonti OSINT, utilizzate dal feed di threat intelligence; - la capacità di arricchimento degli indicatori di compromissione (threat actors, IP addresses, etc.) -l'innovatività e la capacità dei motori di machine learning di correlare le informazioni di sicurezza provenienti da varie fonti, al fine di rendere più rapida l'analisi di tali informazioni e il processo decisionale da parte degli operatori di sicurezza.

AS.2.4	Efficacia, innovatività e semplicità di utilizzo degli strumenti di comunicazione e collaborazione integrati che consentano la condivisione delle informazioni fra gli analisti di sicurezza, al fine di ottimizzare la fase di risposta agli incidenti informatici.
AS.2.5	Varietà, semplicità di utilizzo dei playbook messi a disposizione della soluzione e adattabilità al contesto specifico dell'Amministrazione, al fine di semplificare e accelerare il processo di risposta agli incidenti di sicurezza

Tabella 9 - Requisiti migliorativi di AS SOAR

2.1.4 Requisiti del Secure Email Gateway (SEG)

Nel presente paragrafo sono descritti i **requisiti minimi** e migliorativi relativi ai **SEG**.
Il SEG consente una protezione dalle minacce che provengono dal canale mail attraverso il filtraggio delle mail di spam e dei contenuti dannosi. Il SEG consente l'analisi sia della posta in ingresso sia della posta in uscita consentendo quindi, su quest'ultima, anche di prevenire l'eventuale perdita di dati sensibili contenuti all'interno delle mail.

Per il SEG (per il quale è richiesta la quotazione di una soluzione composta da Appliance fisica hardware e relativo software) sono richieste cinque fasce dimensionali/prestazionali:

- SEG_1 (fascia 1): fino a 500 mail/ora
- SEG_2 (fascia 2): fino a 25000 mail/ora
- SEG_3 (fascia 3): fino a 40000 mail/ora
- SEG_4 (fascia 4): fino a 90000 mail/ora
- SEG_5 (fascia 5): fino a 350000 mail/ora

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

SEG - Tutte le fasce
Requisiti minimi
Mail Transfer Agent
Funzionalità di protezione a più livelli per l'individuazione dello SPAM e la rilevazione di minacce attraverso più meccanismi quali l'analisi approfondita del contenuto delle email e il filtraggio delle URL presenti nel corpo del messaggio
Funzionalità di anti-virus, anti-phishing, anti-BEC, anti-spoofing, anti-spam e anti-malware in grado di identificare virus, worms, ransomware attraverso il riconoscimento di signature e analisi euristica dei contenuti
Protezione da email massive e di marketing
Protezione realtime Office 365 attraverso API o SMTP relay
Identificazione di attacchi di tipo zero-day
Blocco email in base alla lingua utilizzata o specifici charset

Rimozione, tramite l'analisi del contenuto dell'email e degli allegati, di file malevoli. Identificazione, tramite analisi di tipo true file type, della tipologia di file e inclusione URLs potenzialmente pericolosi
Trattamento delle email per quali è stato identificato un virus/malware con varie opzioni quali l'invio di una notifica, la quarantena, l'eliminazione del messaggio, l'inserimento in white/black list
Supporto dei filtri basati sulla reputazione dell'indirizzo IP di provenienza e/o URL
Ispezione sulla posta in uscita e in ingresso
Crittografia dei messaggi in uscita con protollo SSL/TLS
Supporto dell'autenticazione tramite LDAP/AD
Aggiornamenti costanti delle signature attraverso feed di threat intelligence
Possibilità di bloccare mail contenenti documenti di Office che utilizzino MACRO. La soluzione deve segnalare all'amministratore/utente l'avvenuto blocco.
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 per configurazione in alta affidabilità
Supporto dei protocolli SPF, DKIM o in alternativa del protocollo DMARC

Tabella 10 - Requisiti minimi SEG

SEG - Tutte le fasce	
Requisiti migliorativi	
ID	Caratteristica
3.1	Cifratura automatica dei messaggi in uscita per i quali risultano verificate delle politiche di identificazione configurabili (policy based encryption)
3.2	Identificazione di immagini potenzialmente dannose (almeno contenuti pornografici)
3.3	Creazione di regole di spam personalizzate
3.4	Identificazione di testo nascosto all'interno di immagini presenti nelle email
3.5	Possibilità di interfacciarsi con piattaforme di threat intelligence (almeno MISP)
3.6	Possibilità interrogare la base-dati della soluzione tramite API.
3.7	Funzionalità di Data Loss Prevention nell'ispezione delle mail in uscita attraverso l'identificazione di parole chiave o pattern di dati.
3.8	Rimozione del contenuto attivo dell'email (ad esempio la rimozione di MACRO)
3.9	Funzionalità di sandboxing integrata o su cloud del Produttore
3.10	Funzionalità di Cousin Domain Detection

Tabella 11 - Requisiti migliorativi di AQ SEG

Si riportano di seguito le funzionalità aggiuntive relative alla seconda fase e i requisiti migliorativi richiedibili in fase di AS, secondo i vincoli previsti nelle Informazioni sulla procedura.

Funzionalità aggiuntive SEG	
Funzionalità	Fase di AS Requisiti migliorativi associabili
Disponibilità della soluzione su cloud privato	N.A.
Configurazione in alta affidabilità	AS.3.2

Tabella 12 – Funzionalità aggiuntive SEG

SEG	
Requisiti migliorativi di AS	
ID	Caratteristica
AS.3.1	Integrazione con soluzioni di sicurezza richieste dalla PA (soluzioni Anti APT, NGFW, SIEM, etc)
AS.3.2	Configurazione della soluzione in alta affidabilità. Saranno valutate le modalità implementative proposte per la configurazione in alta affidabilità, in termini di disponibilità della soluzione e delle sue componenti in caso di guasto.

Tabella 13 - Requisiti migliorativi di AS SEG

2.1.5 Requisiti dei Secure WEB Gateway (SWG)

Nel presente paragrafo sono descritti i **requisiti minimi** e migliorativi relativi ai **SWG**.
Il SWG consente di proteggere gli utenti dalle minacce derivanti dalla loro navigazione su Internet (download di malware, attacchi informatici…) e di far rispettare agli stessi la compliance aziendale (evitando ad esempio l'accesso a categorie di siti o siti specifici che violano le policy aziendali o che costituiscono una minaccia considerando i relativi contenuti).

Per il SWG (per il quale è richiesta la quotazione di una soluzione composta da Appliance fisica hardware e relativo software) sono richieste quattro fasce dimensionali/prestazionali:

- SWG_1 (fascia 1): fino a 1000 utenti
- SWG_2 (fascia 2): fino a 5000 utenti
- SWG_3 (fascia 3): fino a 10000 utenti
- SWG_4 (fascia 4): fino a 20000 utenti

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

SWG - Tutte le fasce
Requisiti minimi
Funzionalità: - proxy del traffico in modalità trasparente ed esplicita - capacità di filtraggio delle URL - capacità di filtraggio dei contenuti - capacità di filtraggio dei protocolli, tra cui HTTP/HTTPS/FTP - capacità di filtraggio delle applicazioni

Definizione criteri di sicurezza/filtraggio per utente e/o gruppi e definizione di blacklist/whitelist
Supporto del PAC file per l'implementazione in modalità esplicita
URL filtering database suddiviso in categorie pre-definite (almeno 40)
Identificazione dei comportamenti potenzialmente pericolosi, blocco dei siti potenzialmente malevoli o categorizzati come tali e blocco dei file in base all'estensione
Aggiornamenti costanti degli identificativi degli attacchi e classificazione e categorizzazione di nuovi siti aggiornando costantemente il Database della soluzione
Funzionalità di protezione Anti Malware e WEB/IP reputation sul traffico gestito
Identificazione attacchi di tipo zero-day
Applicazione delle policy definite anche ai dispositivi offnet. Per tale funzionalità potrà essere previsto l'utilizzo di agent di tipo tamper-proof da installare sui dispositivi remoti
Supporto dei seguenti meccanismi di autenticazione: Kerberos, NTLM, LDAP, AD
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 per configurazione in alta affidabilità
Funzionalità di SSL/TLS Inspection a livello software

Tabella 14 - Requisiti minimi SWG

SWG - Tutte le fasce	
Requisiti migliorativi	
ID	Caratteristica
4.1	Funzionalità di SSL/TLS Inspection a livello hardware su chipset dedicato
4.2	Supporto del protocollo WCCP per l'implementazione in modalità trasparente
4.3	Funzionalità di file reputation
4.4	Identificazione di testo nascosto all'interno di immagini presenti nel traffico web
4.5	Funzionalità di DLP nell'ispezione del traffico verso server (HTTP POST): - identificazione di parole chiave o pattern di dati - possibilità di effettuare fingerprinting di file/cartelle
4.6	Possibilità interrogare la base-dati della soluzione tramite API.
4.7	Possibilità di configurare delle eccezioni relativamente al traffico da non intercettare in modalità SSL inspection
4.8	Supporto del protocollo ICAP per l'integrazione con Server ICAP esterni

Tabella 15 - Requisiti migliorativi di AQ SWG

Si riportano di seguito le funzionalità aggiuntive relative alla seconda fase e i requisiti migliorativi richiedibili in fase di AS, secondo i vincoli previsti nelle Informazioni sulla procedura.

Funzionalità aggiuntive SWG	
Funzionalità	Fase di AS Requisiti migliorativi associabili
Disponibilità della soluzione su cloud privato	N.A.
Configurazione in alta affidabilità	AS.4.2

Tabella 16 – Funzionalità aggiuntive SWG

SWG	
Requisiti migliorativi di AS	
ID	Caratteristica
AS.4.1	Integrazione con soluzioni di sicurezza richieste dalla PA (soluzioni Anti APT, NGFW, SIEM, etc)
AS.4.2	Configurazione della soluzione in alta affidabilità. Saranno valutate le modalità implementative proposte per la configurazione in alta affidabilità, in termini di disponibilità della soluzione e delle sue componenti in caso di guasto.

Tabella 17 - Requisiti migliorativi di AS SWG

2.1.6 Requisiti della Database Security (DB Security)

Nel presente paragrafo sono descritti i **requisiti minimi** e migliorativi relativi alla **DB Security**.
La DB Security consente di garantire la protezione delle informazioni storicizzate nei DB da minacce che possono essere originate sia esternamente sia internamente al perimetro dell'organizzazione: fanno parte dei primi gli attacchi intenzionali da parte di hacker, fanno parte dei secondi le attività improprie, intenzionali o meno, da parte di utenti interni. Tale obiettivo è realizzato attraverso varie funzionalità che possono riguardare o le istanze dei DB o i dati gestiti da tali istanze o ancora le applicazioni che hanno accesso a tali istanze.

Per la DB Security (per la quale è richiesta la quotazione di una soluzione software) è richiesta la quotazione di ogni elemento/funzionalità relativa alle seguenti configurazioni tipo:

- DB_SEC_CT1: configurazione Tipo 1. Soluzione in alta affidabilità per la sicurezza di due istanze di DB server con le seguenti funzionalità:
  - Transparent Encryption, ossia la cifratura di dati sensibili memorizzati in tabelle o tablespaces in maniera trasparente agli utenti del DB e alle applicazioni che accedono ai dati
  - Gestione delle chiavi di cifratura
  - Security Intelligence, ossia l'identificazione e il blocco di tentativi di violazione delle policy e la conseguente generazione di alert e report specifici;

- DB_SEC_CT2: configurazione Tipo 2. Soluzione in alta affidabilità per la sicurezza di due istanze di DB server con le seguenti funzionalità:
  - Transparent Encryption, ossia la cifratura di dati sensibili memorizzati in tabelle o tablespaces in maniera trasparente agli utenti del DB e alle applicazioni che accedono ai dati
  - Gestione delle chiavi di cifratura

- Security Intelligence, ossia l'identificazione e il blocco di tentativi di violazione delle policy e la conseguente generazione di alert e report specifici;
- Data Masking e Tokenizzazione

Nelle tabelle seguenti si riportano i requisiti minimi e migliorativi relativi alla soluzione di DB Security.

DB Security
Requisiti minimi
Gestione della sicurezza dei dati at rest per la protezione e il controllo dell'accesso ai database
Controllo centralizzato delle policy e la gestione centralizzata delle chiavi di crittografia
Funzionalità di transparent ecryption su dati strutturati
Funzionalità di data masking statico e dinamico per proteggere i campi sensibili di un database
Supporto di DB relazionali (almeno DB Microsoft SQL Server, MySQL, Oracle)
Identificazione e blocco di ogni tentativo di violazione delle policy, con produzione di alert specifici e report.
Funzionalità di reportistica e logging delle attività di accesso ai DB che consentano: - il monitor in real-time attraverso dashboard - la realizzazione di report attraverso template predefiniti - la possibilità di esportare i report -la realizzazione di report personalizzati

Tabella 18 - Requisiti minimi DB Security

DB Security	
Requisiti migliorativi di AQ	
ID	Caratteristica
5.1	Possibilità di effettuare un controllo dei privilegi di accesso ai dati per singolo record e per singolo campo di record.
5.2	Possibilità di interrogare la base dati della soluzione tramite API

Tabella 1 - Requisiti migliorativi di AQ DB Security

Si riportano di seguito le funzionalità aggiuntive relative alla seconda fase e i requisiti migliorativi richiedibili in fase di AS, secondo i vincoli previsti nelle Informazioni sulla procedura.

Funzionalità aggiuntive DB Security	
Funzionalità	Fase di AS Requisiti migliorativi associabili
Supporto a DB non relazionali	AS.5.4
Funzionalità di transparent encryption su dati non strutturati	AS.5.5
Configurazione in alta affidabilità di elementi aggiuntivi non previsti in prima fase	AS.5.6
Soluzione basata su appliance fisiche	da AS 3.1 a AS 3.6
Gestione chiavi di cifratura in ambiente cloud	AS.5.7

Tabella 19 – Funzionalità aggiuntive DB Security

DB Security	
Requisiti migliorativi di AS	
ID	Caratteristica
AS.5.1	Varietà dei DB relazionali supportati (oltre ai minimi previsti in AQ)
AS.5.2	Integrazione con uno specifico sistema HSM richiesto dall'Amministrazione per la generazione e lo storage delle chiavi di crittografia
AS.5.3	Integrazione con una specifica piattaforma di SIEM richiesta dall'Amministrazione
AS.5.4	Varietà dei DB non relazionali supportati
AS.5.5	Efficacia delle funzionalità di transparent encryption su dati non strutturati. Sarà valutata la varietà e numerosità di tipologie di dati non strutturati per la quale viene resa disponibile la funzionalità richiesta
AS.5.6	Modalità per la realizzazione della configurazione in alta affidabilità. Saranno valutate le modalità implementative proposte per la realizzazione della configurazione in alta affidabilità (architettura proposta, HA nativa della soluzione offerta, HA realizzata tramite ambiente di virtualizzazione, ecc.)
AS.5.7	Varietà di ambienti cloud supportati e scalabilità in termini di numero di istanze gestibili

Tabella 20 - Requisiti migliorativi di AS DB Security

2.1.7 Requisiti della Data Loss Prevention (DLP)

Nel presente paragrafo sono descritti i **requisiti minimi** e migliorativi relativi alla **DLP**.
La DLP consente l'ispezione e la classificazione dei dati contenuti in varie fonti - quali file, mail, applicazioni - siano essi a riposo, durante il loro uso oppure durante il loro trasferimento sulla rete. Essa può inoltre prevedere l'applicazione dinamica di policy e diritti di accesso ai dati gestiti.

Per la DLP (per la quale è richiesta la quotazione di una soluzione software) sono richieste quattro fasce dimensionali per l'agent in funzione del numero di endpoint:

- DLP_1 (fascia 1): fino a 500 endpoint;
- DLP_2 (fascia 2): fino a 1000 endpoint;
- DLP_3 (fascia 3): fino a 5000 endpoint;
- DLP_4 (fascia 4): oltre i 5000 endpoint.

Nelle tabelle seguenti si riportano i requisiti minimi e migliorativi relativi alla DLP.

DLP - Tutte le fasce
Requisiti minimi
Compatibilità con endpoint Microsoft Windows
Compatibilità con endpoint Mac OS
Compatibilità con endpoint Linux
Compatibilità con Infrastrutture Desktop Virtuali

Possibilità di definire regole personalizzate di classificazione dei dati sulla base del sistema di classificazione dei dati vigente all'interno dell'organizzazione
Possibilità di creare regole personalizzate in base alle policy aziendali/tipologia di files/estensione/contenuto
Monitoraggio dei dati a garanzia del rispetto delle policy definite
Funzionalità di Data Discovery
Protezione dei dati presenti sull'endpoint di tipo fisso (dati *at rest*) e di tipo dinamico (dati *in uso*) dall'esecuzione di operazioni che violano le policy definite.
Protezione dei dati presenti sui dispositivi di memoria di massa connessi alle postazioni di lavoro attraverso l'identificazione di informazioni sensibili e la verifica che queste siano usate conformemente alle policy definite
Protezione dei dati scambiati verso la rete (dati *in motion*) almeno mediante protocolli FTP/SFTP/FTPS, HTTP/HTTPS, SMTP
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 - realizzazione di report personalizzati
Supporto protocollo IPv6

Tabella 21 - Requisiti minimi DLP

DLP - Tutte le fasce	
Requisiti migliorativi di AQ	
ID	Caratteristica
6.1	Crittografia dei file basata sulle policy aziendali per la protezione dei dati sensibili archiviati in supporti rimovibili
6.2	Rilevazione testo per immagini OCR: possibilità di analizzare il contenuto informativo all'interno di file immagine, quali scansioni di documenti, bloccandone l'eventuale trasmissione (come allegato email, upload web, etc.), sia per email, canali web che per endpoint
6.3	Possibilità di interrogare la base dati della soluzione tramite API

Tabella 22 - Requisiti migliorativi di AQ DLP

Si riportano di seguito le funzionalità aggiuntive relative alla seconda fase e i requisiti migliorativi richiedibili in fase di AS, secondo i vincoli previsti nelle Informazioni sulla procedura.

Funzionalità aggiuntive DLP	
Funzionalità	Fase di AS Requisiti migliorativi associabili
Supporto di dispositivi mobili	AS.6.3
Funzionalità che consentano di valutare il rischio connesso alla eventuale perdita di dati (funzionalità di DLP RISK Assessment)	AS.6.4
Funzionalità che consentano di prevenire la perdita di dati attraverso il monitoraggio costante di diverse istanze di trasferimento dei dati nel corso del tempo, anche di modeste dimensioni (funzionalità di Drip DLP)	AS.6.5

Funzionalità di controllo e visibilità sui dati presenti nel Cloud con l'obiettivo di prevenire perdite di dati e accessi non autorizzati (funzionalità CASB implementata anche attraverso integrazioni con soluzioni specifiche di terze parti)	AS.6.6 e AS.6.7
Analitiche per la rilevazione di potenziali minacce mediante l'esame del traffico di rete e del comportamento utente (UBA)	AS.6.9
Supporto di ulteriori protocolli rispetto ai minimi previsti	AS 6.12

Tabella 23 – Funzionalità aggiuntive DLP

DLP	
Requisiti migliorativi di AS	
ID	Caratteristica
AS.6.1	Possibilità di implementare policy che consentano di prevenire l'invio di dati verso IP appartenenti ad area geografiche considerate rischiose.
AS.6.2	Supporto al *file fingerprinting*
AS.6.3	Integrazione con una piattaforma di MDM specificata dall'Amministrazione
AS.6.4	Capacità della funzionalità DLP Risk Assessment di identificare con accuratezza il livello di rischio associato alla perdita di dati, associato in particolare agli specifici contesti di business dell'Amministrazione
AS.6.5	Capacità della funzionalità di Drip DLP di individuare anche modeste fuoriuscite di quantità di dati che perdurano per archi di tempo brevi o lunghi
AS.6.6	Compatibilità della soluzione CASB con specifiche applicazioni cloud richieste dall'Amministrazione
AS.6.7	Capacità della soluzione CASB di garantire la visibilità e la categorizzazione di applicazioni cloud anche non note (shadow IT) in funzione del loro livello di rischio sulla base di specifici requisiti (ad. es. normativi).
AS.6.8	Capacità della soluzione di supportare, semplificandola, l'attività di classificazione dei dati da parte degli operatori, presente e futura.
AS.6.9	Efficacia delle analitiche messe a disposizione per la rilevazione tempestiva di potenziali minacce che potrebbero implicare la perdita di dati mediante l'analisi del comportamento utente (UBA).
AS.6.10	Funzionalità di *Application awareness,* ovvero funzionalità che consenta di riconoscere le applicazioni e associare policy specifiche in modo da gestire in maniera selettiva e sicura quali dati possono essere trattati e verso quali periferiche o destinazioni esterne
AS.6.11	Numerosità delle versioni di sistemi operativi e infrastrutture desktop virtuali supportate e completezza della funzionalità offerte, anche con particolare riguardo al supporto di sistemi legacy
AS.6.12	varietà e numerosità degli ulteriori protocolli supportati dalla soluzione DLP volti sia a prevenire efficacemente la fuoriuscita di dati sensibili, personali sia ad incrementare il grado di integrità, riservatezza dei dati, preservando al tempo stesso l'operatività degli utenti

Tabella 24 - Requisiti migliorativi di AS DLP

2.1.8 Requisiti del Privileged Access Management (PAM)

Nel presente paragrafo sono descritti i **requisiti minimi** e migliorativi relativi al **PAM**.

Il PAM consente di garantire l'accesso sicuro agli asset dell'organizzazione che sono considerati critici, consentendo nel contempo il rispetto della compliance a standard e/o processi aziendali. Attraverso la soluzione di PAM deve essere possibile:

- identificare gli account privilegiati sugli apparati, sistemi, applicazioni garantendone la loro gestione
- controllare l'accesso a tali account privilegiati
- isolare, monitorare e registrare le azioni svolte durante le sessioni effettuate attraverso gli account privilegiati
- gestire e archiviare in maniera sicura le credenziali utilizzate dagli account privilegiati.

Per il PAM (per il quale è richiesta la quotazione di una soluzione software) sono richieste tre fasce dimensionali in funzione del numero di utenze privilegiate:

- PAM_1 (fascia 1): fino a 25 utenze;
- PAM_2 (fascia 2): fino a 100 utenze;
- PAM_3 (fascia 3): fino a 250 utenze.

Nelle tabelle seguenti si riportano i requisiti minimi e migliorativi relativi alla PAM.

PAM - Tutte le fasce
Requisiti minimi
Gestione delle password di accesso attraverso l'utilizzo di una "cassaforte" elettronica in grado di generare password sicure in maniera dinamica
Encryption delle password salvate almeno tramite protocollo AES a 256bit
Supporto gestione delle chiavi SSH
Isolamento delle sessioni privilegiate
Monitoraggio delle sessioni privilegiate in real time
Tracciatura e registrazione delle attività dell'utente durante la sessione privilegiata, al fine di effettuare audit sulle attività effettuate
Supporto di un'ampia gamma di dispositivi tra i quali desktop windows e linux, server windows e linux, database
Possibilità di limitare l'accesso in base all'orario
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 - la realizzazione di report personalizzati

Tabella 25 - Requisiti minimi PAM

PAM - Tutte le fasce	
Requisiti migliorativi di AQ	
ID	Caratteristica

7.1	Discovery automatico degli account privilegiati
7.2	Supporto all'autenticazione di terze parti (ad es. fornitori, consulenti) che accedono da remoto
7.3	Supporto dispositivi IoS e Android
7.4	Possibilità di utilizzare una password in real-time senza che l'utente conosca mai la password utilizzata
7.5	Supporto della connessione ai sistemi target tramite protocollo IPv6
7.6	Possibilità di interrogare la base dati della soluzione tramite API
7.7	Encryption delle password anche mediante ulteriori protocolli (ad es. RSA)
7.8	Possibilità di definire dei workflow per la gestione del processo autorizzativo degli accessi per gli account privilegiati.
7.9	Possibilità di effettuare un'analisi di dettaglio delle minacce informatiche per identificare, segnalare e bloccare attività privilegiate anomale, anche in funzione del loro grado di criticità.

Tabella 26 - Requisiti migliorativi di AQ PAM

Si riportano di seguito le funzionalità aggiuntive relative alla seconda fase e i requisiti migliorativi richiedibili in fase di AS, secondo i vincoli previsti nelle Informazioni sulla procedura.

Funzionalità aggiuntive PAM	
Funzionalità	Fase di AS Requisiti migliorativi associabili
Gestione dei privilegi di amministratore su macchine Windows e/o UNIX	AS.7.1 e AS.7.2
Gestione degli accessi privilegiati per le applicazioni	AS.7.3
Implementazione di una specifica soluzione per la protezione di Domain Controller in ambiente Windows	AS.7.8
Configurazione in alta affidabilità	AS.7.9

Tabella 27 – Funzionalità aggiuntive PAM

PAM	
Requisiti migliorativi di AS	
ID	Caratteristica
AS.7.1	Supporto di ulteriori specifici sistemi operativi richiesti dall'Amministrazione
AS.7.2	Efficacia delle funzionalità messe a disposizione della soluzione per la gestione dei privilegi di amministratore su macchine Windows e/o UNIX e/o altri sistemi operativi richiesti dall'Amministrazione. Sarà valutata: - il grado di dettaglio delle policy per i privilegi di amministratore e la relativa semplicità d'implementazione; - la capacità della soluzione di garantire un'elevata produttività degli utenti mantenendo al contempo i sistemi sicuri; - la capacità di effettuare un controllo applicativo su un'ampia varietà di applicazioni; - l'integrazione con strumenti di analisi delle minacce informatiche, in modo da identificare, segnalare e bloccare attività privilegiate anomale, anche in funzione del loro grado di criticità

AS.7.3	Efficacia della specifica soluzione per la gestione degli accessi applicativi. Saranno valutate: - la proposizione di modalità implementative della soluzione differenti in relazione alla loro adattabilità al contesto specifico dell'Amministrazione (ad es. agent, agentless) e al fine di evitare l'utilizzo di password embedded nel codice; - la varietà numerosità di ambienti applicativi supportati
AS.7.4	Supporto di dispositivi di rete e di dispositivi e sistemi di sicurezza specifici richiesti dall'Amministrazione
AS.7.5	Integrazione con una specifica piattaforma di vulnerability management richiesta dall'Amministrazione
AS.7.6	Integrazione con una specifica soluzione di MFA richiesta dall'Amministrazione
AS.7.7	Possibilità di limitare l'accesso sulla base della localizzazione dell'utente
AS.7.8	Efficacia della specifica soluzione per la protezione di Domain Controller in ambiente Windows. Saranno valutate: - la numerosità delle tecniche di attacco riconosciute; - la varietà delle azioni di mitigazione degli attacchi messe a disposizione dalla soluzione anche al fine di accelerare la fase di remediation da parte degli operatori di sicurezza
AS.7.9	Configurazione della soluzione in alta affidabilità. Saranno valutate le modalità implementative proposte per la configurazione in alta affidabilità, in termini di disponibilità della soluzione e delle sue componenti in caso di guasto.
AS.7.10	Modalità di implementazione dei workflow per la gestione del processo autorizzativo degli accessi per gli account privilegiati. Saranno premiate soluzioni che consentano di implementare meccanismi di controllo degli accessi a più livelli.

Tabella 28 - Requisiti migliorativi di AS PAM

2.1.9 Requisiti dei Web Application Firewall (WAF)

Nel presente paragrafo sono descritti i **requisiti minimi** e migliorativi relativi ai **WAF**.
Il WAF consente di proteggere le applicazioni web, siano esse interne all'Amministrazione oppure esposte direttamente su internet, da una vasta serie di minacce che spaziano dagli attacchi automatizzati attraverso BOT, *code injection* e *denial of service* (DoS).

Per i WAF (per il quale è richiesta la quotazione di una soluzione composta da Appliance fisica hardware e relativo software) sono richieste tre fasce dimensionali/prestazionali:

- WAF_1 (fascia 1): fino a 500 Mbps di throughput HTTP
- WAF_2 (fascia 2): fino a 5 Gbps di throughput HTTP
- WAF_3 (fascia 3): fino a 10 Gbps di throughput HTTP

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

WAF - Tutte le fasce
Requisiti minimi
Capacità di protezione dagli attacchi applicativi almeno OWASP TOP 10 (ultima versione disponibile alla data di presentazione offerta)
Ispezione Traffico HTTP/HTTPS
Protezione API mediante analisi dei dati JSON e XML
Controllo dell'IP Reputation basata sul rating del produttore ed aggiornata automaticamente
Mitigazione degli attacchi bot
Possibilità di definire BlackList e Whitelist di accesso, anche basandosi sulla georeferenziazione degli IP address
Capacità di rilevamento e mitigazione di attacchi DDOS di tipo applicativo
SSL Offloading
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 29 - Requisiti minimi WAF

WAF - Tutte le fasce	
Requisiti migliorativi	
ID	Caratteristica
8.1	Dashboard di monitoraggio in tempo reale con funzionalità drill-down almeno per: Attacchi, Sessioni, dati Geografici di accesso.
8.2	Virtual Patching
8.3	Ispezione del traffico FTP e FTPS
8.4	Funzionalità di Data Loss Prevention
8.5	Possibilità di interrogare la base dati della soluzione tramite API
8.6	Funzionalità di sandboxing su cloud del Produttore

Tabella 30 - Requisiti migliorativi di AQ WAF

Si riportano di seguito le funzionalità aggiuntive relative alla seconda fase e i requisiti migliorativi richiedibili in fase di AS, secondo i vincoli previsti nelle Informazioni sulla procedura.

Funzionalità aggiuntive WAF	
Funzionalità	Fase di AS Requisiti migliorativi associabili
Disponibilità della soluzione su cloud privato	N.A.
Funzionalità di bilanciamento di livello 7 (modello ISO/OSI) delle Applicazioni	AS.8.4

Configurazione in alta affidabilità	AS.8.3

Tabella 31 – Funzionalità aggiuntive WAF

WAF	
Requisiti migliorativi di AS	
ID	Caratteristica
AS.8.1	Qualità e Innovatività del sistema di apprendimento automatico basato su Machine Learning del comportamento applicativo, in grado di rilevare le azioni che si discostano dal comportamento applicativo appreso, riducendo i falsi positivi.
AS.8.2	Integrazione con soluzioni di sicurezza richieste dalla PA (soluzioni Anti APT, NGFW, SIEM, etc)
AS.8.3	Configurazione della soluzione in alta affidabilità. Saranno valutate le modalità implementative proposte per la configurazione in alta affidabilità, in termini di disponibilità della soluzione e delle sue componenti in caso di guasto.
AS.8.4	Efficacia delle funzionalità aggiuntive di bilanciamento del carico a livello 7 (modello ISO/OSI) rispetto alle minime richieste dalla PA e/o relative modalità di implementazione
AS.8.5	Supporto standard PCI DSS
AS.8.6	Modalità di implementazione, varietà e numerosità delle policy/eccezioni alle policy associabili ad applicazioni in essere presso la PA al fine di semplificare la gestione in sicurezza degli applicativi

Tabella 32 - Requisiti migliorativi di AS WAF

2.1.10 Garanzia dei prodotti

Tutti i prodotti che saranno offerti in seconda fase dovranno prevedere una garanzia di 12 mesi dalla "*Data di accettazione*" della fornitura come definita nel par. 2.2.1.2.
Tale garanzia prevede la sostituzione del prodotto, ovvero la correzione di bachi software, nel caso di vizi del bene, di produzione o di conformità, già presenti al momento della consegna o che si manifestino anche in seguito purché durante il periodo di garanzia. In aggiunta a tale garanzia, l'Amministrazione potrà richiedere il servizio di manutenzione secondo quanto previsto nel successivo paragrafo 2.2.1.3.

2.1.11 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 di realizzazione degli Appalti Specifici 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	2	1	S	Implementare il "logging" delle operazione del server DHCP.	SIEM
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	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	SIEM
ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ					
ABSC_ID			Livello	Descrizione	Ambito Merceologico
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	SIEM
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	SIEM
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	SIEM
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE					
ABSC_ID			Livello	Descrizione	Ambito Merceologico
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	PAM
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	PAM

5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	PAM
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	PAM/SIEM
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	PAM
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	PAM
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	PAM
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	PAM
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	PAM
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	PAM
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	PAM
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/PAM
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Servizi di supporto specialistico/PAM
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Servizi di supporto specialistico/PAM
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Servizi di supporto specialistico/PAM
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/PAM
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Servizi di supporto specialistico/PAM

5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	PAM
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	PAM
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	PAM
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	PAM
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	PAM
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	PAM
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	PAM

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE					
ABSC_ID			Livello	Descrizione	Ambito Merceologico
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	SIEM
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	WAF/SEG/SWG
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	SIEM
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	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	SWG

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	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	SEG
8	9	2	M	Filtrare il contenuto del traffico web.	SWG/WAF
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	SWG/SEG/WAF
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	SWG/SEG/WAF

ABSC 13 (CSC 13): PROTEZIONE DEI DATI					
ABSC_ID			Livello	Descrizione	Ambito Merceologico
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	DLP
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	DLP/DB Security
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.	DLP/SWG
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	DLP
13	6	1	A	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	DLP
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	SWG/WAF/SIEM
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	DLP
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	SWG/WAF

2.2 Servizi

2.2.1 Servizi Base

Gli Aggiudicatari dovranno garantire che tutti i servizi base prestati in fase di AS 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'erogazione dei servizi connessi alla fornitura	
Requisiti migliorativi	
ID	Caratteristica
9.1	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 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 (9.2) e l'erogazione dei servizi di manutenzione (9.3) e hardening su client (9.4) anche ai fini di dimostrare il soddisfacimento dei livelli di servizio offerti dal Concorrente descritti nelle Condizioni di fornitura in base ai seguenti elementi:
9.2	- modalità operative e/o strumenti adottati per una diagnosi proattiva e/o tempestiva di eventuali anomalie software e hardware, che potrebbero compromettere e/o che compromettono la sicurezza dei sistemi dell'Amministrazione; - modalità di rilascio e deployment degli aggiornamenti software, al fine di assicurare la continuità operativa dei sistemi dell'Amministrazione e al contempo la loro sicurezza.
9.3	- 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.
9.4	Modalità operative e strumenti adottati per il servizio di hardening su client al fine di semplificare le fasi di progettazione e/o distribuzione degli adeguamenti software sugli elementi di un cluster omogeneo e su più cluster in parallelo, anche ottimizzando i tempi di rilascio dei deliverable.

Tabella 33 - Requisiti migliorativi relativi alla Struttura organizzativa e alle modalità impiegate per l'erogazione dei servizi

2.2.1.1 *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 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 AQ e in sede di AS.

Si precisa che tutte le eventuali attività propedeutiche all'installazione di apparati hardware sono a carico dell'Amministrazione Contraente (predisposizione delle linee di alimentazione, linee dati, rack, supporti etc…).

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. Si precisa che, laddove per la corretta installazione di un elemento costituito da componenti software sia necessaria l'eventuale preventiva predisposizione del relativo ambiente (sistema operativo, software di virtualizzazione, etc..), il Fornitore dovrà provvedere, se richiesto dall'Amministrazione, anche all'installazione di tali elementi (le eventuali licenze di tali ulteriori elementi sono a carico dell'Amministrazione);
    - la configurazione delle specifiche funzionalità previste in base alla tipologia di elemento installato e alla complessità del sistema nel suo complesso.

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).

L'Aggiudicatario dovrà prestare l'attività di ritiro per lo smaltimento dei materiali e delle apparecchiature sostituite già in possesso dell'Amministrazione Contraente e dichiarate non più utilizzabili. 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.

Si riportano di seguito le personalizzazioni relative alla seconda fase.

Personalizzazioni del *Servizio di installazione e configurazione*
• definizione di processi e modalità operative specifiche del contesto dell'Amministrazione per la realizzazione del servizio
• servizio di pre – installazione/configurazione delle soluzioni in ambiente test
• competenze ed esperienze specifiche del personale addetto al servizio di installazione e configurazione

2.2.1.2 *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 della 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 intenderà positivamente superata solo se tutti gli elementi installati risultino funzionare correttamente, sia singolarmente che interconnessi tra loro in modo che il complesso dei prodotti

implementati operi secondo quanto previsto dai requisiti previsti in AQ ed eventualmente gli ulteriori definiti dall'Amministrazione nel proprio AS.

Al termine di tale verifica, l'Aggiudicatario consegnerà all'Amministrazione Contraente il "*Verbale di Fornitura*" nel rispetto dei termini stabiliti nel paragrafo 4.1.2, o il "*Rapporto di Fine Intervento*" nel rispetto dei termini stabiliti nel paragrafo 4.1.5, 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*". In questo caso l'Amministrazione Contraente sottoscriverà, entro **15 giorni** dalla data di sottoscrizione del "*Verbale di Fornitura*", 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". 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 relative penali.

Qualora anche la seconda Verifica di Conformità abbia esito negativo verranno applicate le penali 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, 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. 3.2.1). 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).

Si riportano di seguito le personalizzazioni relative alla seconda fase.

Personalizzazioni del *Servizio di Supporto alla verifica di conformità*
• definizione di processi e modalità operative specifiche del contesto dell'Amministrazione per la realizzazione del servizio
• competenze ed esperienze specifiche del personale addetto al servizio di supporto alla verifica di conformità

2.2.1.3 *Servizio di manutenzione*

Il servizio di manutenzione è opzionale (sebbene quotato in prima fase) e quindi dovrà essere prestato, a pagamento, dall'Aggiudicatario soltanto se espressamente richiesto dall'Amministrazione nel proprio AS.

Il servizio di manutenzione deve essere prestato dall'Aggiudicatario nel rispetto degli SLA previsti (cfr. par 4.1.5), anche con interventi da effettuarsi presso i siti dell'Amministrazione Contraente, pena l'applicazione delle penali.

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. 4.1.4. Il profilo di qualità selezionato dovrà essere il medesimo per tutti i prodotti che interessano l'Appalto Specifico esperito dall'Amministrazione Contraente.
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.

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 (l'Amministrazione non potrà quindi esperire un AS che abbia ad oggetto il servizio di manutenzione di prodotti già in possesso dell'Amministrazione), con avvio dalla "*Data di accettazione*" definita nel paragrafo 2.2.1.2.

Le attività di manutenzione possono riassumersi in:

- ricezione della chiamata di assistenza da parte dell'Amministrazione e assegnazione del Severity Code (cfr. par. 2.2.1.6)
- risoluzione del problema tramite supporto telefonico all'utente (ove possibile) e/o eventuale intervento/i remoto/i in base alle personalizzazioni previste dalla PA;
- 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 beni 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.

Si riportano di seguito le personalizzazioni relative alla seconda fase.

Personalizzazioni del *Servizio di manutenzione*
• possibilità di predisporre un accesso remoto a supporto delle attività di manutenzione (ad. es. effettuazione di diagnosi attraverso i propri sistemi di gestione e di management per analisi di problematiche e malfunzionamenti segnalati dall'Amministrazione) e relative modalità operative
• definizione di processi e modalità operative specifiche del contesto dell'Amministrazione per la realizzazione del servizio
• supporto diretto della TAC (Technical Assistance Centre) del Produttore e modalità di erogazione di tale supporto
• competenze ed esperienze specifiche del personale addetto al servizio di manutenzione
• definizione di ulteriori severity code, relativi SLA e penali associate

2.2.1.4 *Servizio di supporto specialistico*

Il servizio supporto specialistico è opzionale (sebbene quotato in prima fase), quindi dovrà essere prestato, a pagamento, dall'Aggiudicatario soltanto se espressamente richiesto dall'Amministrazione nel proprio AS.

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.

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, 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. 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 2.2.1.22.2.1.1)
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 34 – Supporto specialistico "Security Principal"

Figura professionale	Senior Security 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 (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 35 – 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 4 (quattro) anni di esperienza nella specifica funzione
Competenze ed esperienze richieste	o analisi dinamica delle vulnerabilità e penetration testing sia in ambito applicativo che sulle infrastrutture di sistema e middleware; o analisi statica del codice sorgente o delle configurazioni di sistema; o disegno e valutazione dei sistemi di gestione per la sicurezza; o gestione processo di hardening di sistemi e piattaforme middleware; o validazione pattern di sviluppo sicuro del codice;

Figura professionale	Senior Security Tester
	- capacità di comprendere l'infrastruttura sotto analisi e le relazioni tra i differenti sistemi; - 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 36 – 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; - 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

Figura professionale	Senior Security Analyst
	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 37 – 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 38 – 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 4.1.5, pena l'applicazione di apposite penali.

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, 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, 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 4.1.5, pena l'applicazione di apposite penali. 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.

Servizio di supporto specialistico		
Requisiti migliorativi		
10.1	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% (arrotondato all'unità superiore)
10.2	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% (arrotondato all'unità superiore)
10.3	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% (arrotondato all'unità superiore)
10.4	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% (arrotondato all'unità superiore)

10.5	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% (arrotondato all'unità superiore)

Tabella 39 - Requisiti migliorativi di AQ relativi al personale del servizio di supporto specialistico

Si riportano di seguito le personalizzazioni relative alla seconda fase e i requisiti migliorativi richiedibili in fase di AS, secondo i vincoli previsti nelle Informazioni sulla procedura.

Personalizzazioni del *Servizio di supporto specialistico*
• Definizione di processi e modalità operative specifiche del contesto dell'Amministrazione per la realizzazione del servizio
• competenze ed esperienze specifiche del personale addetto al servizio di supporto specialistico

Tabella 40 – Personalizzazioni relative al servizio di supporto specialistico

Servizio di supporto specialistico		
Requisiti migliorativi di AS		
ID	Caratteristica	
AS.10.1	Security Principal	Certificazioni Vendor Neutrali Aggiuntive Certificazioni di tipo sales o technical sulle tecnologie presenti nel contesto di riferimento della PA o sulle tecnologie proposte in seconda fase.
AS.10.2	Senior Security Architect	Certificazioni Vendor Neutrali Aggiuntive Certificazioni di tipo sales o technical sulle tecnologie presenti nel contesto di riferimento della PA o sulle tecnologie proposte in seconda fase.
AS.10.3	Senior Security Tester	Certificazioni Vendor Neutrali Aggiuntive Certificazioni di tipo sales o technical sulle tecnologie presenti nel contesto di riferimento della PA o sulle tecnologie proposte in seconda fase.
AS.10.4	Senior Security Analyst	Certificazioni Vendor Neutrali Aggiuntive Certificazioni di tipo sales o technical sulle tecnologie presenti nel contesto di riferimento della PA o sulle tecnologie proposte in seconda fase.

AS.10.5	Junior Security Analyst	Certificazioni Vendor Neutrali Aggiuntive Certificazioni di tipo sales o technical sulle tecnologie presenti nel contesto di riferimento della PA o sulle tecnologie proposte in seconda fase.

Tabella 41 - Requisiti migliorativi di AS relativi al personale del servizio di supporto specialistico

2.2.1.5 *Servizio di hardening su client*

Il servizio di hardening su client è opzionale (sebbene quotato in prima fase) e quindi dovrà essere prestato, a pagamento, dall'Aggiudicatario soltanto se espressamente richiesto dall'Amministrazione nel proprio AS.

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 UNIX/Linux di tipo Client

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

Nel proprio AS l'Amministrazione dovrà:

- identificare 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" software, 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/password)
- dettagliare le caratteristiche di ogni elemento che appartiene ad un *cluster* omogeneo (software, configurazioni, patch installate, ...)
- identificare il numero di elementi appartenenti a ciascun *cluster* omogeneo.

In particolare nel proprio AS l'Amministrazione dovrà dare indicazione della durata richiesta per le attività e/o dei deliverable previsti, che saranno successivamente puntualmente riportati nel "*Piano Operativo"* predisposto dall'Aggiudicatario (cfr. par. 3.2.1) e il cui mancato rispetto sarà soggetto, in caso di inadempienza, alle penali.

In fase di esecuzione il servizio dovrà quindi prevedere:

- 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 progettazione e la realizzazione dell'attività su un singolo elemento di un *cluster* omogeneo
b) 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*).

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 (l'Amministrazione non potrà quindi esperire un AS che abbia ad oggetto unicamente il servizio di *hardening*).

Nel caso in cui l'Amministrazione abbia necessità di effettuare attività di hardening su elementi che non siano di tipo client, potrà avvalersi dello specifico servizio aggiuntivo di *hardening su altri sistemi* di cui al paragrafo 2.2.2.1.

2.2.1.6 ***Servizio di Contact Center ed help desk***

Tale servizio è obbligatorio e il suo costo si intende compreso nel complesso dei corrispettivi previsti. L'Aggiudicatario dovrà assicurare, per ogni AS che si sarà aggiudicato, un servizio di assistenza da remoto, con accesso multicanale (telefono, fax, email, PEC), che dovrà essere reso disponibile alla **data di stipula di ogni AS**. 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'AS.
Il servizio sarà utilizzato per:

a) Contact Center: per fornire alle Amministrazioni supporto informativo sui prodotti e servizi oggetto dello specifico AS, nonché per gli aspetti legati alla fatturazione e rendicontazione, utilizzo e segnalazioni di eventuali anomalie al portale della fornitura (par. 4.1 delle Condizioni di fornitura 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 eventualmente erogato. In tale caso 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 4.1) per quanto attiene le richieste di cui al precedente punto b).

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

- fornire informazioni sullo stato di avanzamento delle attività
- 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 dei relativi AS.

Ogni comunicazione da parte dell'Aggiudicatario o dell'Amministrazione Contraente, avvenuta nell'ambito dell'utilizzo del servizio di help desk 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 agli AS, 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 4.1.4.

Si riportano di seguito le personalizzazioni relative alla seconda fase.

Personalizzazioni del *Servizio di Contact Center ed Help DESK*
• definizione di processi e modalità operative specifiche del contesto dell'Amministrazione per la realizzazione del servizio
• competenze ed esperienze specifiche del personale addetto al servizio
• richiesta di attivazione di ulteriori canali sincroni/asincroni per la gestione delle richieste

2.2.1.7 *Servizio di formazione e affiancamento*

Il servizio di formazione e affiancamento è opzionale (sebbene quotato in prima fase), quindi dovrà essere prestato, a pagamento, dall'Aggiudicatario solo se espressamente richiesto dall'Amministrazione nel proprio AS.

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'AS, 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 servizio di addestramento dovrà essere svolto da personale dotato di conoscenza ed esperienza all'insegnamento dello specifico argomento richiesto in fase di AS.

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 di una percentuale dei partecipanti (definita in fase di AS), 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.

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*".

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 (l'Amministrazione non potrà quindi esperire un AS che abbia ad oggetto unicamente il servizio di formazione e affiancamento).

Si riportano di seguito le personalizzazioni relative alla seconda fase.

Personalizzazioni del *Servizio di formazione e affiancamento*
• modalità di erogazione della formazione (ad es.: modalità di erogazione delle sezioni formative, in e-learning; modalità mista in presenza e in e-learning, ...)
• competenze ed esperienze richieste al personale docente
• bilanciamento tra sezione teorica e sezione pratica
• definizione della percentuale massima di partecipanti per la quale una valutazione negativa prevede la ripetizione della sessione (la percentuale potrà variare da un minimo di 20% a un massimo del 70%)
• tempistiche per l'erogazione dei corsi

Il rispetto dei termini relativi all'erogazione dei corsi richiesti sarà monitorato e soggetto, in caso di inadempienza, a specifica penale

2.2.2 Servizi Aggiuntivi

I servizi aggiuntivi sono servizi che le Amministrazioni Contraenti potranno richiedere in AS, provvedendo autonomamente a definirli in quanto a requisiti, modalità di erogazione, livelli di servizio e base d'asta, in funzione delle proprie specificità e peculiarità tecnologiche ed organizzative, con il vincolo che il valore economico dei servizi aggiuntivi richiesti rimanga nei limiti previsti nelle Informazioni sulla procedura.
Attraverso tali servizi si vuole fornire un elemento di flessibilità che consenta alle Amministrazioni Contraenti di ampliare la proposta del presente AQ.

Tali servizi, evidentemente, non sono oggetto di valutazione tecnica in fase di AQ e agli Offerenti non è richiesta una loro quotazione in prima fase.
Gli Aggiudicatari dovranno garantire in ogni caso che tutti i servizi aggiuntivi prestati in fase di AS siano espletati da personale qualificato, che abbia le idonee competenze in base alle particolari attività richieste e tecnologie descritte dall'Amministrazione.

2.2.2.1 *Servizio di hardening su altri sistemi*

Tale servizio consente alle Amministrazioni Contraenti di richiedere l'effettuazione di attività di hardening su sistemi/apparati/software differenti rispetto a quelli previsti per il servizio di hardening su client. A titolo esemplificativo l'Amministrazione potrà richiedere l'espletamento delle attività di hardening su sistemi quali:

- Web Server
- Application Server
- DB Server
- Router
- Switch
- elementi di tipo IoT/OT.

In sede di AS l'Amministrazione descriverà puntualmente le esigenze connesse a tale servizio. A titolo esemplificativo riporterà:

- i sistemi/apparati/software interessati dall'attività e relativa numerosità
- informazioni tecniche quali modelli hardware, versioni software, livelli di patch, architetture di rete/applicative
- indicazioni di eventuali vulnerabilità da testare o controlli da effettuare
- modalità operative per l'esecuzione del servizio
- richieste di particolari figure e/o competenze per l'esecuzione del servizio
- livelli di servizio
- deliverable attesi.

Le attività effettuate dovranno in ogni caso, per gli elementi pertinenti, essere aderenti a quanto previsto dalle "*Linee guida per adeguare la sicurezza del software di base*" rilasciate da AgID.

2.2.2.2 ***Servizio di Data Assessment***

Tale servizio consente alle Amministrazioni Contraenti di richiedere l'effettuazione di attività utili a:

- verificare quali siano le sorgenti dei dati generati e i repository dei dati utilizzati all'interno del proprio perimetro "aziendale"
- catalogare le sorgenti e i dati
- classificare le sorgenti e i dati in base al contenuto, al contesto o ai fruitori
- verificare il grado di sicurezza di ogni sorgente e dei dati in base alla classificazione effettuata
- pianificare eventuali azioni correttive utili a migliorare il grado di sicurezza dei dati.

In sede di AS l'Amministrazione descriverà puntualmente le esigenze connesse a tale servizio. A titolo esemplificativo riporterà:

- i sistemi interessati dall'attività e relativa numerosità (Database, File Server, Applicazioni, Storage, Apparati utente, ...)
- funzioni aziendali e processi aziendali interessati
- eventuali informazioni tecniche utili a circoscrivere il perimetro dei sistemi interessati, quali prodotti utilizzati, versioni software
- modalità operative per l'esecuzione del servizio
- livelli di servizio
- deliverable attesi.

2.2.2.3 ***Servizio di Privileged Account Assessment***

Tale servizio consente alle Amministrazioni Contraenti di richiedere l'effettuazione di attività utili a:

- verificare quali siano gli account "privilegiati" che sono presenti sui propri sistemi (ad esempio Amministratori di sistema, utenti con credenziali di accesso ad applicazioni "sensibili", ...)
- classificare le utenze privilegiate sulla base dei sistemi interessati, dei ruoli, dei permessi
- verificare la presenza di utenze non necessarie e/o ridondanti

- pianificare eventuali azioni correttive quali la cancellazione di utenze ovvero la modifica dei permessi concessi.

In sede di AS l'Amministrazione descriverà puntualmente le esigenze connesse a tale servizio. A titolo esemplificativo riporterà:

- i sistemi interessati dall'attività e relativa numerosità (Server, Applicazioni, Apparati di rete, ...)
- funzioni aziendali e processi aziendali interessati
- eventuali informazioni tecniche utili a circoscrivere il perimetro dei sistemi interessati, quali prodotti utilizzati, versioni software
- modalità operative per l'esecuzione del servizio
- livelli di servizio
- deliverable attesi.

2.2.2.4 *Servizi professionali erogati dal vendor*

Tale servizio consente alle Amministrazioni Contraenti di richiedere, relativamente alle tecnologie acquistate nell'ambito dell'AS, dei servizi professionali di supporto erogati direttamente dal personale dei vendor delle relative tecnologie.

In sede di AS l'Amministrazione descriverà puntualmente le esigenze connesse a tale servizio. A titolo esemplificativo riporterà:

- i prodotti previsti in AS per il quale è richiesto il servizio professionale erogato dal vendor
- le finalità di tale servizio in termini di impegno, figure, attività previste
- modalità operative per l'esecuzione del servizio
- livelli di servizio
- deliverable attesi.

2.2.2.5 *Servizio di incident response*

Il servizio di incident response consente alle Amministrazioni contraenti di rispondere rapidamente e in modo efficace alle violazioni di sicurezza informatiche che possano compromettere l'integrità, la disponibilità o la riservatezza dei dati dei propri sistemi.
Il servizio di incident response prevede delle fasi ben precise:

- redazione di un piano di incident response, con definizione delle procedure operative da seguire, nonché adozione di misure volte a prevenire il verificarsi degli incidenti di sicurezza;
- identificazione dell'attacco di sicurezza e dello scopo dell'attacco
- contenimento, bonifica e remediation
- ripristino del corretto funzionamento dei sistemi
- verifica ex post della corretta mitigazione dell'incidente informatico e della corretta implementazione di tutte le contromisure adottate.

Il servizio di Incident Response risulta particolarmente utile in tutti quei casi in cui la PA non risulti dotata di un proprio SOC, con un Incident Response Team in grado di effettuare tali attività in autonomia.
In sede di AS l'Amministrazione descriverà puntualmente le esigenze connesse a tale servizio. A titolo esemplificativo riporterà:

- il contesto operativo e di business della PA;
- assets da proteggere;
- ruoli, responsabilità e procedure già in essere che interessano gli assets;
- infrastruttura e policy di sicurezza già in essere;
- risultanze di Risk Assessment precedentemente effettuati;
- modalità e struttura organizzativa richieste per l'esecuzione del servizio;
- livelli di servizio
- deliverable attesi.

2.2.3 Requisiti migliorativi in fase di AS

Si riportano di seguito in tabella l'elenco dei requisiti migliorativi richiedibili in fase di AS per i servizi, secondo i vincoli previsti nelle Informazioni sulla procedura.

Servizi	
Requisiti migliorativi di AS	
ID	Caratteristica
AS.9.1	Ulteriori competenze ed esperienze specifiche del personale addetto ai servizi (ad eccezione del supporto specialistico)
AS.9.2	Certificazioni Vendor Neutrali Aggiuntive del personale addetto ai servizi (ad eccezione del supporto specialistico)
AS.9.3	Certificazioni di tipo *sales* o *technical* del personale addetto ai servizi sulle tecnologie presenti nel contesto di riferimento della PA o sulle tecnologie proposte in seconda fase .(ad eccezione del supporto specialistico)
AS.9.4	Architettura e modalità di implementazione del collegamento (qualora questo non sia messo a disposizione dalla PA) per l'accesso remoto ai sistemi dell'Amministrazione a supporto delle attività di manutenzione, al fine di garantire l'integrità, la riservatezza e la sicurezza dei dati.
AS.9.5	Modelli organizzativi, modalità operative e strumenti adottati per l'erogazione dei servizi aggiuntivi ai fini di dimostrare il soddisfacimento dei livelli di servizio offerti dal Concorrente e ottimizzare i tempi di rilascio dei deliverable attesi

3 GESTIONE DELLA FORNITURA

3.1 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 nelle Condizioni di fornitura parte Generale.

3.2 Appalto Specifico

L'Amministrazione Contraente dovrà individuare alla stipula del Contratto un "*Responsabile dell'Amministrazione*" che sarà responsabile della direzione e del coordinamento delle attività

Analogamente l'Aggiudicatario dell'AS identificherà 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 nelle Condizioni di fornitura parte Generale.

3.2.1 Piano Operativo dell'AS

La fase di esecuzione di ogni AS dovrà prevedere, entro 20 giorni lavorativi dalla data di stipula del Contratto e pena l'applicazione delle penali, la predisposizione da parte dell'Aggiudicatario dell'AS di un "*Piano Operativo*" che riporti almeno:

- l'importo contrattuale 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
- informazione tecniche quali:
  - configurazione Hardware di ogni singolo apparato. L'Aggiudicatario dovrà riportare, per ogni tipologia di apparato, il codice prodotto e la descrizione di ogni elemento costituente;
  - configurazione 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
  - 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 dei 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. 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
- il modello organizzativo impiegato per l'esecuzione delle attività, comprendente i Responsabili previsti in accordo con il successivo paragrafo
- 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
- eventuali attività a carico dell'Amministrazione propedeutiche alla realizzazione della fornitura, quali la categorizzazione degli interventi e l'identificazione delle informazioni utili al calcolo degli indicatori di digitalizzazione di cui alle Condizioni di Fornitura – Parte Generale;
- la durata del Contratto Esecutivo.

Si precisa che la predisposizione del Piano Operativo nei termini previsti include anche il recepimento delle indicazioni e la condivisione dei contenuti con l'Amministrazione Contraente. È quindi onere dell'Aggiudicatario prevedere, nella redazione del documento, una stretta collaborazione con il personale dell'Amministrazione e la condivisione tempestiva dei contenuti con l'Amministrazione Contraente.

3.3 Reporting per le Amministrazioni

3.3.1 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.

3.3.2 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'AS.

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.

4 LIVELLI DI SERVIZIO E QUALITÀ

4.1 Service Level Agreement

I **Service Level Agreement (SLA)** definiscono i parametri di qualità del servizio che devono essere rispettati dall'Aggiudicatario.
Per ciascuno di tali parametri è stabilita una **Soglia Richiesta (SR)**, al superamento della quale scatterà il meccanismo di applicazione delle relative penali.

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 42 - 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.

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 43 – Classificazione dei Severity Code

4.1.1 SLA per l'attivazione della fornitura

La fase di attivazione di ogni AS sarà monitorata in base al seguente parametro di SLA:

- **Tempo di emissione del *"Piano Operativo"***: è definito come il tempo, misurato in giorni solari, che intercorre tra la stipula del contratto e la data di ricezione da parte dell'Amministrazione Contraente del "*Piano Operativo*" (cfr. paragrafo 3.2.1);

Parametro	SR
Tempo di emissione del "*Piano Operativo*"	20 giorni lavorativi

Tabella 44 - SLA per l'attivazione della fornitura

4.1.2 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 2.2.1.2

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 45 - SLA per la consegna, installazione e verifica.

4.1.3 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 46 - SLA per le attività di supporto alla verifica di conformità

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

Di seguito sono elencati i Service Level Agreement che l'Aggiudicatario 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* assegnato).
  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 stipula dell'AS
Disponibilità delle informazioni di contatto relative al servizio di Contact Center ed help desk		Alla data di stipula dell'AS.

Tabella 47 - SLA per i servizi di assistenza e manutenzione

4.1.5 SLA per il servizio di supporto specialistico

Di seguito sono elencati i Service Level Agreement che l'Aggiudicatario 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 48 - SLA per il servizio di supporto specialistico

4.1.6 SLA per il servizio di hardening su client

Di seguito sono elencati i Service Level Agreement che l'Aggiudicatario 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 49 - SLA per il servizio di hardening su client

4.1.7 SLA per il servizio di formazione e affiancamento

Di seguito sono elencati i Service Level Agreement che l'Aggiudicatario 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 50 - SLA per il servizio di formazione e affiancamento

4.1.8 SLA per la gestione della fornitura

Di seguito è elencato il Service Level Agreement che l'Aggiudicatario 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 delle Condizioni di fornitura 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 delle Condizioni di fornitura 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 51 - SLA per la gestione della fornitura

4.1.9 Miglioramento dei SLA in fase di AQ

Gli Offerenti potranno proporre degli SLA migliorati in fase di AQ in accordo con la seguente tabella.

SLA	
Requisiti migliorativi	
ID	Caratteristica
11.1	Tempo di emissione del "*Piano Operativo*": 15 giorni lavorativi
11.2	Tempo di consegna, installazione, configurazione e verifica: 50 giorni solari
	Tempestività del tempo di intervento - Valore minimo richiedibile in AS
11.3	Profilo LP: 6 ore
11.4	Profilo HP: 3 ore
	Tempestività del tempo di ripristino del servizio - Valore minimo richiedibile in AS
11.5	Profilo LP - Severity Code 1: 12 ore
11.6	Profilo LP - Severity Code 2: 16 ore
11.7	Profilo HP - Severity Code 1: 4 ore
11.8	Profilo HP - Severity Code 2: 8 ore

Tabella 52 - Requisiti migliorativi relativi ai SLA

4.1.10 Miglioramento dei SLA in fase di AS

Gli Offerenti potranno proporre degli SLA migliorati in fase di AS in accordo con la seguente tabella.

SLA	
Requisiti migliorativi di AS	
ID	Caratteristica
AS.8.1	Miglioramento dei livelli di servizio richiesti (rispetto ai valori migliorativi previsti in AQ)

4.2 Monitoraggio della qualità erogata

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

- la struttura e qualità 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'intero Accordo Quadro 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'Accordo Quadro ovvero del singolo Contratto, 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 delle Condizioni di fornitura parte Generale.

Nel corso dell'esercizio potrà essere 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.

5 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	Soggetto avente diritto alla penale
Tempo di emissione del "*Piano Operativo*" (par.4.1.1)	Amministrazione Contraente

Tabella 53 - Penali relative all'attivazione della fornitura

Parametro	Soggetto avente diritto alla penale
Tempo di consegna, installazione, configurazione e verifica (par. 4.1.2)	Amministrazione Contraente

Tabella 54 - Penali relative alla consegna, installazione, configurazione e verifica

Parametro	Soggetto avente diritto alla penale
Predisposizione seconda verifica (par. 4.1.3)	Amministrazione Contraente
Predisposizione ulteriore verifica collaudo (par. 4.1.3)	Amministrazione Contraente
Esito negativo seconda verifica (o successive) (par. 4.1.3)	Amministrazione Contraente

Tabella 55 - Penali relative alle attività di supporto alla verifica di conformità

Parametro	**Soggetto avente diritto alla penale**
Tempestività di risposta al disservizio (par. 4.1.4)	Amministrazione Contraente
Tempestività di intervento (par. 4.1.4)	Amministrazione Contraente
Tempestività di ripristino del servizio - Severity Code 1 (par. 4.1.4)	Amministrazione Contraente
Tempestività di ripristino del servizio - Severity Code 2 (par. 4.1.4)	Amministrazione Contraente
Attesa per il servizio di Contact Center ed help desk (par. 4.1.4)	Amministrazione Contraente
Percentuale di chiamate perse (par. 4.1.4)	Amministrazione Contraente
Disponibilità del servizio di Contact Center ed help desk (par. 4.1.4)	Amministrazione Contraente
Disponibilità delle informazioni di contatto relative al servizio di Contact Center ed help desk (par. 4.1.4)	Amministrazione Contraente

Tabella 56 - SLA per i servizi di assistenza e manutenzione

Parametro	Soggetto avente diritto alla penale
Tempo di presa in carico del servizio di supporto (cfr. 4.1.5)	Amministrazione Contraente
Data di completamento dell'intervento (cfr. 4.1.5)	Amministrazione Contraente
Tempo di consegna dei CV delle risorse del servizio di supporto (cfr. 4.1.5)	Amministrazione Contraente
Tempo di sostituzione del personale del servizio di supporto (cfr. 4.1.5)	Amministrazione Contraente

Tabella 57 - **Penali relative al servizio di supporto specialistico**

Parametro	Soggetto avente diritto alla penale
Slittamento di una scadenza per il servizio di hardening su client (cfr.4.1.6)	Amministrazione Contraente

Tabella 58 - **Penali relative al servizio di hardening su client**

Parametro	Soggetto avente diritto alla penale
Data di avvio del servizio di formazione e affiancamento (cfr.4.1.7)	Amministrazione Contraente

Tabella 59 - **Penali relative al servizio di addestramento sulla fornitura**

Parametro	Soggetto avente diritto alla penale
Tempo di gestione delle richieste (par. 4.1.8)	Amministrazione Aggiudicatrice
	Amministrazione Contraente
Tempo di consegna dei dati relativi agli SLA (par. 4.1.8)	Amministrazione Aggiudicatrice
	Amministrazione Contraente

Disponibilità del Portale della Fornitura	Amministrazione Aggiudicatrice
Attivazione del Portale della Fornitura (par. 4.1 delle Condizioni di Fornitura parte Generale)	Amministrazione Aggiudicatrice

Tabella 60 - Penali relative alla gestione della fornitura