acquistinretepa

Cybersecurity – prodotti e servizi connessi

Accordo Quadro 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

GUIDA ALL'ACCORDO QUADRO

Ultimo aggiornamento: [GG/MM/AAAA]

SOMMARIO

DISCLAIMER

La presente guida non intende sostituire né integrare la documentazione contrattuale sottoscritta fra le parti. Pertanto, le informazioni in essa contenute non possono costituire motivo di rivalsa da parte delle Amministrazioni contraenti nei confronti dei Fornitori e/o di Consip né possono ritenersi prevalenti rispetto alla documentazione contrattuale.

1. Premessa

La presente iniziativa si inserisce nell'ambito del **Piano delle Gare Strategiche ICT, concordato tra Consip e AgID,** che ha l'obiettivo, tra le altre cose, di mettere a disposizione delle PP.AA. delle specifiche iniziative finalizzate all'acquisizione di prodotti e di servizi nell'ambito della sicurezza informatica, facilitando l'attuazione del Piano Triennale e degli obiettivi del PNRR in ambito, restando in linea con le disposizioni normative relative al settore della cybersicurezza.

In particolare il presente documento ha l'obiettivo di illustrare l'iniziativa Cybersecurity – prodotti e servizi connessi – Accordo Quadro 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 (di seguito, per brevità, anche AQ), stipulata, ai sensi dell'art 54 comma 4 lett. c) del D.Lgs. 50/2016, con:

- **RTI FASTWEB S.p.A. – FINCANTIERI NEXTECH S.p.A. - N&C S.r.l. – BUSINESS – INTEGRATION PARTNERS S.p.A. - CONSORZIO REPLY PUBLIC SECTOR (nel seguito anche RTI FASTWEB)**
- **RTI TELECOM ITALIA S.p.A. – LEONARDO S.p.A. – DGS S.p.A. – ENGINEERING INGEGNERIA INFORMATICA S.p.A. (nel seguito anche RTI TELECOM)**
- **RTI VODAFONE ITALIA S.p.A. – EUROLINK S.p.A. – ALMAVIVA - THE ITALIAN INNOVATION COMPANY S.p.A. (nel seguito anche RTI VODAFONE)**

Si precisa che il presente AQ prevede **obbligatoriamente** la realizzazione di una seconda fase di rilancio. Le Amministrazioni Contraenti **dovranno quindi realizzare un proprio Appalto Specifico** indicando i beni e i servizi di loro interesse nel rispetto di quanto previsto nella documentazione di gara e nella documentazione a supporto (si faccia riferimento al successivo paragrafo 7).

La presente guida, unitamente a tutta la documentazione relativa all'AQ e alla documentazione di ausilio per la realizzazione degli AS, è disponibile sul sito internet https://www.acquistinretepa.it, nella sezione **Acquista** > **Accordi quadro** > **Cybersecurity – prodotti e servizi connessi**.

Per qualsiasi informazione sull'AQ (condizioni previste, modalità di adesione, etc.) e per il supporto alla navigazione del sito https://www.acquistinretepa.it è attivo il servizio di Call Center degli Acquisti in Rete della P.A. al numero verde 800 753 783.

1.1. Richiesta di abilitazione

Le Amministrazioni che desiderano bandire un Appalto Specifico, dovranno richiedere l'abilitazione all'AQ inviando una mail di richiesta ad XXXXX@acquistinretepa.it.

Nella sezione dedicata all'AQ, sulla Piattaforma AcquistinretePA, avranno a disposizione:

- le offerte tecniche presentate dagli Operatori Economici aggiudicatari dell'AQ; tali offerte contengono le condizioni migliorative offerte dai concorrenti in prima fase, che rimangono valide e vincolanti anche per l'aggiudicazione degli AS;
- le offerte economiche presentate dagli Operatori Economici aggiudicatari dell'AQ; tali offerte contengono il dettaglio dei prezzi unitari offerti in prima fase, che concorrono alla definizione della base d'asta dell'AS stesso;
- il kit per la predisposizione dell'AS contenente i facsimili di documentazione per la predisposizione dell'AS (tra cui la richiesta di offerta, e lo strumento di ausilio alla predisposizione dell'AS in formato xls)
- i riferimenti del Responsabile unico delle attività contrattuali (RUAC) di ogni fornitore aggiudicatario.

2. Oggetto e durata dell'Accordo Quadro

Oggetto della fornitura sono prodotti per la gestione degli eventi di sicurezza e degli accessi, la protezione dei canali email, web e dati e i relativi servizi, base e aggiuntivi, connessi.

In particolare sono previsti i seguenti beni:

- 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 seguenti servizi base connessi alla fornitura:

- installazione e configurazione
- formazione e affiancamento
- manutenzione
- hardening su client
- Contact Center ed help desk
- supporto specialistico

e i seguenti servizi aggiuntivi connessi:

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

Si precisa che in fase di AS l'Amministrazione potrà:

- definire ulteriormente le proprie specifiche esigenze personalizzando i beni e/o i servizi base richiesti nei limiti di quanto previsto all'interno del capitolato tecnico di AQ e 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 in AS, 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 all'interno del capitolato tecnico di AQ e del presente documento, per le quali l'Amministrazione dovrà determinare la relativa sotto base d'asta secondo i vincoli che sono descritti nel paragrafo 7.1.2.

2.1. Beni

2.1.1. Security Information and Event Management (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 sono previste 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, questi ultimi offerti da tutti gli Aggiudicatari dell'AQ.

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: ○ switch e router di almeno due dei seguenti Produttori: Cisco, Juniper, HPE, Huawei, Alcatel-Lucent; ○ sistemi operativi Microsoft Windows e Linux; ○ piattaforma di virtualizzazione VMWare; ○ database Oracle e Microsoft SQL Server; ○ web server Apache e Microsoft IIS; ○ 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 1 - 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	○ switch e router di ulteriori due Produttori (oltre ai due minimi richiesti) sempre tra i seguenti: Cisco, Juniper, HPE, Huawei, Alcatel-Lucent;
1.2	○ sistema operativo Mac OS
1.3	○ piattaforma di virtualizzazione KVM
1.4	○ 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 2 - Requisiti migliorativi di AQ SIEM

Si riportano di seguito le funzionalità aggiuntive relative alla seconda fase con i relativi requisiti migliorativi associabili, come previsti nel paragrafo 7.1.1.

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 3 – Funzionalità aggiuntive SIEM

2.1.2. Security Orchestration, Automation and Response (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 sono previste 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, questi ultimi offerti da tutti gli Aggiudicatari dell'AQ.

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 4 - 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 5 - Requisiti migliorativi di AQ SOAR

Si riportano di seguito le funzionalità aggiuntive relative alla seconda fase con i relativi requisiti migliorativi associabili, come previsti nel paragrafo 7.1.1.

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 6 – Funzionalità aggiuntive SOAR

2.1.3. Secure Email Gateway (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 sono previste 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 relativi al SEG, questi ultimi offerti da tutti gli Aggiudicatari dell'AQ.

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 7 - 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 8 - Requisiti migliorativi di AQ SEG

Si riportano di seguito le funzionalità aggiuntive relative alla seconda fase con i relativi requisiti migliorativi associabili, come previsti nel paragrafo 7.1.1.

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 9 – Funzionalità aggiuntive SEG

2.1.4. Secure Web Gateway (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 sono previste 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 relativi al SWG, questi ultimi offerti da tutti gli Aggiudicatari dell'AQ.

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 10 - 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 11 - Requisiti migliorativi di AQ SWG

Si riportano di seguito le funzionalità aggiuntive relative alla seconda fase con i relativi requisiti migliorativi associabili, come previsti nel paragrafo 7.1.1.

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 12 – Funzionalità aggiuntive SWG

2.1.5. Database Security (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 sono previste due configurazioni:

- 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 DB Security, questi ultimi offerti da tutti gli Aggiudicatari dell'AQ.

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 13 - 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 14 - Requisiti migliorativi di AQ DB Security

Si riportano di seguito le funzionalità aggiuntive relative alla seconda fase con i relativi requisiti migliorativi associabili, come previsti nel paragrafo 7.1.1.

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 15 – Funzionalità aggiuntive DB Security

2.1.6. Data Loss Prevention (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 sono previste 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, questi ultimi offerti da tutti gli Aggiudicatari dell'AQ.

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 16 - 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 17 - Requisiti migliorativi di AQ DLP

Si riportano di seguito le funzionalità aggiuntive relative alla seconda fase con i relativi requisiti migliorativi associabili, come previsti nel paragrafo 7.1.1.

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 18 – Funzionalità aggiuntive DLP

2.1.7. Privileged Access Management (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 sono previste 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 al PAM, questi ultimi offerti da tutti gli Aggiudicatari dell'AQ.

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 19 - 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 20 - Requisiti migliorativi di AQ PAM

Si riportano di seguito le funzionalità aggiuntive relative alla seconda fase con i relativi requisiti migliorativi associabili, come previsti nel paragrafo 7.1.1.

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 21 – Funzionalità aggiuntive PAM

2.1.8. Web Application Firewall (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 sono previste 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 relativi al WAF, questi ultimi offerti da tutti gli Aggiudicatari dell'AQ.

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 22 - 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 23 - Requisiti migliorativi di AQ WAF

Si riportano di seguito le funzionalità aggiuntive relative alla seconda fase con i relativi requisiti migliorativi associabili, come previsti nel paragrafo 7.1.1.

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 24 – Funzionalità aggiuntive WAF

2.2. Servizi base

2.2.1. Servizio di installazione e configurazione

Il servizio di installazione e configurazione è compreso nella fornitura ed il relativo costo incluso nei corrispettivi dei prodotti offerti.

Il servizio comprende tutto quello che è necessario per le attività di installazione e configurazione degli elementi acquistati dall'Amministrazione in sede di AS.

Si precisa che tutte le eventuali attività propedeutiche all'installazione di apparati hardware sono a carico dell'Amministrazione (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 che l'Amministrazione potrà prevedere nel proprio AS.

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

2.2.2. Servizio di supporto alla verifica di conformità

Ai sensi di quanto previsto all'art. 1, comma 6 lett. a) del D.L. 105/2019, la cui efficacia è stata modificata dall'art. 16 comma 9, lett. a) del D.L. n. 82/2021, si precisa innanzitutto che il Fornitore è tenuto a fornire pieno supporto alle Amministrazioni, chiamate a collaborare con il CVCN o con 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 compreso nei corrispettivi dei 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 di cui al paragrafo 5. È facoltà dell'Amministrazione procedere ad ulteriori Verifiche di Conformità ovvero dichiarare risolto di diritto il Contratto di fornitura, in tutto o in parte. Nel caso in cui anche le ulteriori Verifiche di Conformità avessero esito negativo verranno applicate le penali di cui al paragrafo 5, 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. 3.1). 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

2.2.3. Servizio di manutenzione

Il servizio di manutenzione è opzionale e quindi dovrà essere prestato soltanto se espressamente richiesto dall'Amministrazione nel proprio AS.

Il servizio di manutenzione deve essere realizzato 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 indicate al par. 5.

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. Il servizio è previsto per annualità, quindi per 12 mesi o massimo 24 mesi.

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.

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 2.2.2.

Le attività di manutenzione possono riassumersi in:

- ricezione della chiamata di assistenza da parte dell'Amministrazione e assegnazione del Severity Code (cfr. par. **Error! Reference source not found.**)
- 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 inoltre comprende 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 è tenuto a 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

2.2.4. Servizio di supporto specialistico

Il servizio supporto specialistico è opzionale e quindi dovrà essere prestato 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 secondo quanto previsto al par. 5. 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 è 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 2.2.2**Error! Reference source not found.**)
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 è accettata una risorsa in possesso di diploma ma con esperienza lavorativa di almeno 15 anni (di cui almeno 5 anni di provata esperienza nella specifica funzione).

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

Tabella 25 – Supporto specialistico "Security Principal"

Figura professionale	**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 26 – Supporto specialistico "Senior Security Architect"

Figura professionale	**Senior Security Tester**
Titolo di studio	Laurea triennale in discipline scientifiche
Anzianità lavorativa	anzianità lavorativa di almeno 6 (sei) anni nel settore ICT, da computarsi successivamente alla data di conseguimento del diploma di laurea, di cui almeno 4 (quattro) anni di esperienza nella specifica funzione
Competenze ed esperienze richieste	- analisi dinamica delle vulnerabilità e penetration testing sia in ambito applicativo che sulle infrastrutture di sistema e middleware; - analisi statica del codice sorgente o delle configurazioni di sistema;

Figura professionale	Senior Security Tester
	- disegno e valutazione dei sistemi di gestione per la sicurezza; - gestione processo di hardening di sistemi e piattaforme middleware; - validazione pattern di sviluppo sicuro del codice; - capacità di comprendere l'infrastruttura sotto analisi e le relazioni tra i differenti sistemi; - conoscenza approfondita delle diverse tipologie di attacco informatico, delle tecniche di penetration test, degli strumenti software utilizzati e dei più importanti tool ed exploit disponibili pubblicamente; - esperienza nell'analisi delle vulnerabilità di sistemi e reti in esercizio senza impattare sull'operatività ed il funzionamento degli stessi; - conoscenza complessiva delle problematiche di sicurezza dei dati e delle informazioni.

Tabella 27 – Supporto specialistico "Senior Security Tester"

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

Figura professionale	Senior Security Analyst
	configurazioni e analisi di sicurezza; - esperienza nella definizione di regole di correlazione e nel tuning delle stesse; - conoscenza dei processi di reverse engineering dei malware ed esperienza consolidata nella analisi forense di malware mediante strumenti di analisi e attività di reverse; - conoscenza approfondita dei protocolli di rete e della tipologia di traffico all'interno di un contesto complesso con esperienza consolidata nell'analisi forense del traffico di rete e nell'identificazione di anomalie o elementi a supporto per la corretta gestione degli incidenti di sicurezza.

Tabella 28 – Supporto specialistico "Senior Security Analyst"

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

Tabella 29 – Supporto specialistico "Junior Security Analyst"

Inoltre, in ogni AS, deve essere previsto l'impiego di personale in possesso di certificazioni in ambito *security* secondo quanto previsto nella seguente tabella.

Security Principal	Almeno il 50% di risorse offerte (arrotondato all'unità superiore) in possesso della certificazione ISACA CISM (Certified Information Security Manager)
Senior Security Architect	Almeno il 50% di risorse offerte (arrotondato all'unità superiore) in possesso della certificazione (ISC)^2 CISSP (Certified Information System Security Professional)

Senior Security Tester	Almeno il 50% di risorse offerte (arrotondato all'unità superiore) 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+
Senior Security Analyst	Almeno il 50% di risorse offerte (arrotondato all'unità superiore) 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
Junior Security Analyst	Almeno il 50% di risorse offerte (arrotondato all'unità superiore) 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+

È previsto un prezzo per giorno/persona per ogni figura professionale riferiti 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 (cfr. par. 5).

Inoltre l'Aggiudicatario dovrà:

- in caso di servizio richiesto in fase iniziale o con periodicità definita - precedenti punti i) e iii): presentare all'Amministrazione Contraente, entro 20 giorni solari dalla data di stipula del contratto esecutivo, pena l'applicazione delle penali di cui al paragrafo 5**Error! Reference source not found.**, i CV delle risorse proposte per l'erogazione del servizio in cui dovranno essere anche inserite copie delle certificazioni possedute dalle risorse, in accordo con i requisiti minimi o i migliorativi eventualmente offerti;
- in caso di servizio richiesto in modalità "spot" – precedente punto ii): presentare all'Amministrazione Contraente, entro 5 giorni solari dalla data di invio della "*Lettera di presa in carico del servizio di supporto*", pena l'applicazione delle penali di cui al paragrafo 5, 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 (cfr. par. 5). 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.

2.2.5. Servizio di hardening su client

Il servizio di hardening su client è opzionale e quindi dovrà essere prestato 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 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. 3.1) e il cui mancato rispetto sarà soggetto, in caso di inadempienza, alle penali di cui al par. **Error! Reference source not found.**

Il Fornitore è quindi tenuto a realizzare:

- 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.

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 2.3.1.

2.2.6. Servizio di Contact Center ed help desk

Tale servizio è compreso nella fornitura ed il relativo costo compreso nel complesso dei corrispettivi previsti. Per ogni AS l'Aggiudicatario deve garantire un servizio di assistenza da remoto, con accesso multicanale (telefono, fax, email, PEC), 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 è 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 del Capitolato Tecnico parte Generale). Dovranno inoltre essere gestite le chiamate che interessano i prodotti acquistati dalle PA in caso di guasti che intervengano nel periodo di garanzia
b) Help Desk: a completamento del servizio di manutenzione 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.

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 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

2.2.7. Servizio di formazione e affiancamento

Il servizio di formazione e affiancamento è opzionale e quindi dovrà essere prestato soltanto 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.

Lei attività formative **sono 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 è svolto da personale dotato di conoscenza ed esperienza all'insegnamento dello specifico argomento richiesto in fase di AS.

Il Fornitore dovrà predisporre 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 (che l'Amministrazione definirà 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 di cui al par. 5

2.3. Servizi aggiuntivi

I servizi aggiuntivi sono servizi che le Amministrazioni Contraenti possono 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 nel paragrafo 7.

Attraverso tali servizi si vuole fornire un elemento di flessibilità che consenta alle Amministrazioni Contraenti di ampliare quanto previsto nel presente AQ.

2.3.1. 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.

2.3.2. 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

2.3.3. 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.

2.3.4. 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.

2.3.5. 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.

2.4. Durata dell'AQ e dei contratti derivati

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.

3. Gestione della Fornitura

Ai fini della gestione dell'Accordo Quadro, ogni Aggiudicatario ha nominato un **Responsabile unico delle attività contrattuali (RUAC)**, che ha la responsabilità delle seguenti attività:

- cura dei rapporti con la Consip S.p.A. e con AgID e suo diretto ed eventuale coinvolgimento su questioni riguardanti le singole Amministrazioni Contraenti, comunque per motivi di carattere straordinario, e su specifica richiesta di Consip/AgID;
- partecipazione agli incontri di allineamento con Consip/AgID;
- coordinamento dei Responsabili del Fornitore e supervisione delle attività a partire dal momento della stipula dei contratti;
- adozione di idonei strumenti per facilitare la comunicazione e lo scambio di informazioni tra i vari soggetti e attori coinvolti nella fornitura;
- assicurazione di un alto grado di sinergia tra le risorse impiegate nei diversi contratti esecutivi al fine di garantire un costante e adeguato grado di conoscenza e di attenzione ed evitando che medesime criticità possano ripetersi su più contratti;
- impostazione, organizzazione, pianificazione e controllo di tutte le azioni necessarie per garantire il rispetto delle prestazioni richieste, secondo i requisiti tecnici e nei tempi previsti, stabiliti anche con le Amministrazioni (ad esempio controllo del Piano Operativo, controllo dell'avanzamento delle prestazioni, verifica del pieno adempimento degli impegni assunti in offerta tecnica, pianificazione e impiego di risorse quantitativamente e qualitativamente adeguate, attività di valutazione e contenimento dei rischi, efficacia ed efficienza dell'attività di test, etc.);
- monitoraggio dell'andamento delle installazioni e controllo del rispetto dei piani concordati tra i Responsabili del Fornitore e le Amministrazioni Contraenti;
- proposta di eventuali azioni correttive a fronte di situazioni critiche;
- monitoraggio della qualità delle prestazioni erogate e dell'andamento dei livelli di servizio per tutto il periodo di efficacia dei contratti ed individuazione delle eventuali azioni correttive a fronte del mancato rispetto degli SLA previsti;
- reporting mensile, o comunque in ogni caso di esplicita richiesta da parte di Consip, sull'andamento dei contratti;
- gestione dei reclami/disservizi/segnalazioni da parte delle Amministrazioni Contraenti e/o della Consip S.p.A., prevedendo che le eventuali relative deduzioni dovranno essere sottoposte al

cospetto del richiedente entro 3 giorni lavorativi dal ricevimento della segnalazione, pena l'applicazione delle penali secondo quanto stabilito nel Capitolato tecnico Speciale;

- gestione delle criticità e dei rischi complessivi di progetto risolvendo tutti i potenziali conflitti e/o eventuali disservizi.

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 nel Capitolato Tecnico Generale.

3.1. 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 di cui al paragrafo 5, 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 riportate al par. 5. 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 al Capitolato Tecnico 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.

3.2. Reporting 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 descritte nel paragrafo 5.

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 30 - 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 31 – 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*".

Parametro	SR
Tempo di emissione del "*Piano Operativo*"	15 giorni lavorativi

Tabella 32 - 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 2.2.2

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	50 giorni solari

Tabella 33 - 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 34 - 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: 6 ore;
    - HP: 3 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: 12 ore;
  - HP: 4 ore;

  Severity Code 2:
  - LP: 16 ore;
  - HP: 8 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 35 - 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 36 - 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 37 - 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 38 - 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 del Capitolato Tecnico parte Generale).
- **Disponibilità del Portale della Fornitura:** definita su base mensile, come il tempo in cui tutta la catena end to end di responsabilità del Fornitore risulta disponibile (nel quale quindi Portale è interamente fruibile) ed il tempo di misurazione (cfr par. 4.1 del Capitolato Tecnico Parte Generale). Per la quantificazione dell'effettiva disponibilità del Portale raggiunta nel mese, si calcoleranno i tempi di indisponibilità risultanti dalle comunicazioni con il Contact Center relativamente alla segnalazione del guasto/malfunzionamento/disservizio e alla sua risoluzione. Si precisa a tal proposito che non saranno considerati ai fini del calcolo della disponibilità del Portale eventuali "ticket" riconducibili a malfunzionamenti imputabili all'utente o ad elementi della catena end-to-end al di fuori della responsabilità del Fornitore, quali la rete internet.

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

Tabella 39 - SLA per la gestione della fornitura

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 del Capitolato Tecnico 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	Valorizzazione della penale	Soggetto avente diritto alla penale
Tempo di emissione del "*Piano Operativo*" (par.4.1.1)	0,5‰ del valore complessivo del contratto per ogni giorno solare di ritardo	Amministrazione Contraente

Tabella 40 - Penali relative all'attivazione della fornitura

Parametro	Valorizzazione della penale	Soggetto avente diritto alla penale
Tempo di consegna, installazione, configurazione e verifica (par. 4.1.2)	1‰ del valore complessivo del contratto per ogni giorno solare di ritardo	Amministrazione Contraente

Tabella 41 - Penali relative alla consegna, installazione, configurazione e verifica

Parametro	Valorizzazione della penale	Soggetto avente diritto alla penale
Predisposizione seconda verifica (par. 4.1.3)	1‰ del valore complessivo del contratto per ogni giorno solare di ritardo.	Amministrazione Contraente
Predisposizione ulteriore verifica collaudo (par. 4.1.3)	1‰ del valore complessivo del contratto per ogni giorno solare di ritardo.	Amministrazione Contraente
Esito negativo seconda verifica (o successive) (par. 4.1.3)	500 Euro	Amministrazione Contraente

Tabella 42 - Penali relative alle attività di supporto alla verifica di conformità

Parametro	**Valorizzazione della penale**	**Soggetto avente diritto alla penale**

Tempestività di risposta al disservizio (par. 4.1.4)	20€ per ogni punto percentuale di scostamento rispetto al valore target.	Amministrazione Contraente
Tempestività di intervento (par. 4.1.4)	20€ per ogni punto percentuale di scostamento rispetto al valore target.	Amministrazione Contraente
Tempestività di ripristino del servizio - Severity Code 1 (par. 4.1.4)	50€ per ogni punto percentuale di scostamento rispetto al valore target.	Amministrazione Contraente
Tempestività di ripristino del servizio - Severity Code 2 (par. 4.1.4)	30€ per ogni punto percentuale di scostamento rispetto al valore target.	Amministrazione Contraente
Attesa per il servizio di Contact Center ed help desk (par. 4.1.4)	300,00 € per ogni punto percentuale in diminuzione rispetto al 95% dei campioni di misura del parametro, calcolato su un periodo di osservazione mensile	Amministrazione Contraente
Percentuale di chiamate perse (par. 4.1.4)	1.000,00 euro per ogni punto percentuale in aumento rispetto al numero dei campioni di misura del parametro, calcolato su un periodo di osservazione mensile	Amministrazione Contraente
Disponibilità del servizio di Contact Center ed help desk (par. 4.1.4)	200 Euro per ogni giorno solare di ritardo	Amministrazione Contraente
Disponibilità delle informazioni di contatto relative al servizio di Contact Center ed help desk (par. 4.1.4)	100 Euro per ogni giorno solare di ritardo	Amministrazione Contraente

Tabella 43 - SLA per i servizi di assistenza e manutenzione

Parametro	Valorizzazione della penale	Soggetto avente diritto alla penale
Tempo di presa in carico del servizio di supporto (cfr. 4.1.5)	1‰ del valore del servizio per ogni giorno lavorativo di ritardo	Amministrazione Contraente
Data di completamento dell'intervento (cfr. 4.1.5)	1‰ del valore del servizio per ogni giorno lavorativo di ritardo	Amministrazione Contraente

Tempo di consegna dei CV delle risorse del servizio di supporto (cfr. 4.1.5)	1‰ del valore del servizio per ogni giorno lavorativo di ritardo	Amministrazione Contraente
Tempo di sostituzione del personale del servizio di supporto (cfr. 4.1.5)	1‰ del valore del servizio per ogni giorno lavorativo di ritardo	Amministrazione Contraente

Tabella 44 - Penali relative al servizio di supporto specialistico

Parametro	Valorizzazione della penale	Soggetto avente diritto alla penale
Slittamento di una scadenza per il servizio di hardening su client (cfr.4.1.6)	1‰ del valore del servizio per ogni giorno lavorativo di ritardo	Amministrazione Contraente

Tabella 45 - Penali relative al servizio di hardening su client

Parametro	Valorizzazione della penale	Soggetto avente diritto alla penale
Data di avvio del servizio di formazione e affiancamento (cfr.4.1.7)	100 € per ogni giorno lavorativo di ritardo	Amministrazione Contraente

Tabella 46 - Penali relative al servizio di addestramento sulla fornitura

Parametro	Valorizzazione della penale	Soggetto avente diritto alla penale
Tempo di gestione delle richieste (par. 4.1.8)	150 € per ogni giorno lavorativo di ritardo	Amministrazione Aggiudicatrice
	150 € per ogni giorno lavorativo di ritardo	Amministrazione Contraente
Tempo di consegna dei dati relativi agli SLA (par. 4.1.8)	100 € per ogni giorno solare di ritardo	Amministrazione Aggiudicatrice
	100 € per ogni giorno solare di ritardo	Amministrazione Contraente
Disponibilità del Portale della Fornitura	Euro 30,00 per ogni punto decimale (0,1 %) di scostamento tra il valore percentuale misurato ed il valore richiesto dal Capitolato Tecnico	Amministrazione Aggiudicatrice

Attivazione del Portale della Fornitura (par. 4.1 del Capitolato Tecnico parte Generale)	Euro 1.000,00 per ogni giorno solare di ritardo	Amministrazione Aggiudicatrice

Tabella 47 - Penali relative alla gestione della fornitura

6. Portale della fornitura

Ogni Fornitore ha reso inoltre disponibile un **"Portale della Fornitura",** multicanale e raggiungibile tramite Internet per consentire alle singole Amministrazioni di governare agevolmente la fornitura e di promuovere la condivisione e l'esperienza maturata nelle varie iniziative.

Il Portale funge anche da strumento di promozione per la PA e di comunicazione tra la PA e i cittadini/imprese, offrendo a questi ultimi servizi di informazione e monitoraggio circa l'andamento delle varie iniziative.

Il Portale è organizzato nelle seguenti aree di fruizione:

- "Area Comunicazione": è l'area ad accesso pubblico del portale, contiene informazioni di carattere generale sull'AQ e informazioni e dati specifici sull'andamento della fornitura e dei servizi connessi; **(a partire dalla I release del portale).**
- "Area Informativa": è l'area di supporto riservata alla PA e contiene almeno le seguenti informazioni: documentazione aggiornata (normativa, tecnologica e operativa) di riferimento per i prodotti e servizi dell'AQ; la descrizione delle soluzioni migliorative offerte **(a partire dalla I release** del portale relativamente alla **documentazione normativa** e **nella versione completa** relativamente alla **documentazione tecnologica e operativa)**;
- "Area Project Management": è l'area ad accesso riservato e profilato per le singole Amministrazioni tramite la quale è possibile disporre degli strumenti di pianificazione e gestione delle singole iniziative progettuali; deve governare l'esecuzione dell'intero workflow operativo di ciascun Appalto Specifico dal Piano Operativo alla verifica di conformità finale ed eventuali rilevazioni nel periodo di garanzia; il Fornitore quindi prevedrà in questa sezione anche le versioni eventualmente aggiornate del Piano Operativo (**a partire dalla I release del portale**).
- "Area Collaborazione e Monitoraggio": è l'area che contiene:
  - gli strumenti e le informazioni di controllo e governo della fornitura quali cruscotti statici e dinamici relativi ai dati di tutti i Piani Operativi e i Contratti Esecutivi;
  - reportistica sul rispetto dei livelli di servizio e degli indicatori di digitalizzazione; report statici e dinamici relativi ai valori economici dei Contratti Esecutivi con evidenza della capacità contrattuale residuale; i dati devono essere estraibili nei formati maggiormente diffusi per lo scambio dati (es. csv, xml, json, xls, ecc.).

  - gli strumenti di promozione di collaborazione e condivisione tra le PA.
- "Area Osservatori": è l'area che consente agli Organismi di coordinamento e controllo e alla Consip S.p.A. di svolgere le proprie funzioni di monitoraggio sulla qualità dei servizi erogati in AQ.

Tutta la reportistica prodotta relativa ai servizi sarà archiviata e conservata a cura del Fornitore, attraverso un sistema di gestione della documentazione riservata.

Per ogni fornitori il portale è fruibile ai seguenti indirizzi:

- RTI FASTWEB: XXXX
- RTI TELECOM: XXXX
- RTI VODAFONE: XXXX

7. Utilizzo dell'AQ

Come in precedenza evidenziato le Amministrazioni dovranno aderire all'AQ esperendo un proprio AS e stabilendo:

- i beni, corredati dei relativi servizi base obbligatori, che intende richiedere, stabilendo le quantità stimate degli stessi. Si precisa che nell'AS dovrà essere richiesto almeno un prodotto.
- gli eventuali servizi base opzionali che intende richiedere, stabilendo le quantità stimate degli stessi;
- gli eventuali servizi accessori che intende richiedere, stabilendo le quantità stimate degli stessi;
- le eventuali funzionalità aggiuntive, personalizzazioni e i requisiti migliorativi premianti in accordo con quanto previsto nella documentazione di gara
- le basi d'asta, che saranno così determinate:
    - per i beni (comprensivi dei servizi base obbligatori) e per i servizi base opzionali le basi d'asta unitarie saranno pari al valore più elevato offerto tra gli Aggiudicatari del lotto relativamente allo specifico bene/servizio. Resta fermo che ogni Aggiudicatario non potrà offrire, in relazione ai beni e servizi base opzionali, un prezzo superiore a quello da lui offerto in prima fase per il corrispondente bene e servizio base;
    - per le funzionalità aggiuntive relative ai beni (comprensive dell'eventuale manutenzione richiesta) e per i servizi accessori, le basi d'asta saranno autonomamente determinate dall'Amministrazione, con il vincolo che il valore complessivo delle basi d'asta inerenti le funzionalità aggiuntive e i servizi accessori **non potrà essere superiore al 40%** della base d'asta complessiva dell'Appalto Specifico.
- la durata del Contratto, che sarà di massimo 24 mesi in funzione dell'oggetto dell'Appalto Specifico;
- un termine congruo per la presentazione delle offerte che, in ogni caso, dovrà essere idoneo rispetto alla complessità dell'oggetto dell'appalto e il tempo necessario per la presentazione dell'offerta, nonché le ulteriori regole del confronto competitivo.
- in relazione alle procedure afferenti gli investimenti pubblici finanziati, in tutto o in parte, con le risorse previste dal Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021 e dal Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, nonché dal PNC, e fermo restando quanto previsto al comma 7 dell'art. 47 D.l. n. 77/2021:
    - il requisito necessario per il Fornitore relativo alla richiesta di assicurare una quota pari almeno al 30 per cento, delle assunzioni necessarie per l'esecuzione del contratto esecutivo o per la realizzazione di attività ad esso connesse o strumentali, all'occupazione giovanile e femminile. É compito dell'Amministrazione motivare, ai sensi di quanto previsto dal succitato comma 7, la scelta di una quota inferiore al 30 per cento sopra indicato, sulla base delle specificità del singolo appalto specifico.

- almeno un requisito migliorativo dell'offerta tra quelle di cui al criterio AS.9.4 del par. 7.1.1.

A tal fine si fanno inoltre presenti le "*Linee guida volte a favorire la pari opportunità di genere e generazionali, nonché l'inclusione lavorativa delle persone con disabilità nei contratti pubblici finanziati con le risorse del PNRR e del PNC*" pubblicate sulla Gazzetta Ufficiale n. 309 del 30 dicembre 2021.

Si precisa che i Fornitori Aggiudicatari non hanno offerto in prima fase dei prodotti specifici, ma unicamente dei meta-prodotti intesi come l'offerta di riferimento per ogni bene richiesto. Ogni meta-prodotto offerto è caratterizzato dalla sua descrizione funzionale, dai requisiti minimi, dai 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), **che dovrà essere indicata unicamente in risposta all'Appalto Specifico** e potrà quindi variare da AS ad AS anche in base alle eventuali personalizzazioni, funzionalità aggiuntive e requisiti migliorativi espressi dall'Amministrazione Contraente in seconda fase, in accordo con quanto previsto nella documentazione dell'AQ.

Si riporta di seguito una schematizzazione di quanto descritto.

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.

L'affidamento di ciascun Appalto Specifico potrà avvenire unicamente a seguito del rilancio del confronto competitivo invitando tutti gli operatori economici aggiudicatari dell'Accordo Quadro. A tale fine, l'Amministrazione inviterà i Fornitori a presentare offerta mediante invio di una Richiesta di offerta.

Per la procedura di confronto competitivo tra i Fornitori, l'Amministrazione utilizzerà i mezzi telematici messi a disposizione dalla Consip S.p.A.. Alla Richiesta di offerta saranno allegati i documenti che costituiscono la *lex specialis* della fase II, nonché lo schema di contratto che sarà sottoscritto con l'aggiudicatario dell'Appalto Specifico. La procedura di aggiudicazione dell'Appalto Specifico verrà delineata nella Richiesta di offerta nel rispetto di quanto previsto dalla disciplina normativa applicabile.

7.1. Criterio di aggiudicazione dell'Appalto Specifico

Ogni singolo Appalto Specifico verrà aggiudicato dall'Amministrazione sulla base del criterio dell'offerta economicamente più vantaggiosa sulla base del miglior rapporto qualità prezzo ai sensi dell'art. 95 del Codice.

Il punteggio totale (pari a 100) per ogni singolo Appalto Specifico verrà determinato in ragione della seguente formula:

$$PTot_{AS} = PT_{ER} + PT_{AS} + PE_{AS}$$

PUNTEGGIO	*DESCRIZIONE*	*Valore min*	*Valore max*
PT_{ER}	Punteggio Tecnico massimo ereditabile	20	66

PT_{AS}	Punteggio Tecnico assegnato in AS	4	50
PE_{AS}	Punteggio Economico assegnato in AS	30	30
$PTot_{AS}$	PUNTEGGIO TOTALE AS	100	

Dove:

PT_{ER} è il Punteggio Tecnico massimo ereditabile. Il valore massimo attribuibile può variare tra il valore minimo di 20 punti ed il valore massimo di 66 punti, in funzione della scelta dell'Amministrazione in merito ai beni e ai servizi richiesti in AS, secondo quanto stabilito nel presente paragrafo;

PT_{AS} è il Punteggio Tecnico massimo attribuibile in ragione dell'offerta tecnica per l'Appalto Specifico. Il valore massimo attribuibile può variare tra il valore minimo di 4 punti ed il valore massimo di 50 punti, in funzione della scelta dell'Amministrazione in merito ai beni e ai servizi richiesti in AS, secondo quanto stabilito nel presente paragrafo;

PE_{AS} è il Punteggio Economico massimo attribuibile in ragione dell'offerta economica per l'Appalto Specifico il cui valore è sempre pari a 30 punti.;

$PTot_{AS}$ è il Punteggio Totale ottenuto dalla somma del punteggio tecnico PT_{ER}, del punteggio tecnico nell'Appalto Specifico PT_{AS} e del punteggio economico nell'Appalto Specifico PE_{AS}. Il valore massimo attribuibile dovrà essere pari a 100 punti.

I valori dei punteggi massimi attribuibili relativamente a ciascuna voce di punteggio (PT_{ER}, PT_{AS} e PE_{AS}) sono determinati dall'Amministrazione in sede di richiesta di Appalto Specifico, sulla base delle seguenti modalità:

- l'Amministrazione stabilisce autonomamente il valore di PT_{AS} tra il valore minimo (4) e il valore massimo (50) in base ai requisiti migliorativi previsti nell'Appalto Specifico selezionati, sulla base dei beni e servizi richiesti, in accordo a quanto previsto nella successiva tabella "Punteggi di AS";
- sulla base del valore di PT_{AS} viene automaticamente determinato il valore di PT_{ER} come 70 - PT_{AS};
- il valore di PE_{AS} è sempre pari a 30.

Con riferimento a ciascun Appalto Specifico, il concorrente (aggiudicatario dell'Accordo Quadro) dovrà:

- formulare una offerta economica con prezzi che, per i beni (comprensivi dei servizi base obbligatori) e per i servizi base opzionali, non dovranno superare i prezzi offerti dallo stesso concorrente in prima fase,
- garantire la fornitura di beni e la prestazione dei servizi con le caratteristiche minime e migliorative offerte dallo stesso concorrente per l'aggiudicazione della prima fase dell'Accordo Quadro e con le eventuali funzionalità aggiuntive richieste dall'Amministrazione nel proprio AS;

- indicare:
  - i propri "costi della manodopera"
  - gli "oneri aziendali concernenti l'adempimento delle disposizioni in materia di salute e sicurezza" sui luoghi di lavoro
  - di cui all'art. 95, comma 10, del Codice.

Saranno esclusi dal confronto competitivo relativo a ciascun Appalto Specifico i concorrenti che:

- offrano anche solo prezzo superiore al corrispondente valore unitario offerto per l'aggiudicazione dell'Accordo Quadro,
- offrano beni e/o servizi privi delle caratteristiche minime e migliorative offerte per l'aggiudicazione in prima fase dell'Accordo Quadro e delle eventuali funzionalità aggiuntive richieste dall'Amministrazione in seconda fase.

7.1.1. Punteggio tecnico dell'Appalto Specifico

Il Punteggio Tecnico $\mathbf{PT^i}$ assegnato al concorrente i-esimo è ottenuto in ragione della seguente formula:

$$\mathbf{PT^i = PT^i_{ER} + PT^i_{AS}}$$

dove:

$\mathbf{PT^i_{ER}}$ è il Punteggio Tecnico Ereditato dal concorrente i-esimo;

$\mathbf{PT^i_{AS}}$ è il Punteggio Tecnico assegnato al concorrente i-esimo attribuito dalla Commissione giudicatrice nominata dall'Amministrazione in fase di Appalto Specifico.

Il $\mathbf{PT^i_{ER}}$ è a sua volta pari a:

$$\mathbf{PT^i_{ER} = PT^i_{AQ} \times K}$$

dove:

$\mathbf{PT^i_{AQ}}$ è il Punteggio Tecnico assegnato al concorrente i-esimo in fase di AQ in base ai beni e ai servizi richiesti dall'Amministrazione nell'Appalto Specifico, stabilito sommando i punteggi ottenuti dal concorrente in relazione ai sub-criteri di AQ (si faccia riferimento alla Tabella presente al paragrafo 17.1 del Capitolato d'Oneri di AQ) secondo quanto previsto nella seguente tabella.

K è un coefficiente di riproporzionamento il cui valore è pari a ($\mathbf{PT_{ER}/PT_{AQMAX}}$) ossia al punteggio tecnico massimo ereditabile (come fissato dall'Amministrazione in sede di Appalto Specifico) diviso per il punteggio massimo ottenibile in I° fase di AQ in base ai punteggi massimi associati ai beni e ai servizi richiesti dall'Amministrazione nell'Appalto Specifico, secondo quanto previsto nella seguente tabella.

Criteri	Sub-Criteri di AQ	Regola	PT_{AQMAX}
Elementi trasversali	9.1; 9.2; 11.1; 11.2	Sempre ereditati	10
SIEM	1.1; 1.2; 1.3; 1.4; 1.5; 1.6; 1.7	Ereditati se l'AS include il relativo bene	10
SOAR	2.1; 2.2; 2.3		3
SEG	3.1; 3.2; 3.3; 3.4; 3.5; 3.6; 3.7; 3.8; 3.9; 3.10		5,3
SWG	4.1; 4.2; 4.3; 4.4; 4.5; 4.6; 4.7; 4.8		4,1
DB Security	5.1; 5.2		3
DLP	6.1; 6.2; 6.3		5
PAM	7.1; 7.2; 7.3; 7.4; 7.5; 7.6; 7.7; 7.8; 7.9		4,6
WAF	8.1; 8.2; 8.3; 8.4; 8.5; 8.6		11
Servizio di manutenzione (profilo LP)	9.3; 11.3; 11.5; 11.6	Ereditati se l'AS include il relativo servizio	4,6
Servizio di manutenzione (profilo HP)	9.3; 11.4; 11.7; 11.8		5,4
Servizio di supporto specialistico	10.1; 10.2; 10.3; 10.4; 10.5		4
Servizio di hardening su client	9.4		3

Il punteggio PT^{i}_{ER} e il coefficiente K saranno arrotondati alla quarta cifra decimale.

A titolo **esemplificativo** si consideri:

- un Appalto Specifico che includa il bene "SOAR" e il servizio di manutenzione con profilo LP;
- l'i-esimo concorrente che in fase di AQ abbia ottenuto:
  - per l'ambito Elementi trasversali (somma dei punteggi dei criteri di AQ n. 9.1; 9.2; 11.1; 11.2): 6 punti
  - per l'ambito SOAR (somma dei punteggi dei criteri di AQ n. 2.1, 2.2, 2.3): 2 punti
  - per l'ambito Servizio di manutenzione relativo al profilo LP (somma dei punteggi dei criteri di AQ n. 9.3; 11.3; 11.5; 11.6): 4 punti
- che l'Amministrazione decida che il Punteggio Tecnico massimo attribuibile per l'offerta tecnica dell"Appalto Specifico (PT_{AS}) sia pari a 20 punti, selezionati tra gli elementi della successiva tabella.

In tale scenario si avrebbe:

- $PTot_{AS} = PT_{ER} + PT_{AS} + PE_{AS} = 50 + 20 + 30 = 100$
- PT_{AQMAX} = Somma di PT_{AQMAX} per gli ambiti: "Elementi trasversali", "SOAR", "Servizio di manutenzione" = 17,6 punti
- $K = PT_{ER}/PT_{AQMAX} = 50/17,6 = 2,8409$
- PT^{i}_{AQ} = Somma dei punteggi ottenuti dall'i-esimo concorrente in AQ per gli ambiti: "Elementi trasversali", "SOAR", "Servizio di manutenzione" = 12 punti
- $PT^{i}_{ER} = PT^{i}_{AQ} \times K = 12 \times 2,8409 = 34,0908$ punti

Come ausilio alla determinazione dei punteggi ereditati dagli Aggiudicatari è disponibile tra la documentazione a supporto il foglio excel "ID 2174 – Excel di ausilio AS".

Sulla base della composizione del proprio Appalto Specifico, l'Amministrazione dovrà autonomamente scegliere quali sub-criteri di valutazione premiare tra quelli stabiliti nella tabella seguente, sulla base degli elementi previsti e delle proprie valutazioni in termini di rilevanza e/o criticità rispetto all'oggetto dell'appalto.

In particolare, per ciascun sub-criterio di valutazione tecnica, nella Richiesta di offerta di ciascun Appalto Specifico l'Amministrazione dovrà indicare il massimo punteggio attribuibile, che **non potrà essere superiore al punteggio massimo stabilito per ciascun sub-criterio**. Ad esempio, per il sub-criterio AS 1.1 l'Amministrazione potrà assegnare un punteggio tabellare massimo pari o inferiore a due punti e maggiore di zero. Resta inoltre fermo il fatto che l'Amministrazione potrà associare ad un prodotto richiesto unicamente i sub-criteri di valutazione che afferiscono a quello specifico prodotto. Ad esempio al prodotto SIEM potrà essere associato il sub-criterio AS.1.1 **ma non** il criterio AS.5.1.

Criterio		ID	Sub-Criterio di valutazione	punti D max (punteggio massimo assegnabile)	punti T max (punteggio massimo assegnabile)
1	SIEM	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		2
		AS.1.2	Integrazione con specifica piattaforma di vulnerability management richiesta dall'Amministrazione		2
		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.	5	
		AS.1.4	Cattura e analisi dei flussi di rete anche in formato Jflow		0,5
		AS.1.5	Cattura e analisi dei flussi di rete anche in formato Sflow		0,5
		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.	5	

Criterio		ID	Sub-Criterio di valutazione	punti D max (punteggio massimo assegnabile)	punti T max (punteggio massimo assegnabile)
		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.	5	
		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.	2	
2	SOAR	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	4	
		AS.2.2	Integrazione con una specifica piattaforma di Service Management richiesta dall'Amministrazione		2
		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.	5	
		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.	2	

Criterio		ID	Sub-Criterio di valutazione	punti D max (punteggio massimo assegnabile)	punti T max (punteggio massimo assegnabile)
		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	4	
3	SEG	AS.3.1	Integrazione con soluzioni di sicurezza richieste dalla PA (soluzioni Anti APT, NGFW, SIEM, etc)		2
		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.	2	
4	SWG	AS.4.1	Integrazione con soluzioni di sicurezza richieste dalla PA (soluzioni Anti APT, NGFW, SIEM, etc)		2
		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.	2	
5	DB Security	AS.5.1	Varietà dei DB relazionali supportati (oltre ai minimi previsti in AQ)	2	
		AS.5.2	Integrazione con uno specifico sistema HSM richiesto dall'Amministrazione per la generazione e lo storage delle chiavi di crittografia		2
		AS.5.3	Integrazione con una specifica piattaforma di SIEM richiesta dall'Amministrazione		2
		AS.5.4	Varietà dei DB non relazionali supportati	2	
		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	2	
		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.)	2	
		AS.5.7	Varietà di ambienti cloud supportati e scalabilità in termini di numero di istanze gestibili	2	

Criterio		ID	Sub-Criterio di valutazione	punti D max (punteggio massimo assegnabile)	punti T max (punteggio massimo assegnabile)
6	DLP	AS.6.1	Possibilità di implementare policy che consentano di prevenire l'invio di dati verso IP appartenenti ad area geografiche considerate rischiose.		1
		AS.6.2	Supporto al file fingerprinting		1
		AS.6.3	Integrazione con una piattaforma di MDM specificata dall'Amministrazione		2
		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	2	
		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	2	
		AS.6.6	Compatibilità della soluzione CASB con specifiche applicazioni cloud richieste dall'Amministrazione		2
		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).	2	
		AS.6.8	Capacità della soluzione di supportare, semplificandola, l'attività di classificazione dei dati da parte degli operatori, presente e futura.	1	
		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).	5	
		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		1
		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	2	

Criterio		ID	Sub-Criterio di valutazione	punti D max (punteggio massimo assegnabile)	punti T max (punteggio massimo assegnabile)
		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	2	
7	PAM	AS.7.1	Supporto di ulteriori specifici sistemi operativi richiesti dall'Amministrazione		1
		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	5	
		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	5	
		AS.7.4	Supporto di dispositivi di rete e di dispositivi e sistemi di sicurezza specifici richiesti dall'Amministrazione		2
		AS.7.5	Integrazione con una specifica piattaforma di vulnerability management richiesta dall'Amministrazione		2
		AS.7.6	Integrazione con una specifica soluzione di MFA richiesta dall'Amministrazione		2
		AS.7.7	Possibilità di limitare l'accesso sulla base della localizzazione dell'utente		1

Criterio		ID	Sub-Criterio di valutazione	punti D max (punteggio massimo assegnabile)	punti T max (punteggio massimo assegnabile)
		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	2	
		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.	2	
		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.	1	
8	WAF	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.	5	
		AS.8.2	Integrazione con soluzioni di sicurezza richieste dalla PA (soluzioni Anti APT, NGFW, SIEM, etc)		3
		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.	2	
		AS.8.4	Efficacia delle funzionalità aggiuntive di bilanciamento del carico a livello 7 rispetto alle minime richieste dalla PA e/o relative modalità di implementazione	5	
		AS.8.5	Supporto standard PCI DSS		2
		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	3	
9	Servizi	AS.9.1	Ulteriori competenze ed esperienze specifiche del personale addetto ai servizi (ad eccezione del	6	

Criterio		ID	Sub-Criterio di valutazione	punti D max (punteggio massimo assegnabile)	punti T max (punteggio massimo assegnabile)
			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	Misure premiali volte a promuovere l'assunzione di giovani e donne, la parità di genere e le ulteriori misure di conciliazione vita lavoro, indicate in conformità a quanto previsto dall'art. 47, comma 5, Decreto Legge 31 maggio 2021 n. 77.		
		AS.9.5	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.	2	
		AS.9.6	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	7	
10	Servizio di supporto specialistico	Security Principal			
		AS.10.1	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.		1
		Senior Security Architect			
		AS.10.2	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.		1
		Senior Security Tester			
		AS.10.3	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.		0,75

Criterio		ID	Sub-Criterio di valutazione	punti D max (punteggio massimo assegnabile)	punti T max (punteggio massimo assegnabile)
		Senior Security Analyst			
		AS.10.4	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.		0,75
		Junior Security Analyst			
		AS.10.5	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.		0,5
11	SLA	AS.11.1	Miglioramento dei livelli di servizio richiesti (rispetto ai valori migliorativi previsti in AQ)	5	

Si precisa che in fase di Appalto Specifico l'Amministrazione:

- potrà associare alle funzionalità aggiuntive relative ai beni previsti i requisiti migliorativi riportati nelle specifiche tabelle descritte nei precedenti paragrafi;
- dovrà stabilire i punteggi massimi in maniera tale che la somma relativa ai **sub-criteri AS.9.1, AS.9.2, AS.9.3, AS.9.4, AS.10.1, AS.10.2, AS.10.3, AS.10.4 e AS.10.5, non sia superiore a 6**.

Le modalità di assegnazione dei punteggi tabellari e discrezionali saranno le medesime previste per la fase di AQ, per le quali si rimanda a quanto descritto nel Capitolato d'Oneri di AQ. In particolare per i criteri discrezionali è previsto l'utilizzo del confronto a coppie.

7.1.2. Punteggio economico dell'Appalto Specifico

Il Punteggio economico $\mathbf{PE_{AS}}$ sarà assegnato con l'utilizzo della seguente formula **"lineare/concava a punteggio assoluto"***:*

$$Ci = 1-(1-Ri)^k$$

dove:

Ci = *coefficiente attribuito al concorrente i-esimo;*

Ri = *ribasso dell'offerta del concorrente i-esimo determinato come specificato nel seguito*

k=2 *parametro che determina la concavità della curva di punteggio*

Il Ribasso offerto (R) sarà calcolato mediante la formula R = 1 – P/ BA_{AS}, dove P è il prezzo complessivo offerto arrotondato alla seconda cifra decimale, determinato come di seguito descritto, e BA_{AS} è l'Importo totale a base d'asta dell'AS.

La base d'asta dell'AS (BA_{AS}) è determinata come somma delle basi d'asta relative alle forniture (BA_F), ai servizi base (BA_{SB}) e alle funzionalità aggiuntive dei prodotti e servizi aggiuntivi (BA_{SA}).

Relativamente a BA_F e a BA_{SB} la base d'asta è così determinata:

- l'Amministrazione, definendo i prodotti e gli eventuali servizi base oggetto dell'Appalto Specifico, enuclea dall'offerta di ciascun aggiudicatario dell'Accordo Quadro i prezzi relativi ai prodotti e servizi di interesse e li moltiplica per le rispettive quantità richieste nell'Appalto Specifico, calcolando l'offerta più alta, ovvero meno vantaggiosa per l'Amministrazione medesima.
- il valore complessivo di detta offerta (offerta più alta, ovvero meno vantaggiosa per l'Amministrazione) determina l'importo della base d'asta dell'Appalto Specifico, relativamente alla componente $BA_F + BA_{SB}$.

A titolo esemplificativo si consideri un AS con oggetto il prodotto "X" e il servizio base "Y" con l'ipotesi che l'AQ sia stato aggiudicato a tre fornitori:

a) l'Amministrazione definisce l'oggetto dell'Appalto Specifico, richiedendo il prodotto X nella quantità N = 2 e il servizio base Y nella quantità M = 2;
b) l'Amministrazione determina l'importo derivante dall'offerta di AQ per ciascun aggiudicatario sulla base del prezzo unitario offerto e delle relative quantità
c) l'Amministrazione determina la base d'asta dell'Appalto Specifico quale importo pari all'offerta più alta presentata per l'aggiudicazione dell'Accordo Quadro

	Prezzo offerto prodotto X	Prezzo offerto servizio Y	Prezzo complessivo prodotti (Prezzo x Quantità)	Prezzo complessivo servizi (Prezzo x Quantità)	Prezzo complessivo
Fornitore A	50	40	100	80	180
Fornitore B	80	40	160	80	240
Fornitore C	70	60	140	120	260

La base d'asta dell'Appalto Specifico, relativamente a BA_F e a BA_{SB}, è quindi pari a 260.

Relativamente alle funzionalità aggiuntive dei prodotti e ai servizi aggiuntivi l'Amministrazione provvederà a definire autonomamente la relativa base d'asta BA_{SA}. Tale base d'asta, BA_{SA}, **non può essere superiore al 40% della base d'asta complessiva BA_{AS} dell'AS** ($BA_F + BA_{SB} + BA_{SA}$).

Come ausilio alla determinazione della base d'asta di AS è disponibile tra la documentazione a supporto il foglio excel "ID 2174 – Excel di ausilio AS".

7.2. Modalità operative per la realizzazione di un AS

Per la descrizione dettagliata delle attività previste per la realizzazione di un Appalto specifico si faccia riferimento al documento "Guida alla predisposizione dell'AS" disponibile tra la documentazione a supporto.