**CONSIP S.p.A. a socio unico**

**INFORMAZIONI RELATIVE ALLA PROCEDURA APERTA PER L'AFFIDAMENTO DI UN ACCORDO QUADRO IN UN UNICO LOTTO AI SENSI DELL'ART 54 COMMA 4 LETT. C) DEL D. LGS. 50/2016 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 CUI ALL'AVVISO DI PREINFORMAZIONE INVIATO PER LA PUBBLICAZIONE ALLA GUUE IN DATA 25/05/2021**

## 1. PREMESSA

Consip S.p.A. ha inviato per la pubblicazione alla GUUE in data 25/05/2021 un Avviso di preinformazione, al fine di rendere nota l'intenzione di bandire una gara a procedura aperta per l'affidamento di un Accordo Quadro ai sensi dell'art. 54 comma 4 lett. c) del d. lgs. 50/2016, 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.

Contestualmente a tale Avviso la Consip ha reso disponibili, mediante pubblicazione sul sito **www.consip.it, www.acquistinretepa.it**, il presente documento contenente alcune informazioni relative alla procedura di cui sopra e due documenti contenenti le Condizioni della suddetta fornitura (denominati Condizioni di fornitura parte Generale e parte Speciale).

## 2. INFORMAZIONI

### 2.1 OGGETTO

Gara a procedura aperta per l'affidamento di un Accordo Quadro in un unico lotto ai sensi dell'art. 54 comma 4 lett. c) del d. lgs. 50/2016, 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.

***

In particolare la presente procedura sarà finalizzata all'affidamento di un Accordo Quadro **con più operatori economici** ai sensi dell'art. 54 comma 4, lett. c) del d. lgs. n. 50/2016 e dell'art. 2, comma 225, Legge n. 191/2009.
L'affidamento degli Appalti Specifici avverrà riaprendo il confronto competitivo tra gli operatori economici parti dell'Accordo Quadro, sulla base di quanto di seguito precisato.

L'Amministrazione che intende procedere con l'affidamento di un Appalto Specifico consulterà per iscritto gli operatori economici parti dell'Accordo Quadro, invitando gli stessi Fornitori a presentare offerta mediante invio di una Richiesta di offerta.
I confronti competitivi si basano sulle condizioni stabilite nell'Accordo Quadro, se del caso precisandole, sulla base delle altre condizioni nel seguito indicate.
Il confronto competitivo tra operatori economici parti dello stesso Accordo Quadro si svolgerà tramite il Sistema (la piattaforma telematica di negoziazione nella disponibilità di Consip S.p.A.), mediante il quale l'Amministrazione invierà la Richiesta di offerta.

### 2.2 BASI D'ASTA

| n. | Descrizione beni e servizi | CPV | P *(principale)* S *(secondaria)* | Importo |
|---|---|---|---|---|
| 1 | Prodotti per la gestione degli eventi di sicurezza e degli accessi, la protezione dei canali email, web e dati | 48730000-4<br>48760000-3<br>32420000-3 | P | € 97.443.546 |
| 2 | Servizio di installazione e configurazione, servizio di supporto alla verifica di conformità, | 51611100-9<br>72212730-5 | P | |

| | | | | |
|---|---|---|---|---|
| | servizio di Contact Center | 79511000-9 | | |
| 3 | Servizio di manutenzione (comprensivo dell'help desk), servizio di supporto specialistico, servizio di hardening su client, servizio di formazione e affiancamento | 72250000-2<br>72267000-4<br>72000000-5<br>72267100-0<br>72253000-3<br>80500000-9 | P | € 37.556.454 |
| | | | **Importo totale a base d'asta** | **€ 135.000.000** |

Le sotto basi d'asta e le quantità richieste/stimate sono riportate nella sottostante tabella.

| SEZIONE 1 - Security Information and Event Management (SIEM) | | | |
|---|---|---|---|
| N. | voce di offerta economica | quantità richiesta/stimata | sotto base d'asta |
| *1* | SIEM - Fascia 1 [Euro ad unità] | 45 | € 23.792.220,00 |
| *2* | SIEM - Fascia 2 [Euro ad unità] | 30 | |
| *3* | SIEM - Fascia 3 [Euro ad unità] | 25 | |
| *4* | SIEM - Fascia 4 [Euro ad unità] | 20 | |
| *5* | SIEM - Fascia 5 [Euro ad unità] | 20 | |
| *6* | SIEM - Fascia 6 [Euro ad unità] | 20 | |
| SEZIONE 2 - Security Orchestration, Automation and Response (SOAR) | | | |
| n° | voce di offerta economica | quantità richiesta/stimata | sotto base d'asta |
| *7* | SOAR - Configurazione Tipo 1 [Euro a configurazione tipo] | 11 | € 5.691.600,00 |
| *8* | SOAR - Configurazione Tipo 2 [Euro a configurazione tipo] | 7 | |
| SEZIONE 3 - Secure Email Gateway (SEG) | | | |
| n° | voce di offerta economica | quantità richiesta/stimata | sotto base d'asta |
| *9* | SEG - Fascia 1 [Euro ad unità] | 157 | € 11.099.637,00 |
| *10* | SEG - Fascia 2 [Euro ad unità] | 79 | |
| *11* | SEG - Fascia 3 [Euro ad unità] | 53 | |
| *12* | SEG - Fascia 4 [Euro ad unità] | 20 | |
| *13* | SEG - Fascia 5 [Euro ad unità] | 9 | |
| SEZIONE 4 - Secure Web Gateway (SWG) | | | |
| n° | voce di offerta economica | quantità richiesta/stimata | sotto base d'asta |
| *14* | SWG - Fascia 1 [Euro ad unità] | 18 | € 2.604.693,00 |
| *15* | SWG - Fascia 2 [Euro ad unità] | 8 | |
| *16* | SWG - Fascia 3 [Euro ad unità] | 6 | |
| *17* | SWG - Fascia 4 [Euro ad unità] | 1 | |
| SEZIONE 5 - Database Security (DB Security) | | | |
| n° | voce di offerta economica | quantità richiesta/stimata | sotto base d'asta |
| *18* | DB_Security - Configurazione Tipo 1 [Euro a configurazione tipo] | 43 | € 9.778.691,00 |
| *19* | DB_Secuirty - Configurazione Tipo 2 [Euro a configurazione tipo] | 13 | |
| SEZIONE 6 - Data Loss Prevention (DLP) | | | |
| n° | voce di offerta economica | quantità richiesta/stimata | sotto base d'asta |
| *20* | DLP - Fascia 1 [Euro ad unità] | 11490 | € 8.361.726,00 |

| | | | |
|---|---|---|---|
| *21* | DLP - Fascia 2 [Euro ad unità] | 4125 | |
| *22* | DLP - Fascia 3 [Euro ad unità] | 11586 | |
| *23* | DLP - Fascia 4 [Euro ad unità] | 53439 | |
| SEZIONE 7 - Privileged Access Management (PAM) | | | |
| n° | voce di offerta economica | quantità richiesta/stimata | sotto base d'asta |
| *24* | PAM - Fascia 1 [Euro ad unità] | 952 | € 6.720.350,00 |
| *25* | PAM - Fascia 2 [Euro ad unità] | 789 | |
| *26* | PAM - Fascia 3 [Euro ad unità] | 3643 | |
| SEZIONE 8 - Web Application Firewall (WAF) | | | |
| n° | voce di offerta economica | quantità richiesta/stimata | sotto base d'asta |
| *27* | WAF - Fascia 1 [Euro ad unità] | 123 | € 29.394.629,00 |
| *28* | WAF - Fascia 2 [Euro ad unità] | 113 | |
| *29* | WAF - Fascia 3 [Euro ad unità] | 14 | |
| SEZIONE 9 - Servizio di manutenzione | | | |
| n° | voce di offerta economica | quantità richiesta/stimata (espressa in forma percentuale) | sotto base d'asta |
| *30* | Profilo LP (Business Day) [Percentuale/Anno] | 60% | € 19.469.220,00 |
| *31* | Profilo HP (H24) [Percentuale/Anno] | 35% | |
| SEZIONE 10 - Servizio di supporto specialistico | | | |
| n° | voce di offerta economica | Quantità richiesta/stimata | base d'asta unitaria |
| *32* | Security Principal - fascia standard [Euro a giorno/persona] | 341 | € 680,00 |
| *33* | Security Principal - fascia straordinaria [Euro a giorno/persona] | 69 | € 884,00 |
| *34* | Senior Security Architect - fascia standard [Euro a giorno/persona] | 4966 | € 520,00 |
| *35* | Senior Security Architect - fascia straordinaria [Euro a giorno/persona] | 926 | € 676,00 |
| *36* | Senior Security Tester - fascia standard [Euro a giorno/persona] | 1511 | € 460,00 |
| *37* | Senior Security Tester - fascia straordinaria [Euro a giorno/persona] | 436 | € 598,00 |
| *38* | Senior Security Analyst - fascia standard [Euro a giorno/persona] | 5583 | € 500,00 |
| *39* | Senior Security Analyst - fascia straordinaria [Euro a giorno/persona] | 1666 | € 650,00 |
| *40* | Junior Security Analyst - fascia standard [Euro a giorno/persona] | 17266 | € 260,00 |
| *41* | Junior Security Analyst - fascia straordinaria [Euro a giorno/persona] | 4929 | € 338,00 |
| SEZIONE 11 - Servizio di hardening su client | | | |
| n° | voce di offerta economica | quantità richiesta/stimata | sotto base d'asta |
| *42* | Fase di assessment [Euro ad attività] | 186 | € 729.756,00 |
| *43* | Fase di progettazione degli interventi [Euro ad attività] | 186 | |
| *44* | Fase di distribuzione degli interventi - N. elementi del Cluster 2 - 1000 [Euro ad attività] | 149 | |
| *45* | Fase di distribuzione degli interventi - N. elementi del Cluster 1001 - 5000 [Euro ad attività] | 15 | |
| *46* | Fase di distribuzione degli interventi - N. elementi del Cluster maggiori di 5000 [Euro ad attività] | 22 | |
| SEZIONE 12 - Servizio di formazione e affiancamento | | | |

| n° | voce di offerta economica | quantità richiesta/stimata | base d'asta unitaria |
|---|---|---|---|
| *47* | Modulo formativo [Euro a modulo] | 1838 | € 1.562,00 |

L'importo a base di gara è al netto di Iva e/o di altre imposte e contributi di legge nonché degli oneri per la sicurezza dovuti a rischi da interferenze che saranno quantificati dalle singole PPAA in sede di Appalto Specifico.

### 2.3 CONDIZIONI DI PARTECIPAZIONE

#### 2.3.1) ABILITAZIONE ALL'ESERCIZIO DELL'ATTIVITÀ PROFESSIONALE, INCLUSI I REQUISITI RELATIVI ALL'ISCRIZIONE NELL'ALBO PROFESSIONALE O NEL REGISTRO COMMERCIALE

Elenco e breve descrizione delle condizioni:

- iscrizione nel registro tenuto dalla Camera di commercio industria, artigianato e agricoltura oppure nel registro delle commissioni provinciali per l'artigianato per attività coerenti con quelle oggetto della procedura di gara.
  Il concorrente non stabilito in Italia ma in altro Stato Membro o in uno dei Paesi di cui all'art. 83, comma 3, del Codice, presenta dichiarazione giurata o secondo le modalità vigenti nello Stato nel quale è stabilito.

#### 2.3.2) CAPACITÀ ECONOMICA E FINANZIARIA

Elenco e breve descrizione dei criteri di selezione:

- **fatturato specifico medio annuo** nel settore di attività "forniture e servizi inerenti la Sicurezza ICT".

Livelli minimi di capacità eventualmente richiesti: fatturato riferito agli ultimi n. 2 esercizi finanziari disponibili ovvero sia approvati, alla data di scadenza del termine per la presentazione delle offerte, non inferiore ad € 8.000.000, IVA esclusa.

#### 2.3.3) CAPACITÀ PROFESSIONALE E TECNICA

Elenco e breve descrizione dei criteri di selezione:

- possesso valutazione di conformità del proprio sistema di gestione della sicurezza delle informazioni alla norma ISO 27001:2013 o ISO 27001:2014 o ISO 27001:2017.
  Livelli minimi di capacità eventualmente richiesti: valutazione di conformità idonea, pertinente e proporzionata al seguente ambito di attività: progettazione, installazione, manutenzione di sistemi di sicurezza ICT.
- possesso di una valutazione di conformità del proprio sistema di gestione della qualità alla norma UNI EN ISO 9001:2015.
  Livelli minimi di capacità eventualmente richiesti: valutazione di conformità idonea, pertinente e proporzionata al seguente oggetto: progettazione, installazione, manutenzione di sistemi di sicurezza ICT.

### 2.4 CAUZIONE PROVVISORIA

Sarà richiesta la produzione di una cauzione provvisoria ai sensi dell'art. 93 del D.lgs. 50/2016 di importo pari al 2% del prezzo base dell'appalto e precisamente di importo pari a euro 2.700.000, salvo quanto previsto all'art. 93, comma 7 del Codice.

### 2.5 SOPRALLUOGO

Non è previsto il sopralluogo.

### 2.6 CRITERI DI AGGIUDICAZIONE

L'appalto sarà aggiudicato con il criterio **dell'offerta economicamente più vantaggiosa individuata sulla base del miglior rapporto qualità/prezzo.**
La valutazione dell'offerta tecnica e dell'offerta economica sarà effettuata in base ai seguenti punteggi.

| | PUNTEGGIO MASSIMO |
|---|---|
| Offerta tecnica | 70 |
| Offerta economica | 30 |
| TOTALE | **100** |

Il punteggio dell'offerta tecnica è attribuito sulla base dei criteri di valutazione elencati nella sottostante tabella.
In particolare nella colonna "Tipologia Subcriterio" vengono indicati:

- con la lettera D i subcriteri relativi a "**Punteggi discrezionali**", vale a dire i punteggi attribuiti in ragione dell'esercizio della discrezionalità spettante alla commissione giudicatrice;
- con la lettera T i subcriteri relativi a "**Punteggi tabellari**", vale a dire i punteggi attribuiti o non attribuiti in ragione dell'offerta o mancata offerta di quanto specificamente richiesto.

| Criteri di valutazione | | ID | Subcriteri di valutazione | Tipologia Subcriterio |
|---|---|---|---|---|
| 1 | SIEM | *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; | T |
| | | 1.2 | ○ sistema operativo Mac OS | T |
| | | 1.3 | ○ piattaforma di virtualizzazione KVM | T |
| | | 1.4 | ○ piattaforma di virtualizzazione Hyper-V | T |
| | | 1.5 | Filtraggio dei log/eventi ricevuti o prelevati dalle sorgenti per evitare che vengano elaborati e memorizzati | T |
| | | 1.6 | Possibilità di interrogare la base dati della soluzione tramite API | T |
| | | 1.7 | Possibilità di integrare piattaforme di threat intelligence tramite standard STIX/TAXII | T |
| 2 | SOAR | 2.1 | Automazione di azioni basate su scripts | T |
| | | 2.2 | Possibilità di interrogare la base dati della soluzione tramite API | T |
| | | 2.3 | Integrabilità con piattaforme e sorgenti di eventi sicurezza tramite API e/o SDK | T |
| 3 | SEG | 3.1 | Cifratura automatica dei messaggi in uscita per i quali risultano verificate delle politiche di identificazione configurabili (policy based encryption) | T |
| | | 3.2 | Identificazione di immagini potenzialmente dannose (almeno contenuti pornografici) | T |
| | | 3.3 | Creazione di regole di spam personalizzate | T |
| | | 3.4 | Identificazione di testo nascosto all'interno di immagini presenti nelle email | T |
| | | 3.5 | Possibilità di interfacciarsi con piattaforme di threat intelligence (almeno MISP) | T |
| | | 3.6 | Possibilità di interrogare la base-dati della soluzione tramite API | T |

| Criteri di valutazione | | ID | Subcriteri di valutazione | Tipologia Subcriterio |
|---|---|---|---|---|
| | | 3.7 | Funzionalità di Data Loss Prevention nell'ispezione delle mail in uscita attraverso l'identificazione di parole chiave o pattern di dati | T |
| | | 3.8 | Rimozione del contenuto attivo dell'email (ad esempio la rimozione di MACRO) | T |
| | | 3.9 | Funzionalità di sandboxing integrata o su cloud del Produttore | T |
| | | 3.10 | Funzionalità di Cousin Domain Detection | T |
| 4 | SWG | 4.1 | Funzionalità di SSL/TLS Inspection a livello hardware su chipset dedicato | T |
| | | 4.2 | Supporto del protocollo WCCP per l'implementazione in modalità trasparente | T |
| | | 4.3 | Funzionalità di file reputation | T |
| | | 4.4 | Identificazione di testo nascosto all'interno di immagini presenti nel traffico web | T |
| | | 4.5 | Funzionalità di DLP nell'ispezione del traffico verso server (HTTP POST):<br>- identificazione di parole chiave o pattern di dati<br>- possibilità di effettuare fingerprinting di file/cartelle | T |
| | | 4.6 | Possibilità interrogare la base-dati della soluzione tramite API | T |
| | | 4.7 | Possibilità di configurare delle eccezioni relativamente al traffico da non intercettare in modalità SSL inspection | T |
| | | 4.8 | Supporto del protocollo ICAP per l'integrazione con Server ICAP esterni | T |
| 5 | DB Security | 5.1 | Possibilità di effettuare un controllo dei privilegi di accesso ai dati per singolo record e per singolo campo di record | T |
| | | 5.2 | Possibilità di interrogare la base dati della soluzione tramite API | T |
| 6 | DLP | 6.1 | Crittografia dei file basata sulle policy aziendali per la protezione dei dati sensibili archiviati in supporti rimovibili | T |
| | | 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 | T |
| | | 6.3 | Possibilità di interrogare la base dati della soluzione tramite API | T |
| 7 | PAM | 7.1 | Discovery automatico degli account privilegiati | T |
| | | 7.2 | Supporto all'autenticazione di terze parti (ad es. fornitori, consulenti) che accedono da remoto | T |

| Criteri di valutazione | | ID | Subcriteri di valutazione | Tipologia Subcriterio |
|---|---|---|---|---|
| | | 7.3 | Supporto dispositivi IoS e Android | T |
| | | 7.4 | Possibilità di utilizzare una password in real-time senza che l'utente conosca mai la password utilizzata | T |
| | | 7.5 | Supporto della connessione ai sistemi target tramite protocollo IPv6 | T |
| | | 7.6 | Possibilità di interrogare la base dati della soluzione tramite API | T |
| | | 7.7 | Encryption delle password anche mediante ulteriori protocolli (ad es. RSA) | T |
| | | 7.8 | Possibilità di definire dei workflow per la gestione del processo autorizzativo degli accessi per gli account privilegiati | T |
| | | 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 | T |
| 8 | WAF | 8.1 | Dashboard di monitoraggio in tempo reale con funzionalità drill-down almeno per: Attacchi, Sessioni, dati Geografici di accesso | T |
| | | 8.2 | Virtual Patching | T |
| | | 8.3 | Ispezione del traffico FTP e FTPS | T |
| | | 8.4 | Funzionalità di Data Loss Prevention | T |
| | | 8.5 | Possibilità di interrogare la base dati della soluzione tramite API | T |
| | | 8.6 | Funzionalità di sandboxing su cloud del Produttore | T |
| 9 | Struttura organizzativa e modalità impiegate per l'erogazione dei servizi connessi alla fornitura | 9.1 | Qualità dei Centri di Competenza nel settore della Sicurezza ICT, in termini di:<br>- varietà e specificità delle competenze del personale impiegato, acquisite sia in ambito nazionale che internazionale;<br>- tipologie, modalità e frequenza degli aggiornamenti formativi;<br>- numerosità e continuità delle collaborazioni con università, enti di ricerca, start up, produttori di tecnologia;<br>- presenza di laboratori presso i quali analizzare o testare le soluzioni tecnologiche da inserire nel proprio portfolio di offerta.<br><br>Per Centro di Competenza nel settore della Sicurezza ICT si intende una struttura che consenta di: | D |

| Criteri di valutazione | | ID | Subcriteri di valutazione | Tipologia Subcriterio |
|---|---|---|---|---|
| | | | - presidiare il mercato della sicurezza ICT effettuando uno scouting degli ultimi trend evolutivi tecnologici nonché dei prodotti di mercato, al fine di assicurare una proposizione di soluzioni e servizi in grado di proteggere i sistemi della PA dalle minacce cibernetiche in costante evoluzione;<br>- sviluppare e consolidare le competenze necessarie per progettare, realizzare e gestire soluzioni e servizi nell'ambito della sicurezza ICT. | |
| | | *Capacità di ottimizzare le attività di aggiornamento (9.2) e l'erogazione dei servizi di manutenzione (9.3) e hardening su client (9.4) anche ai fini di dimostrare il soddisfacimento dei livelli di servizio offerti dal Concorrente descritti nelle Condizioni di fornitura parte Speciale in base ai seguenti elementi:* | | |
| | | 9.2 | - modalità operative e strumenti adottati per una diagnosi proattiva e/o tempestiva di eventuali anomalie SW e HW, che potrebbero compromettere e/o che compromettono la sicurezza dei sistemi dell'Amministrazione;<br>- modalità di rilascio e deployment degli aggiornamenti sw, al fine di assicurare la continuità operativa dei sistemi dell'Amministrazione e al contempo la loro sicurezza. | D |
| | | 9.3 | - modello organizzativo e strumenti adottati dalle strutture di supporto qualificato e per la logistica, per le attività di ripristino/riparazione dei prodotti software e hardware oggetto della fornitura(es. strutture di coordinamento, di assistenza tecnica hardware e software, magazzini di parti di ricambio, etc.);<br>- modalità e tempistiche di approvvigionamento e gestione delle parti di ricambio. | D |
| | | 9.4 | Modalità operative e strumenti adottati per il servizio di hardening su client al fine di semplificare le fasi di progettazione e/o distribuzione degli adeguamenti sw sugli elementi di un cluster omogeneo e su più cluster in parallelo, anche ottimizzando i tempi di rilascio dei deliverable. | D |
| 10 | Servizio di supporto specialistico | Security Principal | | |
| | | 10.1 | Percentuale di risorse offerte, nell'ambito di ciascun contratto esecutivo, in possesso della certificazione ISACA CISM (Certified Information Security Manager):<br>almeno il 50% (arrotondato all'unità superiore) | T |
| | | Senior Security Architect | | |

| Criteri di valutazione | | ID | Subcriteri di valutazione | Tipologia Subcriterio |
|---|---|---|---|---|
| | | 10.2 | Percentuale di risorse offerte, nell'ambito di ciascun contratto esecutivo, in possesso della certificazione (ISC)^2 CISSP (Certified Information System Security Professional): almeno il 50% (arrotondato all'unità superiore) | T |
| | | Senior Security Tester | | |
| | | 10.3 | Percentuale di risorse offerte, nell'ambito di ciascun contratto esecutivo, in possesso di almeno una delle seguenti certificazioni:<br>EC-Council CEH (Certified Etical Hacker)<br>e/o GIAC Penetration Tester<br>e/o Offensive Security Certified Professional<br>e/o CompTIA Pentest+:<br>almeno il 50% (arrotondato all'unità superiore) | T |
| | | Senior Security Analyst | | |
| | | 10.4 | Percentuale di risorse offerte, nell'ambito di ciascun contratto esecutivo, in possesso di almeno una delle seguenti certificazioni:<br>EC-Council CSA (Certified SOC Analyst)<br>e/o CompTIA CySA+ (Cyber Security Analyst)<br>e/o GIAC Certified Intrusion Analyst:<br>almeno il 50% (arrotondato all'unità superiore) | T |
| | | Junior Security Analyst | | |
| | | 10.5 | Percentuale di risorse offerte, nell'ambito di ciascun contratto esecutivo, in possesso di almeno una delle seguenti certificazioni:<br>EC-Council CSA (Certified SOC Analyst)<br>e/o CompTIA CySA+ (Cyber Security Analyst)<br>e/o GIAC Certified Intrusion Analyst,<br>e/o ISACA CSX-F (Cyber Security Fundamentals)<br>e/o CompTIA Security+:<br>almeno il 50% (arrotondato all'unità superiore) | T |
| 11 | SLA | 11.1 | Tempo di emissione del “Piano Operativo”: 15 giorni lavorativi | T |
| | | 11.2 | Tempo di consegna, installazione, configurazione e verifica: 50 giorni solari | T |
| | | Tempestività del tempo di intervento - Valore minimo richiedibile in AS | | |
| | | 11.3 | Profilo LP: 6 ore | T |
| | | 11.4 | Profilo HP: 3 ore | T |
| | | Tempestività del tempo di ripristino del servizio - Valore minimo richiedibile in AS | | |
| | | 11.5 | Profilo LP - Severity Code 1: 12 ore | T |

| Criteri di valutazione | | ID | Subcriteri di valutazione | Tipologia Subcriterio |
|---|---|---|---|---|
| | | 11.6 | Profilo LP - Severity Code 2: 16 ore | T |
| | | 11.7 | Profilo HP - Severity Code 1: 4 ore | T |
| | | 11.8 | Profilo HP - Severity Code 2: 8 ore | T |

La migliore offerta sarà determinata dal punteggio complessivo (***Ptot***) più alto, che sarà ottenuto sommando il "Punteggio Tecnico" (**PT**) ed il "Punteggio Economico" (**PE**):

**Ptot = PT + PE.**

Il numero degli aggiudicatari dell'Accordo Quadro è determinato in funzione del numero di offerte presenti in graduatoria, sulla base della seguente tabella di corrispondenza:

| *Numero di offerte presenti nella graduatoria dell'AQ (come risultante dal PTot)* | *Numero di aggiudicatari dell'AQ* |
|---|---|
| N=2 | **2** |
| 3 ≤ N < 5 | **3** |
| 5 ≤ N ≤ 7 | **4** |
| N ≥ 8 | **5** |

La procedura non sarà aggiudicata in caso di N < 2.
Successivamente alla stipula dell'Accordo Quadro e per tutta la durata dello stesso, le Amministrazioni potranno aggiudicare uno o più Appalti Specifici basati sull'Accordo Quadro medesimo a seguito del rilancio del confronto competitivo tra gli operatori economici parti dello stesso Accordo Quadro.

**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:

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

Dove:

- **$PT_{ER}$** è il Punteggio Tecnico massimo ereditabile;
- **$PT_{AS}$** è il Punteggio Tecnico massimo attribuibile in ragione dell'offerta tecnica dell'Appalto Specifico;
- **$PE_{AS}$** è il Punteggio Economico massimo attribuibile in ragione dell'offerta economica dell'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.

**Punteggio tecnico dell'Appalto Specifico**

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

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

dove:

- $PT^i_{ER}$ è il Punteggio Tecnico Ereditato dal concorrente i-esimo;
- $PT^i_{AS}$ è il Punteggio Tecnico assegnato al concorrente i-esimo attribuito dalla Commissione giudicatrice in fase di Appalto Specifico.

Il $PT^i_{ER}$ è a sua volta pari a:

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

dove:

- $PT^i_{AQ}$ 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 secondo quanto previsto nella seguente tabella.
- **K** è un coefficiente di riproporzionamento il cui valore è pari a ($PT_{ER}/PT_{AQMAX}$) 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 |
|---|---|---|
| Elementi trasversali | 9.1; 9.2; 11.1; 11.2 | Sempre ereditati |
| SIEM | 1.1; 1.2; 1.3; 1.4; 1.5; 1.6; 1.7 | Ereditati se l'AS include il relativo bene |
| SOAR | 2.1; 2.2; 2.3 | |
| SEG | 3.1; 3.2; 3.3; 3.4; 3.5; 3.6; 3.7; 3.8; 3.9; 3.10 | |
| SWG | 4.1; 4.2; 4.3; 4.4; 4.5; 4.6; 4.7; 4.8 | |
| DB Security | 5.1; 5.2 | |
| DLP | 6.1; 6.2; 6.3 | |
| PAM | 7.1; 7.2; 7.3; 7.4; 7.5; 7.6; 7.7; 7.8; 7.9 | |
| WAF | 8.1; 8.2; 8.3; 8.4; 8.5; 8.6 | |
| Servizio di manutenzione (profilo LP) | 9.3; 11.3; 11.5; 11.6 | Ereditati se l'AS include il relativo servizio |
| Servizio di manutenzione (profilo HP) | 9.3; 11.4; 11.7; 11.8 | |
| Servizio di supporto specialistico | 10.1; 10.2; 10.3; 10.4; 10.5 | |
| Servizio di hardening | 9.4 | |

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 delle proprie valutazioni in termini di rilevanza e/o criticità rispetto all'oggetto dell'appalto.
In particolare nella colonna "Tipologia Subcriterio" vengono indicati:

- con la lettera D i subcriteri relativi a "**Punteggi discrezionali**", vale a dire i punteggi attribuiti in ragione dell'esercizio della discrezionalità spettante alla commissione giudicatrice;
- con la lettera T i subcriteri relativi a "**Punteggi tabellari**", vale a dire i punteggi attribuiti o non attribuiti in ragione dell'offerta o mancata offerta di quanto specificamente richiesto.

| Criterio | | ID | Sub-Criterio di valutazione | Tipologia Subcriterio |
|---|---|---|---|---|
| 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 | T |
| | | AS.1.2 | Integrazione con specifica piattaforma di vulnerability management richiesta dall'Amministrazione | T |
| | | AS.1.3 | Qualità del feed di threat intelligence. Sarà premiata:<br>- la numerosità e la varietà di fonti, fra cui fonti OSINT, utilizzate dal feed di threat intelligence;<br>- la capacità di arricchimento degli indicatori di compromissione (threat actors, IP addresses, etc.)<br>-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. | D |
| | | AS.1.4 | Cattura e analisi dei flussi di rete anche in formato Jflow | T |
| | | AS.1.5 | Cattura e analisi dei flussi di rete anche in formato Sflow | T |
| | | 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. | D |
| | | AS.1.7 | Efficacia delle funzionalità che indirizzino e semplifichino la gestione della compliance al GDPR, in termini di:<br>-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;<br>-semplificazione dell'attività di monitoraggio della compliance in real time;<br>- capacità di individuare i dati associati al GDPR più a rischio. | D |
| | | 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. | D |
| 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 | D |

| Criterio | | ID | Sub-Criterio di valutazione | Tipologia Subcriterio |
|---|---|---|---|---|
| | | AS.2.2 | Integrazione con una specifica piattaforma di Service Management richiesta dall'Amministrazione | T |
| | | AS.2.3 | Qualità del feed di threat intelligence. Sarà premiata:<br>- la numerosità e la varietà di fonti, fra cui fonti OSINT, utilizzate dal feed di threat intelligence;<br>- la capacità di arricchimento degli indicatori di compromissione (threat actors, IP addresses, etc.)<br>-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. | D |
| | | 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. | D |
| | | 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 | D |
| 3 | SEG | AS.3.1 | Integrazione con soluzioni di sicurezza richieste dalla PA (soluzioni Anti APT, NGFW, SIEM, etc) | T |
| | | 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. | D |
| 4 | SWG | AS.4.1 | Integrazione con soluzioni di sicurezza richieste dalla PA (soluzioni Anti APT, NGFW, SIEM, etc) | T |
| | | 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. | D |
| 5 | DB Security | AS.5.1 | Varietà dei DB relazionali supportati (oltre ai minimi previsti in AQ) | D |
| | | AS.5.2 | Integrazione con uno specifico sistema HSM richiesto dall'Amministrazione per la generazione e lo storage delle chiavi di crittografia | T |
| | | AS.5.3 | Integrazione con una specifica piattaforma di SIEM richiesta dall'Amministrazione | T |
| | | AS.5.4 | Varietà dei DB non relazionali supportati | D |
| | | 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 | D |

| Criterio | | ID | Sub-Criterio di valutazione | Tipologia Subcriterio |
|---|---|---|---|---|
| | | 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<br><br>ambiente di virtualizzazione, ecc.) | D |
| | | AS.5.7 | Varietà di ambienti cloud supportati e scalabilità in termini di numero di istanze gestibili | D |
| 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. | T |
| | | AS.6.2 | Supporto al file fingerprinting | T |
| | | AS.6.3 | Integrazione con una piattaforma di MDM specificata dall'Amministrazione | T |
| | | 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 | D |
| | | 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 | D |
| | | AS.6.6 | Compatibilità della soluzione CASB con specifiche applicazioni cloud richieste dall'Amministrazione | T |
| | | 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). | D |
| | | AS.6.8 | Capacità della soluzione di supportare, semplificandola, l'attività di classificazione dei dati da parte degli operatori, presente e futura. | D |
| | | 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). | D |
| | | 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 | T |
| | | 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 | D |

| Criterio | | ID | Sub-Criterio di valutazione | Tipologia Subcriterio |
|---|---|---|---|---|
| | | 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 | D |
| 7 | PAM | AS.7.1 | Supporto di ulteriori specifici sistemi operativi richiesti dall'Amministrazione | T |
| | | 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:<br><br>- il grado di dettaglio delle policy per i privilegi di amministratore e la relativa semplicità d'implementazione;<br>- la capacità della soluzione di garantire un'elevata produttività degli utenti mantenendo al contempo i sistemi sicuri;<br>- la capacità di effettuare un controllo applicativo su un'ampia varietà di applicazioni;<br>- 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 | D |
| | | AS.7.3 | Efficacia della specifica soluzione per la gestione degli accessi applicativi.<br>Saranno valutate:<br>- 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;<br>- la varietà numerosità di ambienti applicativi supportati | D |
| | | AS.7.4 | Supporto di dispositivi di rete e di dispositivi e sistemi di sicurezza specifici richiesti dall'Amministrazione | T |
| | | AS.7.5 | Integrazione con una specifica piattaforma di vulnerability management richiesta dall'Amministrazione | T |
| | | AS.7.6 | Integrazione con una specifica soluzione di MFA richiesta dall'Amministrazione | T |
| | | AS.7.7 | Possibilità di limitare l'accesso sulla base della localizzazione dell'utente | T |
| | | AS.7.8 | Efficacia della specifica soluzione per la protezione di Domain Controller in ambiente Windows. Saranno valutate: | D |

| Criterio | | ID | Sub-Criterio di valutazione | Tipologia Subcriterio |
|---|---|---|---|---|
| | | | - la numerosità delle tecniche di attacco riconosciute;<br><br>- la varietà delle azioni di mitigazione degli attacchi messe a disposizione dalla soluzione anche al fine di accelerare la fase di remediation da parte degli operatori di sicurezza | |
| | | AS.7.9 | Configurazione della soluzione in alta affidabilità. Saranno valutate le modalità implementative proposte per la configurazione in alta affidabilità, in termini di disponibilità della soluzione e delle sue componenti in caso di guasto. | D |
| | | 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. | D |
| 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. | D |
| | | AS.8.2 | Integrazione con soluzioni di sicurezza richieste dalla PA (soluzioni Anti APT, NGFW, SIEM, etc) | T |
| | | 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. | D |
| | | 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 | D |
| | | AS.8.5 | Supporto standard PCI DSS | T |
| | | 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 | D |
| 9 | Servizi | AS.9.1 | Ulteriori competenze ed esperienze specifiche del personale addetto ai servizi (ad eccezione del supporto specialistico) | D |
| | | AS.9.2 | Certificazioni Vendor Neutrali Aggiuntive del personale addetto ai servizi (ad eccezione del supporto specialistico) | D |
| | | 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) | D |

| Criterio | | ID | Sub-Criterio di valutazione | Tipologia Subcriterio |
|---|---|---|---|---|
| | | AS.9.4 | Architettura e modalità di implementazione del collegamento (qualora questo non sia messo a disposizione dalla PA) per l'accesso remoto ai sistemi dell'Amministrazione a supporto delle attività di manutenzione, al fine di garantire l'integrità, la riservatezza e la sicurezza dei dati. | D |
| | | AS.9.5 | Modelli organizzativi, modalità operative e strumenti adottati per l'erogazione dei servizi aggiuntivi ai fini di dimostrare il soddisfacimento dei livelli di servizio offerti dal Concorrente e ottimizzare i tempi di rilascio dei deliverable attesi | D |
| 10 | Servizio di supporto specialistico | Security Principal | | |
| | | AS.10.1 | Certificazioni Vendor Neutrali Aggiuntive<br>Certificazioni di tipo sales o technical sulle tecnologie presenti nel contesto di riferimento della PA o sulle tecnologie proposte in seconda fase. | T |
| | | Senior Security Architect | | |
| | | AS.10.2 | Certificazioni Vendor Neutrali Aggiuntive<br>Certificazioni di tipo sales o technical sulle tecnologie presenti nel contesto di riferimento della PA o sulle tecnologie proposte in seconda fase. | T |
| | | Senior Security Tester | | |
| | | AS.10.3 | Certificazioni Vendor Neutrali Aggiuntive<br>Certificazioni di tipo sales o technical sulle tecnologie presenti nel contesto di riferimento della PA o sulle tecnologie proposte in seconda fase. | T |
| | | Senior Security Analyst | | |
| | | AS.10.4 | Certificazioni Vendor Neutrali Aggiuntive<br>Certificazioni di tipo sales o technical sulle tecnologie presenti nel contesto di riferimento della PA o sulle tecnologie proposte in seconda fase. | T |
| | | Junior Security Analyst | | |
| | | AS.10.5 | Certificazioni Vendor Neutrali Aggiuntive<br>Certificazioni di tipo sales o technical sulle tecnologie presenti nel contesto di riferimento della PA o sulle tecnologie proposte in seconda fase. | T |
| 11 | SLA | AS.11.1 | Miglioramento dei livelli di servizio richiesti (rispetto ai valori migliorativi previsti in AQ) | D |

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 nelle Condizioni di fornitura.

**Punteggio economico dell'Appalto Specifico**

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 ($BA_F$ + $BA_{SB}$ + $BA_{SA}$).

## 2.7 CONDIZIONI RELATIVE AL CONTRATTO D'APPALTO

### 2.7.1 INFORMAZIONI RELATIVE AD UNA PARTICOLARE PROFESSIONE (SOLO PER CONTRATTI DI SERVIZI)

Non applicabile

### 2.7.2 CONDIZIONI DI ESECUZIONE DEL CONTRATTO D'APPALTO

Successivamente alla stipula dell'Accordo Quadro le Amministrazioni legittimate potranno affidare gli Appalti Specifici entro i limiti delle condizioni fissate nell'Accordo Quadro stesso e comunque nel rispetto di quanto previsto dall'art. 1 comma 6 DL 105 2019 (convertito in L 133/2019).

Qualora l'Amministrazione Contraente ricada tra i soggetti di cui all'art. 1, comma 2, lett. a) della legge n. 133/2019 e l'oggetto del proprio Appalto specifico sia destinato a essere impiegato sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui all'art. 1, comma 2, lettera b), della legge n. 133/2019, l'Amministrazione dovrà procedere all'invio della comunicazione di cui all'art 3 del DPR n. 54/2021. Atteso che prima di procedere alla Richiesta di offerta, il Centro di valutazione e certificazione nazionale (CVCN), istituito presso il Ministero dello sviluppo economico, o uno dei Centri di Valutazione (CV), istituiti presso il Ministero dell'interno e il Ministero della difesa, potrà aver riscontrato la comunicazione di cui sopra, prevedendo la necessità di effettuare verifiche preliminari e/o imporre condizioni e test hardware e software su forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui all'art. 1 comma 2 lett. b) legge 133/2019 – l'Amministrazione prevedrà nel proprio contratto esecutivo, il cui schema sarà allegato alla succitata richiesta di offerta - clausole che condizionino, sospensivamente ovvero risolutivamente, il contratto medesimo al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN o da uno dei CV.

Ai sensi di quanto previsto all'art. 1, comma 6 lett. a) del D.L. 105/2019, il Fornitore dovrà fornire pieno supporto alle Amministrazioni chiamate anche a collaborare con il CVCN e 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 L. 133/2019. Il Fornitore dovrà, pertanto, su richiesta dell'Amministrazione, mettere a disposizione il proprio know - how, i prodotti hardware e software oggetto di test, le risorse fisiche (ad es. componenti accessori, realizzazione di test bed, etc), logistiche (ad es. messa a disposizione di sedi idonee all'effettuazione dei test su richiesta dell'Amministrazione) e professionali (ad. es. figure professionali in grado di fornire il necessario supporto alle Amministrazioni sia nella fase che precede l'effettuazione dei test, che durante la loro esecuzione, nonché successivamente, per la produzione di eventuale documentazione tecnico - amministrativa che si rendesse necessaria).

**2.7.3 INFORMAZIONI RELATIVE AL PERSONALE RESPONSABILE DELL'ESECUZIONE DEL CONTRATTO D'APPALTO**

I requisiti professionali relativi al personale incaricato dell'esecuzione del Contratto sono indicati ai paragrafi:

- 2.4.1.1 e 2.4.1.2 delle Condizioni di fornitura parte Generale
- 2.2.1.4 delle Condizioni di fornitura parte Speciale

L'Amministratore Delegato

Ing. Cristiano Cannarsa