GARA PER LA FORNITURA DI SOLUZIONI E SERVIZI DI CYBER SECURITY

DOCUMENTO DI CONSULTAZIONE DEL MERCATO

QUESTIONARIO TECNICO

***Da inviare a mezzo mail all’indirizzo:***

ictconsip@postacert.consip.it

Roma, 03/10/2023

**Premessa**

Il presente documento ha lo scopo di indagare il mercato delle soluzioni e dei servizi di Cyber Security, per pubblicare nuove iniziative in tale ambito, al fine di garantire alle Pubbliche Amministrazioni la disponibilità di strumenti di acquisto idonei ad assicurare la protezione dei propri asset digitali da attacchi e malware informatici in costante evoluzione ed elevare i livelli di cyber security dei medesimi, accrescendo allo stesso tempo la consapevolezza e le competenze delle Amministrazioni in tale ambito. Tali iniziative rappresentano la naturale prosecuzione del percorso di evoluzione cyber già intrapreso da Consip attraverso le tre precedenti iniziative di Sicurezza On Premises (l’Accordo Quadro Multi fornitore con rilancio competitivo “Strumenti di gestione, protezione email web e dati” e l’Accordo Quadro Mono fornitore “Protezione perimetrale, endpoint e anti-APT”) e Sicurezza da remoto (Accordo quadro Multi fornitore “Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni”).

Il presente documento di consultazione del mercato ha l’obiettivo di:

* garantire la massima pubblicità alle iniziative per assicurare la più ampia diffusione delle informazioni;
* ottenere la più proficua partecipazione da parte dei soggetti interessati;
* pubblicizzare al meglio le caratteristiche qualitative e tecniche dei beni e servizi oggetto di analisi;
* ricevere, da parte dei soggetti interessati, osservazioni e suggerimenti per una più compiuta conoscenza del mercato.

In merito alla consultazione del mercato in oggetto, Vi preghiamo di fornire il Vostro contributo - previa presa visione dell’informativa sul trattamento dei dati personali sotto riportata - compilando il presente questionario e inviandolo entro **20 giorni solari** dalla data odierna all’indirizzo PEC ictconsip@postacert.consip.it.

Tutte le informazioni da Voi fornite con il presente documento saranno utilizzate ai soli fini dello sviluppo dell’iniziativa in oggetto.

Consip S.p.A., in ragione di quanto di seguito previsto in materia di trattamento dei dati personali, si impegna a non divulgare a terzi le informazioni raccolte con il presente documento.

L’invio del documento al nostro recapito implica il consenso al trattamento dei dati forniti.

**Dati azienda**

|  |  |
| --- | --- |
| **Azienda** |  |
| **Indirizzo** |  |
| **Nome e cognome del referente** |  |
| **Ruolo in azienda** |  |
| **Telefono** |  |
| **Indirizzo e-mail e pec** |  |
| **Data compilazione del questionario** |  |

**Informativa sul trattamento dei dati personali**

Ai sensi dell'art. 13 del Regolamento europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (nel seguito anche *“Regolamento UE”*), Vi informiamo che la raccolta ed il trattamento dei dati personali (d’ora in poi anche solo “Dati”) da Voi forniti sono effettuati al fine di consentire la Vostra partecipazione all’ attività di consultazione del mercato sopradetta, nell’ambito della quale, a titolo esemplificativo, rientrano la definizione della strategia di acquisto della merceologia, le ricerche di mercato nello specifico settore merceologico, le analisi economiche e statistiche.

Il trattamento dei Dati per le anzidette finalità, improntato alla massima riservatezza e sicurezza nel rispetto della normativa nazionale e comunitaria vigente in materia di protezione dei dati personali, avrà luogo con modalità sia informatiche, sia cartacee.

Il conferimento di Dati alla Consip S.p.A. è facoltativo; l'eventuale rifiuto di fornire gli stessi comporta l'impossibilità di acquisire, da parte nostra, le informazioni per una più compiuta conoscenza del mercato relativamente alla Vostra azienda.

I Dati saranno conservati in archivi informatici e cartacei per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati, conformemente a quanto previsto dagli obblighi di legge.

All’interessato vengono riconosciuti i diritti di cui agli artt. da 15 a 23 del Regolamento UE. In particolare, l’interessato ha il diritto di: i) revocare, in qualsiasi momento, il consenso; ii) ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano, nonché l’accesso ai propri dati personali per conoscere la finalità del trattamento, la categoria di dati trattati, i destinatari o le categorie di destinatari cui i dati sono o saranno comunicati, il periodo di conservazione degli stessi o i criteri utilizzati per determinare tale periodo; *iii)* il diritto di chiedere, e nel caso ottenere, la rettifica e, ove possibile, la cancellazione o, ancora, la limitazione del trattamento e, infine, può opporsi, per motivi legittimi, al loro trattamento; *iv)* il diritto alla portabilità dei dati che sarà applicabile nei limiti di cui all’art. 20 del regolamento UE.

Se in caso di esercizio del diritto di accesso e dei diritti connessi previsti dagli artt. da 15 a 22 del Regolamento UE, la risposta all'istanza non perviene nei tempi indicati e/o non è soddisfacente, l'interessato potrà far valere i propri diritti innanzi all'autorità giudiziaria o rivolgendosi al Garante per la protezione dei dati personali mediante apposito ricorso, reclamo o segnalazione.

L’invio a Consip S.p.A. del Documento di Consultazione del mercato implica il consenso al trattamento dei Dati personali forniti.

Titolare del trattamento dei dati è Consip S.p.A., con sede in Roma, Via Isonzo 19 D/E. Le richieste per l’esercizio dei diritti riconosciuti di cui agli artt. da 15 a 23 del regolamento UE, potranno essere avanzate al Responsabile della protezione dei dati al seguente indirizzo di posta elettronica esercizio.diritti.privacy@consip.it.

**Breve descrizione dell’iniziativa**

Consip, nell’ambito delle sue iniziative relative al Piano Triennale ICT, continua a rendere disponibili Contratti per l’acquisto di soluzioni[[1]](#footnote-2) e servizi di cybersecurity che garantiscano un’adeguata e sempre aggiornata protezione e resilienza delle reti e sistemi informativi delle Pubbliche Amministrazioni, che costituiscono un fattore abilitante per l’aumento di fiducia nei servizi digitali erogati dalle PA stesse, in linea con i principi sanciti dal PNRR.

Il questionario riguarda fornitura di soluzioni e l’erogazione di servizi di cybersecurity ad ampio spettro (sicurezza perimetrale, protezione da minacce avanzate persistenti e zero-day, protezione degli endpoint, etc.), servizi connessi alla fornitura (installazione, configurazione, manutenzione, etc.) e servizi professionali (risk management, hardening, vulnerability management, penetration test, awareness e formazione, etc.).

**Si invitano gli operatori economici interessati, anche se non operanti in tutti gli ambiti di cyber security prospettati in tale documento, a rispondere comunque alla consultazione compilando le sezioni rientranti negli ambiti di propria competenza.**

**Domande – Questionario tecnico**

1. CORE BUSINESS AZIENDALE: riportare una breve descrizione dell’Azienda contenente:
* classificazione ai sensi del d.lgs. n. 36/2023 (operatore economico ex art. 65);
* forma giuridica;
* classificazione impresa (start-up, micro, piccola, media, grande);
* tipologia (es. produttore, distributore, rivenditore, system integrator, società di consulenza, …);
* numero di dipendenti nel biennio precedente alla pubblicazione del presente documento;
* contratto/i collettivo/i di lavoro applicato/i;
* eventuale associazione di categoria di appartenenza;
* eventuale possesso della certificazione della parità di genere di cui all'articolo 46-bis del codice delle pari opportunità tra uomo e donna, di cui al decreto legislativo 11 aprile 2006, n. 198.

|  |
| --- |
|  |

1. CERTIFICAZIONI AZIENDALI: specificare le certificazioni possedute dall’azienda, con particolare riguardo al settore della cybersecurity, precisando anche il settore IAF e lo scope della certificazione medesima:
* ISO 9001;
* ISO 27001;
* ISO 27701;
* ISO 27017;
* ISO 27018;
* ISO 27035;
* ISO 14001;
* ISO 22301;
* Qualificazione dell’Infrastruttura dei Servizi Cloud ai sensi del decreto direttoriale dell’Agenzia per la cybersicurezza nazionale del 2 gennaio 2023 (indicando anche eventuali infrastrutture in corso di qualifica o rinnovo della stessa).

|  |
| --- |
|  |

1. CERTIFICAZIONI DI SOLUZIONE/SERVIZIO: specificare le certificazioni possedute dalle soluzioni/servizi da voi a vario titolo commercializzati:
* certificazioni relative alla sicurezza della catena di approvvigionamento (ad. es. certificato ISO/IEC IS-15408 (standard Common Criteria) per uno specifico livello di garanzia rilasciato o in corso di rilascio da parte dell’OCSI);
* etichette relative all’efficienza energetica dell’hardware;
* qualificazione dei Servizi Cloud di tipo IaaS, PaaS e SaaS, ai sensi del decreto direttoriale dell’Agenzia per la cybersicurezza nazionale del 2 gennaio 2023, con evidenza degli specifici servizi qualificati o in corso di qualifica/rinnovo;
* certificazioni inerenti la commerciabilità dei prodotti hardware e software;
* ulteriori certificazioni e/o etichette utili allo sviluppo dell’iniziativa.

|  |
| --- |
|  |

1. PARTECIPAZIONE A INIZIATIVE ANALOGHE: indicare le iniziative inerenti la fornitura di soluzioni/prestazione di servizi di cybersecurity cui avete partecipato, descrivendo le loro principali caratteristiche (importo e oggetto della gara, anno di partecipazione, etc.), la relativa forma di partecipazione (diretta, indiretta, singola, RTI, Consorzio, rete d’impresa), le attività per le quali si è partecipato (es. fornitura, servizi di sicurezza, servizi professionali, modalità di erogazione, etc.) e i relativi ambiti (es. fornitura next generation firewall, servizio di risk management, servizio anti-APT, etc.). Descrivere anche le eventuali partecipazioni a iniziative assimilabili, attinenti il settore della cyber security maturate in contesti internazionali (ivi incluse iniziative bandite da altre centrali di committenza europee)

|  |
| --- |
|  |

1. CONTRATTI ANALOGHI: tenendo conto della descrizione dell’iniziativa riportata nella premessa, indicare nella sottostante tabella i contratti analoghi inerenti la fornitura di soluzioni e/o l’erogazione di servizi di cyber security nei tre anni precedenti alla pubblicazione del presente documento, anche a favore di soggetti privati, specificando l’oggetto in maniera quanto più dettagliata possibile, la Committente laddove possibile o in subordine l’ambito (es Telco, Finance, etc), il periodo di esecuzione, la tipologia delle prestazioni rese, le modalità di erogazione (on premise o as a service) la durata, l’importo fatturato e il relativo periodo di fatturazione.

| **Oggetto (descrizione di dettaglio) contratto analogo** | **Committente** | **Periodo esecuzione** | **Tipologia prestazioni rese** | **Modalità di erogazione** | **Durata** | **Valore totale [€]** | **Periodo di fatturazione** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

1. FATTURATO GLOBALE: indicare il fatturato globale maturato nel triennio precedente a quello di pubblicazione del presente documento, espresso in milioni di Euro, specificando la quota parte relativa alla Pubblica Amministrazione.

|  |  |
| --- | --- |
| **Anno** | **Fatturato Globale (M€)** |
| N-2: \_\_\_\_ |  |
| *di cui PA* |  |
| N-1: \_\_\_\_ |  |
| *di cui PA* |  |
| N: \_\_\_\_ |  |
| *di cui PA* |  |

1. FATTURATO SPECIFICO TRIENNIO PRECEDENTE: indicare il fatturato in soluzioni (erogati on premises da remoto) e servizi di cyber security maturato nel triennio precedente a quello di pubblicazione del presente documento, espresso in milioni di Euro, specificando la quota parte relativa alla Pubblica Amministrazione. Se possibile, indicare anche l’indice medio di redditività del settore conseguito negli ultimi tre anni

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **A=B+C** | **B** | **C** | **D** | **E=A+D** |  |
| **Anno** | **Fatturato complessivo in soluzioni di Cyber Security (M€)** | **Fatturato per soluzioni di Cyber security erogate on premises** | **Fatturato per soluzioni di Cyber security erogate in modalità as a service** | **Fatturato Servizi di Cyber Security (M€)** | **Fatturato complessivo Soluzioni e Servizi di Cyber Security (M€)** | **Indice medio di redditività** |
| N-3: \_\_\_\_ |  |  |  |  |  |  |
| *di cui PA* |  |  |  |  |  |  |
| N-2: \_\_\_\_ |  |  |  |  |  |  |
| *di cui PA* |  |  |  |  |  |  |
| N-1: \_\_\_\_ |  |  |  |  |  |  |
| *di cui PA* |  |  |  |  |  |  |

1. TREND FATTURATO SPECIFICO TRIENNIO SUCCESSIVO: indicare il trend di fatturato atteso in soluzioni (erogati on premises da remoto)) e servizi di cyber security per il triennio successivo a quello di pubblicazione del presente documento, espresso in milioni di Euro, specificando la quota parte relativa alla Pubblica Amministrazione.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Anno** | **Fatturato Soluzioni di Cyber Security erogate on premises (M€ o % rispetto all’anno precedente)** | **Fatturato Soluzioni di Cyber Security erogate in modalità as a service (M€ o % rispetto all’anno precedente)** | **Fatturato Servizi di Cyber Security (M€ o % rispetto all’anno precedente)** | **Fatturato Totale Soluzioni e Servizi di Cyber Security (M€ o % rispetto all’anno precedente)** |
| N: \_\_\_\_ |  |  |  |  |
| *di cui PA* |  |  |  |  |
| N+1 \_\_\_\_ |  |  |  |  |
| *di cui PA* |  |  |  |  |
| N+2: \_\_\_\_ |  |  |  |  |
| *di cui PA* |  |  |  |  |

1. AMBITO OFFERTA SOLUZIONI/SERVIZI: con riferimento al settore della cybersecurity, specificare l’ambito d’offerta delle vostre soluzioni/servizi, tenendo conto di quelli indicati nella successiva tabella 1 e ulteriori ambiti di vostra competenza. Compilare la tabella 1 come segue:
2. descrivere, per ciascun ambito, le tipologie di soluzioni e/o servizi che si è in grado di offrire, in termini di caratteristiche tecniche, sia di base che innovative, funzionalità, modalità di erogazione, livelli di servizio;
3. indicare il grado di interoperabilità delle soluzioni, per i quali siete Reseller/Distributori/System Integrator o Vendor, con soluzioni di terze parti e descrivere le modalità utilizzate per garantirne l’integrazione (protocolli standard/proprietari, implementazioni ad hoc,…). Specificare, inoltre, la presenza di eventuali vincoli tecnici che limitino la piena interoperabilità.
4. specificare quali test comparativi eseguiti sulle soluzioni di sicurezza cibernetica da società di analisi e/o certificazione IT indipendenti si ritiene siano validi e/o utili ad effettuare una valutazione oggettiva degli stessi;
5. descrivere i servizi connessi alla fornitura delle soluzioni (ad. es. installazione, configurazione, assistenza, manutenzione), indicando quelli che come Fornitore / System Integrator si è in grado di erogare autonomamente e quelli che invece sono erogati direttamente dal Produttore della soluzione o da Terzi, specificandone le modalità di erogazione e i livelli di servizio;
6. descrivere i servizi professionali offerti in termini di figure professionali impiegate (numero, tipologia, skill, esperienza pregressa e certificazioni possedute dalle risorse), modalità di esecuzione e strumenti adottati a supporto (innovativi, certificati, etc), task e deliverable e indicatori di perfomance;
7. indicare e descrivere le modalità di vendita/erogazione (appliance fisica, appliance virtuale, software, servizio (ad es. on premise e/o “as a service” / cloud qualificato ACN), giorno persona, etc.). Nel caso di licenze, specificarne la tipologia: utente, processore, macchina. Per i servizi cloud specificare l’ubicazione geografica del Data Center da cui viene erogato il servizio e dei siti di Business Continuity e Disaster Recovery
8. indicare e descrivere le modalità di pricing (modalità a canone periodico per unità di misura (es. licenza, eventi gestiti), modalità a consumo (pay per use), prezzo a corpo per appliance, una tantum, giorni persona, ecc.) e la disponibilità di listini pubblici;
9. descrivere la relativa catena di vendita (Produttore, Distributore, Reseller o System Integrator, erogazione tramite partner terzi). Indicare, laddove applicabile, la tipologia di partnership (es rivenditori semplici, rivenditori qualificati dal produttore quali certificazioni per rivendita e/o erogazione di servizi, etc.) e le scontistiche di soluzione/servizio a cui si ha accesso.

Tabella 1

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **AMBITO** | **CARATTERISTICHE TECNICHE (BASE, INNOVATIVE), FUNZIONALITÀ, MODALITÀ DI EROGAZIONE, LIVELLI DI SERVIZIO** | **INTEROPERABILITÁ DELLE SOLUZIONI**  | **TEST COMPARATIVI ESEGUITI DA SOCIETÀ DI ANALISI E/O CERTIFICAZIONE IT INDIPENDENTI**  | **SERVIZI CONNESSI ALLA FORNITURA (EROGATI AUTONOMAMENTE/DAL PRODUTTORE DELLA SOLUZIONE O DA TERZI E RELATIVE MODALITÀ DI EROGAZIONE E LIVELLI DI SERVIZIO** | **MODALITÀ DI VENDITA/EROGAZIONE** | **MODALITÀ DI PRICING** | **CATENA DI VENDITA** |
| NGFW (Network Generation Firewall) |   |   |   |   |   |   |   |
| WAF (Web Application Firewall) |   |   |   |   |   |   |   |
| Protezione ANTI-APT (Advanced Persistant Threat) |   |   |   |   |   |   |   |
| AntiDDOS (Distributed Denial of Service)  |   |   |   |   |   |   |   |
| NAC (Network Access Control) |   |   |   |   |   |   |   |
| SWG (Secure Web Gateway) |   |   |   |   |   |   |   |
| SEG (Secure Email Gateway) |   |   |   |   |   |   |   |
| Secure DNS (Domain Name System) |   |   |   |   |   |   |   |
| PAM (Privileged Account Management) |   |   |   |   |   |   |   |
| EPP/EDR (Endpoint Protection/ Endpoint Detection and Response) |   |   |   |   |   |   |   |
| SPP (Server Protection Platform) |   |   |   |   |   |   |   |
| XDR (Extended Detection & Response)  |   |   |   |   |   |   |   |
| MDR (Managed Detection and Response) |   |   |   |   |   |   |   |
| DLP (Dataloss / leak prevention) |   |   |   |   |   |   |   |
| SIEM (Security Information and Event Management) |   |   |   |   |   |   |   |
| SOAR (Security Orchestration, Automation and Response) |   |   |   |   |   |   |   |
| SOC (Security Operations Center) |   |   |   |   |   |   |   |
| Threat Intelligence Data Feed / Vulnerability Data Feed  |   |   |   |   |   |   |   |
| Static application security testing  |   |   |   |   |   |   |   |
| Dynamic application security testing  |   |   |   |   |   |   |   |
| Mobile application security testing  |   |   |   |   |   |   |   |
| Database security  |   |   |   |   |   |   |   |
| IAM (Identity & Access Management) |   |   |   |   |   |   |   |
| IAG (Identity & Access Governance) |   |   |   |   |   |   |   |
| Servizi ZTNA (Zero Trust Network Access) |   |   |   |   |   |   |   |
| Servizi CASB (Cloud Access Security Broker) |   |   |   |   |   |   |   |
| Continuous Vulnerability Management |  |  |  |  |  |  |  |
| **Altro (specificare ulteriori soluzioni e servizi che si è in grado di offrire)** |   |   |   |   |   |   |   |
| **Servizi professionali** | **Figure professionali impiegate (numero, tipologia, skill)** | **Esperienza pregressa e certificazioni possedute dalle figure professionali** | **Modalità di esecuzione** | **Strumenti adottati a supporto (innovativi, certificati, etc)** | **Task e deliverable** | **Indicatori di perfomance** |  |
| Risk Management |   |   |   |   |   |   |  |
| Vulnerability Management |   |   |   |   |   |   |  |
| Penetration Test |   |   |   |   |   |   |  |
| Servizio di Hardening |   |   |   |   |   |   |  |
| Servizio di Patching |   |   |   |   |   |   |  |
| Servizio di Awareness e Formazione |   |   |   |   |   |   |  |
| Servizi di compliance (GDPR, ISO 27001, etc) |   |   |   |   |   |   |  |
| Servizio di gestione della sicurezza della catena di approvvigionamento |   |   |   |   |   |   |  |
| **Altro (specificare ulteriori servizi che si è in grado di offrire)** |   |   |   |   |   |   |  |

1. REVISIONE PREZZI – Specificare gli indici di andamento dei costi/prezzi di mercato a vostro avviso applicabili alle soluzioni /servizi di cyber security oggetto d’indagine, di cui tener conto per una periodica revisione dei prezzi. Indicare anche eventuali variazioni intervenute sui prezzi delle soluzioni/servizi rispetto alle precedenti edizioni delle gare di Sicurezza on Premises (ID 2174 - Sicurezza On Premises - strumenti di gestione, protezione email, web e dati 1; ID 2367 - Sicurezza On Premises - protezione perimetrale, endpoint e anti-APT 1) e Sicurezza da remoto (ID 2296 - Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni).

|  |
| --- |
|  |

1. SERVIZI PROFESSIONALI – REFERENZE AZIENDALI: con riferimento ai servizi professionali di cui alla tabella 1, indicare e descrivere le referenze aziendali (ad esempio oggetto, durata, importo economico dei servizi e clienti) maturate nel settore specifico nell’arco del precedente triennio.

|  |
| --- |
|  |

1. PERIMETRO SOLUZIONI E SERVIZI - EDIZIONI PRECEDENTI: con riferimento alle soluzioni e servizi disponibili nelle edizioni precedenti (ID 2174 - Sicurezza On Premises - strumenti di gestione, protezione email, web e dati 1; ID 2367 - Sicurezza On Premises - protezione perimetrale, endpoint e anti-APT 1, ID 2296 – Sicurezza da remoto) si chiede di indicare quali sono, a vostro avviso, quelli che ritenete opportuno aggiornare in termini di:
	* 1. Per le soluzioni:
			1. caratteristiche tecniche (obsolete, minime/essenziali, aggiuntive, innovative);
			2. modalità di vendita/pricing;
			3. metriche e fasce di pricing;
		2. Per i servizi:
			1. caratteristiche tecniche (obsolete, minime/essenziali, aggiuntive, innovative);
			2. caratteristiche organizzative;
			3. livelli di servizio;
			4. modalità di erogazione;
			5. metriche e fasce di pricing.

Qualora si ritenga opportuno inserire ulteriori soluzioni e/o servizi, descriverli puntualmente secondo quanto indicato negli elenchi numerati di cui sopra.

Tabella 2 (riferimento gare “Sicurezza on premises” ID 2174 e ID 2367)

| **Prodotti** | **Caratteristiche tecniche (obsolete, minime/ essenziali, aggiuntive, innovative)** | **Modalità di vendita/ pricing** | **Metriche e fasce di pricing** |
| --- | --- | --- | --- |
| SIEM (Security Information and Event Management) |  |  |   |
| SOAR (Security Orchestration, Automation and Response) |  |  |   |
| SEG (Secure Email Gateway) |  |  |  |
| SWG (Secure Web Gateway) |  |  |  |
| DB-SECURITY(Data Base – Security) |  |  |   |
| DLP(Dataloss / leak prevention) |  |  |  |
| PAM(Privileged Account Management) |  |  |  |
| WAF(Web Application Firewall) |  |  |  |
| NGFW(Network Generation Firewall) |  |  |  |
| NAC(Network Access Control) |  |  |  |
| EPP/EDR(Endpoint Protection/ Endpoint Detection and Response) |  |  |  |
| SPP(Server Protection Platform) |  |  |  |
| Protezione ANTI-APT(Advanced Persistant Threat) |  |  |  |

Tabella 3 (riferimento gare “Sicurezza on premises” ID 2174 e ID 2367)

| **Servizi** | **Caratteristiche tecniche (obsolete, minime/ essenziali, aggiuntive, innovative)** | **Caratteristiche organizzative** | **Livelli di servizio** | **Modalità di erogazione** | **Metriche e fasce di pricing** |
| --- | --- | --- | --- | --- | --- |
| Installazione e configurazione |  |  |  |  |  |
| Supporto alla verifica di conformità |  |  |  |  |  |
| Manutenzione |  |  |  |  |  |
| Supporto Specialistico |  |  |  |  |  |
| Hardening su client  |  |  |  |  |  |
| Hardening su altri sistemi |  |  |  |  |  |
| Data Assessment |  |  |  |  |  |
| Privileged Account Assessment |  |  |  |  |  |
| Servizi professionali erogati dai vendor |  |  |  |  |  |
| Incident Response |  |  |  |  |  |
| Formazione e affiancamento |  |  |  |  |  |

Tabella 4 (Riferimento gara “Sicurezza da remoto” ID 2296)

| **Soluzioni** | **Caratteristiche tecniche (obsolete, minime/ essenziali, aggiuntive, innovative)** | **Modalità di vendita/ pricing** | **Metriche e fasce di pricing** |
| --- | --- | --- | --- |
| SOC (Security Operation Center) |  |  |   |
| Next Generation Firewall |  |  |   |
| Web Application Firewall |  |  |  |
| Continuous Vulnerability Management |  |  |  |
| Threat Intelligence & Vulnerability Datafeed |  |  |  |
| Protezione Navigazione Internet e Posta Elettronica  |  |  |  |
| Protezione End-Point |  |  |  |
| Formazione e Security Awareness |  |  |  |
| Gestione delle identità e accesso utente |  |  |  |
| Security Strategy |  |  |  |
| Vulnerability Assessment |  |  |  |
| Test del codice (statico, dinamico e mobile) |  |  |  |
| Supporto all’analisi e gestione degli incidenti |  |  |  |
| Penetration testing |  |  |  |
| Compliance Normativa |  |  |  |

1. MANODOPERA: con riferimento ai servizi on premises di cui alla tabella 3, indicare se e quali siano le prestazioni che a vostro parere possono essere configurate come manodopera, in tutto o in parte, dettagliando l’attività di manodopera stessa e specificandone l’incidenza percentuale rispetto alla fornitura dei prodotti. Per le attività di manutenzione, laddove applicabile, indicare dettagliatamente gli ambiti e le attività in capo ai produttori e quelli in capo ai System Integrator, specificandone la relativa incidenza in termini di costi ed effort risorse.

|  |
| --- |
|  |

1. GDPR: indicare quali garanzie in termini di conoscenza specialistica, processi, strumenti, risorse e misure tecniche ed organizzative, la vostra azienda è in grado di mettere a disposizione per assicurare che il trattamento di dati personali avvenga in conformità al Regolamento Europeo 2016/679.

|  |
| --- |
|  |

1. OSSERVAZIONI SULLE PRECEDENTI EDIZIONI: indicare se esistono a vostro giudizio aspetti delle precedenti iniziative che potrebbero essere modificati e per quali ragioni.

|  |
| --- |
|  |

1. COPERTURA GEOGRAFICA: indicare le aree del territorio italiano coperte direttamente dalla Vostra struttura logistica, in relazione alle differenti tipologie di attività (ad. es., fornitura, installazione, configurazione, manutenzione, etc.).

|  |
| --- |
|  |

1. PRINCIPIO DNSH (Do No Significant Harm): indicare e descrivere le azioni volte a soddisfare il principio DNSH in relazione alle soluzioni e servizi di cyber security oggetto d’indagine.

|  |
| --- |
|  |

1. PARITA’ DI GENERE, GENERAZIONALE E INCLUSIONE LAVORATIVA DI PERSONE CON DISABILITA’: indicare e descrivere le azioni volte a promuovere la parità di genere, generazionale e l’inclusione lavorativa in ottemperanza a quanto previsto dall’art. 47 del D.L. 77/2021 per i servizi di cyber security oggetto d’indagine.

|  |
| --- |
|  |

1. Sostenibilità ambientale e sociale: indicare e descrivere le soluzioni tecnico/organizzative connesse alle soluzioni e servizi di cyber security oggetto d’indagine, volte a promuovere la sostenibilità ambientale e sociale, i relativi indicatori di misura proposti o utilizzati e il possesso di certificazioni o etichette ambientali e/o sociali.

Si cita a titolo esemplificato e non esaustivo:

* soluzioni/iniziative volti a promuovere:
	+ il bilanciamento vita privata – vita lavorativa;
	+ l’integrazione nel tessuto territoriale;
* soluzioni e/o politiche aziendali adottate per ridurre l’impatto ambientale in termini di dematerializzazione delle risorse (inclusa l’energia), uso efficiente delle risorse, riduzione o eliminazione delle sostanze pericolose, riduzione dei rifiuti in un’ottica di ciclo di vita, pratiche di riciclo delle risorse utilizzate/economia circolare.

|  |
| --- |
|  |

1. INNOVAZIONE E DATA/ASSET PROTECTION: indicare e descrivere le iniziative, collaborazioni e soluzioni innovative volte alla protezione dei dati e dei propri asset aziendali nonché altre modalità esecutive in grado di apportare benefici per l’esecuzione delle attività oggetto dell’appalto.

Si cita a titolo esemplificato e non esaustivo:

* partnership con enti di ricerca / istituti universitari/start-up e PMI;
* iniziative/soluzioni innovative volte alla protezione dei dati, dei propri asset aziendali ~~e~~ alla brand reputation.

|  |
| --- |
|  |

1. EVOLUZIONE NORMATIVA: descrivere quali sono i principali punti di attenzione di tipo normativo, ivi inclusi i riferimenti puntuali, da tenere in considerazione nello sviluppo dell’iniziativa (si cita a titolo esemplificativo e non esaustivo la direttiva NIS 2 ed il prossimo recepimento da parte degli Stati Membri, Strategia di cybersicurezza nazionale 2022-2026 e relative misure, etc.).

|  |
| --- |
|  |

1. PROCEDURA DI VALUTAZIONE DEL CVCN, VERIFICHE E ISPEZIONI: in considerazione della normativa vigente, tra cui il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, del DPR 5 febbraio 2021, n. 54 e del Decreto Del Presidente Del Consiglio Dei Ministri 15 giugno 2022, si richiama l’attenzione sulle procedure di valutazione dei CVCN, di verifica ed ispezioni. A tal riguardo si chiede di manifestare la conoscenza di tali previsioni e la disponibilità ad essere soggetti a obblighi di collaborazione e supporto con i CVCN, nonché a sostenere gli adempimenti connessi in termini di risorse, tempi ed eventualmente di oneri economici. Indicare, in tale contesto, ulteriori elementi/informazioni in vostro possesso circa le tempistiche di messa in esecuzione dell’appalto in costanza di tali valutazioni, ispezioni e verifiche.

|  |
| --- |
|  |

1. MANIFESTAZIONE DI INTERESSE A PARTECIPARE: indicare per quali ambiti la Vostra azienda sarebbe interessata a partecipare ad un’iniziativa relativa alla fornitura di soluzioni e erogazione di servizi di cybersecurity.

|  |
| --- |
|  |

1. INFORMAZIONI AGGIUNTIVE: indicare ulteriori elementi/informazioni che ritenete possano essere utili per lo sviluppo di una possibile iniziativa.

|  |
| --- |
|  |

Con la sottoscrizione del Documento di Consultazione del mercato, l’interessato acconsente espressamente al trattamento dei propri Dati personali più sopra forniti.

|  |
| --- |
| **Firma operatore economico** |
| [Nome e Cognome] |
| *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* |

1. Il riferimento al termine “soluzioni” deve essere inteso nella duplice accezione di prodotti hardware e software installati in modalità “on-premise”, ossia presso le infrastrutture delle Pubbliche Amministrazioni, quanto nella accezione di soluzione tecnologica erogata da remoto, in modalità “as a service”, tramite Centri servizi e/o Cloud Service Provider. [↑](#footnote-ref-2)