ACQUISIZIONE DI BENI/SERVIZI DI SICUREZZA INFORMATICA

DOCUMENTO DI CONSULTAZIONE DEL MERCATO

QUESTIONARIO

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

ictconsip@postacert.consip.it

Roma, 06/06/2019

**Premessa**

La presente consultazione del mercato è finalizzata alla raccolta di informazioni per l’avvio di iniziative che avranno ad oggetto beni o servizi di Sicurezza Informatica in favore della Pubblica Amministrazione.

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 30 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’eventuale iniziativa in oggetto.

Consip S.p.A., in ragione 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** |  |
| **Fax** |  |
| **Indirizzo e-mail** |  |
| **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 Vostra, 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’obiettivo del questionario**

Il presente questionario si pone l’obiettivo di analizzare il mercato della fornitura di beni e/o servizi finalizzati alla realizzazione/gestione e ammodernamento dei sistemi di sicurezza informatica delle Pubbliche Amministrazioni, con l’obiettivo di monitorare i sistemi e servizi e mantenerli costantemente aggiornati ai target di sicurezza in continua evoluzione, in coerenza con le previsioni del Programma Triennale ICT e con gli standard/linee guida vigenti.

Il questionario riguarda soluzioni di sicurezza informatica ad ampio spettro (ad titolo esemplificativo e non esaustivo sicurezza perimetrale, protezione da minacce avanzate persistenti e zero-day, protezione degli endpoint), servizi connessi alle soluzioni, servizi professionali (risk assessment, vulnerability assessment, penetration test, awareness, etc.) volti a garantire l’aderenza nel tempo delle soluzioni di sicurezza informatica alle specifiche esigenze di Pubbliche Amministrazioni differenti (rischi specifici, gap di sicurezza, etc.).

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

**Domande – Questionario**

1. CORE BUSINESS AZIENDALE: riportare una breve descrizione dell’Azienda (appartenenza dell’impresa alle PMI, settori di attività, CCNL applicato, core business, numero di dipendenti dell’azienda nei tre anni precedenti alla pubblicazione del presente documento, appartenenza ad associazioni di categoria, altro)

|  |
| --- |
|  |

1. CERTIFICAZIONI AZIENDALI: specificare le certificazioni possedute dall’azienda, con particolare riguardo al settore della sicurezza informatica (ad es. certificazione ISO 9001:2015, ISO 27001:2017).

|  |
| --- |
|  |

1. CONTRATTI ANALOGHI: indicare i contratti eseguiti, possibilmente nei tre anni precedenti alla pubblicazione del presente documento o in corso di esecuzione, relativamente al settore della sicurezza informatica, in ambito pubblico e privato, specificando il Committente (laddove possibile), la durata del contratto, l’importo fatturato e descrivendo l’oggetto dell’appalto.

|  |
| --- |
|  |

1. PARTECIPAZIONE A INIZIATIVE ANALOGHE: indicare le iniziative inerenti la fornitura di prodotti/prestazione di servizi di sicurezza informatica cui avete partecipato nei tre anni precedenti alla pubblicazione del presente documento, descrivendo le loro principali caratteristiche (importi, oggetto della gara, 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 assessment, servizio anti-APT, etc.)

|  |
| --- |
|  |

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.). Si chiede inoltre di indicare la distribuzione geografica dei centri servizi per la modalità di erogazione “as a service”, specificando anche l’ubicazione dei centri di Disaster Recovery e Business Continuity.

|  |
| --- |
|  |

1. AMBITO OFFERTA SERVIZI PROFESSIONALI: con riferimento al settore della sicurezza informatica, specificare i servizi professionali offerti rispetto a quelli indicati a titolo esemplificativo e non esaustivo nelle successive tabelle e, per ciascun servizio, compilare la relativa tabella:
2. indicando le referenze aziendali (ad esempio oggetto, durata, importo economico dei servizi e clienti) maturate nel settore specifico nell’arco del precedente quinquennio;

| **Servizi Professionali** | **Referenze Aziendali** |
| --- | --- |
| Vulnerability Assessment |  |
| Penetration test |  |
| Risk assessment |  |
| Servizio di awareness |  |
| Compliance GDPR |  |
| Altro (specificare) |  |

1. descrivendo le modalità di esecuzione e gli strumenti adottati a supporto, tasks e deliverables, indicatori di performance (ad esempio, per il vulnerability assessment, descrivere le fasi che lo caratterizzano: eventuale assessment iniziale degli asset informatici, eventuale discovery della rete tramite tool specifici, eventuali report prodotti con un’indicazione degli indici di rischio delle vulnerabilità, periodicità di esecuzione, etc.);

| **Servizi Professionali** | **Modalità di esecuzione e strumenti adottati a supporto, Tasks e Deliverables, Indicatori di Performance** |
| --- | --- |
| Vulnerability Assessment |  |
| Penetration test |  |
| Risk assessment |  |
| Servizio di awareness |  |
| Compliance GDPR |  |
| Altro (specificare) |  |

1. descrivendo le modalità di vendita/pricing (ad. es. task, corpo, giornate persona, etc.);

| **Servizi Professionali** | **Modalità di vendita/pricing** |
| --- | --- |
| Vulnerability Assessment |  |
| Penetration test |  |
| Risk assessment |  |
| Servizio di awareness |  |
| Compliance GDPR |  |
| Altro (specificare) |  |

1. descrivendo le tipologie di figure professionali da impiegare per l’erogazione di tali servizi (ad esempio, senior o junior security architect o security analyst, etc.);

| **Servizi Professionali** | **Tipologie di figure professionali**  |
| --- | --- |
| Vulnerability Assessment |  |
| Penetration test |  |
| Risk assessment |  |
| Servizio di awareness |  |
| Compliance GDPR |  |
| Altro (specificare) |  |

1. Descrivendo gli skills, l’esperienza maturata a livello aziendale dalle risorse e le certificazioni da queste possedute; indicare possibilmente per ciascuna figura professionale anche il numero di risorse aziendali e il relativo inquadramento contrattuale;

| **Servizi Professionali** | **Skills, Esperienza pregressa e Certificazioni possedute dalle risorse a livello aziendale**  |
| --- | --- |
| Vulnerability Assessment |  |
| Penetration test |  |
| Risk assessment |  |
| Servizio di awareness |  |
| Compliance GDPR |  |
| Altro (specificare) |  |

1. Descrivendo i piani di formazione aziendali dedicati alle risorse di cui al punto precedente;

| **Servizi Professionali** | **Piani di Formazione aziendali dedicati alle risorse** |
| --- | --- |
| Vulnerability Assessment |  |
| Penetration test |  |
| Risk assessment |  |
| Servizio di awareness |  |
| Compliance GDPR |  |
| Altro (specificare) |  |

1. RISK ASSESSMENT: per quanto concerne in particolare questo servizio, qualora rientri fra quelli presenti nei vostri ambiti d’offerta, descrivere le aree tematiche di analisi (organizzativa, fisica, logica, reti di trasmissione, continuità operativa, etc) e il relativo processo, dalla survey iniziale, fino alla relativa conclusione, con rilascio degli output attesi dall’Amministrazione (ad es. piano degli interventi), descrivendo anche le fasi intermedie del processo stesso e i relativi deliverables specifici prodotti nonché indicatori di performance ad hoc.

|  |
| --- |
|  |

1. AMBITO OFFERTA FORNITURE/SERVIZI: con riferimento al settore della sicurezza informatica, specificare l’ambito d’offerta della vostre forniture/servizi **(servizi ulteriori rispetto a quelli professionali riportati al quesito 6)**, tenendo conto di quelli indicati a titolo esemplificativo e non esaustivo nella successiva tabella 1 o ulteriori ambiti. Compilare la tabella 1 e, in particolare, la colonna “Offerta del fornitore”:
* descrivendo, per ciascun ambito, i tipi di prodotti e/o servizi che si è in grado di offrire, in termini di caratteristiche tecniche, sia di base che innovative, funzionalità, modalità di esecuzione (laddove applicabile);
* descrivendo, per quanto concerne i prodotti, i servizi connessi alla fornitura degli stessi (ad. es, installazione, configurazione, assistenza, manutenzione) indicando quelli che il Fornitore/System Integrator è in grado di erogare autonomamente e quelli che invece sono erogati direttamente dal Produttore o da Terzi;
* indicando e descrivendo le modalità di vendita/erogazione (appliance fisica, appliance virtuale, software, servizio (ad es. on premise e/o “as a service”), etc.). Nel caso di licenze, specificarne la tipologia: utente, processore, macchina;
* indicando e descrivendo le modalità di pricing (modalità a canone periodico per unità di misura (es. licenza), modalità a consumo (pay per use), prezzo a corpo per appliance, una tantum, giorni persona, ecc.).

Tabella 1

|  |  |
| --- | --- |
| **Ambito** | **Offerta del fornitore** |
| Network Generation Firewall (NGFW) |   |
| Intrusion Detection and Prevention System |   |
| Web Application Firewall |   |
| Protezione anti-APT |  |
| Network Access Control (NAC) |   |
| Secure web gateway |  |
| Secure email gateway |  |
| Secure DNS |  |
| Privileged Account Management |  |
| Endpoint Protection |  |
| Dataloss/leak prevention |  |
| Servizi di monitoraggio e prevenzione incidenti informatici /Security Information and Event Management (SIEM) |  |
| Threat Intelligence Data Feed / Vulnerability Data Feed  |  |
| Static application security testing |  |
| Dynamic application security testing |  |
| Mobile application security testing |  |
| Database security |  |
| Identity &Access Management |  |
| Firma digitale remota, sigillo elettronico, timbro elettronico, marca temporale e certificati TLS/SSL |  |
| Altro (specificare) |  |

1. FATTURATO: indicare il fatturato specifico dell’azienda (privati e mercato Pubblica Amministrazione) nel settore della sicurezza informatica, suddiviso in fornitura, installazione, configurazione, manutenzione e gestione di soluzioni per la sicurezza informatica ed erogazione di servizi professionali di sicurezza, nel triennio precedente all’anno corrente, ripartito, laddove possibile, nei vari ambiti. A titolo esemplificativo e non esaustivo, si riporta di seguito un elenco dei possibili ambiti.

Si chiede di indicare inoltre l’incidenza del costo del personale rispetto al fatturato indicato per i servizi connessi alla fornitura e per l’erogazione dei servizi professionali di sicurezza.

Tabella 2

Se disponibile il dettaglio per ambito, ripartire il fatturato di ciascun ambito in fornitura, installazione e configurazione, manutenzione e gestione di soluzioni per la sicurezza informatica ed erogazione di servizi professionali di sicurezza (ad esempio come riportato in tabella).

|  | **Fatturato 2016 Privati** | **Fatturato 2016 PA** | **Fatturato 2017 Privati** | **Fatturato 2017 PA** | **Fatturato 2018 Privati (anche stimato)** | **Fatturato 2018 PA (anche stimato)** |
| --- | --- | --- | --- | --- | --- | --- |
| **Totale Fatturato in Euro** |  |  |  |  |  |  |
| **Ambito** |  |  |  |  |  |  |
| Network Generation Firewall (NGFW) | x Euro di fornituray Euro di installazione e configurazionez Euro di manutenzionet Euro di gestione |  |  |  |  |  |
| Intrusion Detection and Prevention System |  |  |   |  |  |  |
| Web Application Firewall |  |  |  |  |  |  |
| Protezione anti-APT |  |  |  |  |  |  |
| Network Access Control (NAC) |  |  |  |  |  |  |
| Secure web gateway |  |  |  |  |  |  |
| Secure email gateway |  |  |  |  |  |  |
| Secure DNS |  |  |  |  |  |  |
| Privileged Account Management |  |  |  |  |  |  |
| Endpoint Protection |  |  |  |  |  |  |
| Dataloss/leak prevention |  |  |  |  |  |  |
| Servizi di monitoraggio e prevenzione incidenti informatici /Security Information and Event Management (SIEM) |  |  |  |  |  |  |
| Threat Intelligence Data Feed / Vulnerability Data Feed  |  |  |  |  |  |  |
| Static application security testing |  |  |  |  |  |  |
| Dynamic application security testing |  |  |  |  |  |  |
| Mobile application security testing |  |  |  |  |  |  |
| Database security |  |  |  |  |  |  |
| Identity &Access Management |  |  |  |  |  |  |
| Firma digitale remota, sigillo elettronico, timbro elettronico, marca temporale e certificati TLS/SSL |  |  |  |  |  |  |
| Altro (specificare) |  |  |  |  |  |  |
| **Servizi Professionali** |  |  |  |  |  |  |
| Vulnerability Assessment |  |  |  |  |  |  |
| Penetration test |  |  |  |  |  |  |
| Risk assessment |  |  |  |  |  |  |
| Servizio di awareness |  |  |  |  |  |  |
| Compliance GDPR |  |  |  |  |  |  |
| Altro (specificare) |  |  |  |  |  |  |

|  |
| --- |
|  |

1. COMPETITOR NELL’AMBITO DELL’OFFERTA: indicare i vostri principali competitor sul mercato italiano per i prodotti/servizi da voi proposti nelle risposte alle domande 6 e 8.

|  |
| --- |
|  |

1. CATENA DI VENDITA: descrivere, per ciascuno dei prodotti/servizi da voi indicati in tabella 1, la relativa catena di vendita (Produttore, Distributore, Reseller o System Integrator, erogazione tramite partner terzi).

|  |
| --- |
|  |

1. CARATTERISTICHE TENICHE PRODOTTI E/O SERVIZI: rispetto a quanto da voi indicato nelle risposte alle domande 6 e 8, descrivere le caratteristiche minime che ritenete debba possedere il relativo prodotto/servizio di sicurezza informatica e gli elementi che ritenete maggiormente indicativi ai fini di un’eventuale valutazione tecnica migliorativa (ad. es. caratteristiche dei sistemi HW/SW, livelli di servizio richiesti, modalità di erogazione, etc.).

|  |
| --- |
|  |

1. INTEROPERABILITÁ: vi chiediamo di indicare il grado di interoperabilità dei prodotti per i quali siete Reseller/Distributori/System Integrator o Vendor con prodotti di terze parti e descrivere le modalità utilizzate per garantirne l’integrazione (protocolli standard/proprietari, implementazioni ad hoc,…). Vi chiediamo di indicare la presenza di eventuali vincoli tecnici che limitino la piena interoperabilità.

|  |
| --- |
|  |

1. CARATTERISTICHE PECULIARI NELL’AMBITO DELL’OFFERTA: rispetto a quanto da voi indicato nelle risposte alle domande 6 e 8, descrivere eventuali elementi della vostra offerta tali da rendervi leader del mercato o interlocutore unico (ad es. unica soluzione sul mercato in grado di svolgere determinate funzionalità o rispettare determinati parametri di performance) in termini di prodotti, caratteristiche tecniche, funzionalità e/o servizi in confronto a quanto proposto dai vostri diretti competitor. Si chiede di fornire indicazioni di dettaglio su quali siano tali elementi caratterizzanti.

|  |
| --- |
|  |

1. INDICATORI DI PERFORMANCE: indicare e descrivere gli indicatori di qualità che si ritiene possano essere più appropriati ed oggettivamente misurabili, al fine di valutare nel tempo la performance del fornitore relativamente alla realizzazione e gestione di soluzioni di sicurezza informatica, sia in termini di prodotti che di servizi.

|  |
| --- |
|  |

1. CERTIFICAZIONI DI PRODOTTO/SERVIZIO: indicare le certificazioni di prodotto/servizio, rilasciate da Organismi Nazionali/Internazionali/Società/Terze Parti indipendenti ed ampiamente riconosciute, che si ritengono necessarie o opzionali per i prodotti/servizi offerti.

|  |
| --- |
|  |

1. TEST PRODOTTI: specificare quali test comparativi eseguiti sui prodotti di sicurezza cibernetica da società di analisi e/o certificazione di ricerca IT indipendenti si ritiene siano validi e/o utili ad effettuare una valutazione oggettiva degli stessi.

|  |
| --- |
|  |

1. GDPR: Indicare quali garanzie in termini di conoscenza specialistica, affidabilità, risorse, nonché in ordine all’adozione di misure tecniche, logiche 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. GPP (Green Public Procurement): descrivere eventuali aspetti relativi all’impatto ambientale che ritenete sia opportuno vengano presi in considerazione in un’iniziativa di sicurezza informatica, sia in termini di requisiti minimi che di requisiti premianti. A riguardo, specificare se la Vostra azienda sia in possesso di specifiche certificazioni.

|  |
| --- |
|  |

1. TREND EVOLUTIVI: sulla base della Vostra esperienza e della visione del mercato in cui operate, descrivere i principali trend evolutivi nel settore della sicurezza informatica (in termini di prodotti, servizi, certificazioni aziendali, professionali e di prodotto, evoluzione mercato in generale), anche tenendo conto di quella che è stata e sarà l’evoluzione normativa in tale campo.

|  |
| --- |
|  |

1. MANIFESTAZIONE DI INTERESSE A PARTECIPARE: indicare se la Vostra azienda sarebbe interessata a partecipare ad un’iniziativa relativa all’acquisizione/gestione di soluzioni di sicurezza informatica ed eventualmente per quali ambiti.

|  |
| --- |
|  |

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] |
| *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* |