CAPITOLATO TECNICO

SERVIZI SPECIALISTICI DI SW SECURITY

INDICE

1 PREMESSA

1.1 DEFINIZIONI

Nel corpo del documento, ai termini di cui appresso, viene attribuito il significato riportato a fianco di ciascuno di essi:

- CONSIP: la società che, in qualità di stazione appaltante, affida il servizio oggetto del presente Capitolato;

- SOGEI: la Società Generale di Informatica S.p.A. Committente;

- AMMINISTRAZIONE: si intende il Ministero dell'Economia e delle Finanze, che è proprietario dell'intero capitale di Sogei, con riferimento alle proprie strutture organizzative destinatarie dei servizi erogati dalla Sogei sia attraverso infrastrutture proprietarie che attraverso infrastrutture proprietarie delle singole strutture organizzative; rientrano nella presente definizione le altre Amministrazioni, ivi compresi gli Enti e le Società Pubbliche per cui Sogei svolge e/o svolgerà attraverso le proprie infrastrutture informatiche, per disposizione legislativa o amministrativa (decreto ministeriale, decreto di natura normativa o decreto presidenza consiglio dei ministri), ogni altra attività di natura informatica. Resta fermo che la Sogei potrà utilizzare il contratto per affidamenti di analogo oggetto per esigenze societarie o per altri clienti per i quali Sogei opera già o opererà in virtù di provvedimenti di legge, provvedimenti ministeriali o atti/disposizioni amministrative. Si precisa che per analogo oggetto si dovrà intendere che l'ambito applicativo, funzionale e tecnologico, nonché il contesto organizzativo nel quale i servizi dovranno essere erogati, siano strettamente coerenti con quelli descritti nella presente gara e che le modalità operative risultino compatibili con l'organizzazione, gli strumenti e le competenze richieste dalla documentazione di gara;

- Capitolato tecnico: il presente documento che enuncia le specifiche tecniche alle quali dovrà conformarsi il servizio di fornitura;

- Contratto: il contratto che verrà stipulato tra la SOGEI e l'impresa che enuncia le regole giuridiche alle quali si dovrà conformare il servizio di fornitura;

- Fornitura: il complesso dei beni oggetto del presente Capitolato;

- Società: la società aggiudicataria della fornitura;

- Responsabile delle attività contrattuali: la persona individuata dalla Società come interlocutore di Sogei e responsabile di tutte le attività contrattuali.

1.2 CONTESTO TECNICO-ORGANIZZATIVO

Sogei, negli ultimi anni, il settore dello sviluppo di programmi e applicativi è andato incontro a cambiamenti radicali. Con l'esigenza crescente di accelerare lo sviluppo dei software, i team di sviluppo e quello operativo hanno iniziato a lavorare in maniera sempre più integrata (DevOps).

Da questo modello denominato appunto DevOps (crasi dei termini development e operations) si è passati ad un'ottica DevSecOps, cioè ad un approccio in cui la sicurezza sia prevista e garantita sin dalle prime fasi dello sviluppo di un'applicazione.

Nel corso degli ultimi anni la Sogei ha avviato diversi progetti, che in ottica DevSecOps, hanno consentito di effettuare lo shift left dei controlli di sicurezza del software.

Per far questo sono stati messi a disposizione dei gruppi di sviluppo gli strumenti necessari a spostare questi controlli nelle prime fasi dello sviluppo, riducendo il tempo e il costo degli interventi ed evitando il replicarsi di vulnerabilità note nei moduli sviluppati successivamente.

Per raggiungere tale obiettivo sono sti avviati i progetti relativi alle analisi:

- SAST (Static Application Security Testing) - si basa sulla verifica automatica del codice sorgente alla ricerca di vulnerabiltà

- DAST (Dynamic Application Security Testing) - lo scanner simula attacchi web, non distruttivi, verso il server dove è in esecuzione il codice applicativo, con lo scopo di individuare vulnerabilità di sicurezza o problematiche di configurazione.

- SCA (Software Conposition Analysis) – scanner che consente di individuare le componenti open source vulnerabili utilizzate all'interno delle applicazioni.

Al momento attuale sia l'analisi SAST sia SCA sono integrate all'interno delle nostre pipeline di sviluppo.

In maniera analoga si sta procedendo con l'analisi DAST che al momento è in fase pilota.

2 OGGETTO

Si riportano di seguito in dettaglio le caratteristiche tecniche e le quantità necessarie per ciascun bene/servizio.

2.1 CARATTERISTICHE TECNICHE

Di seguito riportiamo la descrizione dei servizi richiesti:

a) Ottimizzazione tool in pipeline DevSecOps Checkmarx SAST, DAST, SCA

Attraverso l'analisi dell'attuale infrastruttura DevSecOps, IMQ Minded Security offrirà servizi volti a migliorare l'efficacia e l'efficienza dei tool SAST, DAST, SCA utilizzati nelle pipeline.

b) Cloud Pentesting guidelines

Il Cloud Pentesting è un processo di valutazione delle vulnerabilità e dei rischi associati all'infrastruttura cloud, al fine di garantire la sicurezza e la protezione dei dati sensibili.

Il servizio fornito da IMQ Minded Security prevede lo sviluppo di una metodologia avanzata per il Cloud Pentesting con un focus specifico su AWS (Amazon Web Services) e Azure (Microsoft Azure).

c) Formazione su advanced Web Application Penetration Testing

Il servizio prevede una **formazione avanzata** sul Penetration Testing delle applicazioni web, e fornisce una panoramica dettagliata delle tecniche avanzate di test e delle strategie di attacco utilizzate dagli hacker per compromettere le applicazioni web.

d) SDLC Assessment con formalizzazione della roadmap e linea guida aziendale

Il servizio consente di valutare la maturità del ciclo di vita dello sviluppo del software (SDLC), tramite il framework OWASP Software Security 5D, consentendo alle organizzazioni di identificare aree di miglioramento e implementare misure per mitigare i rischi di sicurezza.

Nella tabella 1 si riportano i singoli servizi oggetto del presente capitolato con gli effort stimati:

Tabella 1

Servizio	Effort stimato (gg)
Ottimizzazione tool in pipeline DevSecOps Checkmarx SAST, DAST, SCA	10
Cloud Pentesting guidelines	10
Formazione su advanced Web Application Penetration Testing	10
SDLC Assessment con formalizzazione della roadmap e linea guida aziendale	10

Per svolgere i servizi indicati nella tabella 1 viene richiesto il seguente profilo professionale:

- Principal Security Consultant/ Senior Application Security Expert.

3 MODALITA' DI ESECUZIONE DEL SERVIZIO

Per l'esecuzione dei servizi illustrati nel paragrafo 2.1 del presente Capitolato tecnico, il Direttore dell'esecuzione di Sogei invierà una richiesta tramite email al responsabile della fornitura che dovrà mettere a disposizione i professionisti specializzati del singolo servizio entro 10 giorni dal ricevimento della stessa.

A termine della singola prestazione, Sogei effettua la verifica di conformità che dovrà essere controfirmata dalle parti e accompagnata alla fattura per il pagamento.

4 DURATA

Il contratto avrà efficacia dalla sua stipula fino per una durata di 24 mesi.

5 RESPONSABILE DELLE ATTIVITÀ CONTRATTUALI

Il fornitore dovrà comunicare a Consip, mediante compilazione del facsimile "*Scheda anagrafica e tracciabilità dei flussi*", contestualmente alla presentazione dell'offerta, il nominativo del Responsabile del contratto, nonché un numero di telefono e un indirizzo e-mail al quale indirizzare eventuali comunicazioni.

La Società deve provvedere in piena autonomia al coordinamento e all'organizzazione delle attività nel rispetto delle specifiche e dei tempi forniti da Sogei.

Sarà compito del Responsabile del contratto curare la gestione amministrativa del contratto e delle attività legate alla fatturazione e verificare il rispetto di tutti gli adempimenti contrattuali.

6 VERIFICA DI CONFORMITA'

La verifica di conformità verrà effettuata ai sensi dell'art. 116 Comma 2 del Decreto legislativo 36/2023 Il collaudo finale o la verifica di conformità deve essere completato non oltre sei mesi dall'ultimazione dei lavori o delle prestazioni.

A completamento della verifica positiva sarà prodotto il "Verbale di conformità" che dovrà essere sottoscritto dal Responsabile della Fornitura e dal Responsabile Sogei.

La Verifica di conformità si intende positivamente superata solo nel caso in cui le prestazioni contrattuali siano state eseguite a regola d'arte sotto il profilo tecnico e funzionale, in conformità e nel rispetto delle condizioni, modalità, termini e prescrizioni espresse nel presente Capitolato tecnico.

Tale Verbale dovrà essere allegato alle fatture al fine del pagamento dei corrispettivi alla Società.

7 FATTURAZIONE

Per il pagamento dei servizi oggetto del presente capitolato tecnico si fa riferimento a quanto disciplinato nelle condizioni contrattuale al paragrafo Fatturazione e modalità di pagamento:

"*(il presente comma trova applicazione in caso di servizi a consumo) Ai fini del pagamento del corrispettivo indicato nel presente contratto, il Fornitore potrà emettere fattura successivamente alla approvazione da parte della Committente del "consuntivo attività", contenente il dettaglio delle prestazioni professionali erogate nel periodo di riferimento, nonché della verifica di conformità positiva. Nella fattura dovrà essere indicato il periodo temporale di riferimento.*".

8 PENALI

Si applicheranno le penali nei seguenti casi:

- per ogni giorno lavorativo di ritardo rispetto ai tempi di risposta, di cui al paragrafo 3, si applicherà una penale dello 0,3 per mille dell'ammontare contrattuale

E comunque il valore complessivo delle penali non possono superare il 10 per cento dell'ammontare contrattuale.