



Consip S.p.A.

"Affidamento del servizio di supporto specialistico per attività di Penetration test e Vulnerability Assessment"

CAPITOLATO TECNICO

AFFIDAMENTO DEL SERVIZIO DI SUPPORTO SPECIALISTICO PER ATTIVITÀ DI PENETRATION TEST E VULNERABILITY ASSESSMENT



INDICE

1	PREMESSA	3
1.1	Definizioni.....	3
2	OGGETTO DEL SERVIZIO.....	5
2.1	Modalità di erogazione del servizio.....	6
2.2	Livelli di servizio.....	6
3	GESTIONE DEL SERVIZIO	7
3.1	Responsabile delle attività contrattuali	7
3.2	Modalità di comunicazione	7
3.3	Adempimenti per la Sicurezza.....	7
3.4	Luogo di svolgimento	7
3.5	Obblighi di riservatezza	8
3.6	Tutela delle piattaforme.....	8
4	PENALI	9
5	MODALITÀ DI FATTURAZIONE.....	10



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., beneficiaria del Servizio;
- Capitolato tecnico: il presente documento che enuncia le specifiche tecniche alle quali dovrà conformarsi il servizio;
- Contratto: il contratto che verrà stipulato tra la SOGEI e l'impresa che enuncia le regole giuridiche alle quali si dovrà conformare il servizio;
- Servizio: il complesso delle attività oggetto del presente Capitolato;
- Società: la società aggiudicataria del servizio;
- Piattaforme: Servizi Portali internet Agenzie fiscali Dipartimento Finanze e MEF (n. 16), come da elenco
 - www.agenziademanio.gov.it
 - www.cerdef.it
 - www.agenziadoganemonopoli.gov.it
 - www.agenziaentrateriscossione.gov.it
 - www.agenziaentrate.gov.it
 - www.anpr.interno.it
 - portaleassistenza.agenziaterritorio.it
 - www.portalefederalismofiscale.gov.it
 - portalepa.agenziademanio.it
 - www.mef.gov.it
 - www.rgs.mef.gov.it
 - www.dt.mef.gov.it
 - www.dag.mef.gov.it
 - www.quellocheconta.gov.it
 - www.publicdebt.net
 - <https://portaleservizi.mef.gov.it>
- Orario di servizio: insieme delle fasce orarie nelle quali deve essere assicurata la disponibilità dei servizi applicativi ed infrastrutturali dei portali delle Agenzie fiscali e del Dipartimento delle Finanze; tali fasce orarie sono le seguenti: Lunedì/Venerdì 8:00/20:00 e Sabato 8:00/14:00, esclusi festivi;



Consip S.p.A.

“Affidamento del servizio di supporto specialistico per attività di Penetration test e Vulnerability Assessment”

- Disservizio: si intende una qualunque anomalia funzionale, interruzione o la non completa disponibilità a carico delle Piattaforme che siano diretta o indiretta conseguenza delle attività descritte nel presente documento;
- Responsabile delle attività contrattuali: la persona individuata dalla Società come interlocutore di Sogei e responsabile di tutte le attività contrattuali
- Sistema Informativo: il sistema informativo della fiscalità con sede in Via Mario Carucci 99.



2 OGGETTO DEL SERVIZIO

Il presente Capitolato disciplina l'affidamento del servizio di supporto specialistico per attività di Penetration Test e Vulnerability Assessment per 6 (sei) mesi, da erogarsi in favore della Sogei, ivi comprese tutte le attività connesse allo svolgimento delle prestazioni medesime così come regolamentate, oltre che dal presente Capitolato, anche dallo Schema di contratto e dalle Condizioni Particolari di RdO.

In particolare si richiede l'acquisizione di un servizio di "Full Security Audit" con la finalità di accertare lo stato generale di sicurezza delle Piattaforme alla luce delle modifiche occorse nel tempo dagli ultimi test effettuati previsti dal processo di produzione e dagli esiti di test effettuati su piattaforme tecnologicamente analoghe, che hanno evidenziato delle criticità.

Per l'esecuzione del servizio in oggetto, la Società dovrà impegnarsi ad eseguire le seguenti attività:

- Esecuzione di un Web Penetration Test, con approccio black box, dei servizi esposti dalle Piattaforme per l'individuazione di eventuali vulnerabilità applicative ed infrastrutturali, carenze sui livelli di protezione, configurazioni improprie e opportunità di miglioramenti per ridurre la superficie d'attacco.
- Produzione di un security e technical report contenente i risultati del Web Penetration Test che dovrà includere tutte le evidenze relative ad eventuali vulnerabilità riscontrate. Per ogni eventuale vulnerabilità enucleata nella documentazione la Società si impegna a fornire una classificazione dei livelli di rischio (Alto, Medio, Basso), della difficoltà di sfruttamento di tale vulnerabilità e opportuni suggerimenti per i rimedi.
- Verifica dell'efficacia degli eventuali rimedi adottati dal Committente sulla base del Piano di azione redatto, con una nuova esecuzione di Web Penetration Test mirato alle vulnerabilità evidenziate nel precedente security e technical report.
- Produzione di un report conclusivo con gli esiti della verifica.

La Società dovrà redigere un Piano operativo con la pianificazione delle attività di cui sopra tenendo conto dei livelli di servizio di cui al paragrafo 2.2, da sottoporre all'approvazione della Sogei.

Il piano operativo sarà condiviso in una riunione di startup del progetto tra Società e Sogei che darà inizio alle attività ed avrà la finalità anche di condividere l'organizzazione degli interventi, vista la complessità e la numerosità degli ambiti coinvolti, che sono sotto controllo e monitoraggio attivo.

In particolare dovrà essere stabilito l'ordine degli interventi sui 16 siti indicati al precedente paragrafo 1.1, che sarà condiviso tra le parti sulla base di priorità, complessità, fattibilità nel tempo o altre condizioni che saranno stabilite per le vie brevi e che porteranno alla definizione del suddetto Piano operativo.



2.1 MODALITÀ DI EROGAZIONE DEL SERVIZIO

La Società dovrà eseguire le prestazioni oggetto del presente capitolato a perfetta regola d'arte, con la necessaria diligenza e competenza professionale e con risorse qualificate secondo i requisiti indicati nel presente Capitolato.

Tutte le attività dovranno essere svolte in collaborazione con i responsabili Sogei, secondo modalità opportunamente concordate e secondo il Piano operativo condiviso.

2.2 LIVELLI DI SERVIZIO

Il Servizio dovrà essere erogato secondo la pianificazione concordata con Sogei mediante il Piano operativo di cui al precedente paragrafo 2 che, in ogni caso, dovrà essere consegnato entro 5 (cinque) giorni decorrenti dalla data di stipula del contratto.

In particolare la Società si impegna a:

- a) concludere le attività di Web Penetration Test di cui al paragrafo 2 entro 10 (dieci) giorni lavorativi decorrenti dalla data di avvio riportata nel Piano operativo approvato;
- b) produrre il primo security e technical report di cui al paragrafo 2 entro 10 (dieci) giorni lavorativi decorrenti dal termine dell'attività di Web Penetration Test;
- c) concludere le attività relative al secondo Web Penetration Test di verifica conclusiva entro 10 (dieci) giorni decorrenti dalla comunicazione di disponibilità di Sogei.
- d) produrre il report conclusivo entro 10 (dieci) giorni lavorativi dal termine dell'attività di Web Penetration Test di verifica.



3 GESTIONE DEL SERVIZIO

Il contratto avrà efficacia dalla data della sua stipula, per 6 (sei) mesi e, comunque, sino al completo adempimento di tutte le attività e obbligazioni contrattuali.

3.1 RESPONSABILE DELLE ATTIVITÀ CONTRATTUALI

La Società dovrà comunicare a Consip, trasmettendolo con la documentazione per la stipula, il nominativo del Responsabile del Servizio, 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, che sarà l'unico interlocutore di Sogei, curare la gestione amministrativa del contratto e delle attività legate alla fatturazione e verificare il rispetto di tutti gli adempimenti contrattuali.

3.2 MODALITÀ DI COMUNICAZIONE

La Società si impegna a comunicare a Consip, contestualmente alla presentazione della documentazione per la stipula, un numero di fax, un indirizzo e-mail, un indirizzo pec e un numero di telefono al quale rivolgersi, senza alcun limite sul numero di chiamate, per ogni comunicazione relativa al servizio. L'organizzazione del suddetto servizio di comunicazione dovrà essere a carico della Società.

Resta inteso che, per tutta la durata contrattuale, la Società dovrà garantire la piena funzionalità dei suddetti mezzi di comunicazione comunicando tempestivamente a Sogei eventuali modifiche.

3.3 ADEMPIMENTI PER LA SICUREZZA

La Società s'impegna a porre in essere quanto necessario a garantire l'esecuzione delle attività in piena aderenza con le disposizioni del D. Lgs. 81/2008 "Testo Unico sulla sicurezza durante il lavoro", cooperando e coordinandosi, in particolare, con i referenti della Committente e degli uffici dell'Amministrazione Finanziaria presso cui dovranno essere svolte le attività contrattuali, ai fini degli adempimenti di cui al comma 2 dell'art. 26 del citato decreto.

Si evidenzia che le attività di cui al presente capitolato rientrano nelle fattispecie di cui al comma 3-bis del suddetto articolo, per le quali non sussiste l'obbligo di redigere il DUVRI (Documento Unico di Valutazione dei Rischi da Interferenze).

3.4 LUOGO DI SVOLGIMENTO

Considerando la disponibilità delle Piattaforme su rete pubblica le attività oggetto del presente Contratto potranno essere effettuate sia da remoto sia presso la sede Sogei Via Mario Carucci 99, Roma, previo accordo tra la Società e Sogei.

Resta inteso che eventuali costi di trasferimento e soggiorno del personale che svolge attività nell'ambito del presente Capitolato sono comunque a carico della Società.



3.5 OBBLIGHI DI RISERVATEZZA

La Società aggiudicataria si impegna ad adottare tutte le misure necessarie per garantire la massima riservatezza delle informazioni raccolte durante le attività descritte nel presente Capitolato tecnico e a non divulgare, in nessun caso, a terzi i predetti dati, documenti, informazioni o parti di essi senza il preventivo ed esplicito accordo della Sogei. In questo senso verrà redatto e sottoscritto da Sogei e Società, apposito NDA (Non Disclosure Agreement).

3.6 TUTELA DELLE PIATTAFORME

Considerando la natura delle attività descritte nel presente Capitolato tecnico, la Società si impegna, durante l'esecuzione delle stesse, a non compromettere la disponibilità dei servizi delle Piattaforme e a non adottare azioni che ne possano corrompere l'integrità e la riservatezza dei processi e dei dati da essa gestiti e in generale a determinare situazioni di Disservizio, con particolare riguardo all'Orario di servizio.



4 PENALI

Sogei applicherà le penali, secondo le modalità previste in contratto, nei seguenti casi:

- per ogni giorno lavorativo di ritardo rispetto ai livelli di servizio indicati al precedente paragrafo 2.2, Sogei si riserva di applicare una penale pari allo 0,3‰ (zerovirgolate per mille) dell'importo contrattuale.

Nell'ipotesi in cui l'importo delle penali applicabili superi l'ammontare del 10% (dieci per cento) dell'importo contrattuale complessivo, la Sogei avrà diritto il diritto di risolvere, totalmente o parzialmente, il contratto in danno della Società, salvo il diritto dell'eventuale maggior danno.



5 MODALITÀ DI FATTURAZIONE

La Società potrà emettere fattura secondo i seguenti criteri:

- Emissione della prima fattura di valore pari al 80% dell'importo contrattuale al momento della consegna del primo security e technical report di cui al paragrafo 2 relativo al 50% dei siti indicati;
- Emissione della seconda ed ultima fattura di valore pari al 20% dell'importo contrattuale al momento della consegna dei report conclusivi di cui al paragrafo 2.

Tutte le fatture dovranno riportare il numero di repertorio del contratto ed il codice CIG.

Si precisa che la mancanza di uno di questi elementi consente a Sogei di rifiutare la fattura entro il termine previsto.