CAPITOLATO TECNICO

SERVIZIO DI SUPPORTO SPECIALISTICO IN MATERIA DI SICUREZZA INFORMATICA E PRIVACY

SOMMARIO

PREMESSA

Il presente capitolato contiene le specifiche tecniche cui deve conformarsi il servizio richiesto.

Viene inoltre fornito un glossario dei termini più significativi presenti all'interno del capitolato.

Amministrazione finanziaria	Il complesso delle Strutture Organizzative del Ministero dell'Economia e delle Finanze interessate dal servizio, ed in particolare il Dipartimento Finanze, le Agenzie delle Entrate, delle Dogane e del Territorio, nonché l'Amministrazione Autonoma dei Monopoli di Stato
Capitolato Tecnico	Il presente documento che indica l'insieme delle specifiche tecniche alle quali dovrà essere conforme il servizio.
Contratto	L'atto, conforme allo schema di contratto, che verrà stipulato tra la Sogei e la Società per l'esecuzione del servizio
Responsabile di progetto Sogei	Indica il riferimento Sogei responsabile dell'area nel cui ambito vengono erogate, da parte del personale della Società, le prestazioni professionali richieste per lo svolgimento delle attività.
Servizio	Complesso delle attività previste nel presente capitolato
Sistema informativo	Sistema informativo della fiscalità e Sistema informativo aziendale, con sede in Roma, in via Mario Carucci 99
Società	La Società aggiudicataria del servizio
Sogei	SOGEI, Società Generale d'Informatica S.p.a.
SGSIT	Sistema di Governo della Sicurezza IT
SGP	Sistema di Gestione per la Privacy
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni
Verbale di affidamento	Comunicazione con cui SOGEI affiderà alla Società le attività del progetto

1. CONTESTO DI RIFERIMENTO

Le esigenze di riservatezza, integrità e disponibilità dei dati sono sempre state una priorità per Sogei a causa della natura e delle dimensioni del patrimonio informativo gestito e

della rilevanza degli investimenti sostenuti per la realizzazione e conduzione del Sistema Informativo.

In uno scenario come quello attuale, caratterizzato da una sempre maggiore apertura dei sistemi elaborativi e delle banche dati agli utenti (cittadini, professionisti, Pubblica Amministrazione, Enti Pubblici, Imprese, etc.), attraverso la fornitura di molteplici servizi via rete, Sogei deve assicurare adeguati livelli di sicurezza tramite l'adozione di idonee misure organizzative, tecniche ed operative. Sogei, inoltre, deve garantire la tutela dei dati personali e la riservatezza delle informazioni, attenendosi alle disposizioni del D.lgs. 196/2003 ed alle istruzioni impartite dai Titolari del trattamento dei dati che deve gestire.

La sicurezza in Sogei viene assicurata e attuata attraverso la valutazione dei rischi e la predisposizione del Piano degli interventi volti a mitigarli. A tale scopo si avvale di:

- un sistema di Governo della sicurezza IT che fornisce l'indirizzo della sicurezza IT nel rispetto delle normative vigenti e dei vincoli contrattuali stipulati con il Ministero e le Agenzie;
- un insieme di sistemi di gestione integrati tra loro per l'implementazione delle strategie, politiche e linee guida definite dal Governo; in particolare tali sistemi riguardano la sicurezza delle informazioni e la privacy.

Il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), conformemente allo standard UNI CEI ISO/IEC 27001:2013, fornisce il metodo e gli strumenti per effettuare l'analisi dei rischi e predisporre il piano operativo per il loro trattamento.

Per ciascun servizio erogato, il sistema misura le probabilità che possano avverarsi specifiche minacce, verifica l'efficacia delle misure di sicurezza predisposte a livello applicativo, tecnico ed organizzativo, valuta il rischio residuo e conseguentemente permette di pianificare le eventuali azioni correttive per ridurre tale rischio a livelli più bassi.

Nel contesto appena descritto riveste particolare importanza la progettazione delle suddette misure di sicurezza: per gestire un tale patrimonio informativo è necessario classificare le informazioni e stabilire differenti requisiti di protezione in funzione della loro criticità.

Il Sistema di Gestione della Privacy (SGP) è stato messo in atto per proteggere Sogei dalle conseguenze derivanti dalla eventuale inosservanza della normativa vigente in materia di privacy (D.lgs 196/03, Provvedimenti e Linee guida del Garante).

1.1 SISTEMA DI GOVERNO DELLA SICUREZZA IT

Il Sistema di Governo della Sicurezza IT è costituito dall'insieme strutturato di politiche, processi, linee guida e strumenti a supporto utile a:

- supportare gli obiettivi di business;
- garantire la conformità alle normative vigenti;
- assicurare la soddisfazione degli attori coinvolti, interni ed esterni all'azienda.

Per conseguire tali finalità il Sistema di Governo individua e valuta i rischi inerenti alla sicurezza IT e identifica le linee evolutive necessarie alla loro mitigazione.

L'approccio per l'individuazione dei rischi è basato in particolare sulla valutazione del rischio di non conformità a vincoli e requisiti di sicurezza IT espressi:

- dalla normativa vigente applicabile a Sogei (Codice Privacy e Provvedimenti del Garante applicabili all'azienda, D.lgs. 231/2001),
- dall'Amministrazione (misure di sicurezza esplicitamente richieste a Sogei nelle lettere di designazione come Responsabile del trattamento) e dagli altri stakeholder, interni ed esterni,
- dall'adozione di standard internazionali e best practice (ISO 27001, NIST Cyber Security Framework).

I processi operativi di governo devono perseguire i seguenti obiettivi:

- individuare ed aggiornare la mappa dei rischi di sicurezza IT con riferimento alla non conformità a requisiti derivanti da norme, vincoli contrattuali e standard internazionali applicabili a Sogei;
- individuare le aree di rischio (ambiti di sicurezza) prioritarie per poter indirizzare le attività di audit ed assessment messe in atto dal Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) e dal Sistema di Gestione della Privacy (SGP) per la verifica della conformità dell'infrastruttura IT e delle procedure operative ai requisiti classificati nell'area in esame;
- definire un piano integrato di interventi di sicurezza per contrastare i rischi individuati, ottimizzando l'impiego delle risorse e analizzando i costi rispetto ai benefici;
- verificare l'attuazione del piano di interventi e monitorare il conseguimento del livello di sicurezza e conformità normativa atteso.

Nell'ambito dei processi di Governo, la definizione di un programma di audit e assessment riveste un ruolo primario in quanto permette di verificare la conformità aziendale alle prescrizioni legislative in materia di sicurezza informatica e privacy.

Sono sottoposte ad audit le aree di rischio che richiedono riscontri oggettivi e puntuali ed in cui il campione da sottoporre alle attività di ispezione è sufficientemente limitato. Sono invece sottoposte ad assessment le aree di rischio più estese per cui può essere sufficiente in prima analisi una autovalutazione da parte delle strutture organizzative interessate; in tali casi può seguire all'assessment un audit mirato alla valutazione di specifici aspetti o criticità emerse.

A valle degli audit e degli assessment, il Governo della sicurezza prevede la definizione di Linee Evolutive di interventi necessari a mitigare i rischi che potrebbero provocare, oltre a danni di tipo operativo, sanzioni di natura penale, amministrativa e contrattuale per Sogei. Il Piano Esecutivo degli Interventi di sicurezza contiene le Linee Evolutive approvate dalla Direzione e pianificate dalle strutture aziendali coinvolte.

1.2 SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Il SGSI si applica ai beni aziendali ed ai servizi che vengono erogati da Sogei.

Ai fini della gestione della sicurezza delle informazioni è stato adottato un modello di gestione del rischio per Perimetri, ovvero per servizi verticali erogati esternamente ai clienti istituzionali o internamente a Sogei.

Il Perimetro raggruppa i beni aziendali che concorrono all'erogazione del servizio, distinti in:

- **Beni Informativi**, ovvero le informazioni da salvaguardare;
- **Beni Infrastrutturali**, ovvero le risorse aziendali utilizzate per trattare le informazioni, a loro volta suddivisi nelle seguenti tipologie:

- servizio tecnico
- hardware
- logistica
- software applicativo
- trattamento cartaceo
- persone
- processo di supporto.

In particolare i beni infrastrutturali devono proteggere le informazioni, contrastando le minacce cui queste sono soggette, con opportune misure di protezione.

Nell'ambito della definizione e attuazione del SGSI è stata sviluppata l'applicazione ARPA. Essa permette di effettuare la gestione dell'inventario dei beni, l'assessment e il trattamento del rischio, la produzione dei prospetti da inserire nella documentazione prevista dallo standard UNI CEI ISO/IEC 27001:2013.

L'applicazione costituisce un supporto operativo alle attività di gestione della sicurezza ed un modello utile per l'integrazione con altre basi dati aziendali (Catalogo dei servizi, Repository dei dati,..).

Il SGSI è altresì integrato con il Sistema di Gestione della Privacy (SGP) in termini di procedure operative e controlli contenenti le misure minime di sicurezza stabilite dal D.lgs. 196/2003 per determinare un grado di attenzione focalizzato sugli aspetti privacy.

Attualmente è in fase di estensione il campo di applicazione del SGSI, per consentire il raggiungimento di:

- una certificazione ISO27001 **per processi di gestione delle infrastrutture tecnologiche** oltre a quella già in essere dei **servizi** critici erogati ai clienti istituzionali o internamente,
- una certificazione ISO27001 integrata con il Sistema di Qualità ISO 9001.

1.3 SISTEMA DI GESTIONE DELLA PRIVACY

Per garantire la tutela dei dati personali, nel rispetto del Decreto Legislativo 30 giugno 2003, n. 196 (Codice Privacy), Sogei ha messo a punto un Sistema di Gestione della Privacy.

Tutte le attività societarie sono svolte in coerenza con tale Sistema che definisce, tra l'altro, i ruoli e le responsabilità di tutti i soggetti coinvolti nel trattamento dei dati e le procedure organizzative che devono essere seguite.

Il complesso di informazioni, indicazioni e modalità comportamentali messe a punto per adempiere a quanto previsto dalla predetta normativa sono raccolte, in modo sistematico, nel sistema documentale della privacy.

Sogei, in ambito privacy, assume il duplice ruolo di:

- **Titolare,** per il trattamento dei dati personali di propria competenza, relativi a tutto il personale e familiari, ai visitatori e collaboratori esterni, ai fornitori, a coloro che inviano il curriculum all'azienda per una possibile assunzione e ai membri dei vari organi societari e quant'altro;
- **Responsabile**, per il trattamento dei dati personali di cui sono Titolari l'Amministrazione Finanziaria e gli altri Enti che ad essa fanno capo, da cui ha ricevuto specifiche designazioni.

2. OGGETTO DEL SERVIZIO

Il servizio richiesto alla Società riguarda il supporto specialistico alle seguenti attività:

1. pianificazione e conduzione di audit ed assessment in ambito SGSI e SGP per la valutazione della conformità ai requisiti di sicurezza e privacy;
2. aggiornamento dell'impianto normativo dei requisiti di sicurezza e privacy applicabili a Sogei in relazione alle evoluzioni di legge;
3. certificazione UNI CEI ISO/IEC 27001:2013 per particolari servizi erogati da Sogei e per i processi per la gestione delle infrastrutture tecnologiche;
4. monitoraggio dell'attuazione del Piano Esecutivo degli Interventi di sicurezza e del livello di sicurezza e conformità alla normativa vigente;
5. predisposizione di corsi formativi in ambito SGSI e SGP;
6. evoluzione del SGP;
7. realizzazione di un sistema di governance, risk e compliance a supporto del Sistema di Governo della Sicurezza IT.

La descrizione dettagliata delle attività sopra elencate, le modalità di svolgimento, l'entità dell'impegno previsto nel periodo contrattuale e le caratteristiche del servizio, nonché le modalità di affidamento sono riportate nei paragrafi successivi.

2.1 Pianificazione e conduzione di audit e Assessment

La conduzione di audit/assessment è svolta per verificare la conformità ai requisiti di sicurezza e privacy derivanti dalla normativa vigente e dagli standard e il grado di affidabilità dei controlli attuati.

Per l'assessment la verifica avviene attraverso l'analisi di questionari di autovalutazione compilati da parte delle strutture interessate, mentre per l'audit detta verifica viene effettuata attraverso l'analisi dei processi e delle procedure delle strutture sottoposte a audit e dei test puntuali sui controlli attuati.

Attività da svolgere:

- selezionare i requisiti di sicurezza presenti nelle politiche e nelle procedure operative differenziati per ogni specifico contesto da analizzare;
- predisporre i questionari di audit/assessment con i requisiti di sicurezza da verificare;
- creare dei report sintetici e di dettaglio con i risultati;
- individuare le carenze e/o non conformità e definire dei piani di intervento.

Output da consegnare:

- questionari di audit/assessment;
- report con i risultati di dettaglio per individuare eventuali carenze rispetto ai requisiti richiesti;
- monitoraggio sintetico della rispondenza alla normativa vigente;
- piani di intervento per correggere/eliminare eventuali carenze.

2.2 AGGIORNAMENTO IMPIANTO NORMATIVO DI RIFERIMENTO

Per garantire la conformità alle normative vigenti e agli standard internazionali in materia di sicurezza informatica e privacy, Sogei ha definito un modello integrato di multicompliance che consente di:

- identificare i requisiti di sicurezza e tutela della privacy e le misure organizzative da implementare per i sistemi informativi gestiti e progettati;
- assicurare l'efficacia del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) e del Sistema di Gestione della Privacy (SGP);
- definire piani di audit/assessment multidisciplinari per verificare che tutti i requisiti cogenti siano soddisfatti.

A fronte delle continue evoluzioni regolamentari e degli sviluppi del contesto organizzativo interno, è necessario aggiornare periodicamente il modello per garantire il controllo costante delle attività di mantenimento della conformità.

Attività da svolgere:

- aggiornare il censimento di riferimento dei requisiti per la conformità a norme, vincoli contrattuali e standard relativi alla privacy e alla sicurezza informatica (framework multicompliance); particolare rilievo avrà l'analisi del recepimento del nuovo Regolamento Europeo per la protezione dei dati personali.

Output da consegnare:

- framework multicompliance.

2.3 CERTIFICAZIONE UNI CEI ISO/IEC 27001:2013 DI PARTICOLARI SERVIZI EROGATI DA SOGEI E PROCESSI PER LA GESTIONE DELL'INFRASTRUTTURA

È richiesto il supporto per le attività di certificazione UNI CEI ISO/IEC 27001:2013 per alcuni servizi di natura applicativa erogati da Sogei. e per i processi di gestione dell'infrastruttura.

A tutela del patrimonio informativo gestito dalla Sogei, è necessario infatti effettuare la valutazione puntuale del rischio connesso con l'erogazione dei singoli servizi, al fine di:

- garantire la massima sicurezza delle informazioni gestite;
- razionalizzare e visualizzare, anche a livello contrattuale, attività che oggi sono comprese, ma senza specifica evidenza, nell'ambito degli obiettivi di sviluppo e conduzione;
- definire le misure di sicurezza in funzione della classificazione dei dati connessi con l'erogazione dei singoli servizi, disegnando differenti soluzioni tecnico/organizzative;
- pianificare gli interventi di ottimizzazione dei livelli di sicurezza per i servizi erogati.

II percorso di certificazione prevede verifiche della documentazione e verifiche sul campo.

Attività da svolgere*:*

- revisione e aggiornamento del sistema documentale del SGSI al fine di conseguire la certificazione dei processi IT infrastrutturali del data center, in modalità integrata con il sistema di gestione della qualità ISO9001;
- pianificazione ed esecuzione dell'analisi di dettaglio del rischio per tutti i servizi/processi individuati da Sogei;
- stesura del relativo piano di trattamento del rischio.

Output da consegnare:

- documentazione inerente la certificazione UNI CEI ISO/IEC 27001:2013.

2.4 MONITORAGGIO PIANO ESECUTIVO INTERVENTI E INDICATORI DI RISCHIO

L'utilizzo e la diffusione di un sistema di misurazione finalizzato al monitoraggio dell'attuazione delle strategie ed alla verifica dei risultati ottenuti rispetto agli obiettivi prefissati, riveste un ruolo di notevole rilevanza per il governo della sicurezza.

In tal senso, nell'ambito del Sistema per il Governo della Sicurezza IT, viene effettuato un monitoraggio periodico del Piano Esecutivo degli Interventi di sicurezza aziendale.

Il monitoraggio avviene attraverso la raccolta dell'avanzamento mensile degli interventi fornito dalle Funzioni aziendali coinvolte e nella predisposizione di una relazione di sintesi per la Direzione.

Per rappresentare inoltre il rischio corrente a cui è soggetta l'azienda relativamente alla sicurezza IT, sono stati individuati ad esempio i seguenti indicatori:

- valori dei livelli di conformità ai requisiti normativi/standard rilevati dalle attività di audit/assessment;
- valori dello stato d'avanzamento degli interventi contenuti nella relazione di sintesi;
- valori di performance delle misure di sicurezza IT adottate per mitigare i rischi, raccolti attraverso il Sistema di Misurazione per la Sicurezza delle Informazioni (SMSI), adottato in azienda nell'ambito del sistema SGSI, che misura il livello di efficacia e di efficienza dei controlli di sicurezza attuati.

In sintesi l'indicatore di rischio IT è una misura ottenuta applicando un algoritmo a specifiche misure base allo scopo di:

- consentire, a chi è responsabile della gestione della sicurezza, di tradurre gli obiettivi di business in obiettivi di sicurezza IT;
- consentire il monitoraggio degli interventi definiti nel Piano Esecutivo aziendale e orientati alla mitigazione dei rischi di sicurezza;
- offrire ai diversi livelli aziendali la possibilità di controllare, attraverso una serie di indicatori, l'andamento delle variabili che hanno impatto sulla sicurezza IT e di definire le opportune azioni.

Attività da svolgere:

- predisposizione relazioni mensili di sintesi per il monitoraggio del Piano Esecutivo Annuale degli Interventi di sicurezza;

- definizione degli opportuni indicatori di conformità ed efficienza dei controlli di sicurezza attuati, da elaborare per rappresentare gli indicatori di rischio nei diversi ambiti di interesse.

***Output da consegnare*:**

- relazioni mensili di sintesi del Piano Esecutivo Annuale;

- studio per la definizione di indicatori di conformità ed efficienza e relativa documentazione delle specifiche di rilevazione delle misure e di calcolo.

2.5 PREDISPOSIZIONE DI CORSI FORMATIVI IN AMBITO SGSI E SGP

La formazione del personale su tematiche di sicurezza delle informazioni e privacy è fondamentale per la corretta applicazione delle politiche di sicurezza definite.

***Output da consegnare*:**

È richiesto il supporto per la redazione ovvero l'aggiornamento di quanto di seguito esplicitato.

In particolare:

- predisposizione di corsi su tematiche inerenti il Sistema di Gestione per la Sicurezza delle Informazioni e della Privacy;

- predisposizione di corsi di aggiornamento su specifiche tematiche in ambito sicurezza informatica (awareness, cybersecurity, …).

2.6 EVOLUZIONE DEL SISTEMA DI GESTIONE DELLA PRIVACY

Il Sistema di Gestione della Privacy evolve di pari passo con la normativa vigente e i provvedimenti emessi dal Garante, recependo anche le istanze di miglioramento provenienti dagli stakeholder interni.

***Output da consegnare*:**

- predisposizione di regolamenti, policy aziendali e procedure relative all'attuazione degli adempimenti previsti dalle normative vigenti in ambito privacy, con particolare riguardo al nuovo Regolamento Europeo per la protezione dati personali, al D.lgs. 196/2003 e ai provvedimenti dell'Autorità Garante applicabili tanto nelle relazioni con i dipendenti, quanto nei rapporti con soggetti esterni;

- revisione della documentazione del Sistema di Gestione della Privacy, con riferimento alla razionalizzazione e semplificazione degli adempimenti e al recepimento del nuovo Regolamento europeo in via di emanazione;

- predisposizione di specifiche applicative per l'evoluzione delle applicazioni del Sistema Informativo Aziendale a supporto del SGP.

2.7 REALIZZAZIONE DI UN SISTEMA DI GOVERNANCE, RISK E COMPLIANCE

È richiesto supporto alle fasi di analisi, progettazione e implementazione di una piattaforma di Governance, Risk e Compliance a supporto del Sistema di Governo della Sicurezza IT, basata sul prodotto RSA Archer.

Attività da svolgere:

È richiesto il supporto per analisi, progettazione e implementazione delle seguenti funzionalità:

- definizione e popolamento della libreria di controlli di sicurezza e privacy;
- integrazione con il Repository aziendale di asset IT;
- distribuzione e raccolta di questionari di assessment contenenti i requisiti di sicurezza differenziati per contesto di analisi e per struttura organizzativa;
- reporting di dettaglio sulle eventuali carenze e non conformità ai requisiti dichiarate in auto-valutazione dalle strutture coinvolte;
- rilevazione di misure relative alla efficacia ed efficienza dei controlli IT;
- dashboard di valutazione della conformità e del rischio IT.

Output previsti:

- documento di analisi e progettazione della piattaforma
- implementazione e attivazione delle funzionalità contenute nel suddetto documento sulla piattaforma di Governance, Risk e Compliance.

3. ENTITÀ E DURATA DELL'IMPEGNO

Il servizio coprirà un arco temporale di 24 mesi, a partire dalla stipula del contratto.

Per il servizio richiesto l'impegno è indicativamente stimato in 530 giorni/persona così suddivisi per le diverse figure professionali richieste:

- N. 100 g/p per il Capo progetto;
- N. 150 g/p per il Consulente esperto in ambito sicurezza delle informazioni;
- N. 100 g/p per il Consulente esperto in ambito normativo;
- N. 180 g/p per il Consulente esperto in ambito governance-risk-compliance.

SOGEI si riserva la facoltà di modificare la precedente ripartizione del numero di giornate tra le diverse figure professionali sulla base delle reali esigenze emerse durante lo svolgimento delle attività e previo accordo con il Capo Progetto.

4. ORARIO E LUOGO DI PRESTAZIONE DEI SERVIZI

Le attività oggetto del servizio verranno svolte, salvo diversa indicazione della SOGEI, presso la sede di Sogei di Roma.

La Società dovrà comunicare alla Sogei, entro cinque giorni dalla data di stipula del contratto, l'ubicazione delle proprie sedi, ove saranno svolte le attività, ove consentito da Sogei in relazione alle attività affidate, e dovrà provvedere al coordinamento ed all'organizzazione delle stesse effettuate presso le proprie sedi.

Le attività verranno svolte all'interno di gruppi di lavoro formati dal personale della Società e da personale Sogei.

Le risorse dovranno prestare il proprio servizio nei giorni feriali compresi dal lunedì al venerdì dalle ore 9:00 alle ore 18:00,.

Resta inteso che i costi di trasferimento e soggiorno del personale che svolge le attività al di fuori delle sedi della Società stessa sono comunque a carico della Società.

5. ARTICOLAZIONE DEL SERVIZIO

5.1 GENERALITÀ

Per una perfetta esecuzione del servizio la Società dovrà mettere a disposizione di SOGEI risorse qualificate in base alle caratteristiche descritte da SOGEI nel presente capitolato.

La Società deve provvedere a svolgere il servizio richiesto nel rispetto delle specifiche e dei tempi forniti da SOGEI; deve provvedere inoltre al coordinamento ed all'organizzazione delle attività assegnate.

La Società non potrà utilizzare, a nessun titolo, la documentazione fornita dalla SOGEI al di fuori delle attività oggetto del presente capitolato.

Tutta la documentazione prodotta a supporto delle attività oggetto del servizio dovrà essere conforme agli standard aziendali SOGEI, essere redatta in lingua italiana e non riportare alcun marchio o logo societario identificativo del fornitore.

La Società metterà a disposizione della SOGEI tutto quanto necessario per l'espletamento del servizio oggetto della fornitura. Al termine delle attività quanto prodotto sarà consegnato a SOGEI, completo delle eventuali licenze e di quanto necessario per un successivo utilizzo autonomo da parte di SOGEI, senza necessità di intervento da parte della Società aggiudicatrice.

Per l'espletamento del servizio, la SOGEI metterà a disposizione della Società la documentazione necessaria.

Sogei concorderà una "riunione di avvio"da effettuarsi entro 10 giorni dalla stipula del contratto. All'avvio operativo del progetto, il responsabile Sogei condividerà con la

Società, ferme restando le linee operative individuate, un approfondimento sugli obiettivi da perseguire per ciascuna di esse e le modalità di erogazione delle attività progettuali.

Sulla base delle informazioni acquisite nella "riunione di avvio", la Società predisporrà un Piano di Lavoro, da consegnare a Sogei entro 10 giorni lavorativi dalla riunione di avvio, che dovrà mantenere aggiornato per consentire l'esecuzione e il monitoraggio della fornitura.

Il Piano di Lavoro, in accordo con il referente SOGEI, potrà essere soggetto a modifiche e ulteriori pianificazioni, secondo le esigenze e gli indirizzi strategici che emergeranno nel corso dei lavori, fermo restando la conclusione delle attività in oggetto entro il periodo di durata del contratto.

Il Piano di Lavoro dovrà indicare:

- le attività, codificate in maniera univoca, e le relative date di inizio e fine;
- le risorse allocate su ciascuna attività in termini di giorni/persona suddivise per mese e per profilo professionale;
- i prodotti di fornitura (output) delle singole attività e le relative date di consegna previste.

Entro 10 giorni lavorativi dalla consegna del Piano di Lavoro SOGEI, con una apposita comunicazione esecutiva formalizzata nel documento "Verbale di affidamento", notificherà l'approvazione del Piano autorizzando le attività in base alla pianificazione effettuata.

Entro le date di scadenza previste dal Piano di Lavoro, la Società dovrà provvedere alla consegna degli output delle attività secondo le modalità di comunicazione concordate, affinché SOGEI ne dia approvazione formale.

Nel caso venissero richieste modifiche o integrazioni degli output, il materiale modificato dovrà essere riconsegnato entro il termine indicato nella richiesta stessa.

A seguito della consegna da parte della Società degli output previsti, la SOGEI si riserva di valutare la coerenza e la completezza di quanto prodotto rispetto a quanto pianificato/previsto.

Con cadenza mensile verranno convocati degli incontri di condivisione dello stato di avanzamento lavori ai quali dovrà necessariamente prendere parte il Referente/coordinatore delle attività e nel corso dei quali la Società dovrà presentare una relazione (Stato Avanzamento Lavori - SAL) indicante:

- le attività concluse con la relativa codifica;
- l'indice degli output consegnati con l'evidenza di quelli consegnati nell'ultimo mese;
- l'avanzamento delle attività;

- il riepilogo dei giorni persona impiegati per l'esecuzione delle attività equivalenti alle attività concluse e la realizzazione degli output consegnati, coerentemente con quanto previsto nel Piano di Lavoro.
- il Piano di Lavoro aggiornato con le ripianificazioni necessarie e corredato dall'indicazione dei razionali delle eventuali ripianificazioni, e di ogni altra informazione utile al controllo delle attività. Il piano di lavoro aggiornato dovrà essere consegnato a Sogei entro 5 giorni lavorativi dal termine della riunione di condivisione.

Entro 10 giorni SOGEI comunicherà per iscritto alla Società l'approvazione formale del SAL e del Piano di Lavoro aggiornato. Non è prevista l'approvazione per tacito assenso.

La SOGEI si riserva la facoltà di sospendere, in qualunque momento, le attività affidate alla Società e di richiedere la consegna di quanto eventualmente prodotto al momento della richiesta di sospensione; in tale ipotesi verranno riconosciuti alla Società i corrispettivi per le attività riconosciute fino alla predetta data di sospensione.

5.2 RESPONSABILE DELLA SOCIETÀ PER LE ATTIVITÀ CONTRATTUALI

Prima della stipula del contratto, la Società dovrà comunicare alla SOGEI il nominativo del proprio rappresentante designato quale responsabile delle attività contrattuali e del coordinamento delle stesse.

Tale responsabile sarà, per gli aspetti amministrativi, l'interlocutore unico della SOGEI per l'organizzazione ed il coordinamento delle risorse della Società che saranno impegnate nelle attività contrattuali.

Sarà cura del responsabile verificare il rispetto di tutti gli adempimenti contrattuali, curando in particolare il rispetto dei tempi e delle modalità di consegna della documentazione prevista nei paragrafi successivi.

Per facilitare e velocizzare l'attività amministrativa di entrambe le parti, ogni comunicazione riguardante aspetti contrattuali dovrà essere scambiata, sia in formato cartaceo che elettronico, tra SOGEI e la Società.

5.3 MODALITÀ DI COMUNICAZIONE

Al fine di assicurare il coordinamento del servizio, il responsabile contrattuale dovrà garantire la reperibilità negli orari di esecuzione del servizio.

A tal fine la Società comunicherà alla SOGEI, prima della stipula del contratto, un numero di telefono, almeno due numeri di fax e un indirizzo di e-mail ai quali potrà essere inviata ogni comunicazione relativa all'esecuzione delle attività contrattuali.

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 alla SOGEI eventuali modifiche di numerazione.

5.4 RISERVATEZZA

La Società non potrà utilizzare, a nessun titolo, la documentazione e qualunque informazione di cui venga a conoscenza nell'espletamento delle attività oggetto del presente capitolato tecnico.

Inoltre, per quanto concerne i trattamenti dei dati personali connessi con l'adempimento delle obbligazioni contrattuali, la Società dovrà attenersi alle disposizioni previste dal Decreto Legislativo 30 giugno 2003, n. 196 – Codice in materia di trattamento di dati personali.

6. REQUISITI DELLE FIGURE PROFESSIONALI RICHIESTE PER LO SVOLGIMENTO DEL SERVIZIO

Il team di lavoro dovrà essere composto da:

- n. 1 Capo Progetto
- n. 2 Consulenti esperto in ambito tecnico-organizzativo
- n. 1 Consulente esperto in ambito tecnico-normativo
- n. 1 Consulente esperto in ambito governance-risk-compliance

La Società dovrà fornire entro 15 (quindici) giorni solari dalla data di stipula del contratto l'elenco delle risorse che utilizzerà nell'esecuzione del servizio. Eventuali variazioni (in ingresso o in uscita) alla composizione dell'elenco del personale dichiarato dovranno essere comunicate anticipatamente e debitamente motivate.

La Società dovrà inoltre fornire, con un preavviso di cinque giorni, l'elenco delle ulteriori risorse che utilizzerà nell'esecuzione del servizio per eventuali particolari esigenze tecniche.

Unitamente agli elenchi dei nominativi delle risorse, dovranno essere consegnati i relativi Curriculum Vitae, al fine di consentire alla SOGEI la valutazione delle risorse, la verifica dei livelli di conoscenza e della generale idoneità allo svolgimento delle attività richieste.

I "curriculum vitae" delle risorse dovrà presentato secondo il modello "Europass Curriculum Vitae (ex Curriculum Vitae Europeo)" http://www.lavoro.gov.it/Lavoro/Europalavoro/SezioneCittadini/Orientarsi/EuropassCurri

culumVitae/ e dovranno essere firmati e sottoscritti, come previsto dal D.Lgs. 30 giugno 2003 n. 196.

In considerazione della particolare natura dell'incarico affidato alla SOGEI dall'Amministrazione finanziaria e dei vincoli gravanti, ai sensi delle vigenti disposizioni in materia sul personale addetto all'espletamento dell'incarico, il personale della Società dovrà essere di gradimento della SOGEI. Pertanto la Società si impegna fin d'ora a sostituire il personale che non abbia l'approvazione della SOGEI stessa, entro cinque giorni solari dalla richiesta della SOGEI.

Qualora la sostituzione fosse fatta in ritardo o la nuova risorsa fosse ancora inadeguata e si dovesse ricorrere a un'ulteriore sostituzione, verranno applicate le penali del caso, secondo le modalità previste nel presente capitolato.

Alla terza sostituzione, relativa alla medesima figura professionale, ritenuta non idonea da SOGEI, la stessa SOGEI potrà rescindere dal contratto ed incamerare la cauzione.

Le risorse assegnate non possono essere sostituite dalla Società durante l'esecuzione delle attività; qualora intervenissero eventi non dipendenti dalla Società (per esempio dimissioni) che costringessero alla sostituzione di una risorsa, la Società dovrà farsi carico del periodo di affiancamento/istruzione necessario per rendere la nuova risorsa autonoma per il servizio.

La Società dovrà mettere a disposizione le risorse in conformità con la tipologia e la quantità richiesta e nelle date previste per l'inizio delle singole attività secondo quanto indicato nel Piano di Lavoro.

Di seguito i requisiti previsti per le figure professionali richieste:

6.1 CAPO PROGETTO

Il Capo progetto dovrà garantire:

- l'analisi delle attività da svolgere;
- il coordinamento delle attività svolte dalla Società;
- la qualità dei output documentali ovvero la loro rispondenza agli obiettivi, la loro chiarezza, completezza e sinteticità;
- il rispetto degli standard aziendali forniti dalla Sogei;
- il perseguimento ed il raggiungimento, nei tempi e nei modi stabiliti, degli obiettivi previsti nel piano di lavoro;
- il processo di rilevazione e reporting dei servizi erogati anche ai fini della loro fatturazione;

- la partecipazione alle riunioni di revisione ed avanzamento lavori, per la valutazione dello stato delle attività del progetto, la valutazione dei potenziali rischi, la formulazione di proposte di soluzioni e l'esame dei risultati.

Requisiti richiesti:

1. essere in possesso di diploma di laurea in ingegneria o in discipline scientifiche-economiche;
2. essere in possesso della qualificazione di "Lead Auditor" secondo la norma ISO/IEC 27001;
3. possedere una esperienza di almeno 48 mesi maturata negli ultimi 7 anni nella partecipazione a progetti per la realizzazione e conduzione di sistemi di gestione della sicurezza delle informazioni con particolare riferimento alla serie ISO/IEC 27000;
4. possedere una esperienza di almeno 36 mesi maturata negli ultimi 5 anni nella responsabilità di progetti, nella applicazione di metodologie di *project management* e di analisi e valutazione dei processi.
5. possedere una esperienza di almeno 12 mesi maturata negli ultimi 3 anni nella responsabilità di progetti di analisi del rischio su processi di business (organizzativi, legali, procedurali e tecnologici) in accordo con le linee guida dello standard ISO/IEC 27005.

Inoltre, saranno valutati i seguenti requisiti migliorativi come nel dettaglio riportato nella Lettera di richiesta di offerta:

1. possesso di una certificazione di project management (PMI, PRINCE2, ecc.);
2. possesso della certificazione CISSP – "Certified Information Systems Security Professional" oppure "CISA - Computer Information System Auditor" oppure CISM – "Certified Information Security Manager";
3. possesso di un attestato di qualificazione "Lead Auditor" ISO 27001;
4. possesso di una certificazione o attestato di formazione in ulteriori standard inerenti la sicurezza informatica (ISO 20000, ITIL, COBIT, ISO31000, COSO)
5. esperienza di almeno 12 mesi in ambito Cyber Security nella gestione di progetti per l'organizzazione, la realizzazione e la conduzione di servizi di CERT.

6.2 CONSULENTE ESPERTO

Per quanto riguarda l'attività della figura di Consulente Esperto, sono richiesti tre diversi skill professionali relativi alla sicurezza delle informazioni:

- consulente esperto in ambito tecnico-organizzativo
- consulente esperto in ambito tecnico-normativo
- consulente esperto in ambito governance-risk-compliance.

6.2.1 Consulente esperto in ambito tecnico-organizzativo

Requisiti richiesti*:*

1. essere in possesso di diploma di laurea in ingegneria o in discipline scientifiche-economiche;
2. possedere una esperienza di almeno 36 mesi maturata negli ultimi 5 anni nella partecipazione a progetti per:
    a. realizzazione e conduzione di sistemi di gestione della sicurezza delle informazioni con particolare riferimento alla serie ISO/IEC 27000;
    b. definizione di politiche e procedure operative, tecnologiche e organizzative di sicurezza.
3. possedere una esperienza di almeno 12 mesi maturata negli ultimi 3 anni nella partecipazione a progetti con obiettivo specifico di analisi e di valutazione dei rischi:
4. possedere una esperienza di almeno 12 mesi maturata negli ultimi 3 anni in attività di audit e di assessment della sicurezza informatica;
5. possedere una esperienza di almeno 36 mesi maturata negli ultimi 5 anni in ambito di sistemi centrali e distribuiti, di architetture di rete, di protocolli di comunicazione e delle principali infrastrutture di sicurezza (firewall intrusion detection, antimalware, PKI, Identity Management, ecc.).

Inoltre, ~~si richiede il possesso di almeno due tra i seguenti requisiti~~ saranno valutati i seguenti requisiti migliorativi come nel dettaglio riportato nella Lettera di richiesta di offerta :

1. possesso della qualificazione di "Lead Auditor" secondo la norma ISO/IEC 27001;
2. possesso della certificazione CISSP – "Certified Information Systems Security Professional" oppure "CISA - Computer Information System Auditor";
3. possesso della certificazione CISM – "Certified Information Security Manager";
4. possesso di una certificazione o attestato di formazione in ulteriori standard inerenti la sicurezza informatica (ISO 20000, ITIL, COBIT, ISO31000, COSO).

6.2.2 Consulente esperto in ambito tecnico-normativo

Requisiti richiesti:

1. essere in possesso di diploma di laurea in ingegneria o in discipline scientifiche-economiche-giuridiche;
2. possedere una esperienza di almeno 48 mesi maturata negli ultimi 5 anni nella partecipazione a progetti per l'attuazione, in aziende di grandi dimensioni, degli aspetti relativi al D. Lgs. 196/2003 (Codice in materia di protezione dei dati personali), in riferimento a:

a. implementazione delle misure di sicurezza tecnico-organizzative previste in particolare nella "Parte I Titolo V - Sicurezza dei dati e dei sistemi", nell'"Allegato B" del citato D. Lgs. 196/2003 e nei principali provvedimenti del Garante (posta elettronica e internet, videosorveglianza)

b. redazione di politiche, regolamenti, procedure e clausole contrattuali per l'applicazione della normativa sulla sicurezza informatica e privacy

c. attività di audit sull'attuazione dei relativi adempimenti

3. possedere una esperienza di almeno 12 mesi maturata negli ultimi 3 anni nella partecipazione a progetti per l'attuazione delle "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" (G.U. n. 300 del 24 dicembre 2008 e modifiche in base al provvedimento del 25 giugno 2009);

Inoltre, saranno valutati i seguenti requisiti migliorativi:

1. possesso della qualificazione di "Lead Auditor" secondo la norma ISO/IEC 27001;

2. possedere una esperienza di almeno 12 mesi maturata negli ultimi 3 anni nella partecipazione a progetti per l'attuazione dei controlli relativi al Dlgs 231/2001 "Responsabilità amministrativa delle società e degli enti", con particolare riguardo ai controlli inerenti la sicurezza delle informazioni;

3. possedere una esperienza di almeno 12 mesi maturata negli ultimi 3 anni nella partecipazione a progetti per l'attuazione degli aspetti relativi al D. Lgs. 196/2003 con riferimento a forniture di dati al Titolare nonché, su richiesta del Titolare stesso, trasferimento di dati a soggetti terzi, operanti sul territorio nazionale o all'estero.

6.2.3 Consulente esperto in ambito governance-risk-compliance

Requisiti richiesti*:*

1. essere in possesso di diploma di laurea in ingegneria o in discipline scientifiche;

2. possedere una esperienza di almeno 36 mesi maturata negli ultimi 5 anni nella partecipazione a progetti per l'attuazione, in aziende di grandi dimensioni, di piattaforme di governance-risk-compliance in ambito sicurezza delle informazioni, finalizzate a implementare:

a. sistemi multi-compliance per analisi del rischio, basati su politiche, regolamenti, procedure, standard e normative su sicurezza informatica e privacy

b. piani e attività di audit sull'attuazione dei relativi adempimenti

c. dashboard e report direzionali sullo stato del rischio aziendale

3. possedere le certificazioni "RSA Archer Administration" e "RSA Archer Advanced Administration" con una esperienza documentata di almeno 12 mesi maturata negli ultimi 3 anni nella partecipazione a progetti di sviluppo su piattaforma RSA Archer.

Inoltre, saranno valutati i seguenti requisiti migliorativi*:*

1. possesso della qualificazione di "Lead Auditor" secondo la norma ISO/IEC 27001;
2. possesso di una certificazione o attestato di formazione in ulteriori standard inerenti la sicurezza informatica (ISO 20000, ITIL, COBIT, ISO31000, COSO).

7. CONSUNTIVAZIONE DELLE ATTIVITÀ SVOLTE

A seguito della consegna, da parte della Società degli output, previsti per ogni singola attività, secondo le scadenze previste nel Piano di Lavoro, la SOGEI si riserva di valutare la coerenza e la completezza di quanto prodotto rispetto a quanto pianificato/previsto.

A fronte delle conclusione delle singole attività e successivamente all'approvazione da parte ~~approvate~~ della SOGEI degli output previsti, sulla base di quanto riportato nel Piano di Lavoro, la Società potrà consuntivare ed emettere fattura per il numero di giorni e tipologia di figura professionale effettivamente impiegati.

La consuntivazione deve essere effettuata mediante la compilazione del modulo "Dichiarazione delle prestazioni rese" contenente l'indicazione nominativa e quantitativa delle risorse impiegate dalla Società e presentata entro il terzo giorno lavorativo del mese successivo a quello in cui sono state concluse le attività.

Il modulo "Dichiarazione delle prestazioni rese" firmato dovrà essere allegato alla fattura.

Detto modulo dovrà essere sottoscritto dal responsabile della Società e dal Direttore dell'esecuzione di Sogei, previa verifica degli output attesi nel periodo.

8. Livelli di servizio

Di seguito, in forma tabellare, vengono rappresentati i livelli di servizio che il fornitore dovrà rispettare a partire da una determinata data/evento. Nelle note si riportano eventuali specificazioni.

PRODOTTO	EVENTO	GIORNI	NOTE
Comunicazione	Stipula del contratto	5 giorni solari	

dell'ubicazione sedi per lo svolgimento delle attività			
Piano di lavoro (iniziale)	Riunione per avvio operativo del progetto	10 giorni lavorativi	
Piano di lavoro/ SAL (aggiornamento periodico)	Incontro di aggiornamento	cadenza mensile	

ADEMPIMENTO	EVENTO	GIORNI	NOTE
Consegna CV risorse impiegate/da impiegare	Stipula del contratto	15 giorni solari	
Consegna nuovo CV in caso di non accettazione o di richiesta sostituzione risorsa	Dalla comunicazione di non accettazione/ dalla richiesta di sostituzione	5 giorni solari	
Consegna nuovo CV in caso di sostituzione risorsa richiesta dall'impresa	Prima dell'effettiva sostituzione	almeno 5 giorni solari	Il CV deve essere allegato alla comunicazione di richiesta sostituzione
Disponibilità della risorsa per un colloquio	Dalla richiesta	3 giorni lavorativi	Colloquio presso la sede SOGEI

9. PENALI

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

- per ogni giorno di ritardo nella comunicazione dei riferimenti richiesti (sedi, fax, caselle di posta elettronica, ubicazione delle sedi ecc.) a vario titolo, Sogei applicherà una penale pari all'1 per mille dell'importo contrattuale;

- per ogni giorno di ritardo nella comunicazione delle risorse impegnate, nella consegna della dichiarazione delle ulteriori risorse, ovvero nella sostituzione delle risorse, Sogei applicherà una penale pari all'1 per mille dell'importo contrattuale

- per ogni giorno di ritardo nella consegna degli output delle attività, rispetto alle date fissate nel Piano di Lavoro, ovvero nella consegna delle modifiche o integrazioni richieste agli output del servizio verrà applicata una penale pari all'1 per mille dell'importo contrattuale;

- Sogei si riserva di applicare le penali fino ad un importo massimo pari al 10 (dieci) per cento dell'importo complessivo contrattuale. Per l'applicazione delle penali Sogei si riserva la facoltà di compensare il credito con quanto dovuto al Fornitore. Qualora l'importo complessivo delle penali inflitte all'Impresa raggiunga la somma complessiva pari al 10% del corrispettivo globale, la Sogei ha facoltà, in qualunque tempo, di risolvere di diritto il presente contratto con le modalità nello stesso espresse, oltre il risarcimento di tutti i danni