ALLEGATO 3

CAPITOLATO TECNICO

SERVIZI PROFESSIONALI FINALIZZATI ALLA PROGETTAZIONE E REALIZZAZIONE DI UN SISTEMA PER LA VERIFICA DELLA SICUREZZA DELL'INFORMAZIONE NELL'AMBITO DEI SISTEMI INFORMATIVI DEL DAG-MEF

INDICE

1 PREMESSA 3

2 OGGETTO DEL SERVIZIO RICHIESTO 3

3 ENTITÀ DELL'IMPEGNO 4

4 MODALITÀ DI EROGAZIONE DEL SERVIZIO 5

4.1 Generalità 5

4.2 Responsabile del servizio 6

4.3 Luogo di svolgimento 6

4.4 Modalità di consegna 6

4.5 Consuntivazione delle attività svolte e fatturazione 6

5 REQUISITI PROFESSIONALI RICHIESTI 7

5.1 Requisiti minimi dei Professionisti 8

6 PENALI 9

1 PREMESSA

La funzione di Internal Audit del DAG-MEF è preposta alla verifica e valutazione dell'adeguatezza dei processi organizzativi ed IT, promuovendone il miglioramento continuo, ed effettua interventi di audit atti a prevenire possibili frodi informatiche, anche attraverso l'analisi dei rischi dei processi anzidetti. A supporto di tali attività l'Amministrazione intende dotarsi di un Sistema per la Verifica della Sicurezza dell'Informazione.

La funzione di Internal Audit del DAG-MEF è inquadrata all'interno della Direzione dei Sistemi Informativi e dell'Innovazione.

Le principali funzioni svolte dalla Direzione dei sistemi informativi e dell'innovazione sono: definizione delle specifiche esigenze funzionali e delle conseguenti prestazioni e modalità operative che devono essere assicurate, nell'ambito dei sistemi informativi trasversali del Ministero e dei sistemi informativi specifici per lo svolgimento dei compiti istituzionali del Dipartimento, in materia di acquisti, logistica, personale ed altri servizi dipartimentali; pagamento delle retribuzioni per il personale delle amministrazioni dello Stato (per maggiori informazioni consultare il link: http://www.dag.mef.gov.it/noi_siamo/organigramma/index_DSII.html).

Il sistema informatico a supporto delle attività del Dipartimento si avvale di una infrastruttura composta da:

- circa 230 server fisici
- circa 1000 server virtuali
- circa 450 apparati

2 OGGETTO DEL SERVIZIO RICHIESTO

L'esigenza è costituita dall'acquisizione di servizi professionali di alto profilo, necessari per la progettazione e realizzazione di un Sistema per la Verifica della Sicurezza dell'Informazione e per la successiva assistenza tecnica all'Amministrazione durante le prime attività di verifica.

Più compiutamente, tali servizi professionali verranno impiegati per:

- definire un modello per la gestione integrata della sicurezza dell'informazione, anche in ambito Governance IT;
- sviluppare un modello di rischio per gli aspetti di cyber security (policy di sicurezza e gestione degli incidenti informatici) e la sicurezza dell'informazione in generale;
- definire un processo tramite il quale verificare in maniera rapida ed efficace i livelli di sicurezza raggiunti nella protezione dell'informazione; tale processo di verifica dovrà portare alla definizione della metodologia per svolgere una verifica della sicurezza dell'informazione nell'ambito della gestione dell'infrastruttura IT;
- individuare i livelli ottimali di protezione dell'informazione, nel senso del migliore bilanciamento tra il rischio di non rispetto dei livelli di protezione obiettivo e gli obiettivi di razionalizzazione della spesa
- definire in modo ottimale i requisiti di gestione della sicurezza dell'informazione nell'ambito di contratti di servizio;

- monitorare in tempo reale il rischio di non mantenimento dei livello obiettivo di sicurezza dell'informazione;
- predisporre la documentazione necessaria al funzionamento del Sistema (es. linee guida, procedure, manuali) e all'efficace operatività dell'Amministrazione;
- progettare la soluzione informatica in attuazione dei modelli disegnati, allo scopo di velocizzare e semplificare il processo di verifica e controllo. La componente informatica sarà basata su prodotti di mercato la cui individuazione avverrà attraverso tecniche di software selection, in ottemperanza a quanto previsto dalla Circolare AGID n. 63 del 2013;
- supportare il personale dell'Amministrazione durante le prime verifiche di Audit per trasferire le conoscenze del Sistema.

Il Sistema dovrà essere integrabile con la metodologia che l'Amministrazione ha già adottato per l'attività di Audit in ambito applicativo.

Tutte le attività richieste dovranno essere eseguite in considerazione degli standard di settore accettati a livello Internazionale.

3 ENTITÀ DELL'IMPEGNO

L'impegno è complessivamente stimato in 220 giornate lavorative così suddivise per figura professionale:

FIGURA PROFESSIONALE	GIORNI / PERSONA STIMATI
Information Security Auditor	100
Governance of Enterprise IT Expert	70
Information Security Expert	50

La durata del servizio è di 12 mesi salvo esaurimento anticipato del massimale di contratto.

Si precisa che le quantità sopra riportate sono indicative e non vincolanti e che nell'ambito dello svolgimento delle attività e nel limite del corrispettivo, si potranno verificare variazioni del mix di figure professionali richiesto. In tal caso L'Amministrazione e l'aggiudicatario provvederanno a concordare e a formalizzare nel Piano di lavoro, secondo le esigenze espresse dalla stessa L'Amministrazione, il mix delle figure professionali da utilizzare.

Il corrispettivo complessivo massimo non potrà comunque essere superiore al prezzo totale complessivo offerto dall'Aggiudicatario calcolato sulla base delle tariffe unitarie offerte.

La distribuzione dell'impegno potrebbe non essere lineare nei 12 mesi della durata contrattuale, pertanto potranno essere previsti periodi a intensità lavorativa variabile in cui l'Aggiudicatario dovrà assicurare il pieno supporto a L'Amministrazione.

L'Aggiudicatario si impegna a garantire il supporto richiesto dalla L'Amministrazione secondo le modalità e nei termini definiti tra le Parti.

4 MODALITÀ DI EROGAZIONE DEL SERVIZIO

4.1 GENERALITÀ

L'erogazione dei servizi professionali potrà essere richiesta dall'Amministrazione nell'arco dei 12 mesi successivi alla data di stipula del contratto, anche non in un'unica soluzione e finalizzati alla realizzazione di singole attività tra quelle oggetto della fornitura.

Ad ogni richiesta dell'Amministrazione, il fornitore dovrà produrre entro 5 giorni lavorativi una pianificazione di dettaglio con tempi, giorni/persona e deliverable prodotti, da sottoporre all'approvazione dell'Amministrazione (Piano di lavoro). La data di approvazione del Piano dei lavori costituirà l'inizio delle attività.

Nel corso dell'affidamento deve essere assicurato al personale dell'Amministrazione il trasferimento costante delle conoscenze e del know-how sulle attività condotte dal Fornitore. L'affiancamento al personale dell'Amministrazione dovrà essere organizzato secondo modalità da concordare e potrà prevedere sessioni riassuntive, di lavoro congiunto, presentazioni, etc. senza comportare un costo aggiuntivo per il Committente.

Tutta la documentazione prodotta durante lo svolgimento delle attività dovrà essere redatta in conformità agli standard documentali forniti dall'Amministrazione. A corredo delle attività svolte dovrà essere prodotta almeno la seguente documentazione:

- Documento di analisi del framework di Governance IT da adottare nella sicurezza delle informazioni;
- Documento di analisi del modello di Sistema di Gestione per la Sicurezza delle Informazioni;
- Sviluppo del modello di analisi e gestione del rischio IT;
- Manuale di sviluppo del processo di verifica della sicurezza dell'informazione;
- Documentazione a supporto delle attività di verifica;
- I report di dettaglio delle evidenze individuate;
- L'executive summary.

L'executive summary, in particolare, dovrà illustrare brevemente, con un linguaggio non tecnico, le metodologie impiegate per l'esecuzione delle attività e i risultati conseguiti, al fine di fornire al Management di riferimento le informazioni necessarie al processo decisionale.

Il personale del Fornitore che sarà coinvolto nello svolgimento della attività dovrà essere munito di un proprio personal computer con il software correttamente licenziato e aggiornato, anche per quanto riguarda le componenti per la sicurezza informatica (es. antivirus).

4.2 RESPONSABILE DEL SERVIZIO

La Società aggiudicataria dovrà comunicare a Consip, trasmettendolo con la documentazione per la stipula , il nominativo e i riferimenti del proprio Responsabile del servizio, che sarà l'interlocutore unico dell'Amministrazione per gli aspetti amministrativi.

Sarà cura del responsabile verificare il rispetto di tutti gli adempimenti contrattuali.

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 il responsabile dell'Amministrazione e quello della Società aggiudicataria.

4.3 LUOGO DI SVOLGIMENTO

Il servizio potrà essere espletato presso la sede dell'Aggiudicatario ovvero presso la sede Amministrazione in Roma, su richiesta dell'Amministrazione stessa.

Gli eventuali costi di trasferimento e soggiorno sono a carico dell'Aggiudicatario e devono intendersi compresi nel Prezzo offerto.

4.4 MODALITÀ DI CONSEGNA

Tutta la documentazione dovrà essere prodotta nel formato richiesto, anche elettronico. Tutti i prodotti consegnati su CD/DVD o in via telematica dovranno essere esenti da virus o malfunzionamenti.

La consegna telematica dovrà avvenire tramite posta elettronica, agli indirizzi che saranno indicati dall'Amministrazione. Nel caso in cui la documentazione sia richiesta su CD/DVD, questi ultimi dovranno essere accompagnati dalla lettera di consegna.

4.5 VERIFICA DI CONFORMITÀ

La verifica di conformità verrà effettuata ai sensi dell'art. 314 del DPR 207/2010 al completamento di ciascuna attività svolta.

A completamento della verifica positiva sarà prodotto il "Verbale di conformità" che dovrà essere sottoscritto dal Responsabile del servizio e dal Responsabile dell'Amministrazione.

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.

4.6 CONSUNTIVAZIONE DELLE ATTIVITÀ SVOLTE E FATTURAZIONE

La consuntivazione avverrà al momento della chiusura del verbale di verifica della/e fornitura/e, scaturite dalle singole richieste del Committente/Amministrazione che si susseguiranno durante tutta la validità del contratto, sulla base del corrispondente numero di giorni/persona riportati nel Piano di lavoro approvato. La data del verbale di verifica positivo verrà considerata quale "Data di Accettazione" da parte del Committente e tale documento dovrà essere allegato alle fatture.

Per la fatturazione si applica quanto previsto dal Contratto all'art. 19 comma 1bis: "Ai fini del pagamento del corrispettivo indicato nell'ordine di acquisto, per l'erogazione di servizi a consumo il Fornitore potrà emettere fattura successivamente alla approvazione da parte dell'Amministrazione 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".

5 REQUISITI PROFESSIONALI RICHIESTI

La Società aggiudicataria dovrà garantire l'impegno per tutto il periodo contrattuale delle seguenti figure professionali:

- Information Security Auditor;
- Governance of Enterprise IT Expert;
- Information Security Expert.

Per le prestazioni richieste il Fornitore si obbliga ad avvalersi di personale specializzato con contratto di lavoro subordinato ovvero con rapporto di lavoro comunque riconducibile a una delle tipologie contrattuali ammesse dalla Legge n. 183/2014 e successivi Decreti attuativi, nonché di lavoratori autonomi (nel rispetto di quanto previsto all'art. 105, comma 3, del d. lgs. n. 50/2016).

La Società fornirà all'Amministrazione entro 10 giorni dalla stipula del contratto, i curricula delle risorse che intende impiegare, firmati e sottoscritti dalle stesse come previsto dal D.Lgs. 30 giugno 2003 n. 196.

L'Amministrazione si riserva la facoltà di verificare i curricula dei singoli Professionisti successivamente alla stipula del contratto attraverso un colloquio e prove pratiche, per esaminare sia i livelli di conoscenza sia la generale idoneità allo svolgimento delle attività richieste e, nel caso si ritengano non adeguati ai profili professionali indicati, l'Amministrazione potrà chiederne la sostituzione.

L'Aggiudicatario, si impegna a sostituire il Professionista, entro 5 giorni dalla richiesta di sostituzione avanzata dall'Amministrazione, con altro Professionista avente i medesimi requisiti offerti.

Il Professionista assegnato dalla Società non può essere sostituito dalla Società durante l'esecuzione dell'incarico; qualora intervenissero eventi non dipendenti dalla Società (per esempio dimissioni o indisponibilità) che costringessero alla sostituzione del Professionista, la Società dovrà proporre un nuovo Professionista – che abbia i medesimi requisiti minimi del Professionista sostituito – da sottoporre alla approvazione dall'Amministrazione e dovrà farsi carico del periodo di affiancamento/istruzione necessario per rendere il nuovo Professionista autonomo e produttivo.

Qualora il nuovo Professionista risultasse inadeguato allo svolgimento dell'incarico e si dovesse ricorrere a un'ulteriore sostituzione, saranno applicate le penali previste dallo schema di contratto.

<u>Vincoli temporali relativi all'inserimento e sostituzione delle risorse professionali</u>

ADEMPIMENTO	EVENTO	LIMITE	NOTE

		TEMPORALE	
Consegna nuovo CV in caso di non accettazione o di richiesta sostituzione risorsa da parte dell'Amministrazione	Comunicazione di non accettazione/ richiesta di sostituzione	3 giorni solari	
Consegna nuovo CV in caso di sostituzione risorsa richiesta dall'Aggiudicatario	Effettiva sostituzione	almeno 3 giorni solari	Il CV deve essere allegato alla comunicazione di richiesta sostituzione
Disponibilità della risorsa per un colloquio	Richiesta da parte dell'Amministrazione	3 giorni solari	Colloquio presso la sede dell'Amministrazione
Inserimento della risorsa dalla data di accettazione del CV	Accettazione della risorsa da parte dell'Amministrazione	1 giorno lavorativo	

5.1 REQUISITI MINIMI DEI PROFESSIONISTI

Di seguito si riportano i requisiti minimi necessari, a pena di non accettazione, dei profili professionali richiesti per lo svolgimento del servizio.

INFORMATION SECURITY AUDITOR

Laureato con almeno 7 anni di esperienza su verifiche di sicurezza informatica, analisi del rischio IT, sistemi di controllo interno e valutazioni di conformità, deve possedere almeno le seguenti caratteristiche:

- Laurea magistrale/specialistica;
- esperienza in analisi del rischio informatico;
- esperienza di audit interni (di prima parte) su tematiche di sicurezza IT;
- conoscenza di ISO/IEC 20000, ITIL e CMMI;
- conoscenza di ISO/IEC 27005;
- conoscenza della norma UNI EN ISO 19011:2012;
- conoscenza del framework Cobit5;
- conoscenza di standard internazionali per la pratica professionale dell'internal auditing (IIA);
- possesso di certificazione ISO 27001 Lead Auditor;
- possesso di certificazione CISA.

GOVERNANCE OF ENTERPRISE IT EXPERT

Laureato con almeno 10 anni di esperienza nei processi di organizzazioni IT, nella progettazione e realizzazione di sistemi di gestione e governo dell'IT. Ha maturato esperienza in modelli per l'ottimizzazione del rischio aziendale e definizione degli accordi contrattuali con terze parti. deve possedere almeno le seguenti caratteristiche:

- Laurea magistrale/specialistica;
- conoscenza della norma ISO 31000:2009;
- conoscenza della normativa Italiana e Comunitaria in materia di Privacy;
- conoscenza della norma ISO/IEC 38500:2015;
- conoscenza di ISO 20000, ITIL e CMMI;
- possesso di certificazione Cobit5 Foundation o CGEIT.

INFORMATION SECURITY EXPERT

Laureato con almeno 7 anni di esperienza nell'ambito della gestione della sicurezza dell'informazione che include anche l'analisi forense ed attività di APT (Advanced Penetration Testing) e VA (Vulnerability Assessment); deve possedere almeno le seguenti caratteristiche:

- Laurea magistrale/specialistica in discipline tecniche;
- conoscenza delle norme ISO/IEC 27000;
- conoscenza delle policy di sicurezza del SANS Institute;
- conoscenza del Framework Nazionale per la Cyber Security;
- conoscenza del Framework OWASP;
- possesso di certificazione CISSP (Certified Information Systems Security Professional) o CISM o equivalenti.

6 PENALI

In aggiunta alle penali previste nel contratto all'art. 15, l'Amministrazione applicherà le seguenti penali.

L'Amministrazione applicherà una penale pari all'1 (uno) per mille dell'importo totale del contratto per ogni giorno lavorativo di ritardo nella consegna prevista del Piano di Lavoro, da consegnare entro 5 (cinque) giorni lavorativi dalla richiesta di avvio dei lavori.

L'Amministrazione applicherà una penale pari all'1 (uno) per mille dell'importo totale del contratto per ogni giorno lavorativo di ritardo nella consegna dei deliverable delle attività rispetto ai tempi previsti nel Piano di lavoro approvato.

L'Amministrazione applicherà una penale pari all'1 (uno) per mille dell'importo complessivo contrattuale per ogni giorno lavorativo di ritardo maturato rispetto ai vincoli temporali relativi all'inserimento e sostituzione delle risorse professionali di cui al paragrafo 5.