REGIONE AUTONOMA DELLA SARDEGNA

ENTE FORESTE DELLA SARDEGNA

Direzione Generale
Servizio IT

Allegato A

CAPITOLATO TECNICO

PROCEDURA APERTA PER L'AFFIDAMENTO DI SERVIZI PROFESSIONALI PER L'ANALISI E LA REDAZIONE DI DOCUMENTAZIONE INERENTE LA GESTIONE DELLA SICUREZZA INFORMATICA. DETERMINA A CONTRARRE N. 212 DEL 23.11.2011 CIG. 3600409F7B.

1 Premessa 3
2 Obiettivi e oggetto della gara 4
3 Importo a base d'asta 4
4 Esecuzione contrattuale, penali 4
5 Servizi specifici richiesti 4
5.1 Risk Management 5
5.2 Penetration Test & Vulnerability Assessment 7
5.3 DPS – Documento Programmatico per la Sicurezza 8
6 Modalità di effettuazione della prestazione 9
6.1 Direzione lavori e collaudo 9
6.2 Sede e luogo di lavoro 10

1 Premessa

L' Ente Foreste Della Regione Sardegna, di seguito EFDS, è un Ente strumentale della Regione Sardegna la cui missione è lo sviluppo e la valorizzazione del patrimonio forestale e faunistico del territorio regionale, nonché la creazione e diffusione di una cultura che contempli valori naturalistici, storici e culturali propri della Sardegna.

La struttura dell'Ente è organizzata come di seguito descritto:

Una **Direzione Generale** con sede a Cagliari articolata nei seguenti servizi centrali:

- Servizio programmazione, contabilità bilancio e appalti
- Servizio tecnico
- Servizio del personale
- Servizio affari generali e legali
- Servizio antincendi, protezione civile e delle infrastrutture
- Servizio innovazione tecnologica

N. 6 **Servizi territoriali provinciali** dislocati nei seguenti comuni

- Decimomannu
- Sassari
- Oristano
- Nuoro
- Lanusei
- Tempio Pausania

Ad ogni servizio Territoriale fanno capo i **Complessi Forestali**, che risultano essere una unità intermedia di gestione, diffusa su diversi comuni della regione. Le sedi dei suddetti complessi risultano essere dei fabbricati, tipicamente di piccola entità su cui si estende l'infrastruttura di rete dell'Ente.

Maggiori informazioni sulla struttura dell'Ente sono reperibili nel sito istituzionale dell'Ente:

http://www.sardegnaforeste.it

Il coordinamento informatico dell'Amministrazione è svolto per il tramite della Servizio per l'innovazione Tecnologica presso la Direzione generale.

2 Obiettivi e oggetto della gara

Obiettivo della gara, di cui il presente documento costituisce il Capitolato Tecnico, è consentire all'Amministrazione l'acquisizione di servizi professionali riguardanti la sicurezza informatica dell'Ente.

A tal fine l'impresa selezionata dovrà:

- Analizzare lo stato attuale della sicurezza dei sistemi informativi dell'Ente Foreste Della Sardegna.
- Identificare soluzioni e procedure in grado di migliorare la sicurezza dei Sistemi Informativi dell'Ente Foreste Della Sardegna con particolare riferimento agli obblighi di legge derivanti dal **D.L. n. 196 del 2003**
- Redigere e fornire la documentazione che descriverà il livello di sicurezza attualmente raggiunto dai sistemi dell'Ente
- Redigere e fornire la documentazione che fornirà all'ente le indicazioni delle azioni da intraprendere (con relative tempistiche e costi) per di migliorare la sicurezza dei Sistemi Informativi dell'EFDS
- Redigere e fornire la documentazione necessaria per l'adeguamento agli obblighi di legge in materia di trattamento e sicurezza dei dati.

I servizi specifici e la relativa documentazione richiesta sono meglio dettagliati nel successivo art. 4 L'Ente si impegna ad osservare gli obblighi di cui al D.Lgs. 30 giugno 2003 n. 196 e di cui al presente Capitolato nonché alle disposizioni dell'Autorità Garante in materia di protezione dei dati personali.

3 Importo a base d'asta

L'importo a base d'asta ammonta a € 49.000 oltre Iva di legge.

4 Esecuzione contrattuale, penali

Come indicato nell'art. 16 del disciplinare di gara Le prestazioni contrattuali dovranno essere eseguite entro 180 giorni naturali consecutivi dalla stipula del contratto. Il contratto si intende eseguito con

l'esecuzione dei servizi, la consegna della documentazione a corredo e degli eventuali tool software offerti.
Per i ritardi agli adempimenti contrattuali verranno applicate le penali di cui all'art. 22 del disciplinare. In particolare:
L'impresa, è soggetta a penalità quando effettua in ritardo la consegna della fornitura: 0,1% dell'importo contrattuale per ogni giorno di ritardo riferito ai tempi contrattuali;

Si ribadisce che, In caso di collaudo negativo, all'appaltatore verranno imputati, oltre agli oneri relativi ad un totale controllo e rettifica degli elaborati difettosi, anche le panali di ritardata consegnai ritardi del periodo compreso fra la data del rifiuto e quella di riconsegna degli elaborati corretti.

Qualora a seguito dell'applicazione delle suddette penali la percentuale delle stesse dovesse superare il 10% il RUP proporrà alla stazione appaltante la risoluzione del contratto per grave inadempimento. Fatto salvo il risarcimento del maggior danno.

.

5 Servizi specifici richiesti

La gara, con il presente Capitolato, deve selezionare un impresa in grado di erogare i seguenti servizi professionali:

5.1 Risk Management

Si intende l'attività finalizzata a identificare, controllare, eliminare o minimizzare i rischi reali cui è soggetto il Sistema Informativo dell'Ente.

Tale processo include l'analisi dell'infrastruttura tecnologica, organizzativa e procedurale dell'Ente mirata alla definizione di un piano per la gestione delle risorse (fisiche, logiche ed organizzative) che consente di assicurare il contenimento dei rischi entro limiti accettabili.

Devono essere previste le seguenti attività fondamentali:

L'analisi del rischio, dove è importante classificare le informazioni, individuare le minacce, identificare il livello di rischio associato alle classi di informazione individuate.

Il controllo del rischio, dove s'identificano le modalità (es. trasferimento dei rischi a terzi, riduzione del valore dell'informazione, riduzione delle vulnerabilità, ecc..) con cui l'amministrazione decide di gestire i rischi associati.

In particolare si specifica che:

1) La norma ISO 27001 - *Specifiche per il sistema di gestione della sicurezza delle informazioni (ISMS)* costituisce riferimento concettuale per l'attività di gestione del rischio; pertanto la scelta della metodologia (quantitativa/qualitativa), la produzione documentale e l'eventuale tool per la suddetta attività deve essere coerente con la suddetta norma.

2) L'analisi dei rischi dovrà essere utile, praticabile, affidabile nei risultati e rappresentativa della realtà e pertanto la metodologia che verrà utilizzata per tale analisi dovrà possedere le seguenti caratteristiche principali:

   a. **Ripetibilità e riproducibilità:** possibilità di ripetere nel tempo l'analisi dei rischi ottenendo gli stessi risultati a parità di ogni condizione, da parte di qualunque operatore.

   b. **Comprensibilità:** i criteri adottati nell'espressione dei parametri che compongono il rischio (probabilità di accadimento, valore delle informazioni, ecc…) devono essere trasparenti e comprensibili. Questo anche al fine di consentire il riutilizzo dei risultati in operazioni seguenti. Analogamente comprensibili devono essere i risultati prodotti.

   c. **Condivisione:** i valori attribuiti alle informazioni devono essere condivisi tra le funzioni aziendali interessate.

   d. **Coerenza:** i valori attribuiti alle informazioni devono essere coerenti con quanto stabilito dalle politiche di sicurezza di alto livello, essendo in genere la definizione delle politiche di alto livello a monte dell'operazione di analisi dei rischi.

   e. **Attinenza al dominio:** la definizione del dominio di applicazione del sistema di gestione della sicurezza delle informazioni deve essere coerente con il dominio definito per l'analisi dei rischi.

   f. **Riutilizzabilità:** i risultati intermedi o finali dell'attività di analisi dei rischi devono poter essere riutilizzabili in caso di variazioni delle condizioni (valori delle informazioni, minacce, vulnerabilità, ecc…). Questo per permettere economie in tutti i casi in cui l'analisi dei rischi vada ripetuta in quanto le condizioni sono variate. Inoltre, implicito nel concetto di sistema di gestione c'è il concetto di miglioramento, e la misura del miglioramento passa anche per la revisione dell'analisi dei rischi.

g. **Adeguatezza al livello di consapevolezza in azienda:** la complessità di una metodologia per l'analisi dei rischi deve essere adeguata al livello di consapevolezza esistente in azienda sui temi relativi alla sicurezza delle informazioni. Ciò per evitare gli insuccessi derivanti dall'introduzione di sistemi di gestione e processi non recepiti e lasciati allo stato di elementi avulsi dalla cultura aziendale, attuati solo perché la norma lo richiede.

h. **Modularità realizzativa:** i risultati del processo di analisi dei rischi devono essere disponibili in tempi utili, commisurati con il livello della minaccia e con il piano temporale predisposto per la realizzazione dell'intero sistema di gestione della sicurezza.

i. **Fattibilità in termini economici:** il budget allocato per l'implementazione del sistema di gestione della sicurezza contempla una porzione allocata per l'analisi dei rischi, che è uno dei processi coinvolti. La complessità e il livello di dettaglio dell'analisi dei rischi devono essere commisurati con la previsione di spesa.

j. **Sintesi nei risultati:** i risultati prodotti dal processo di analisi dei rischi devono essere sintetici e facilmente accessibili nel mettere in relazione le informazioni (o le classi di informazioni) e le risorse con il livello di rischio associabile ad esse.

Si specifica che questo servizio dovrà essere relativo alla sede della Direzione Generale e in almeno uno dei Servizi Territoriali che verrà scelto dalla direzione di esecuzione del contratto.

5.2 Penetration Test & Vulnerability Assessment

Dovranno essere utilizzate di Tecniche di penetration test (PT) e vulnerability assessment (VA) per verificare, dall'esterno o dall'interno del perimetro aziendale, le vulnerabilità a cui i sistemi sono esposti.

L'attività di Vulnerability Assessment dovrà identificare le vulnerabilità informatiche presenti nei sistemi informativi/informatici e redigere piani di rientro e di mitigazione del rischio.

L'attività di Penetration Test dovrà simulare e/o effettuare attacchi informatici mirati ai sistemi, al fine di produrre dettagliato report su ciò che è stato identificato e sviluppare piani di rientro con metodologie di mercato e tempistiche di massima;

Gli ambiti di analisi specifici delle attività sopra citate dovranno essere i seguenti:

- **Network**
- **Server/host**

- **Applicazioni**.

In particolare si specifica che:

1) Il servizio Vulnerability Assessment (nel seguito VA) dovrà essere erogato tramite l'impiego di strumenti aggiornati con le informazioni relative a vulnerabilità e minacce più recenti e le relative attività devono essere effettuate dall'impresa secondo le best practice di settore più diffuse e mature.
2) Il servizio di Penetration Test (nel seguito PT) dovrà essere erogato tramite l'impiego di strumenti che consentano di ricostruire le attività effettuate nel corso delle simulazioni d'attacco; le relative attività devono essere effettuate dall'impresa secondo le best practice di settore più diffuse e mature.
3) L'impresa dovrà fornire la registrazione completa di tutte le attività riguardanti i PT.
4) Le attività di PT dovranno essere in grado di simulare attacchi interni, attacchi dalla intranet e attacchi da Internet.
5) I servizi di Vulnerability Assessment e Penetration Test devono essere erogati con la garanzia di mantenere la continuità operativa dei sistemi, servizi e infrastrutture oggetto di test. I test che potrebbero comportare disservizio o danneggiamento devono essere preventivamente autorizzati.
6) Il personale del'Ente deve poter partecipare, come osservatore, a tutte le attività di VA & PT mentre sia le informazioni del sistema di VA che quelle acquisite nel corso dei PT devono essere accessibili solo in lettura.
7) L'Impresa dovrà dare la disponibilità ad effettuare le attività di VA e PT in orari compatibili con le esigenze dell'Ente.
8) I servizi di cui al presente paragrafo riguarderanno un numero di apparati orientativamente non maggiore di 150.

5.3 DPS – Documento Programmatico per la Sicurezza

Dovrà essere redatto il **Documento programmatico della Sicurezza (nel seguito: DPS) previsto dal codice in materia di protezione dei dati personali (D.L. n. 196 del 2003)**, attraverso l'effettuazione delle seguenti fasi:

1. Analisi dello scenario, con indicazione delle varie tipologie di dato trattato dell'Ente Foreste Della Sardegna in riferimento alle necessità di riservatezza, derivante da dettato normativo, oltre che la verifica della adeguatezza dei sistemi attualmente in uso;
2. Descrizione delle metodologie, sistemi, dotazioni e procedure eventualmente necessarie ad integrare i sistemi in uso per poter pienamente rispondere al disposto delle normative di settore. Detta attività dovrà produrre una analisi dei tempi e dei costi di implementazione.

Entrambe le fasi dovranno essere descritte in apposita documentazione.

6 Modalità di effettuazione della prestazione

1) Tutte le attività devono essere accompagnate da un progetto con relativo diagramma di GANTT particolareggiato e devono essere previste almeno le seguenti fasi:
   a. Riunione di apertura di presentazione dell'attività con relativa formazione dei referenti dell'Ente
   b. Produzione del GANTT contenente le attività pianificate
   c. Inizio dell'attività
   d. Presentazione dei risultati
2) Tutti i servizi dovranno essere svolti con assoluta regolarità e puntualità e l'impresa risponderà direttamente di tutte le inadempienze e/o disservizi, incluso l'operato del proprio personale e di qualsiasi responsabilità ed onere verso terzi in dipendenza del servizio stesso, lasciando indenne e sollevato da ogni incombenza l'EFDS.
3) Tutto il materiale e tutto quanto occorra per l'espletamento del servizio sarà approntato a cura e spese dell'aggiudicatario.

6.1 Direzione lavori e collaudo

L'Ente Foreste Della Sardegna provvederà alla nomina del Direttore dell'Esecuzione del contratto (art. 299 e seg. del DPR 207/2011), il quale avrà i compiti di coordinamento logistico ed operativo, necessario a garantire l'esatto svolgimento dei servizi richiesti.

Durante lo svolgimento dell'appalto, il personale dell'Ente, se appositamente autorizzato, potrà svolgere l'attività di affiancamento agli operatori della ditta appaltatrice (di seguito denominata D.A.) al fine di ricevere una formazione "on the job". L'Amministrazione si riserva, con ampia e insindacabile facoltà e senza che la D.A. nulla possa eccepire, di effettuare verifiche e controlli circa la perfetta osservanza da parte della D.A. stessa di tutte le disposizioni contenute nel presente capitolato ed in modo specifico, controlli di rispondenza e di qualità.

Qualora il controllo qualitativo e quantitativo dovesse risultare non conforme al capitolato, la D.A. dovrà provvedere ad eliminare le disfunzioni rilevate. I controlli e le verifiche del personale effettuati dall'Ente Foreste non liberano la D.A. dagli obblighi e responsabilità inerenti il contratto.

Entro 6 mesi dalla consegna definitiva di tutti gli elaborati dovrà essere redatto il verbale di collaudo o Certificato di regolare Fornitura.

E' facoltà della D.A. d'intesa con l'eventuale collaudatore, suggerire, motivandola, una eventuale prassi operativa atta a rimuovere eventuali inconvenienti riscontrati.

In caso di collaudo negativo, alla D.A. verranno imputati, oltre agli oneri relativi ad un totale controllo e rettifica degli elaborati difettosi, anche i ritardi del periodo compreso fra la data del rifiuto e quella di riconsegna degli elaborati stessi, e le conseguenti penali.

6.2 Sede e luogo di lavoro

Le prestazioni oggetto dell'appalto dovranno essere svolte prevalentemente presso la sede della Ditta aggiudicataria fatte salve quelle che presuppongono interazioni con il personale dell'Amministrazione, che verranno effettuate nelle sedi che l'Amministrazione stessa indicherà con apposita comunicazione.

IL Direttore del Servizio

Giuliano Patteri

Il Responsabile del Procedimento
Ing. Giuliano Patteri