COMUNE DI CASTELSARDO

Provincia di Sassari

AREA TECNICA ED AMBIENTALE

Via V. Emanuele n. 2 - 07031 - Castelsardo - tel. 079/478400 fax 079/4780900 PEC: protocollo@pec.comune.castelsardo.ss.it
Area Tecnica - Via P. Sassu n. 3 – e-mail: ut@comune.castelsardo.ss.it

MANIFESTAZIONE DI INTERESSE E RICERCA DI MERCATO

per l'affidamento del SERVIZIO DI AMMINISTRATORE DI SISTEMA con SUPPORTO E ASSISTENZA TECNICO INFORMATICA – CIG Z52343C08A

SI RENDE NOTO

Che questa amministrazione intende eseguire un'indagine di mercato, finalizzata all'individuazione di operatori economici interessati a partecipare a successiva procedura di richiesta di offerta, per l'affidamento del servizio di amministratore di sistema e supporto e assistenza tecnica al sistema informatico dell'Ente, da effettuarsi ai sensi dell'art. 1 commi 1 e 2 lett. a) della Legge n. 120 del 11 settembre 2020.

La procedura sarà effettuata sul portale di e-procurement della centrale di committenza regionale, Sardegna CAT.

1. OGGETTO DEL SERVIZIO

L'affidamento riguarda l'incarico di amministratore di sistema per la gestione e la manutenzione del sistema informatico dell'Ente, nonché il servizio di supporto e assistenza tecnica sull'intera rete (circa 50 postazioni di lavoro dislocate su tre diverse sedi).

Le prestazioni richieste sono le seguenti:

- Affiancamento dell'Ente nella definizione delle politiche informatiche;
- Analisi funzionale del sistema informatico dell'Ente volta ad identificare eventuali deficit tecnici e organizzativi dell'apparato, con indicazione di eventuali soluzioni correttive da intraprendere (quantificazione e qualificazione dei fabbisogni del parco macchine, di funzionalità dei programmi, ecc….);
- Programmazione, installazione e monitoraggio dei firewall;
- Predisposizione di capitolati tecnici d'appalto per l'acquisizione di strumentazione hardware e prodotti software necessari per l'implementazione e l'adeguamento del sistema informatico comunale;
- Interfaccia tecnica tra l'Ente e i fornitori di hardware e software per l'individuazione delle migliori soluzioni tecniche, secondo il principio di efficacia ed economicità della spesa;
- Adeguamento alle misure minime di sicurezza, in conformità alla normativa in materia di privacy;
- Gestione dei servizi erogati in Intranet, inclusa la gestione delle cartelle di rete condivise e personali e la gestione delle basi dati degli applicativi;

- Analisi funzionale dei sistemi informatici operativi sulla rete interna dell'Ente, atta ad identificare e sanare eventuali criticità tecniche ed organizzative;

- Verifica dell'idoneità dei sistemi informatici predisposti per ospitare i dati e le applicazioni critiche dell'Ente ed indicazione di eventuali soluzioni correttive da intraprendere;
- Verifica dell'idoneità degli ambienti individuati per ospitare le apparecchiature informatiche critiche dell'Ente ed indicazione di eventuali soluzioni correttive da intraprendere;
- Esecuzione periodica di test di funzionamento dei dispositivi di continuità dell'alimentazione elettrica collegati alle apparecchiature informatiche dell'Ente e segnalazione di eventuali avarie riscontate;
- Supporto informatico agli incaricati del trattamento dei dati circa il corretto uso della propria postazione di lavoro, di internet, della posta elettronica e degli altri strumenti elettronici utilizzati per fini lavorativi nel rispetto di quanto previsto dalla normativa vigente;
- Supporto e consulenza alle varie Aree dell'Ente per la soluzione dei problemi pratici di funzionamento della dotazione informatica;
- Supporto nell'installazione e configurazione dei software specifici per la pubblica amministrazione e dei dispositivi di firma digitale;
- Installazione o ripristino di sistemi operativi, software antivirus, pacchetti applicativi purché gli stessi siano corredati dei relativi supporti di installazione originali e dotati di regolare licenza di utilizzo;
- Configurazione apparati di stampa e scansione sulla rete locale e sulle singole postazioni di lavoro;
- Individuazione e proposta adozione soluzioni software open source di comprovata stabilità di funzionamento per la produttività personale;
- Assistenza diretta, telefonica e teleassistenza dal lunedì al venerdì e nei giorni di apertura degli uffici comunali;
- Gestione dei sistemi di autenticazione informatica con riferimento al personale costituente la dotazione organica dell'Ente, ai lavoratori a tempo determinato, ai collaboratori, agli amministratori, agli addetti alla manutenzione hardware e software con obbligo di sostituzione autonoma della componente riservata della credenziale di autenticazione con periodicità semestrale in caso di trattamento di dati personali e trimestrali nell'ipotesi di trattamento di dati sensibili e giudiziari;
- Attribuzione di credenziali di autenticazione strutturate per mantenere caratteristiche di robustezza, inviolabilità nel rispetto della segretezza della componente riservata della credenziale di autenticazione ai sensi delle vigenti normative con correlata attività di costante informazione rivolta a lavoratori ed amministratori, in ordine alle metodiche di gestione delle stesse credenziali al fine di garantire la salvaguardia dei requisiti di disponibilità, integrità e riservatezza dei dati;
- Gestione dei profili di autorizzazione dei Responsabili e degli Incaricati interni del trattamento dei dati, in conformità all'organizzazione degli uffici e dei servizi e delle funzioni attribuite;
- Segnalazioni ai Responsabili del Trattamento dei dati di eventuali violazioni delle policy di uso delle credenziali di autenticazione e delle politiche di sicurezza;
- Assistenza ai Responsabili del trattamento dei dati dell'Amministrazione per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'Incaricato;
- Verifica almeno semestrale circa la sussistenza dei requisiti di accesso al sistema informatico e di conservazione dei profili assegnati a ciascun dipendente incaricato del trattamento dei dati, congiuntamente ai Responsabili del trattamento dei dati, dalla quale scaturirà una lista degli Incaricati individuati per classi omogenee di incarico e relativi profili di autorizzazione;
- Definizione e messa a regime delle procedure per l'adozione di sistemi di protezione contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quiquies del codice penale mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale;
- Definizione e messa a regime delle procedure di adozione di aggiornamenti periodici di programmi per elaboratore volti a prevenirne le vulnerabilità ed a correggerne i difetti con cadenza almeno annuale per il trattamento di dati personali e semestrale in caso di trattamento di dati sensibili e giudiziari;
- Definizione e messa a regime delle procedure per l'esecuzione di copie di sicurezza, effettuate con cadenza almeno settimanale, che garantiscano l'Ente contro il rischio di perdita di dati e consentano, in caso di evento dannoso, l'avvio del Piano di Continuità Operativa;
- Definizione e messa a regime delle procedure contro l'accesso abusivo a dati sensibili e giudiziari di cui all'art. 615-ter del codice penale mediante l'utilizzo di idonei sistemi elettronici;

- Definizione e messa a regime delle procedure per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti;
- Definizione e messa a regime delle procedure preordinate a garantire che i supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati siano distrutti o resi inutilizzabili, ovvero possano essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non siano intelligibili e tecnicamente in alcun modo ricostruibili;
- Definizione e messa a regime delle politiche informatiche secondo le tempistiche e le modalità segnalate nelle "Linee guida per il disaster recovery delle PA", emanate da DigitPA, ovvero secondo le specifiche indicazioni presenti nel Piano di Continuità Operativa e Disaster Recovery dell'Ente;
- Messa a regime delle procedure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati, con la strumentazione tecnica in dotazione e con quanto dichiarato nel Piano di Continuità Operativa e di Disaster Recovery;
- Predisposizione di soluzioni atte alla registrazione dei file di log relativi all'autenticazione informatica dell'Amministratore di Sistema sui sistemi informatici dell'Ente, per un tempo non inferiore ai sei mesi, su supporti non riscrivibili. Tali soluzioni di registrazioni avranno caratteristiche di completezza, inalterabilità e possibilità di verifica dell'integrità dei dati per il raggiungimento dello scopo di verifica per cui sono richieste, avranno inoltre il riferimento temporale e la descrizione dell'evento che le ha generate e saranno conservate per un congruo periodo, non inferiore ai sei mesi;
- In generale, esecuzione di tutte le attività obbligatorie dettate dal Garante della Privacy con Provvedimento generale del 27/11/2008 (G.U. n. 300 del 24/12/08) "Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di sistema", anche alla luce delle nuove norme introdotte al Codice privacy dal D.lgs. 101/2018;
- porre in essere qualsiasi ulteriore attività, sopra non elencata, finalizzata a garantire il regolare funzionamento dell'infrastruttura tecnologica dell'ente ed il corretto utilizzo della stessa, anche sotto il profilo della sicurezza, da parte degli utenti interni ed esterni all'organizzazione.

Nell'espletamento dell'incarico devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte dell'Amministratore di Sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste.
Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

L'incaricato avrà l'obbligo di:

a) conoscere e impegnarsi a rispettare, sotto la propria responsabilità, quanto indicato nell'Allegato B - "Disciplinare tecnico in materia di misure minime di sicurezza" al Codice della Privacy e nella Circolare AgID del 17 marzo 2017 in merito alle misure minime di sicurezza ICT;
b) svolgere il servizio con impegno, diligenza e professionalità, rispettando il codice di comportamento adottato dal comune;
c) rispettare le norme in materia di tutela della salute e della sicurezza nei luoghi di lavoro ex D.lgs. n. 81/2008;
d) attenersi agli obblighi di assoluta riservatezza connessi al suo incarico;
e) trattare dati personali solo se indispensabile all'assolvimento degli incarichi assegnati;
f) seguire le prescrizioni impartite dal titolare, tra cui l'obbligo di rispettare il segreto sulle informazioni e sui dati personali di cui viene, anche accidentalmente, a conoscenza nell'esercizio della propria funzione (art. 326 codice penale e art. 15 D.P.R. n. 3/1957); tale obbligo permarrà anche dopo la cessazione dell'incarico.

L'amministrazione comunale procederà con cadenza almeno annuale alla verifica dell'operato dell'Amministratore di Sistema al fine di verificare l'aderenza della sua attività alle vigenti disposizioni normative, anche avvalendosi di esperto in materia.

Per l'espletamento dell'incarico, al fine di garantire il corretto funzionamento, l'evoluzione e l'implementazione del sistema informativo comunale sono richiesti almeno due accessi mensili presso le sedi comunali.

Nel corso degli accessi, l'incaricato dovrà garantire la presenza in loco per l'intera giornata.

A seguito degli accessi tecnici eseguiti dovrà essere redatto apposito report, con indicazione specifica delle operazioni compiute, al fine di attestare la conformità delle operazioni eseguite alle prescrizioni di legge.

Per le attività svolte, l'incaricato dovrà relazionare in merito almeno annualmente e comunque preventivamente alla liquidazione di ogni pagamento dovuto per l'incarico.

Il servizio avrà durata **triennale,** con possibilità di proroga su facoltà dell'amministrazione, nelle more del nuovo affidamento del servizio.

2. IMPORTO BASE DI GARA

L'importo a base di gara per il triennio è pari a € 24.000,00 (€ 8.000,00 annuale).

3. REQUISITI DI PARTECIPAZIONE

Sono ammessi a partecipare alla procedura di cui al presente avviso i soggetti di cui all'art. 45 del D.Lgs 50/2016 in possesso dei seguenti requisiti:

- Non trovarsi in alcuna delle cause di esclusione previste dall'art. 80 del D.Lgs 50/2016 succitato
- esperienza professionale inerente il servizio da affidare ovvero aver svolto prestazioni professionali similari per conto di enti pubblici, nell'ultimo triennio.

A tal fine va allegato il curriculum.

Il soggetto che dovrà svolgere l'incarico di amministratore di sistema deve essere una persona fisica e pertanto in caso di partecipazione alla presente procedura da parte di società, dovrà essere indicata la persona fisica che svolgerà le funzioni di amministratore di sistema.

4. MODALITÀ E TERMINI DI PRESENTAZIONE:

Per partecipare alla procedura i soggetti interessati dovranno caricare sulla piattaforma di Sardegna CAT entro il giorno indicato sul portale, i seguenti documenti:

- istanza di manifestazione d'interesse firmata digitalmente, secondo il modulo allegato al presente avviso;
- curriculum formativo e professionale.

5. CRITERIO DI AFFIDAMENTO

Si procederà all'affidamento diretto ai sensi dell'art. 1 commi 1 e 2 lett. a) della Legge n. 120 del 11 settembre 2020, previa richiesta di più offerte da valutarsi con il criterio del prezzo più basso.

6. PUBBLICAZIONE DELL'AVVISO:

Il presente avviso sarà pubblicato su:

- Albo pretorio on-line della stazione appaltante;
- Profilo di committente: www.comune.castelsardo.ss.it;
- Sito internet Regione Autonoma della Sardegna: www.regione.sardegna.it;
- Piattaforma Sardegna CAT.

7. ALTRE INFORMAZIONI

L'Amministrazione si riserva la facoltà di interrompere in qualsiasi momento il procedimento, ovvero di sospendere, modificare, annullare il medesimo o di non dare seguito all'affidamento, senza che i soggetti partecipanti possano vantare pretesa alcuna.

Per tutto quanto non meglio specificato valgono le vigenti disposizioni in materia di appalti, al quale si fa espresso rinvio.

Ai sensi dell'art. 13 del D.Lgs 196/2003, come modificato dal D. Lgs. 101/2018 il trattamento dei dati personali sarà effettuato secondo l'informativa di seguito riportata.

IL RESPONSABILE DEL PROCEDIMENTO
Dott.ssa Maria G. Pattarino

PATTARINO MARIA GIUSEPPA LUCIA
03.12.2021
15:44:33
GMT+00:00