

Richiesta preventivo per consulenza e manutenzione e assistenza tecnico-informatica hardware e software

20 Dicembre 2017

Prestazioni richieste

- Consulenza, manutenzione e assistenza informatica su tutte le apparecchiature (computer, stampanti, fax, scanner, periferiche di rete) di qualsiasi marca utilizzate all'interno della sede dell'Ordine;
- Installazione, manutenzione e riparazione hardware;
- Installazione software aggiuntivi;
- Installazione e manutenzione degli antivirus e dei programmi di sicurezza antimalware, da farsi periodicamente così come la scansione dei vari computer ed i collegati aggiornamenti dei sistemi operativi;
- Assistenza software per i sistemi operativi di uso comune (Windows) e i pacchetti di uso generalizzato (Office);
- Consulenza e assistenza per la gestione della rete informatica, comprese consulenza, manutenzione e assistenza di eventuali dispositivi per gestione diversificata e la configurazioni della rete interna ed internet.

In una prima fase sarà richiesto in particolare supporto per adeguare la sede dell'Ordine e i dispositivi presenti alle "Misure minime di sicurezza ICT per le pubbliche amministrazioni", emanate da AGID (CIRCOLARE 18 aprile 2017, n. 2/2017.Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»), perseguendo il criterio "minimo". Per i dettagli si veda il paragrafo "Adeguamento alle misure minime di sicurezza ICT per le pubbliche amministrazioni".

Modalità

Il servizio di assistenza/manutenzione dovrà essere effettuato presso la sede dell'Ordine in via Galvani 15, Pistoia, secondo le seguenti modalità:

- controlli periodici on-site;
- consulenza telefonica ed assistenza operativa telefonica per soluzione piccoli problemi che non richiedono intervento diretto sul posto;

- possibilità di utilizzo di software di controllo remoto per assistenza;
- intervento diretto on-site (entro un massimo di un giorno lavorativo dalla chiamata) per ripristino elementi software/hardware non funzionanti.

Oneri e condizioni

- Nel caso di rotture di hardware e di necessità di reperire i materiali per le riparazioni necessarie o per mantenere in efficienza quelle ancora funzionanti, l'assistenza dovrà provvedere direttamente alla ricerca degli stessi e sottoporre i costi al Consiglio dell'Ordine, il quale, se li riterrà congrui e convenienti, autorizzerà l'intervento di riparazione. La manodopera sarà comunque coperta dal contratto di manutenzione.
- Il fornitore sarà l'esclusivo responsabile sia nei confronti del Committente che di terzi in relazione a tutto il personale adibito al servizio e dovrà garantire il rispetto di tutte le disposizioni legislative e regolamentari vigenti in materia di lavoro, ivi compresi quelli in materia di igiene e sicurezza, nonché la disciplina previdenziale ed infortunistica, assumendo a proprio carico tutti i relativi oneri e spese.
- Il fornitore dovrà garantire la massima riservatezza in merito ai dati e le informazioni di cui venga in possesso e/o a conoscenza rispettando altresì il divieto della loro divulgazione sotto qualsiasi forma e di non farne oggetto di utilizzazione a qualsiasi titolo. In particolare per quanto riguarda i dati personali e sensibili, dovranno essere rispettati tutti gli adempimenti previsti dal D.lvo 196/2003 e successivi aggiornamenti.
- In caso di inosservanza degli obblighi di riservatezza, il fornitore sarà tenuto a risarcire tutti i danni che dovessero derivare alla stessa amministrazione appaltante.

Apparecchiature e dispositivi

Le apparecchiature oggetto di assistenza, allo stato attuale sono le seguenti:

- 1 computer desktop adibito al lavoro di segreteria;
- 1 computer portatile a disposizione delle commissioni e dei docenti per le attività formative;
- 1 tablet a disposizione degli organizzatori delle attività formative;
- 1 fax;
- 1 stampante/scanner/fotocopiatrice;
- 1 proiettore;
- vari dispositivi per la gestione della rete LAN (modem, router, switch);
- 1 disco di rete per backup periodici.

Il servizio di manutenzione e assistenza dovrà essere garantito anche in caso di potenziamento/ampliamento delle attrezzature in uso.

Requisiti per la presentazione delle offerte

Per poter presentare l'offerta sono necessari i seguenti requisiti:

- iscrizione ad un Ordine Provinciale degli Ingegneri, tra le province toscane;
- iscrizione al terzo settore, Ingegneria dell'Informazione;

- possesso di RCA professionale in corso di validità.

Modalità di presentazione delle offerte

L'offerta potrà essere presentata entro e non oltre il 15 Gennaio 2018, via PEC all'indirizzo ordine.pistoia@ingpec.eu o personalmente presso la sede dell'Ordine in Via Galvani 15, in orario di apertura della Segreteria, e dovrà contenere:

- Profilo professionale e Curriculum Vitae
- Offerta tecnica, con descrizione generale della soluzione proposta, comprese caratteristiche, modalità e tempi di erogazione dei servizi.
- Offerta economica, che comprenda il costo del canone annuo del servizio di assistenza (con eventuali variazioni per gli anni successivi al primo) e il costo orario di intervento.

Valutazione delle offerte

Le offerte saranno valutate dal Consiglio dell'Ordine, che prenderà in considerazione sia i costi presentati che le caratteristiche del servizio offerto, tenendo conto in particolare di:

- profilo professionale e precedenti esperienze;
- costi del servizio;
- tempi di completamento del setup del sistema;
- tempi e garanzie di intervento per assistenza sul sistema;
- eventuali proposte migliorative, purché ritenute coerenti e utili rispetto ai servizi richiesti.

Il Consiglio dell'Ordine si riserva la facoltà di non aggiudicare la fornitura, nelle modalità presentate nel presente documento, nel caso nessuna delle offerte presentate si riveli valida e giudicata congrua.

Durata del contratto

La durata del contratto è fissata in anni 1 (uno) con decorrenza dalla firma del contratto, con possibilità di rinnovo tacito per altri 2 (due) anni.

Adeguamento alle misure minime di sicurezza ICT per le pubbliche amministrazioni, criterio medio.

ABSC 2 (CSC 2): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID	Descrizione
1.1.1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4
1.3.1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.
1.4.1	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID	Descrizione
2.1.1	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.
2.3.1	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID	Descrizione
3.1.1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.
3.2.1	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.
3.2.2	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.
3.3.1	Le immagini d'installazione devono essere memorizzate offline.
3.4.1	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID	Descrizione
4.1.1	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.
4.4.1	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.
4.5.1	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.
4.5.2	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.
4.7.1	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.
4.8.1	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).

4.8.2	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.
-------	---

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID	Descrizione
5.1.1	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.
5.1.2	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.
5.2.1	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.
5.3.1	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.
5.7.1	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).
5.7.3	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).
5.7.4	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).
5.10.1	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.
5.10.2	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.
5.10.3	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.
5.11.1	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.
5.11.2	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.

ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE

ABSC_ID	Descrizione
8.1.1	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.
8.1.2	Installare su tutti i dispositivi firewall ed IPS personali.
8.3.1	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.
8.7.1	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.
8.7.2	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.
8.7.3	Disattivare l'apertura automatica dei messaggi di posta elettronica.
8.7.4	Disattivare l'anteprima automatica dei contenuti dei file.

8.8.1	Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.
8.9.1	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.
8.9.2	Filtrare il contenuto del traffico web.
8.9.3	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID	Descrizione
10.1.1	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.
10.3.1	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.
10.4.1	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID	Descrizione
13.1.1	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica
13.8.1	Bloccare il traffico da e verso url presenti in una blacklist.