Carrara, 30 dicembre 2017

Bando per assegnazione di incarico per attività di consulenza, assistenza tecnica e manutenzione in ambito informatico sia hardware che software.

Tale incarico nasce dalla necessità di adeguare la sede dell'Ordine e i dispositivi in essa 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»).

In data 20.12.2017 il Consiglio dell'Ordine degli Ingegneri della Provincia di Massa Carrara ha approvato l'emanazione del presente bando di gara, finalizzato al raggiungimento del livello di sicurezza definito "minimo". Per ulteriori dettagli si rimanda al successivo paragrafo "Adeguamento alle misure minime di sicurezza ICT per le pubbliche amministrazioni".

1. Prestazioni richieste

- Consulenza, assistenza informatica ed eventuale manutenzione su tutte le apparecchiature (computer, stampanti, fax, scanner, periferiche di rete) utilizzate all'interno della sede dell'Ordine;
- Installazione, manutenzione e riparazione hardware;
- Installazione sistemi operativi sui computer della sede dell'Ordine e regolare aggiornamento;
- Installazione software aggiuntivi;
- Installazione degli antivirus e dei programmi di sicurezza anti-malware, e manutenzione degli stessi da effettuarsi a cadenza periodica in concomitanza con le scansioni sui computer della sede dell'Ordine;

Piazza Matteotti, 4 - 54033 Carrara (MS)
Tel./Fax 0585 70466
Email ordine@ordineingegnerimassacarrara.it

- Assistenza software per i sistemi operativi di uso comune (e.g. Windows) e i pacchetti di uso generalizzato (e.g. Office);
- Consulenza e assistenza per la gestione della rete informatica, compresa manutenzione e gestione della configurazione della rete interna ed internet.

2. Modalità di fornitura dei servizi

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

- controlli periodici da eseguire on-site;
- consulenza e assistenza telefonica per soluzione piccoli problemi che non richiedono intervento diretto sul posto;
- possibilità di utilizzo di software di controllo per assistenza remota;
- intervento diretto on-site (entro un massimo di un giorno lavorativo dalla chiamata) per ripristino elementi software/hardware non funzionanti.

La sede dell'Ordine è attualmente situata in piazza Matteotti 4, Carrara (MS).

3. Oneri e condizioni

- Nel caso di guasto hardware e di necessità di reperire i materiali per le riparazioni necessarie o per mantenere in efficienza quelle ancora funzionanti, il Fornitore 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. Il costo di manodopera dovrà in ogni caso essere contemplato nel contratto generale 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

Piazza Matteotti, 4 - 54033 Carrara (MS)
Tel./Fax 0585 70466
Email ordine@ordineingegnerimassacarrara.it

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.

4. Dotazioni attuali dell'Ordine

Le apparecchiature e i dispositivi oggetto di assistenza, allo stato attuale sono i seguenti:

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

Il servizio di manutenzione e assistenza dovrà essere garantito anche in caso di sostituzione o ampliamento dei dispositivi attualmente in uso.

5. Requisiti per la presentazione delle offerte

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

- Iscrizione ad un Ordine Provinciale degli Ingegneri;
- Iscrizione al terzo settore, Ingegneria dell'Informazione;
- Possesso di RCA professionale in corso di validità.

6. Modalità di presentazione delle offerte

L'offerta potrà essere presentata entro e non oltre il 31 Gennaio 2018, via PEC all'indirizzo ordine.massacarrara@ingpec.eu o personalmente presso la sede

Piazza Matteotti, 4 - 54033 Carrara (MS)
Tel./Fax 0585 70466
Email ordine@ordineingegnerimassacarrara.it

dell'Ordine in piazza Matteotti 4, Carrara (MS), 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 sia il costo del canone annuo del servizio di assistenza (con eventuali variazioni per gli anni successivi al primo) che il costo orario di intervento.

7. 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;
- Entità economica dell'offerta;
- 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 il contratto di fornitura nelle modalità presentate nel presente documento, nel caso in cui nessuna delle offerte presentate si riveli valida e giudicata congrua.

8. Durata del contratto

La durata del contratto è fissata in anni 1 (uno) con decorrenza dalla firma del contratto, con opzione di rinnovo annuale sino all'anno 2020.

Piazza Matteotti, 4 - 54033 Carrara (MS)
Tel./Fax 0585 70466
Email ordine@ordineingegnerimassacarrara.it

9. Adeguamento alle misure minime di sicurezza ICT per le pubbliche amministrazioni (estratto da Allegato 1, Circ.2/2017 del 18.04.2017)

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso.

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

Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione.

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.

Piazza Matteotti, 4 - 54033 Carrara (MS)
Tel./Fax 0585 70466
Email ordine@ordineingegnerimassacarrara.it

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER
Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.

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
Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.

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

Piazza Matteotti, 4 - 54033 Carrara (MS)
Tel./Fax 0585 70466
Email ordine@ordineingegnerimassacarrara.it

	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
Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

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

Piazza Matteotti, 4 - 54033 Carrara (MS)
Tel./Fax 0585 70466
Email ordine@ordineingegnerimassacarrara.it

	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): DIFESE CONTRO I MALWARE

Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.

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 rimuovibili 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).

Piazza Matteotti, 4 - 54033 Carrara (MS)
Tel./Fax 0585 70466
Email ordine@ordineingegnerimassacarrara.it

ABSC 10 (CSC 10): COPIE DI SICUREZZA

Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.

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

Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti.

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.

Piazza Matteotti, 4 - 54033 Carrara (MS)
Tel./Fax 0585 70466
Email ordine@ordineingegnerimassacarrara.it