ALL. 1

PROVINCIA REGIONALE DI PALERMO

UFFICIO GESTIONE RETI E APPLICATIVI

ACQUISIZIONE DI UN SISTEMA DI SICUREZZA ANTIVIRUS CENTRALIZZATO PER LA PROVINCIA REGIONALE DI PALERMO

☒ CAPITOLATO TECNICO

☐ CAPITOLATO SPECIALE D'ONERI

PROVINCIA REGIONALE DI PALERMO

1. INTRODUZIONE

Il presente Capitolato Tecnico disciplina gli aspetti tecnici della fornitura, per la Provincia Regionale di Palermo, dei prodotti software antivirus per la realizzazione dell'infrastruttura del sistema Antivirus e dei Servizi a questa connessi.

In questo capitolato tecnico vengono riportate le caratteristiche minime richieste per l'offerta:

- le certificazioni previste per il Fornitore cui deve obbligatoriamente rispondere per poter partecipare alla gara e fornire i servizi
- i requisiti di conformità cui devono necessariamente rispondere i prodotti offerti
- le condizioni e le modalità di erogazione dei Servizi connessi alla fornitura

Nel corpo del Capitolato, ai termini di cui appresso, viene attribuito il significato riportato a fianco di ciascuno di essi:

- **Capitolato tecnico**: il presente documento
- **Fornitura**: la vendita del software ed i relativi servizi di consegna, installazione, configurazione, collaudo e manutenzione in garanzia
- **Impresa**: l'Impresa aggiudicataria
- **Fornitore:** si intende l'Impresa Fornitrice aggiudicataria della gara
- **Amministrazione:** si intende la Provincia Regionale di Palermo
- **Data accettazione/collaudo fornitura:** si intende la data in cui il collaudo della fornitura dà esito positivo e la fornitura viene formalmente accettata dall'Amministrazione
- **Vendor:** si intende il Produttore del software
- **Endpoint:** si intende il computer (server, desktop, o portatile) in uso presso l'Amministrazione

1.1 Sistema antivirus attualmente in uso

Attualmente è in esercizio presso l'Amministrazione un sistema antivirus di classe Enterprise (la suite di Computer Associates *e*Trust® ITM Antivirus r8.1.) dedicato alla protezione dei circa 900 Endpoints.

Il sistema gestisce centralmente la distribuzione degli aggiornamenti antivirus per tutti gli Endpoints.

2. OGGETTO DELLA FORNITURA

2.1 Descrizione

Oggetto del presente Capitolato è la fornitura di prodotti e servizi per il sistema antivirus centralizzato dell'Amministrazione e l'erogazione dei servizi ad essa correlati.

Il sistema di sicurezza antivirus da realizzare, basato su un prodotto antivirus in versione Enterprise, gestito centralmente da una Consolle di management e monitorato da un Cruscotto Centrale, dovrà assicurare la protezione dalle minacce a tutti gli Endpoints (server, desktop e portatile) dell'Amministrazione.

Per tale sistema antivirus a protezione degli Endpoints la fornitura comprenderà:

- prodotti software antivirus per 900 Endpoints
- consolle di management e cruscotto centrale
- Servizi di installazione, configurazione ed attivazione delle consolle di management e del cruscotto Centrale
- Servizi di pianificazione e test della installazione dei nuovi prodotti su 10 (dieci) Endpoints indicati dall'Amministrazione
- Servizi di Consulenza specialistica
- Servizi di assistenza e manutenzione

2.2 Quantitativi

2.2.1 Prodotti software

Dovranno essere forniti i seguenti quantitativi relativi ai prodotti software:

PRODOTTO	DESCRIZIONE	Quantità
Software di protezione dell'Endpoint	Software di protezione dell'Endpoint con le caratteristiche specificate al par. 4.1	900
Consolle e cruscotto	Consolle di management e cruscotto centrale con le caratteristiche specificate al par. 4.2	1

Tutti i prodotti forniti devono essere di unico Vendor e la loro versione deve essere non inferiore alla più recente disponibile alla data del 01/06/2011.

2.2.2 Servizi

Dovranno essere erogati i seguenti servizi:

Tipologia Servizio	**Quantità**	**Unità di misura**
Servizi di consegna come specificati al par. 5.1	1	Cad
Servizi di installazione, configurazione ed attivazione delle consolle di management e del cruscotto Centrale come specificati al par. 5.2	2	Giornate lavorative
Servizi di pianificazione e test della installazione dei i nuovi prodotti su 10 (dieci) Endpoints indicati dell'Amministrazione come specificati al par. 5.3	2	Giornate lavorative
Servizi di Consulenza specialistica come specificati al par. 5.4	4	Giornate lavorative
Servizi di assistenza e manutenzione per 36 mesi come specificati al par. 5.5	1	Cad

3. CERTIFICAZIONI E REQUISITI DI CONFORMITÀ

I servizi richiesti dovranno essere erogati da un Team composto da almeno 2 (due) professionisti con Certificazione Ufficiale del Vendor, rilasciata da almeno un anno, per i prodotti oggetto della fornitura.

I componenti del Team devono essere in possesso dei seguenti requisiti.

- Esperienza nell'Ambito della progettazione dal punto di vista Ingegneristico nel settore Tlc e Security
- Provata esperienza nell'area della sicurezza antivirus del Vendor sia dal punto di vista organizzativo che tecnico specialistico
- Conoscenza delle tecniche di controllo di qualità su progetti analoghi
- Conoscenza operativa su tutti gli aspetti legali, organizzativi e tecnici che riguardano il mondo della protezione del business e dei dati aziendali.

Almeno uno dei componenti del Team con Certificazione Ufficiale del Vendor per i prodotti oggetto della fornitura dovrà operare on site presso l'Amministrazione durante l'erogazione dei servizi di cui ai paragrafi 5.2, 5.3, 5.4 e 5.5.

4. SISTEMA ANTIVIRUS DI CLASSE ENTERPRISE

4.1 Software di protezione per gli Endpoints

I prodotti software antivirus a protezione degli Endpoints dovranno avere le seguenti funzionalità:

- Antivirus
- Application & Device control
- Personal firewall

per ognuna delle quali nel seguito verranno specificate le caratteristiche qualitativamente minime.

I prodotti devono poter essere installati sugli Endpoints sia in locale che da remoto. Per l'installazione da remoto dovrà in ogni caso essere garantita la possibilità d'installazione mediante almeno una di queste modalità:

- attraverso la consolle di gestione (push remoto)
- attraverso i prodotti di software distribution utilizzati dall'Amministrazione (OCS Inventory)
- attraverso un sistema di software distribution proposto dal Fornitore.

I prodotti devono:

- poter essere installati, disabilitati e rimossi dalla consolle di cui al successivo paragrafo 4.2. "**Consolle di management e Cruscotto Centrale**"
- garantire che le configurazioni di scansione non possano essere modificate dall'utente
- garantire un livello di scalabilità in grado di supportare fino a 1.500 nodi
- consentire l'aggiornamento diretto e automatico dai server del Vendor nel caso in cui l'Endpoint non sia connesso alla rete aziendale ma direttamente alla rete Internet
- garantire che gli aggiornamenti delle *signature* avvengano attraverso il trasferimento non dell'intero pacchetto di *signature* ma attraverso la trasmissione del solo "delta" di aggiornamento
- integrarsi con soluzioni di Active Directory, PKI e LDAP

Dovrà essere fornita tutta la documentazione relativa ai sistemi software oggetto della fornitura (technical reference, operator & service guide, installation guide, tuning guide etc.). La documentazione dovrà essere redatta in lingua italiana, o in subordine in lingua inglese, e dovrà essere fornita su supporto cartaceo (manuali) ed elettronico (CD-ROM).

4.1.1. Antivirus

L'antivirus dovrà prevedere una *suite* di moduli in grado di intercettare un virus prima che questo possa danneggiare il computer ospite. Essa dovrà:

- supportare almeno i sistemi operativi Microsoft
- supportare sia piattaforme workstation che server;
- garantire il funzionamento sia in ambienti fisici che virtuali.

La *suite* per quello che concerne gli ambienti Microsoft dovrà garantire la piena compatibilità con tutti i sistemi e, in maniera obbligatoria, con le versioni workstation e server, in tutte le loro architetture (32 e 64 bit) a partire da Windows 2000 fino a Windows Seven.

Per quanto riguarda le nuove versioni degli ambienti Microsoft che dovessero rendersi disponibili durante il periodo di assistenza di tre anni, il Fornitore si impegna, su richiesta dell'Amministrazione, a fornire senza costi aggiuntivi, gli opportuni upgrade alle versioni che supportino i nuovi sistemi operativi fino alla misura del 10% delle licenze fornite.

La *suite* dovrà essere in grado di intercettare, bloccare e rimuovere, anche tramite diversi moduli eventualmente aggiuntivi e/o predisposti all'occorrenza, almeno le principali tipologie di minacce informatiche quali: operating sistem viruses, macro viruses, script minaccia, worms, backdoors / bots, trojan, spyware, adware, rootkit, botnet.

La *suite* dovrà essere in grado di effettuare:

- verifica della integrità del settore di boot, del Master Boot Record (MBR) e dei file di sistema durante la fase iniziale di avvio del sistema
- scansione in tempo reale della memoria
- scansione in tempo reale dei file in ingresso ed in uscita
- capacità di individuazione di tutte le tipologie di codice nocivo (cavalli di troia, backdoor, macro virus, ecc.)
- blocco preventivo degli attacchi di tipo buffer overflow
- rilascio da parte del produttore di aggiornamenti giornalieri del file delle firme
- possibilità di programmare scansioni del file system ad intervalli regolari

- distribuzione centralizzata degli aggiornamenti per computer connessi in rete locale
- possibilità di effettuare gli aggiornamenti attraverso Internet in assenza di collegamento alla rete locale
- capacità di isolare i file infetti per i quali il prodotto non sia in grado di compiere operazioni di pulizia.

Il modulo antispyware dovrà garantire le seguenti caratteristiche:

- scansione in tempo reale di memoria e processi per bloccare lo spyware prima che si installi
- rilascio da parte del produttore di aggiornamenti giornalieri del file delle firme
- funzionamento "euristico" per garantire la possibilità di fermare spyware anche in assenza di firme specifiche
- integrazione con il motore antivirus per garantire una logica univoca di funzionamento, sia verso l'utente (interfaccia grafica) che verso la consolle di gestione (reportistica)
- integrazione di funzionalità anti-Adware e similari tipologie di minacce.

La *suite* fornita dovrà:

- essere in grado di intercettare il codice minaccia sia sulla base di impronte caratteristiche (*signature*) sia in base alla rilevazione di comportamenti ritenuti potenzialmente dannosi (modulo di scansione euristica)
- disporre di funzionalità di quarantena della minaccia individuata e di remediation successiva
- disporre di funzionalità di scan del sistema attivabili sia in base ad una schedulazione preventiva che in modalità manuale
- disporre di funzionalità di scansione in tempo reale dei dispositivi rimovibili in grado di rilevare una minaccia anche se presente solo in questi supporti (ad esempio chiavetta USB, scheda SD)
- essere predisposta per verificare eventuali minacce contenute in file compressi delle tipologie più diffuse quali ed es.: file .zip, file .rar, etc.
- adottare un'architettura di tipo plug-in, con possibilità di aggiungere nuovi moduli con nuove funzionalità senza dover procedere alla reinstallazione di tutto il prodotto
- permettere di configurare la priorità di esecuzione del processo di scansione antivirus (manuale/automatica)

- garantire che non siano modificabili dall'utente le configurazioni di download degli aggiornamenti.
- disporre di vari livelli di auditing e logging in modo da tracciare puntualmente tutte le attività amministrative effettuate sull'infrastruttura e tutti gli eventi riguardanti infezioni in corso, aggiornamenti effettuati e/o falliti.
- deve essere in grado di allertare, con opportuni messaggi, sia l'utente sia la consolle di gestione, in caso di mancato aggiornamento o di basi virali outdated.
- deve garantire funzionalità di Host Intrusion Prevention System (HIPS).

4.1.2. Personal Firewall

Il modulo Personal Firewall deve disporre di funzionalità di network firewalling in grado di gestire le connessioni alla postazione per singolo indirizzo IP o "range" di indirizzi, per singola porta TCP/UDP o "range" di porte.

Il modulo di Personal Firewall dovrà essere in grado di applicare configurazioni e politiche specifiche in base alla rete cui la postazione è collegata (LAN o Internet). Ad esempio il portatile del dipendente utilizzato in Amministrazione o a casa, dovrà poter adottare politiche di sicurezza differenti.

4.1.3. Application & Device Control

La *suite* dovrà comprendere un modulo in grado controllare l'accesso ai dispositivi periferici dell'Endpoint.

Dovrà essere inoltre prevista la possibilità di bloccare automaticamente applicazioni sconosciute o sospette se non incluse in un database di applicazioni affidabili.

Il modulo dovrà essere in grado di impedire l'esecuzione di applicativi non autorizzati inclusi in una blacklist gestita dall'amministratore.

Il modulo deve contemplare la possibilità di assegnare politiche di sicurezza in base all'ubicazione fisica dell'Endpoint. Ad esempio il portatile del dipendente utilizzato in Amministrazione o a casa, dovrà poter adottare politiche di sicurezza differenti.

4.2. Consolle di Management e Cruscotto Centrale

4.2.1. Consolle di Management

I prodotti di Protezione per gli Endpoint dovranno essere monitorati e gestiti attraverso una consolle di management specifica, installata presso una delle sedi dell'Amministrazione.

Attraverso la consolle di management il system administrator potrà controllare e configurare tutti i prodotti installati, ivi inclusi gli agent o i moduli aggiuntivi previsti dal presente Capitolato.

La consolle di management dovrà rendere disponibili informazioni relative almeno ai seguenti aspetti:

- profili di sicurezza attualmente utilizzati
- indicatori sui livelli di sicurezza attuali per le varie funzionalità e per i vari gruppi di utenti
- possibilità di lettura dei dati di configurazione fino al singolo Endpoint
- informazioni di early warning.
- indicatori di sicurezza su Internet, in termini di livello, di minacce presenti in rete e la loro tipologia
- indicatori dello stato di sicurezza interna navigabili fino ai singoli eventi di sicurezza.

La consolle di management deve assicurare le seguenti funzioni di gestione:

- consentire la disattivazione/attivazione di specifiche funzionalità/policy, sia per un singolo che per un gruppo di Endpoint/utenti
- gestire ruoli differenziati di accesso alla consolle (almeno amministratore e auditor)

4.2.2. Cruscotto Centrale

Il cruscotto centrale dovrà consentire la visione integrata delle varie informazioni e dei report provenienti dai prodotti sottostanti.

Attraverso il cruscotto centrale deve essere possibile visualizzare tutti i profili di sicurezza e le politiche di applicazione definite per le Società del Amministrazione, nonché dei Gruppi utenti fino al dettaglio del singolo utente.

Il cruscotto centrale dovrà evidenziare tutte le situazioni di violazione della sicurezza che si verificassero nelle varie funzionalità.

Il cruscotto relativo all'Application Control dovrà segnalare tutte le anomalie rilevate a livello di integrità delle applicazioni sugli Endpoints.

4.2.3. Funzionalità di Reporting

I prodotti e sistemi installati devono consentire un'attività di reporting che riguardi le seguenti informazioni:

- eventi di sicurezza occorsi;
- statistiche sull'andamento delle infezioni (suddivisi per tipologie di virus e per Endpoint);

Dai report si dovrà evincere in maniera chiara lo stato dell'intera infrastruttura e degli Endpoint serviti. Dovranno essere incluse tutte le informazioni relative alle versioni (di engine antivirus e di pattern scaricati) installate sugli Endpoints.

Dovrà essere possibile produrre report in forma grafica in modo da fornire una panoramica veloce sullo stato dell'intera infrastruttura; dovranno inoltre essere previsti opportuni warning su situazioni potenzialmente pericolose (p. es. engine non aggiornati, pattern datati, agenti antivirus non funzionanti o con problemi).

Per quanto concerne auditing e logging, la soluzione deve garantire, per tutte le sue componenti, opportuni livelli di auditing in grado di tracciare tutte le attività amministrative che comportano un cambio nelle configurazioni delle componenti della soluzione sui server e sugli Endpoint.

5. SERVIZI

5.1. Servizi di consegna

L'impresa dovrà provvedere a consegnare, entro 5 giorni lavorativi dalla stipula del contratto:

- il Piano operativo, nel quale dovranno essere indicati, in modo puntuale ed esaustivo:
  a. le attività di installazione della consolle di management e del cruscotto centrale, la tempistica, la pianificazione
  b. i nominativi delle risorse coinvolte per l'espletamento dei servizi di cui ai paragrafi 5.2, 5.3, 5.4 e 5.5, i loro *curricula* e le certificazioni del Vendor da loro possedute
- le licenze da fornire attraverso l'apertura di appositi codici (grant number) dedicati.

Il Piano operativo sarà sottoposto alla valutazione della Amministrazione che ne comunicherà l'esito all'Impresa nei tempi e modi stabiliti nel Capitolato Speciale d'oneri.

Qualora non venga rispettata la scadenza di cui sopra o le certificazioni risultino difformi da quelle richieste l'Amministrazione applicherà le sanzioni disciplinate nel Capitolato Speciale d'oneri salvo in ogni caso il risarcimento al maggior danno.

5.2. Servizi di installazione, configurazione ed attivazione delle consolle di management e del cruscotto Centrale

L'Impresa dovrà provvedere, a proprio esclusivo onere:

- alla verifica della configurazione dei sistemi su cui installare la consolle di management
- all'installazione delle console di sicurezza secondo i requisiti espressi dall' Amministrazione e le specifiche concordate
- alla configurazione del prodotto di gestione antivirus centralizzato
- alla installazione e configurazione del cruscotto centrale di monitoraggio

I servizi di installazione, configurazione ed attivazione delle consolle di management e del cruscotto Centrale dovranno essere conclusi entro il termine di 5 (cinque) giorni lavorativi a decorrere dalla data di comunicazione all'impresa della valutazione con esito positivo del "Piano operativo" così come stabilito nel Capitolato Speciale d'oneri.

Qualora non venga rispettata tale scadenza, l'Amministrazione applicherà le penali disciplinate nel Capitolato Speciale d'oneri salvo in ogni caso il risarcimento del maggior danno.

5.3. Servizi di pianificazione e test della installazione dei i nuovi prodotti

L'Impresa dovrà provvedere, a proprio esclusivo onere:

- alla produzione di una checklist con le procedure operative da seguire passo passo per l'installazione dei nuovi prodotti sugli Endpoints
- alla installazione dei nuovi prodotti su 10 (dieci) Endpoints indicati dell'Amministrazione
- alla produzione di un piano di test per verificare tutte le funzionalità del software di protezione per gli Endpoints specificate al paragrafo 4.1 sui 10 Endpoints di cui al punto precedente

- alla verifica della funzionalità del sistema antivirus sui 10 Endpoints di cui al punto precedente.

La procedura di installazione dei nuovi prodotti deve prevedere la rimozione preventiva dell'attuale *suite* antivirus dagli Endpoints. La installazione sui 10 (dieci) Endpoints dovrà essere effettuata in parte da remoto ed in parte on-site come indicato dall'Amministrazione.

Le installazioni e le verifiche della funzionalità dovranno essere effettuate alla presenza di personale dell'Amministrazione.

I servizi di pianificazione e test della installazione dei nuovi prodotti dovranno essere conclusi entro il termine di 5 (cinque) giorni lavorativi a decorrere dalla data di comunicazione all'impresa della valutazione con esito positivo del "Piano operativo", così come stabilito nel Capitolato Speciale d'oneri.

Qualora non venga rispettata tale scadenza l'Amministrazione applicherà le penali disciplinate nel Capitolato Speciale d'oneri salvo in ogni caso il risarcimento al maggior danno.

Si precisa qui che l'installazione dei prodotti su tutti gli Endpoints (ad eccezione dei 10 Endpoints su cui sono state effettuate le installazioni di test di cui sopra) sarà eseguita a cura dell'Amministrazione dopo che verranno completati, da parte dell'Impresa, i servizi di consegna, installazione e pianificazione e test della installazione dei i nuovi prodotti.

5.4. Servizi di consulenza specialistica

L'impresa dovrà fornire 4 giorni di consulenza specialistica, da fruire a richiesta nell'arco di 36 mesi, per supporto alla configurazione del prodotto.

Ad esempio il Fornitore dovrà implementare alcuni profili di sicurezza tipo, definiti dall'Amministrazione, per i prodotti oggetto della fornitura.

5.5. Servizi di assistenza e manutenzione

Il Fornitore dovrà provvedere a fornire un servizio di aggiornamento software per tre anni a decorrere dalla data del collaudo.

Tale manutenzione e assistenza riguarda:

- aggiornamento signature antivirus
- aggiornamenti software di tutte le componenti (agent, consolle, etc.)
- possibilità di sottoporre file sospetti al produttore al fine di verificare la presenza di codice malevolo; si richiede un tempo di risposta di 24 ore solari
- servizio informativo erogato direttamente dal produttore

Il Fornitore deve garantire all'Amministrazione, a fronte della pubblicazione di una vulnerabilità di sicurezza relativa al software utilizzato per espletare le funzionalità descritte nel presente Capitolato, un adeguato supporto specialistico per l'individuazione e l'immediata attuazione di soluzioni temporanee, in attesa che il Vendor risolva in modo strutturato la problematica di sicurezza.

Il Fornitore è obbligato, in caso di malfunzionamento del sistema Antivirus, intendendosi per malfunzionamento qualsiasi anomalia funzionale che, indirettamente, provochi l'interruzione o la non completa disponibilità del servizio all'utenza e, in ogni caso, ogni difformità del prodotto in esecuzione dalla relativa documentazione tecnica e manualistica d'uso, a ripristinare, in loco, la piena funzionalità del sistema.

La richiesta di assistenza potrà essere effettuata a mezzo telefono, FAX, e-mail. A tal proposito il Fornitore dovrà fornire un numero di telefono, FAX ed un indirizzo e-mail al quale indirizzare le richieste di assistenza.

Tale servizio dovrà essere garantito, dalle ore 08:00 alle ore 18:00, per tutti i giorni feriali dell'anno, con i seguenti livelli di servizio:

- Presa in carico del problema: entro 4 ore lavorative dalla chiamata
- Intervento: entro 8 ore lavorative dalla chiamata

A seguito della richiesta di assistenza, qualora non vengano rispettati i livelli servizio indicati, l'Amministrazione applicherà le penali indicate nel Capitolato Speciale d'oneri, salvo in ogni caso il risarcimento al maggior danno.