CAPITOLATO TECNICO

PER L'ACQUISIZIONE DI UN SISTEMA DI SICUREZZA ANTIVIRUS CENTRALIZZATO PER L'AZIENDA TUTELA DELLA SALUTE (ATS) SARDEGNA

Sommario

Art. 1 - Premessa

L'Azienda per la Tutela della Salute (in seguito denominata per brevità ATS o Azienda Sanitaria o Amministrazione), costituita da otto Aree Socio-Sanitarie Locali (brevemente ASSL), le cui denominazioni sono riportate nella tabella seguente:

TABELLA 1: DENOMINAZIONE ASSL	
Sigla	**Denominazione**
ASSL 1	Area Socio Sanitaria di Sassari
ASSL 2	Area Socio Sanitaria di Olbia
ASSL 3	Area Socio Sanitaria di Nuoro
ASSL 4	Area Socio Sanitaria di Lanusei
ASSL 5	Area Socio Sanitaria di Oristano
ASSL 6	Area Socio Sanitaria di Sanluri
ASSL 7	Area Socio Sanitaria di Carbonia
ASSL 8	Area Socio Sanitaria di Cagliari

intende acquisire un sistema centralizzato per la gestione della Sicurezza Informatica a protezione del proprio sistema informativo.

Art. 2 - Analisi del contesto attuale

Attualmente sono presenti e installati in ATS diversi software Antivirus. Questa situazione disomogenea è dovuta all'unione di otto diverse e separate Ex-Aziende, in un'unica realtà regionale.

Nella tabella seguente viene riportata una stima delle quantità dei dispositivi presenti in ogni singola ASSL nonché il tipo di antivirus in essi installati:

TABELLA 2: STIMA NUMERO DISPOSITIVI PER SINGOLA ASSL						
ASSL	**Postazioni di Lavoro da Tavolo**		**Postazioni di Lavoro Note Book**		**Server Virtuali e Fisici**	
	Stima Quantità	**Tipo Antivirus Installato**	**Stima Quantità**	**Tipo Antivirus Installato**	**Stima Quantità**	**Tipo Antivirus Installato**
ASSL 1	1900	Sophos	200	Sophos	80	Sophos
ASSL 2	1400	Karspersky	100	Karspersky	60	Karspersky
ASSL 3	1400	McAfee	100	McAfee	60	McAfee
ASSL 4	600	Trend Micro worry-free business security	50	Trend Micro worry-free business security	30	Trend Micro worry-free business security
ASSL 5	1500	Sophos	100	Sophos	60	Sophos
ASSL 6	700	Eset Nod32	50	Eset Nod32	30	Eset Nod32
ASSL 7	1500	Sophos	100	Sophos	60	Sophos

ASSL 8	3000	Sophos	300	Sophos	120	Karspersky
Totali	**12000**		**1000**		**500**	

I dispositivi elencati nella precedente tabella sono disomogenei non solo nella tipologia ma anche da un punto di vista "generazionale", essendo stati acquistati in diversi periodi con diversi sistemi operativi ai quali è necessario garantire la compatibilità e protezione.
Nella tabella seguente vengono riportati i Sistemi Operativi presenti e attualmente installati in azienda:

TABELLA 3: SISTEMI OPERATIVI PRESENTI	
Tipo di Postazione	**Tipologia del sistema Operativo**
Postazioni di Lavoro da Tavolo	Win Xp, Win 7, Win 8, Win 10, linux, iOS
Note Book	Win Xp, Win 7, Win 8, Win 10, macOS
Server Virtuali e Fisici	Win Server 2003, Win Server 2008, Win Server 2012, Win Server 2019, Linux

Art. 3 - Oggetto dell'appalto

L'oggetto dell'appalto consiste in:

- Fornitura di **n. 8.400 licenze client** antivirus per la protezione delle postazioni di lavoro fisse, notebook con architettura centralizzata in cloud con possibilità di gestione per singola ASSL;
- Fornitura di **n. 500 licenze server** antivirus per la protezione delle macchine server virtuali e fisiche con architettura centralizzata in cloud con possibilità di gestione per singola ASSL;
- Fornitura di una soluzione centralizzata in cloud e della componente locale una per ciascuna delle otto ASSL afferenti al progetto;
- Servizio di installazione e configurazione dell'intero sistema antivirus proposto e migrazione;
- Servizio di reportistica;
- Servizio di formazione e consulenza;
- Servizio di assistenza e manutenzione.

Art. 4 - Durata del contratto – Importo a Base d'Asta

4.1 - Durata del contratto

La durata contrattuale del presente appalto è stabilita in **2 (due) anni,** decorrenti dalla data del verbale di avvio del servizio.
L'ATS si riserva la facoltà di recesso anticipato, anche senza alcun motivo imputabile alla Ditta aggiudicataria, in qualsiasi momento prima della naturale scadenza del medesimo, senza che la Ditta appaltatrice possa avanzare riserva alcuna o richiesta di indennizzo o pretesa a qualunque titolo:

- qualora si decidesse l'interruzione e/o la soppressione del servizio;
- a seguito di intervenuti riassetti e modifiche di organizzazione regionale/aziendale;
- a seguito di Convenzioni a carattere nazionale (CONSIP SPA) o regionale (CAT Sardegna) aventi ad oggetto l'affidamento dei servizi oggetto del presente Capitolato, alle quali ATS è obbligata ad aderire ai sensi della normativa vigente, salvo che la Ditta appaltatrice non ritenga opportuno adeguare la propria offerta rispetto a quella più vantaggiosa.

Resta inteso che l'eventuale risoluzione del contratto comunque dovrà avvenire con preavviso di almeno **60 (sessanta) giorni** da parte dell'Amministrazione. In caso di recesso sono dovuti esclusivamente i corrispettivi fino alla data di svolgimento del servizio. Il mancato preavviso comporta l'automatica prosecuzione del contratto sino alla sua scadenza naturale.

4.2 - Base d'Asta

L'importo complessivo posto a base di gara per la fornitura completa compresa installazione, configurazione e servizi accessori è determinato per singola licenza sia per Postazione di Lavoro che per Server in **12,00 Euro/Anno** da cui risulta **12,00 Euro x 8900 Licenze x 2 anni = 213.600,00 Euro/Biennio** IVA esclusa.

Non saranno ammesse offerte pari o superiori all'importo posto a base d'asta.

Il prezzo unitario offerto deve intendersi comprensivo di tutti i costi, nessuno escluso, che la Ditta partecipante dovrà sostenere, in caso di aggiudicazione, per l'espletamento di tutte le attività previste e dettagliate nel presente Capitolato Tecnico.

L'offerta economica dovrà essere formulata secondo il criterio dell'offerta economicamente più vantaggiosa.

Art. 5 - Caratteristiche tecniche e funzionali minime richieste del sistema antivirus proposto

Il sistema antivirus proposto dovrà consentire di svolgere le seguenti attività, tutte legate alla sicurezza contro gli attacchi per i dispositivi riportati nelle tabelle precedenti al fine di:

- identificare, valutare e rimediare efficacemente ai punti deboli degli endpoint, riducendo l'esposizione e inoltre, scoprire e priorizzare eventuali vulnerabilità di sistemi operativi e di applicativi;
- attivare azioni di monitoraggio comportamentale, protezione da minacce zero-day, controllo applicazioni, controllo dispositivi e controllo contenuti;
- fornire una gestione centralizzata semplice per una facile implementazione e applicazione delle policy di sicurezza per qualsiasi tipo e numero di endpoint, indipendentemente dalla loro collocazione, individuando le parti infette del sistema e le relative azioni di bonifica, indicando laddove necessario l'intervento manuale;
- rilevare e permettere il monitoraggio di connessioni sospette ed i trasferimenti dei dati verso l'esterno;
- fornire uno strumento di controllo sui tentativi di attacco al corretto funzionamento degli applicativi web e stand-alone;

Inoltre il sistema dovrà essere scalabile, supportando necessità di sicurezza mutevoli in previsione di attivazione di nuovi strumenti e funzionalità, man mano che le esigenze di sicurezza dell'Azienda si evolvono e dovrà fornire protezione a tutti i tipi di endpoint: fisici, virtuali e cloud, indipendentemente dal fattore di forma: workstation, server, embedded, mobile o dal sistema operativo: Windows, VMware, Linux e Mac.
L'intero sistema di sicurezza non deve richiede hardware aggiuntivo rispetto a quello già esistente nell'ATS.
Nel particolare, il sistema proposto dovrà garantire i seguenti requisiti minimi:

- fornire protezione a tutte le principali tipologie di attacchi, compresi virus, adware, backdoor, BHO, dialer, fraudtool, hijacker, HTML, keylogger, LSP, ramsonware, rootkit, spyware, trojan, PUP, worm, man in the browser.
- fornire protezione ai dispositivi per quel che riguarda tutti gli attacchi definiti Zero-Day.
- eseguire un controllo in tempo reale di tutti i file in entrata e in uscita in un determinato sistema, fornendo visibilità e informazioni sulle attività sospette dell'endpoint.
- garantire metodi di analisi basati su: firme (signatures), tecnologie euristiche, analisi telemetriche.
- permettere agli amministratori di gestire gli aggiornamenti dei dispositivi in maniera dinamica, eventualmente con l'utilizzo di macchine intermedie (cash), in modo tale da poter scegliere di erogare gli aggiornamenti nei dispositivi in maniera costante, manuale o automatica e distribuita.
- essere dotato di un sistema di gestione centralizzata tramite console Amministratore con caratteristiche descritte in seguito nell'apposito paragrafo.
- attivare azioni anti-phishing: il sistema deve essere in grado di riconoscere un sito di phishing e segnalarlo all'utente, consentendo la navigazione solo dopo espressa autorizzazione.
- effettuare analisi comportamentali, da realizzare sia su processi eseguiti dagli endpoint (file avviati, creati e modificati), che da azioni dell'utente.
- fornire funzionalità di Web filtering, bloccando siti dai contenuti indesiderati in base all'URL o a determinate parole chiave.
- capacità di ricerca, all'interno della rete aziendale, di postazioni non protette dall'antivirus con relativi alert da inviare all'amministratore IT.
- produrre indicatori KPIs (Key Performance Indicators) attraverso report (vulnerabilità, tentativi di accessi fraudolenti, indicatori sulle infezioni trattate). I dati devono essere disponibili e filtrabili tramite una Dashboard e scaricabili in formato open.

Il controllo della suite di sicurezza dovrà avvenire utilizzando una console di amministrazione centralizzata, scalabile, semplice, gestibile in remoto da più posizioni attraverso interfaccia Web-based e utilizzabile ovunque e con qualsiasi dispositivo fisso o mobile.
La console dovrà essere intuitiva e compatta in modo da visualizzare e gestire, con il minimo delle schermate, la sicurezza in tutti gli ambienti aziendali: cloud, macchine fisiche e virtuali e dispositivi mobili.
Report predefiniti disponibili dalla console per gli amministratori, o eventuale numero di widget o elementi che possono essere combinati per la realizzazione di report personalizzati, dettagliando, oltre al numero, anche una descrizione degli stessi;

Dovrà essere possibile prevedere uno o più utenti amministratori a livello globale. Inoltre, definendo delle marco-aree (come ad esempio le attuali 8 ASSL), si dovranno poter configurare ulteriori amministratori locali. È richiesto, per gli amministratori, un meccanismo di doppia autenticazione, mediante OTP o meccanismo similare.
L'ambiente di management per gli amministratori dovrà permettere il governo dell'intero sistema e allo stesso tempo, una gestione semplificata in termini di:

- suddivisione del parco installato in aree separate con relativi amministratori;
- distribuzione del sistema antivirus ai vari endpoint;
- organizzazione della distribuzione degli aggiornamenti;
- visualizzazione di alert, relativi alle criticità su eventuali infezioni;
- possibilità di generare dei report grafici, esportabili su file in formato open, per l'analisi della sicurezza del parco installato;
- esatta individuazione della postazione infetta e del tipo di attacco;
- possibilità, da console, di poter eseguire interventi da remoto di primo livello quali scansione, azioni di disinfezione o protezione, messa in isolamento, riavvio o arresto della macchina;

L'architettura individuata come inderogabile è quella cloud-based; nell'offerta dovrà essere specificato in dettaglio lo schema logico dell'applicazione con i relativi flussi di funzionamento per le principali attività indicate nei punti precedenti.

Art. 6 - Servizio di installazione sistema antivirus e migrazione

L'offerta tecnica dovrà prevedere nel dettaglio le modalità di installazione del software antivirus e degli altri eventuali moduli per ulteriori funzioni proposte, se separati da esso, in tutti le tipologie di dispositivi descritti nelle tabelle precedenti.

E' richiesta, come caratteristica minima della fornitura, la funzionalità di migrazione per le postazioni di lavoro. Tale funzionalità deve permettere il passaggio dall'attuale software antivirus a quello oggetto della fornitura, e deve poter essere gestita dalla console centralizzata.

Nell'offerta il fornitore dovrà indicare, in base alla situazione dell'attuale installato, la percentuale di postazioni che possono essere migrate dalla console (e quindi da remoto) sul totale del parco. Tale percentuale non dovrà comunque essere inferiore alla percentuale delle macchine facenti parte degli attuali domini stimata circa nel 60% del totale delle postazioni di lavoro attualmente in produzione.

In particolare, è richiesta la predisposizione di un piano di transizione che preveda ogni aspetto della migrazione dal sistema corrente attualmente in uso.

Il piano di transizione dovrà comprendere ogni aspetto relativo alla migrazione; sarà quindi onere della Ditta aggiudicataria gestire e risolvere le problematiche di natura tecnica, operativa e gestionale, rapportandosi direttamente con l'attuale fornitore del servizio anche per il recupero incondizionato di eventuali dati elaborati negli anni pregressi.

La Ditta aggiudicataria, tramite console (da remoto), dovrà farsi carico, secondo la percentuale di postazioni dichiarata, della migrazione dal vecchio sistema verso il nuovo entro **90 (novanta) giorni solari** dalla stipula del contratto di aggiudicazione.

Art. 7 - Servizio di reportistica

Durante la fase di installazione/migrazione dei Dispositivi verso il nuovo sistema antivirus, il fornitore dovrà produrre, con cadenza almeno mensile, dei report da consegnare al personale preposto del Servizio Infrastrutture, Tecnologie dell'Informazione e delle Comunicazioni competente.

Dai report dovrà essere possibile discernere non solo le macchine già migrate al nuovo sistema rispetto al vecchio installato, ma deve essere anche possibile operare interrogazioni secondo:

- versione del Sistema Operativo;
- distinzione dominio/non a dominio;
- raggruppamento secondo sito geografico;
- raggruppamento secondo subnet;
- elenco macchine in cui la procedura di installazione/migrazione non è andata a buon fine;

Inoltre, è richiesto che i report siano disponibili secondo i comuni formati open utilizzabili per l'elaborazione su fogli elettronici.

Art. 8 - Servizio di formazione e consulenza

L'offerta tecnica dovrà prevedere la formazione e la consulenza ai tecnici afferenti al Servizio Infrastrutture, Tecnologie dell'Informazione e delle Comunicazioni nelle singole ASSL. In particolare essa dovrà prevedere:

- almeno n. 3 (tre) giornate per ASSL di formazione per il personale dei Servizi Informatici in loco al momento dell'avvio ed installazione del sistema con rilascio di certificato e test di verifica di apprendimento; ove i test non fossero superati, la Ditta aggiudicataria dovrà effettuare in loco ulteriore formazione. Si prevedono circa 20 operatori da formare.

Inoltre dovrà essere prevista:

- consulenza telefonica o via e-mail tutti i giorni feriali in orario d'ufficio;
- obbligo di effettuare formazione-consulenza in loco in caso di aggiornamenti o per particolari e non preventivabili, ma motivate, esigenze aziendali;
- fornitura di manuali di consultazione (o altro tipo di documentazione) riportanti le istruzioni per l'utilizzo dei software forniti e in cui siano specificate le procedure per le operazioni più comuni.

Art. 9 - Servizio di assistenza tecnica e manutenzione e livelli di servizio

9.1 - Assistenza tecnica e manutenzione

La Ditta aggiudicataria dovrà fornire tutte quelle attività che garantiscono nel tempo il corretto funzionamento del servizio, nonché l'assistenza necessaria ai tecnici delle Infrastrutture per il corretto utilizzo del sistema antivirus proposto.

Le attività che dovranno essere garantite per l'intera durata del contratto sono di seguito descritte.

Servizio di manutenzione ed assistenza telefonica, ovvero:

- manutenzione correttiva: che comprende la diagnosi e la rimozione delle cause e degli effetti delle malfunzioni delle procedure e dei programmi;
- manutenzione adeguativa/evolutiva: che comprende l'attività di manutenzione volta ad assicurare la costante aderenza delle procedure e dei programmi alla evoluzione dell'ambiente tecnologico del sistema informativo ed al cambiamento dei requisiti (organizzativi, normativi, d'ambiente);
- assistenza telefonica: che comprende l'assistenza su chiamata ("help-desk") fornita al tecnico delle Infrastrutture a fronte di esigenze nell'utilizzo dell'antivirus, attuata principalmente attraverso il supporto telefonico. L'assistenza telefonica "help-desk" dovrà essere prestata mediante un Numero Verde (o comunque a carico della Ditta aggiudicataria), secondo il seguente minimo schema orario:

  Dal Lunedì al Venerdì per tutta la durata del contratto:
  Mattina: dalle ore **8:00** alle ore **13:30**
  Pomeriggio: dalle **14:30** alle ore **18:00**

9.2 - Livelli minimi di servizio

I Livelli Minimi di Servizio richiesti, stabiliti sulla base della classificazione di gravità dei problemi sono riportati nella tabella seguente:

TABELLA 4: LIVELLI MINIMI DEL SERVIZIO MANUTENTIVO		
Tipo	**Descrizione malfunzionamento**	**Tempi max. di risoluzione**
Bloccanti	Malfunzionamenti che provocano l'interruzione di attività operative.	**Entro 2 ore lavorative.**
Gravi	Malfunzionamenti che provocano l'interruzione parziale delle funzionalità, ma che consentono la prosecuzione delle attività operative.	**Entro 4 ore lavorative.**
Lievi	Malfunzionamenti che non provocano interruzioni operative.	**Entro 24 ore lavorative.**

A titolo di esempio, rientrano nella categoria dei problemi bloccanti la mancata raggiungibilità della console centralizzata, oppure un diffuso malfunzionamento nel parco macchine ATS dovuto ad un aggiornamento dell'antivirus.

I problemi gravi sono quelli dovuti alla discontinuità di servizio relativa ad una singola postazione di lavoro, a seguito di un malfunzionamento causato da un aggiornamento dell'antivirus o per una operazione similare.

I problemi di lieve entità possono essere in casi in cui le attività delle postazioni di lavoro possono proseguire nonostante si rilevino dei malfunzionamenti del sistema. Sempre a titolo meramente esemplificativo, si può ipotizzare il caso in cui l'installazione o l'aggiornamento dell'antivirus non va a buon fine; questa operazione non impedisce il funzionamento della Postazione ma in questo caso la criticità risiede nella mancata copertura della postazione stessa.

Sarà carico dell'aggiudicatario intervenire, e se necessario on-site e con i propri mezzi, per la risoluzione del malfunzionamento riportato in tabella secondo le tempistiche indicate negli SLA; la SC Infrastrutture, Tecnologie dell'Informazione e delle Comunicazioni verrà coinvolto in tutte le attività per le quali occorra supporto infrastrutturale e altre attività necessarie non riportate nel capitolato.

Inoltre, dovrà essere disponibile traccia degli interventi svolti, con un archivio condiviso consultabile dallla SC Infrastrutture, Tecnologie dell'Informazione e delle Comunicazioni previo rilascio di credenziali idonee.

Art. 10 - Proposte migliorative su ambiti non previsti in Capitolato

L'offerta tecnica potrà prevedere proposte migliorative su ambiti non espressamente previsti nel presente Capitolato, purché coerenti con gli obiettivi del progetto e che tendano comunque a migliorare il servizio offerto su parti specifiche o nel suo complesso.

Art. 11 - Certificazioni richieste

I concorrenti devono essere in possesso delle seguenti certificazioni:

Certificazione UNI EN ISO 9001/2008, in corso di validità, per servizi inerenti l'oggetto dell'appalto rilasciata da primario ente certificatore o analoga certificazione riconosciuta a livello UE, pena l'esclusione.

Certificazione UNI EN ISO 27001/2005, in corso di validità, rilasciata da primario ente certificatore per il sistema di gestione della sicurezza delle informazioni o analoga certificazione riconosciuta a livello UE, pena l'esclusione.

Art. 12 - Normativa

Il sistema informatico proposto deve essere creato, fornito, installato e mantenuto nel rispetto della normativa vigente in particolare:

- Legge 196/2003 (Legge Privacy)
- Codice Amministrazione Digitale (CAD)
- Specifiche AGID
- GDPR, General Data Protection Regulation: regolamento (UE) n. 2016/679