ISTITUTO REGIONALE DEL VINO E DELL`OLIO
Protocollo N.0001511/2024 del 16/02/2024

REGIONE SICILIANA

ISTITUTO REGIONALE DEL VINO E DELL'OLIO

RETTIFICA AVVISO DI PRE-INFORMAZIONE
ai sensi dell'art. 81 del D. Lgs. 36/2023

L'IRVO, Istituto regionale del vino e dell'Olio, via Libertà 66, Ente Pubblico Reginale non economico vigilato dall'Assessorato Agricoltura, che svolge attività di ricerca e promozione a supporto della filiera vitivinicola ed olearia siciliana;
Codice NUTS IRVO Palermo: ITG12
PEC: direzione.irvos@messaggipec.it
TEL: 091 6278111
SITO Internet: www.irvos.it
Indirizzo per informazioni: vincenzo.caselli@regione.sicilia.it
intende affidare, ai sensi dell'art. 50 comma 1 lett. b) una **piattaforma di gestione antivirus degli Endpoint dell'IRVO per max 100 dispositivi**
CATEGORIA MERCEOLOGICA: software antivirus
CODICE/I CPV: 32420000-3
CODICE NUTS: Palermo ITG12

L'incarico, di importo inferiore a 140.000 €, verrà stipulato mediante affidamento diretto del servizio/fornitura ai sensi dell'art. 50 comma 1 lett. b) del D. Lgs. 36/2023, senza consultazione di più operatori economici.

Entro 30 giorni sarà inoltrato ODA sul portale acquisti della P.A., in relazione all'accordo quadro "Cybersecurity 2" per un incarico biennale, o in alternativa RdO sul MEPA per l'aggiornamento dell'antivirus attualmente in dotazione Symantec Endpoint Security (SEP) Ver. 14.3.1 come da capitolato allegato in calce, per anni 3.

L'importo presuntivo stimato della fornitura è di € 5.000.

Il presente avviso di pre-informazione sostituisce quello precedentemente pubblicato e viene inserito sul sito internet dell'Istituto in data 16/2/2024; non vincola l'Amministrazione allo svolgimento della procedura.
L'appalto non rientra nell'ambito di applicazione dell'AAP.

U.O. UFFICIO DIREZIONE
Dott. Vincenzo Caselli

Il RUP

CAPITOLATO della Fornitura (in caso di acquisto tramite RdO)

Il presente capitolato riguarda l'aggiornamento della piattaforma Symantec Endpoint Security (SEP) Ver. 14.3.1, attualmente in uso all'Ente, all'ultima versione equivalente disponibile alla data attuale, le attività di migrazione/aggiornamento del server e dei client ed il mantenimento per almeno 3 anni degli aggiornamenti sia del software che dei database delle minacce.
Il sistema attuale è composto dal Symantec Protection Manager, installato su un Server Windows 2008 R2 presso la nostra sede di Palermo, che dovrà essere migrato su di un nuovo Server Windows 2019 e da svariati client Windows dalla versione 7 in poi sia a 32 che a 64 bit su cui gira il software client in modalità sia gestita che non gestita.

Prodotti da fornire:
n. 1 Symantec Protection Manager per il Server;
n. 80 Licenze Symantec Endpoint Protection per Windows sia Workstation che Server sia 32 che 64 bit;

Tutte le licenze dovranno essere in versione Government e, se previsto dal Symantec, come aggiornamento dalla versione precedente già in possesso dell'Ente.

Caratteristiche dei prodotti

I prodotti forniti dovranno garantire almeno le stesse funzionalità della versione attuale in merito alle seguenti funzionalità:

- Controllo centralizzato dei client gestiti tramite il Protection Manager per il controllo e la modifica delle policy, la gestione del Server e dei Client, la reportistica in merito ad anomalie e/o eventi di rilevazione di minacce;
- Possibilità di installazione da remoto tramite la console di gestione in modalità push ovvero tramite pacchetti preconfigurati sia in modalità gestita che non gestita;
- Aggiornamento continuo del Protection Manager con eventuali nuove versioni per tutta la durata del contratto;
- Aggiornamento continuo dei client tramite il server in modalità gestita o direttamente da Symantec tramite connessione Internet che potrebbe avvenire anche tramite proxy autenticato per tutta la durata del contratto;
- Possibilità di programmare scansioni tramite policy distribuite dal Server ovvero programmate dall'utente nei client non gestiti;
- Protezione dei client da Virus, Macro Virus, Script Malevoli, Worms, Backdoor, Trojan, Spyware, Adware, Rootkit, Botnet, Boot Record Virus, Attacchi Buffer Overflow, etc. che possano presentarsi in:
  - Avvio del sistema, boot sector;
  - Moduli caricati in memoria;
  - File presenti sui filesystem locali, di rete e sui supporti rimovibili, anche compressi nei più comuni formati (zip, rar, 7z, etc.);
  - Messaggi di posta elettronica scaricati tramite i client di posta più diffusi;
  - Link malevoli presenti in siti web visualizzati tramite i browser più diffusi;
  - Macro virus in documenti, fogli di calcolo, presentazioni, etc.;
  - Attacchi via rete locale ovvero tramite altri PC infetti.

Fornitura ed assistenza

Il fornitore dovrà fornire i prodotti su supporto fisico oppure tramite download dal sito del produttore, i codici di licenza, la documentazione anche in formato digitale.

Lo stesso dovrà provvedere all'assistenza, anche da remoto, al personale sistemistico dell'Ente per tutte le attività di migrazione/aggiornamento del Server ed il deployment dei pacchetti client.