SÍNDIC
EL DEFENSOR DE LES PERSONES

PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS PER A LA CONTRACTACIÓ DE L'ACTUALITZACIÓ DE LA SOLUCIÓ DE SEGURETAT (ANTIVIRUS) I SERVEI DE MANTENIMENT CORRECTIU (EXPEDIENT SGC-2025/09)

SÍNDIC
EL DEFENSOR DE LES PERSONES

ÍNDEX

SÍNDIC
EL DEFENSOR DE LES PERSONES

1. Objecte del contracte

L'objecte d'aquest contracte és l'actualització de la solució de seguretat d'endpoint de l'organització de Symantec Endpoint Security (SES) a Symantec Endpoint Security Complete (SES Complete). Aquesta actualització inclou la provisió de llicències, la instal·lació del software, la configuració dels sistemes, la integració amb la infraestructura existent incloent telèfons mòbils, i un servei de manteniment anual que inclou una bossa de 50 hores per a suport tècnic i tasques de manteniment. Facilitant el futur compliment de l'ENS.

2. Context actual

L'organització actualment disposa de Symantec Endpoint Security (SES), que proporciona protecció bàsica per a un total de 110 usuaris/equips. No obstant això, les amenaces cibernètiques han evolucionat, i és imprescindible implementar una solució que integri capacitats avançades de detecció, resposta i gestió centralitzada. Amb l'actualització a SES Complete, es busca millorar la seguretat, minimitzar els riscos associats i garantir la continuïtat de les operacions. Aquesta actualització és fonamental per protegir adequadament tots els dispositius i garantir una resposta efectiva davant de possibles incidents de seguretat.

3. Requeriments tècnics del servei

Els requisits tècnics per a **Symantec Endpoint Security Complete (SES Complete)** inclouen:

- **Solució SaaS (Cloud)**: La solució ha de ser basada en el núvol, permetent una gestió centralitzada i una disponibilitat immediata de les funcionalitats de seguretat per a tots els endpoints.
- **Compatibilitat multiplataforma**: Ha de ser compatible amb sistemes operatius **Windows**, **macOS, andorid, IOS** i **Linux**, garantint la protecció dels dispositius independenment del sistema operatiu utilitzat.
- **Mobile Threat Defense**: La llicència de **SES** ha de permetre la seva utilització també en dispositius mòbils, incloent **iOS** i **Android**, proporcionant protecció contra amenaces específiques per a mòbils.
- **Secure Connections**: Capacitat per protegir els dispositius contra atacs en xarxes no segures, com ara xarxes Wi-Fi públiques, assegurant que les connexions siguin segures durant la navegació i la comunicació.
- **Endpoint Detection & Response (EDR)**: Capacitat per identificar, analitzar i respondre a incidents de seguretat en temps real, amb funcionalitats d'investigació forense per a una millor comprensió de les amenaces.
- **Targeted Attack Analysis**: Anàlisi avançada per detectar i mitigar atacs dirigits, incloent la identificació de patrons i tècniques emprades pels atacants.
- **Active Directory Defense**: Funcionalitats per prevenir atacs de moviment lateral dins de la xarxa mitjançant controls a nivell de controlador de domini, protegit l'entorn d'actuacions no autoritzades.
- **Application Control & Application Isolation**: Capacitat per controlar l'accés i l'execució d'aplicacions, així com aïllar aplicacions potencialment perilloses per evitar la seva interacció amb altres sistemes.

- **XDR vinculat amb CASB**: Integració amb solucions de **Cloud Access Security Broker (CASB)** per proporcionar una visibilitat i control millorat sobre l'ús de serveis en el núvol.
- **Multiarquitectura**: Capacitat de desplegament en entorns **On-Premise**, **Híbrid** o **Cloud**, oferint flexibilitat en la implementació segons les necessitats de l'organització.
- **Nombre d'usuaris/equips**: La solució ha de ser capaç de gestionar un total de **110 usuaris/equips**, garantint que cada un d'ells estigui degudament protegit i monitoritzat.

4. Funcionalitats de la prestació:

Les funcionalitats que el nou servei ha de proporcionar inclouen:

- **Protecció proactiva**: Capacitat de monitorització contínua dels endpoints amb alertes immediates en cas d'activitats sospitoses.
- **Automatització de respostes**: Implementació de protocols automàtics per contenir amenaces, incloent aïllament de dispositius compromesos.
- **Actualitzacions automàtiques**: Capacitat per actualitzar el software de manera automatitzada per garantir la protecció davant de les últimes amenaces.
- **Reporting avançat**: Generació d'informes detallats sobre l'estat de seguretat, incidents ocorreguts, i accions correctives implementades.
- **Suport i formació**: Provisió de recursos formatius per a l'usuari final, així com assistència tècnica en temps real.
- **Funcionalitat de Mobile Threat Defense**: Protecció dels dispositius mòbils contra amenaces i vulnerabilitats específiques.
- **Seguretat de connexions**: Protecció contra atacs en xarxes públiques mitjançant mecanismes de seguretat avançats.
- **Detecció d'incidències amb EDR**: Capacitats per detectar i respondre a incidents de seguretat en temps real.
- **Anàlisi de ciberatacs dirigits**: Capacitats avançades d'anàlisi per detectar atacs específics i implementar mesures de defensa.
- **Control d'aplicacions**: Capacitat per gestionar i restringir l'ús d'aplicacions, així com per aïllar aplicacions no segures.
- **Integració XDR i CASB**: Visibilitat i control sobre l'ús de serveis en el núvol per millorar la seguretat general de l'organització.

5. Característiques del lliurament, instal·lació i posada en funcionament del maquinari

El pla de treball inclourà:

- Lliurament de llicències: lliurament i activació de les llicències per a SES Complete.
- Instal·lació: instal·lació del software, definició de polítiques per tots els tipus de dispositiu inclòs telèfons mòbils, incloent les configuracions necessàries a la infraestructura per a una integració adequada amb els sistemes operatius i aplicacions existents. Com son els servidors, portàtils i dispositius mòbils android i ios.

- Posada en funcionament: verificar la correcta instal·lació i funcionament de la solució, incloent proves de seguretat i funcionalitat.
- Formació inicial: Sessions de formació per a l'equip tècnic i per als usuaris finals sobre l'ús i gestió de SES Complete , tant a dispositius portàtils com a servidors.

6. Manteniment Correctiu

El manteniment del servei inclourà:

- **Bossa d'hores**: Una bossa de 50 hores anuals per a suport tècnic i tasques de manteniment, que es podran utilitzar per a les següents activitats:
    - **Assistència tècnica**: Resolució d'incidències, configuració de nous dispositius, i consultes generals. Configuració de les polítiques tant de portàtils/servidors com de dispositius mòbils.
    - **Revisions de seguretat**: Anàlisi de vulnerabilitats i revisió de les configuracions de seguretat per garantir que es mantinguin les millors pràctiques.
    - **Actualitzacions i parches**: Implementació d'actualitzacions de seguretat i parches necessaris.
    - **Optimització del rendiment**: Anàlisi del rendiment del sistema i ajustaments necessaris per millorar la seva eficiència.
    - **Formació addicional**: Sessions de formació per al personal sobre noves funcionalitats o canvis en la política de seguretat.

Tasques dins de la bossa d'hores (50 hores anuals)

1. **Assistència tècnica** (16 hores)
    - **Resolució d'incidències**: Atendre i resoldre incidents relacionats amb el software de seguretat, incloent problemes d'instal·lació, configuració i operativitat.
    - **Configuració de nous dispositius**: Configurar i integrar nous endpoints a la solució de seguretat, incloent dispositius mòbils i portàtils.
    - **Suport remot**: Proporcionar suport tècnic remot per a l'equip d'IT de l'organització en temps real.
2. **Revisions de seguretat** (10 hores)
    - **Anàlisi de vulnerabilitats**: Realitzar una avaluació periòdica de vulnerabilitats per identificar i mitigar riscos potencials.
    - **Revisió de configuracions**: Avaluar i ajustar les configuracions de seguretat per assegurar que es mantinguin actualitzades amb les millors pràctiques.

3. **Actualitzacions i parches** (8 hores)
    - **Implementació d'actualitzacions**: Aplicar actualitzacions de software, incloent parches de seguretat i noves funcionalitats.
    - **Verificació de compatibilitat**: Comprovar que les actualitzacions no afectin la funcionalitat d'altres sistemes o aplicacions.
4. **Optimització del rendiment** (6 hores)
    - **Anàlisi del rendiment**: Monitorar el rendiment de la solució de seguretat i identificar àrees d'optimització.
    - **Ajustaments de configuració**: Realitzar canvis en la configuració per millorar la velocitat i l'eficiència del sistema.
5. **Formació addicional** (6 hores)
    - **Sessions de formació per a l'equip d'IT**: Proporcionar formació específica sobre noves funcionalitats i millores del software.
    - **Capacitació per a usuaris finals**: Organitzar tallers o sessions informatives per als usuaris finals sobre bones pràctiques de seguretat i ús del sistema.
6. **Monitoratge i informes** (2 hores)
    - **Generació d'informes de seguretat**: Crear informes sobre l'estat de seguretat de l'organització, incidents ocorreguts i accions correctives.
    - **Monitoratge continu**: Supervisar el sistema per detectar anomalies i comportaments sospitosos.
7. **Consultoria i recomanacions** (2 hores)
    - **Recomanacions de millora**: Proporcionar consells i recomanacions per millorar les polítiques de seguretat i la infraestructura tecnològica.
    - **Assessorament sobre noves amenaces**: Informar sobre tendències i noves amenaces en el panorama de la ciberseguretat.

Resum de les hores per tasca

- **Assistència tècnica**: 16 hores
- **Revisions de seguretat**: 10 hores
- **Actualitzacions i parches**: 8 hores
- **Optimització del rendiment**: 6 hores
- **Formació addicional**: 6 hores
- **Monitoratge i informes**: 2 hores

- **Consultoria i recomanacions**: 2 hores

7. **Garantia de l'actualització de la solució d'antivirus.**

L'empresa adjudicatària ha de prestar una garantia de fabricant amb cobertura per a actuacions davant de possibles incidències que pateixi la solució d'antivirus com a mínim durant vigència del contracte. Si s'acredita l'existència de vicis o defectes en la prestació del servei, s'actuarà d'acord amb l'article 305 de la Llei de contractes del sector públic (LCSP).

El licitador, en cas de no ésser el fabricant del producte, haurà de presentar un certificat d'aquest conforme la garantia del serveis objecte del contracte està contractada directament al fabricant.

Jordi Clemente Pascual
Coordinador TIC
Barcelona, en la data de la signatura electrònica