PLEC DE PRESCRIPCIONS TÈCNIQUES PER AL SUBMINISTRAMENT EN MODALITAT D'ARRENDAMENT D'ÚS DE LLICÈNCIES I FUTURES ACTUALITZACIONS DE PROGRAMARI ANTIVIRUS

1.- Objecte del contracte

L'objecte del present plec és determinar les condicions tècniques que han de regir la contractació del subministrament en modalitat d'arrendament d'ús de les llicències i futures actualitzacions del programari antivirus "WatchGuard EPDR" per a llocs de treball i servidors. La contractació d'un servei de protecció completa d'equips (els llocs de treball dels usuaris i servidors) controlant el comportament de cada un dels processos executats al parc informàtic de l'Ajuntament de Tortosa a més de proveir dels mitjans de detecció i desinfecció de *malware*. Així com les eines necessàries per a la seva gestió i administració per part del propi Ajuntament i el servei de suport per part del fabricant.

Actualment l'Ajuntament disposa de 501 llicències de la versió del producte "WATCHGUARD EPDR", en modalitat d'arrendament d'ús que deriven del contracte adjudicat el passat 9 de maig de 2022 per un període de 3 anys. 400 llicències, que atén les necessitats dels diferents departaments municipals i que es gestionat per la unitat de Sistemes d'Informació. I 101 llicències que gestiona Tortosa Activa per protegir els equips del centre que es destinen a la realització de programes subvencionats.

L'objectiu és seguir unificant aquestes necessitats mitjançant la realització d'un sol contracte, que ha de resultar més eficient, flexible i econòmic per a l'Ajuntament, si bé mantenint la possibilitat de facturació del contracte per centres de cost a l'efecte de fer més eficient la imputació de costos pels diferents programes subvencionats.

L'objecte del present contracte consisteix en la contractació del subministrament en modalitat d'arrendament d'ús, de les llicències per un període de tres (3) anys següent:

Nom del Producte	Número de llicències
WatchGuard EPDR 3 anys	501

Les llicències subministrades han de permetre mantenir totes les configuracions de perfils, grups, etc. que ja es troben definides actualment així com l'històric i donar continuïtat al sistema de seguretat sense escletxes en el moment del canvi així com disposar del suport especialitzat durant el període de vigència del contracte.

2.- Requisits tècnics

2.1. – Actius a protegir

La solució ha de donar protecció inicialment a 501 equips. La solució ha de ser escalable i permetre que, si durant la durada del contracte fossin necessàries llicències addicionals,

aquestes s'integren funcionalment dintre de la solució oferta.

2.2.- Ubicació plataforma

Amb la finalitat de reduir els costos de manteniment i explotació de la solució, no haurà de ser necessari l'ús d'una plataforma interna, es precisa una solució basada en *cloud*. És requisit mínim que la plataforma on s'allotgi la infraestructura es trobi fora de les nostres instal·lacions i operada pel fabricant de la solució en un model *cloud*, el qual permeti el creixement i escalabilitat de la plataforma. Assegurant que independentment del nombre de nodes de la instal·lació la plataforma funcioni amb el mateix nivell d'eficiència i eficàcia.

Existeixen nodes que estan distribuïts per diferents seus i fins i tot en mobilitat per la qual cosa aquests aprofitaran la disponibilitat de la infraestructura *cloud* perquè estiguin integrats de forma completa en la configuració i actualització de la solució.

La plataforma de gestió ha de cobrir els principals nivells de certificació com és la ISO 27001.

2.3.- Components del servei

2.3.1. Infraestructura Cloud

La solució proveirà, des del núvol, el conjunt de servidors, bases de dades i processos de tractament de la informació relacionada amb el servei. Els processos capturats dels clients seran tractats en el núvol de tal forma que l'impacte sobre els sistemes corporatius sigui mínim.

2.3.2. Agent, a desplegar en els equips.

L'agent desplegat permetrà la comunicació i gestió de punt la protecció d'antivirus tradicional així com de la protecció de processos desconeguts.

Recollirà la informació corresponent als esdeveniments i els components que els produeixen, sense recopilar informació, ni documents d'usuari. L'impacte sobre els dispositius del parc haurà de ser menor al 5% de rendiment de la CPU, memòria i disc.

L'agent ha de ser capaç de protegir equips de sobretaula, portàtils i smartphones amb els sistemes operatius següents:

- Des de Microsoft Windows 10 i posteriors.
- Des de Microsoft Windows 2012 fins a Microsoft Windows Server 2022 i posteriors.
- MacOs, iOs, Android o Linux.

La desinstal·lació de la protecció haurà de protegir-se mitjançant contrasenya.

La solució deu poder desplegar-se de manera silenciosa mitjançant els següents mecanismes: per adreça IP, rang d'adreces IP, nom de màquina i grups de Directori Actiu basat en polítiques de domini.

2.3.3. Consola Web

La solució proporcionarà una interfície en el qual es puguin consultar les dades en temps real, descarregar informes/alertes, accedir a la configuració i disposar de les actualitzacions dels agents.

Els administradors municipals del servei podran gestionar des d'una única consola i de manera centralitzada, mitjançant qualsevol navegador web la seguretat i productivitat de totes les estacions de treball i servidors Windows fins i tot ordinadors portàtils o smartphones i oficines remotes.

2.4.- Protecció

La solució estarà basada en múltiples tecnologies de protecció que permet substituir el producte d'antivirus tradicional per un complet servei de seguretat gestionada.

La solució WatchGuard EPDR estarà basada en les funcionalitats de protecció de endpoints (EPP) i de detecció i resposta (EDR) en un sol producte per a obtenir la màxima seguretat contra les sofisticades amenaces als endpoints. Combinant les tècniques tradicionals basades en signatures amb funcions i serveis avançats per a proporcionar una oferta única i completa. Permetrà la supervisió contínua dels endpoints, la detecció i la classificació de tota l'activitat, podent revelar i bloquejar els comportaments anòmals d'usuaris, màquines i processos. Al mateix temps, descobrir proactivament noves tècniques i tàctiques d'atacs informàtics i evasió per a protegir ràpidament els nostres equips. Aquests avanços afegeixen immediatament una capa intel·ligent addicional de protecció per a avançar-se als atacants

Característiques clau

- EDR per a la supervisió contínua que impedeix l'execució de processos desconeguts.
- Detecció i resposta automàtiques per a atacs dirigits i vulnerabilitats en la memòria.
- Zero Trust Application i Threat Hunting com a serveis administrats.
- Anàlisis de comportament i detecció de scripts, macros, etc. d'indicadors d'atacs (IoA).
- Funcionalitats de protecció de endpoints, com el filtrat de direccions URL, el control de dispositius i el firewall gestionat.
- Un agent lleuger i una consola basada en el núvol fàcil d'usar amb informes detallats.

Protecció contra ciberatacs moderns

El producte ha de ser una solució de ciberseguretat per a portàtils, equips de sobretaula, smartphones i servidors que combine la més àmplia gamma de tecnologies de protecció de endpoints (EPP) amb funcionalitats EDR. Ha de protegir els usuaris d'amenaces avançades, amenaces avançades persistents (APT), malware de dia zero, ransomware, suplantació d'identitat, rootkits, vulnerabilitats en la memòria i atacs sense malware. A més ha de proporcionar funcionalitats de IDS, firewall, control de dispositius i filtrat de contingut i de direccions URL. EPDR ha d'automatitzar de manera única les accions de prevenció, detecció, contenció i resposta per a aconseguir una seguretat definitiva que sigui fàcil de gestionar i implementar.

Abast i solució de problemes de seguretat

L'oferta de seguretat s'ha de completar amb eines de monitoratge, anàlisi forense i resolució, que delimitin l'abast dels problemes detectats i els solucionen.

El monitoratge aportarà dades valuoses sobre el context en el qual es succeiran els problemes de seguretat. Amb aquesta informació, l'administrador podrà determinar l'abast dels incidents i implantar les mesures necessàries per a evitar que tornin a produir-se.

La solució ha de disposar d'un equip d'experts en ciberseguretat que analitzi qualsevol activitat sospitosa que possiblement estigui relacionada amb els atacs informàtics i investigui els indicadors d'atac per a trobar tècniques d'evasió i posada en perill. També ha de buscar de manera proactiva patrons de comportament anòmal que no hagin estat identificats anteriorment en la xarxa per a ajudar al fet que els clients de EPDR:

- Redueixin el MTTD i el MTTR (temps mitjà de detecció i temps mitjà de resposta).
- Creï noves regles que representin nous IOA que puguin ser lliurats als endpoints per a protegir-los ràpidament contra nous atacs.
- Obtingui recomanacions sobre com mitigar un atac i reduir la superfície d'atac per a evitar ser víctima de futurs atacs.

Multiplataforma

La solució ha de ser un servei multiplataforma allotjat al núvol i compatible amb Windows, MacOs, iOS, Linux, Android i amb entorns virtuals i VDI, tant persistents com no persistents.

A més, la solució no ha de necessitar nova infraestructura IT en l'empresa per a la seva gestió i manteniment.

2.5.- Certificacions i esquema nacional de seguretat

La solució obligatòriament ha d'estar inclosa en el "Catàleg de Productes de Seguretat de les Tecnologies de la Informació i la Comunicació." (CPSTIC) Publicat pel CCN (Centre Criptogràfic Nacional), dins de la família de protecció del Lloc de treball com a QUALIFICAT.

La solució ha de tenir la certificació de garantia EAL2+ en avaluació de l'estàndard Common Criteria (https://www.commoncriteriaportal.org/)

Tecnologia Cloud Pública, és obligatòria que tingui la certificació de conformitat enfront del ENS, de categoria alta.

3.- Suport tècnic 24x7x365

S'establirà el manteniment i assistència tècnica que permeti assegurar el correcte funcionament en tots els llocs i servidors de l'organització mitjançant:

- Servei de suport ofert pel fabricant per telèfon en català o castellà amb telèfon d'accés prioritari.
- Service Packs i hotfixes: accés a les millores tècniques del producte durant el temps d'activació del servei
- Web de suport: accés a fòrums, blogs, informació sobre últimes amenaces, enciclopèdia de virus, ...

- Suport tècnic via email 24x7x365, per tècnics certificats en la solució implementada
- Accés a anàlisi online de virus ocults
- Accés il·limitat al Helpdesk: sense límit d'incidències

El contracte haurà d'incloure una visita a l'Ajuntament de Tortosa cada sis mesos d'una durada de 4 hores per part d'un tècnic especialista en la solució del fabricant, a petició del responsable del contracte de l'Ajuntament de Tortosa.

4.- Condicions de Lliurament

El lliurament de l'objecte del contracte es realitzarà per l'empresa adjudicatària segons les indicacions que li facilitarà el responsable del contracte.

L'empresa adjudicatària haurà de lliurar el corresponent document en el qual consti el número de llicències a lliurar, així com el número de contracte d'aquestes i el número de client atorgat pel fabricant a l'Ajuntament de Tortosa.

5.- Termini del lliurament

L'empresa es compromet a iniciar la instal·lació del producte objecte del present contracte de manera immediata un cop formalitzat aquest contracte, entenent per "formalització" la signatura per ambdues parts i, si escau, el compliment de qualsevol altra condició prèvia expressament establerta en aquest document. En cap cas el termini d'inici de la instal·lació podrà excedir de 48 hores des de la formalització del contracte. L'incompliment d'aquesta obligació facultarà la part contractant a exigir el compliment immediat amb caràcter d'urgència, així com a reclamar els danys i perjudicis que se'n derivin.

Tortosa,

El responsable del contracte