D00676d7423b010abbe07e53e40a0a35l

COPIA AUTÉNTICA que puede ser comprobada mediante el Código Seguro de Verificación en https://sede.talavera.org/validacionDoc?entidad=45165

1. OBJETO DEL CONTRATO

El presente contrato tiene por objeto dotar a los equipos y sistemas del Ayuntamiento de Talavera de la Reina de una protección completa contra virus, software malicioso (antimalware), bloqueo de correo no deseado (antispam), Spyware y amenazas de seguridad.

Dicha protección deberá ser capaz de bloquear y eliminar software maliciosos mediante el uso clásico de detección de archivos y paginas web infectadas.

Así mismo la protección deberá ser capaz de clasificar el software que se ejecuta en los puestos de trabajo para monitorizar el comportamiento de dicho software y poder discernir acciones malicioso de las confiables.

2. PARQUE DE EQUIPOS A PROTEGER

El parque de equipos que debe cubrir la solución propuesta será de 400 puestos.

3. REQUERIMIENTOS TÉCNICOS DE LA SOLUCIÓN SOFTWARE

3.1. Ubicación Plataforma de la solución

La solución deberá estar basada en la nube con el fin de recudir costos tanto en hardware como en personal de mantenimiento de la solución. De manera que la infraestructura donde se aloje la solución sea fuera de las instalaciones del Ayuntamiento. La ubicación de la plataforma deberá estar alojada en la **Union Europea.**

3.2. Infraestructura

Se deberá proveer, **desde la nube**, el conjunto de procesos, BBDD y servidores necesarios para el tratamiento de la información relacionada con el servicio, de manera que los procesos capturados por los agentes instalados en los equipos serán tratados en la nube minimizando el uso de recursos en los equipos clientes.

3.3. Consola de administración

Se deberá proporcionar una interfaz web en la cual se pueda acceder/modificar la configuración y actualización de los agentes desplegados, consultar datos en tiempo real, descarga de informes, gestión de alertas, etc..

Se deberá poder gestionar desde una única consola web de manera centralizada, usando cualquier navegador actual, la seguridad y configuración de todas las estaciones de trabajo y servidores de todos los equipo y servidores del parque de la corporación municipal, incluyendo equipo y oficinas remotas.

Documento firmado por:	Cargo:	Fecha/hora:
JOSE LUIS SERRANO MORENO	TECNICO MEDIO INFORMATICO	01/10/2021 11:21

D00676d7423b010abbe07e53e40a0a35l

COPIA AUTÉNTICA que puede ser comprobada mediante el Código Seguro de Verificación en https://sede.talavera.org/validacionDoc?entidad=45165

3.4. Agentes

El agente desplegado en los equipos deberá suponer un impacto mínimo en el rendimiento de los mismos.

Se encargara de recoger la información correspondiente a los eventos y componentes que los producen, sin recopilar ningún tipo de documento ni información de los usuarios.

Deberá ser capaz de ofrecer protección a equipos de sobremesa, portátiles y servidores, al menos, de los siguientes sistemas operativos:

- Windows 7 y superiores
- Windows Server 2003 y superiores.

El agente así mismo deberá contar con protección contra intentos de desinstalación no autorizados, bien por parte del propio usuario del equipo como de procesos maliciosos.

El despliegue deberá poder realizarse de manera silenciosa mediante al menos los siguientes métodos:

- Rango IP
- Grupos de Directorio Activo mediante GPO
- Instalación en sito mediante instalador personalizado.
- Envió de enlace por correo electrónico u otro método con acceso al instalador.

Con el fin de garantizar el impacto mínimo en los equipo la solución deberá tener un único agente centralizado por equipo y no estar compuesto de varios agentes independientes.

3.5. Características del Protección

La solución deberá constas al menos de las siguientes partes:

3.5.1. EPP: Endpoint Protection Platform

Se requerirá una solución clásica EPP, con al menos las siguientes funcionalidades:

- Detección y desinfección para archivos, correo y web contra cualquier tipo de amenaza.
  - Detección de malware por comportamiento.
  - Detección y bloqueo de paginas web con contenido malicioso.
- Firewall gestionado en local o bien de manera remota mediante la consola centralizada.
  - Prevención de intrusiones.
  - Bloqueo de conexiones entrantes y salientes de aplicaciones.

Documento firmado por:	Cargo:	Fecha/hora:
JOSE LUIS SERRANO MORENO	TECNICO MEDIO INFORMATICO	01/10/2021 11:21

D006676d7423b010abbe07e53e40a0a35l

COPIA AUTÉNTICA que puede ser comprobada mediante el Código Seguro de Verificación en https://sede.talavera.org/validacionDoc?entidad=45165

- Administración de reglas para denegar/permitir trafico, especificando aplicaciones, protocolos y/o puertos.
- Bloque de acceso a paginas no deseadas. Sistema basado en listas blancas y negras de sitios, ip y/o dominios.
- Bloqueo de acceso a dispositivos locales específicos, como pueden ser unidades USB, dispositivos de captura, impresión, etc.. de manera que se pueda impedir entrada de virus/malware y/o fugas de información.

3.5.2. EDR: Endpoint Detection and Response

Será necesario incorporar una solución EDR que proporcione monitorización y análisis continuo para detectar y prevenir, de forma proactiva, amenazas avanzadas que haya pasado el primer corte del EPP.

- Amenazas zero-day
- Malware avanzado
- Troyanos de nueva generación indetectables por el EPP.
- Programas potencialmente no deseados.
- Captura de posibles amenazas.
- Monitorización y clasificación de procesos.
- Sistema de anti-exploit.

El EDR deberá ser capaz de clasificar todos los procesos ejecutados en la máquina, de manera que se produzca un bloqueo de los procesos desconocidos que se intenten ejecutar para evitar la posibilidad de dañar los datos accesibles por la maquina.

El sistema anti-exploit debe realizar la detección y bloqueo de exploits conocidos y desconocidos.

Posibilidad de establecer niveles de bloqueo (mas o menos restrictivos) según la confianza que se tenga de los procesos conocidos.

Así mismo se debe poder definir la capacidad de los propios usuarios para desbloquear individualmente procesos bloqueados por el sistema.

3.5.3. Servicio de alerta de amenazas

Se requiere un servicio que alerte y tome las medidas correctivas adecuadas cuando sea detectada una actividad anómala en los equipos basada en el comportamiento normal auditado anteriormente en el parque de equipos.

Este servicio deberá estar ofrecido por el fabricante de la solución EDR por técnicos especializados usando los datos que haya recogido en la auditoria forense.

Deben poder realizar la alerta y la inclusión en la inteligencia del sistema EDR de las medidas correctivas.

Documento firmado por:	Cargo:	Fecha/hora:
JOSE LUIS SERRANO MORENO	TECNICO MEDIO INFORMATICO	01/10/2021 11:21

D00676d7423b010abbe07e53e40a0a35l

COPIA AUTÉNTICA que puede ser comprobada mediante el Código Seguro de Verificación en https://sede.talavera.org/validacionDoc?entidad=45165

3.5.4. Sistema de Informes

El sistema debe generar información forense relacionada con cada equipo de tal forma que pueda ser explotada posteriormente.

El sistema deberá incluir informe por amenaza detectada en la que se correlacionen las acciones que ha hecho el proceso o en el contexto que ha estado envuelto, por ejemplo si ha sido descargado de Internet o ha sido extraído de un fichero comprimido.

Se valorara mucho un entorno amigable y fácil de seguir, sin exigir grandes conocimientos de amenazas avanzadas. Además debe incluir informes de estado de las protecciones, de las detecciones de malware y algún informe ejecutivo con el resumen de la información global.

Los informes se deben de poder obtener de forma inmediata con los datos en tiempo real y también de forma periódica por correo electrónico y en diferentes formatos para su posterior tratamiento.

3.6. CERTIFICACIONES Y ESQUEMA NACIONAL DE SEGURIDAD

La solución obligatoriamente tiene que estar incluida en el “Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación.” (CPSTIC) Publicado por el CCN (Centro Criptográfico Nacional), dentro de la categoria “Explotación de la Seguridad” como CUALIFICADO y ENS Medio o Alto.

3.7.- SOPORTE TÉCNICO

Se establecerá el mantenimiento y asistencia técnica que permita asegurar el correcto funcionamiento en todos los puestos y servidores de la organización. Mediante:

- Servicio de soporte ofrecido por el fabricante por teléfono en castellano con teléfono.
- Service Packs y hotfixes: Acceso a las mejoras técnicas del producto durante el tiempo de activación del servicio
- Web de soporte: Acceso a foros, blogs, información sobre últimas amenazas, enciclopedia de virus, …
- Soporte técnico vía email 24x7x365, por técnicos certificados en la solución implementada.
- Aviso sobre alertas y vulnerabilidades detectadas por el fabricante para actuar de forma preventiva y correctiva.
- Acceso a análisis online de virus ocultos
- Acceso ilimitado al Helpdesk: sin límite de incidencias

Documento firmado por:	Cargo:	Fecha/hora:
JOSE LUIS SERRANO MORENO	TECNICO MEDIO INFORMATICO	01/10/2021 11:21

Además de las características citadas consideradas como requisitos, las ofertas podrán incluir otros servicios con respecto a soporte y atención, que podrán ser valoradas de forma adicional en la baremación de la solución. Estas características son:

- Atención de incidencias graves relacionadas con software malicioso o epidemias "in situ" en las dependencias del Ayuntamiento, por personal cualificado del fabricante o del proveedor adjudicatario.

- Formación adicional sobre nuevas versiones o características avanzadas con posterioridad a la fase de implantación durante la duración del contrato. Podrá ser presencial o en remoto.

- Monitorización y sistema de alertas de los equipos del ayuntamiento. El proveedor podrá proporcionar un sistema de monitorización sobre los equipos del ayuntamiento, de forma que de forma proactiva avise y tenga control del estado del parque y genere las alertas en su caso al personal del ayuntamiento.

4. MEJORAS

Las propuestas podrán presentar características en su solución por encima de los requerimientos citados en el presente pliego. Se considerarán como mejoras y por lo tanto podrán valorarse dentro de los criterios de adjudicación, los siguientes aspectos:

- El software instalado en los equipos junto con la consola de administración podrá permitir además de la función fundamental de antivirus otras funciones adicionales de interés, como:
    1. Inventario hardware del parque de equipos.
    2. Inventario software (de todo el software instalado en los equipos).
    3. Control remoto del equipo.
    4. Instalación remota de software en los equipos (cualquier software, no sólo el relacionado con el antivirus).
- Características de la solución antivirus que no siendo un requisito citado en el punto 2 del presente pliego, mejore o amplíe la funcionalidad de la solución dentro del objeto del contrato, teniendo en cuenta características únicamente de antivirus, antimalware, antispam o amenazas de seguridad.

D00676d7423b010abbe07e53e40a0a35l

COPIA AUTÉNTICA que puede ser comprobada mediante el Código Seguro de Verificación en https://sede.talavera.org/validacionDoc/?entidad=45165

Documento firmado por:	Cargo:	Fecha/hora:
JOSE LUIS SERRANO MORENO	TECNICO MEDIO INFORMATICO	01/10/2021 11:21