AYUNTAMIENTO DE CIUDAD REAL

PRESCRIPCIONES TÉCNICAS PARA EL CONTRATO DE SUMINISTRO, INSTALACIÓN, CONFIGURACIÓN Y MANTENIMIENTO DE LA PLATAFORMA DE ANTIVIRUS DE PUESTOS DE TRABAJO Y SERVIDORES, ASÍ COMO LAS HERRAMIENTAS PARA SU ADMINISTRACIÓN, PARA ESTE EXCMO. AYUNTAMIENTO.

PRIMERA.- OBJETO DEL CONTRATO.

Es objeto del presente contrato el suministro, instalación, configuración y mantenimiento de la plataforma de antivirus de puestos de trabajo y servidores, así como las herramientas necesarias para su administración en el Sistema Informático del Ayuntamiento de Ciudad Real.

La necesidad del mismo viene determinada por los siguientes motivos:

El Ayuntamiento de Ciudad Real en la actualidad dispone de 500 licencias de antivirus, concretamente el NOD32, las citadas licencias caducan en el presente año, por tanto es necesaria la contratación de la adquisición, mantenimiento de la plataforma de antivirus para este Ayuntamiento, tanto para los puestos de trabajo como los servidores en el entorno operativo Windows, así como las herramientas necesarias para su administración en nuestro sistema informático.

La citada compra es necesaria, obligatoria para tener actualizados nuestros equipos de trabajo y servidores. La solución deberá garantizar el cumplimiento de los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información que constituye el Esquema Nacional de Seguridad (ENS). En concreto se deberá asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de datos, informaciones y servicios utilizados en medios electrónicos, que son objeto de la presente contratación.

SEGUNDA.- REQUERIMIENTOS DEL SUMINISTRO.

Se solicita la adquisición, instalación, configuración y mantenimiento de 500 licencias de software antivirus que incluyan funcionalidades de antivirus, sistema de protección contra amenazas avanzadas y análisis de código desconocido para la protección de equipos de trabajo y servidores corporativos, así como el software necesario para su instalación, gestión y administración centralizada.

La solución de protección de puestos de trabajo debe estar soportada en sistemas operativos Microsoft Windows, así como Windows Server, Linux.

2.1.- Protección endpoint tradicional de antivirus. Requisitos mínimos:

- Protección antimalware en ficheros, correo electrónico de cliente y navegación.
- Análisis de comportamiento para identificar posibles amenzas.
- Control de inicio y actividad de aplicaciones, protección de claves de registro, directorios de sistemas, etc.
- Control de acceso a dispositivos.
- Acceso continuo a bases de datos sobre nuevas amenazas, enlaces web y software de confianza.
- Actualiación de parcheado automático de vulnerabilidades y bases de firmas.
- Capacidad de bloqueo o finalización del agente malicioso y posibilidad de desinfección del equipo.

Se valorará:

- Mínimo impacto en el sistema (consumo de recursos, rendimiento del sistema y de las aplicaciones, fiabilidad..)
- Plugin específico para cliente Microsof Outlook.
- Facilidades para la gestión de parches y vulneralidades.
- Descubrimiento-inventario de activos hardware y software de puestos de trabajo.
- Cifrado de datos en archivos, carpetas y disco completo y en dispositivos de almacenamiento extraible y herramientas de recuperación para descifrar datos.
- Inclusión de detección y bloqueo a ataques de red.
- Capacidad de firewall.

2.2.- Protección contra amenazas desconocidas y avanzadas. Requisitos mínimos:

Además de la protección tradicionl del antivirus se requiere que el sistema propuesto incorpore, de forma integrada, la prevención, detección y solución de incidencias ante ataques e infecciones de este tipo de amenzas desconocidas y avanzadas.

- Análisis de comportamiento de los procesos que se estén ejecutando para identificar posibles amenazas.
- Gestión de lista blanca para garantizar la ejecución de programas ampliamente conocidos con posibilidad de inclusión de software propio en dicha lista. El sistema permitirá bloquear programas o restringir sus permisos, cuando no estén incluidos en listas blancas o se encuentre en listas negras.
- Análisis avandas sobre URLs y archivos descargados de Internet mediante navegación.
- Inspección de correo electrónico de forma transparente para el usuario, con análisis de ficheros adjuntos y enlaces.
- Capacidad de bloqueo o finalización del agente malicioso y posibilidad de desinfección del equipo.

Se valorará:

- Seguridad y privacidad en la gestion de los eventos. El tipo y cantidad de información que el sistema exija enviar al exterior y las medidas para garantizar la protección de dicha información.
- Análisis de reputación de ejecutables desconocidos.
- Capacidad de extacción del fichero causante de la infección.
- Creación y utilización de indicadores de compromiso.
- Inspección de protocolos.

2.3.- Análisis avanzado de código desconocido. Requisitos mínimos:

La plataforma ofertada será capaz de realizar un análisis avanzado de amenazas ejecutando código sospechoso en un entorno seguro y controlado (sandbox), para evaluar aquellos archivos que no hayan podido ser detectados por la plataforma, ni catalogados adecuamente por el antivirus y el sistema anti-amenazas.

- Análisis en sistemas operativos Microsoft Windows, Linux.
- Análisis en ejecutables, archivos comprimidos y documentos infectables para Microsoft Office y Adobe Reader.
- Integración con el resto de elementos de la solución, antivirus y anti-amenazas con comunicación automática en caso positivo.

Se valorará:

- Seguridad y privacidad de la arquitectura de la solución, en particular que la solución sea on-premise, lo que garantizaría máxima privacidad, el tipo y cantidad de información que el sistema exija enviar al exterior así como las medidas para garantizar su protección.
- Disponibilidad de API que permita que cualquier producto o persona autorizada envíe muestras y obtegan resultado de la ejecución.
- Mayor cantidad de tipos de ficheros analizables.
- Mayor número de sistemas operativos sobre los que se realiza el análisis.

2.4.- Integración del sistema y herramienta de gestión. Requisitos mínimos:

Los distintos subsistemas que se suministren deben tener la posibilidad de ser configurados a través de una herramienta de gestión que permita administrar y personalizar sus funcionalidades.

- Todos los componenetes ofertados deben formar parte de una solución completa a la que de cobertura un único fabricante para facilitar su integración, gestión y soporte.

- Integración con Directorio Activo.
- Diferentes roles de administración que permitan acceso a diversas funcionalidades de la consola.
- Gestión de políticas de configuración a dispositivos.
- Instalación, actualización y desistalación de los componenetes de la solución.
- Generación y personalziación de informes.
- Recogida de eventos de auditoría, eventos críticos, etc y notificación de los mismos.

Se valorará:

- Seguridad y privacidad de la arquitectura de la solución, en particular que la herramienta de gestión sea on-premise, lo que garantizaría máxima privacidad, si fuera una solución basada en la nube, se valorará el tipo y cantidad de información que el sistema exija enviar al exterior y las medidas para garantizar su protección.
- Consola de gestión única para administrar todas las funcionalidades solicitadas.
- Gestión con agente único en el puesto final.
- Herramienta de backup y restore integrada.
- Gestión y personalización de alertas, avisos y notificaciones.

TERCERA.- SERVICIOS DE INSTALACIÓN Y PLAZO DE EJECUCIÓN.

En el supuesto de resultar adjudicadas unas licencias de antivirus diferentes, a la que este Ayuntamiento tiene actualmente que es "ESET NOD32", el adjudicatario se debe comprometer a desinstalar de todos los equipos municipales (aproximadamente 450), el software correspondiente, dejando limpios los mismos para la nueva instalación.

El contratista deberá prestar los servicios de soporte necesarios para la puesta en marcha del proyecto, por lo que se deberán proporcionar todos los servicios necesarios para realizar la instalación y configuración del producto en la plataforma informática del Ayuntamiento, definición de políticas de seguridad, así como las tareas necesarias para la migración, en su caso, de los agentes actuales instalados en los equipos a la plataforma ofertada.

El licitador deberá presentar la planificación prevista para la completa ejecución del proyecto.

El plazo máximo para la implantación de la plataforma completa (consola de gestión y la instalación en todos los equipos de trabajo), será de 1 mes a contar desde la firma del contrato.

Deberá proporcionar toda la documentación técnica del sistema ofertado, así como la de las configuraciones instaladas.

CUARTA.- FORMACIÓN Y DOCUMENTACIÓN.

El licitador deberá incluir en su propuesta el detalle de los cursos de formación para la completa transferencia de conocimientos al personal técnico de este Ayuntamiento, con indicación del contenido y número de jornadas de que constará. Esta formación deberá ser oficial del fabricante y realizar en las instalaciones del Ayuntamiento. Se valorará el contenido y jornadas de la citada formación.

QUINTA.- GARANTÍA, SOPORTE Y MANTENIMIENTO.

La solución oferta, deberá estar garantizada por el fabricante por un plazo mínimo de cuatro años desde la fecha de instalación y activación de la plataforma completa o de la proteccción endpoint tradicional, con el fin de que la solución completa tenga una fecha única de fin de garantía, coincidiendo con la fecha de finalización del contrato.

Se dejará constancia de la fecha de inicio y fin del mantenimiento contratado en la correspondiente acta de recepción.

El licitador deberá especifidar en su oferta las condiciones del soporte indicando el procedimiento completo de gestión, tiempos de respuesta, franja horaria, etc.

Los requerimientos mínimos son los siguientes:

- Obligatoriamente el soporte técnico ofrecido por el fabricante debe ser directamente desde España.
- Posibilidad de reportar un número ilimitado de incidencis y de consultas.
- Posibilidad de recibir avisos cuando surjan alertas de seguridad de nuevo malware.
- En caso de detectarse una infección masiva, el contratista, previa petición del Ayuntamiento, deberá asignar un técnico, bien de una forma remota o presencial para ayudar en las tareas de eliminación de la infección.
- La oferta incluirá el compromiso de vida útil del sistema a adquirir por un periodo mínimo de cuatro años desde el momento de publicación del presente procedimiento de contratación.

- El mantenimiento de las licencias incluye el suministro de las nuevas versiones de los productos, así como las actualizaciones de los mismos durante el priodo contratado. Dichas versiones del producto y actualiaciones estarán accesibles a través de la web del fabricante y se podrán descargar de forma manual o automática mediante las utilidades de actualización que inclya el propio software.

- Se valorarán las concidiones de garantía, soporte y mantenimiento ofrecidas en la medida que superen los requerimientos mínimos solicitados en el presente apartado.

SEXTA.- DURACIÓN CONTRATO.

- La duración del presente contrato, será de cuatro años, por lo que el presupuesto total de estos 4 años será de (2.650,00€ x 4 = 10.600,00€), sin I.V.A, el importe del I.V.A. (21%),

es de (10.600,00 x 21% = 2.226,00€), haciendo un total I.V.A., incluido de 10.600,00€ + 2.226,00€ = 12.826,00€.

SÉPTIMA.- FORMA DE PAGO.

- La forma de pago será por facturación trimestral del servicio contratado
- Se presentará una factura a través de la plataforma Face.

OCTAVA.- DOTACIÓN PRESUPUESTARIA.

El importe de este suministro se hará con cargo al crédito existente en el Presupuesto Municipal, partida 9201.22798 .- Contratos Mantenimiento Informáticos: Administración General.

NOVENA.- PENALIZACIÓN.

- Es una obligación esencial. El retraso de 15 días en las entregas marcadas, supondrá una penalización del 10% de contrato el primer año. Un retraso de 1 mes supondrá una penalización del 20% de contrato el primer año. Un retraso en la implantación, superior a 1 mes será causa para la resolución del contrato.

DÉCIMA.- EXCLUSIÓN DEL PROCESO DE LICATACIÓN DE AQUELLAS OFERTAS QUE EN LA PROPUESTA TÉCNICA NO SE AJUSTE A LOS REQUISITOS DE LOS PLIEGOS.-

- A la hora de valorar la propuesta técnica, se excluirán aquellas ofertas que no concreten de forma suficiente, clara y extensa, los recursos utilizados.

DÉCIMOSEGUNDA.- CAUSAS ESPECÍFICAS DE RESOLUCIÓN DEL CONTRATO POR INCUMPLIMIENTO DE OBLIGACIONES ESENCIALES.

- Trasvase de conocimiento. La empresa adjudicataria atenderá a cuentas cuestiones técnicas se soliciten y se hará documentalmente a cuantas solicitudes de información e

informes sean necesarios. El no cumplimiento reiterado previo apercibimiento, será causa para la resolución del contrato.

- Si tras la puesta en marcha, las pruebas que realice el Ayuntamiento se considera que el proyecto implantado no se ajusta a lo exigido en el pliego y firmado en el contrato, será causa para la resolución del contrato.

Ciudad Real, 4 de Julio de 2.019

Fdo: Juan Vicente Guzmán González
Jefe Sección Informática.