PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SUMINISTRO DE 8.000 LICENCIAS DE ANTIVIRUS KASPERSKY PARA LA CONSEJERÍA DE INCLUSIÓN SOCIAL, JUVENTUD, FAMILIAS E IGUALDAD

1. INTRODUCCIÓN

Las soluciones antivirus son programas que tienen como función la detección y eliminación de los virus informáticos y demás programas maliciosos, en su conjunto conocidos como malware, interceptando las vías conocidas de infección y notificando posibles incidentes de seguridad. La detección se realiza principalmente comparando el código de cada archivo con una base de datos de códigos de virus ya identificados (también conocidos como firmas o vacunas), por lo que es importante actualizar con la mayor frecuencia estas bases de datos a fin de evitar que un virus nuevo no sea detectado. También a estos programas se les ha agregado funciones avanzadas, como la búsqueda de comportamientos típicos de virus, técnica conocida como heurística.

La información alojada en los sistemas de la Consejería de Inclusión Social, Juventud, Familias e Igualdad (CISJUFI) puede ser de interés para los intrusos que día a día mejoran sus técnicas para robar datos, por lo que se hace necesaria una protección total para los puestos de trabajo y servidores que los prevenga de intrusos y los proteja contra la fuga de datos.

2. OBJETO DEL CONTRATO

Constituye el objeto de este contrato el suministro de una solución antivirus de puesto de trabajo y servidor, con suscripción de actualizaciones y soporte, para la CISJUFI, incluyendo los servicios centrales, delegaciones territoriales y centros periféricos.

El plazo de vigencia del contrato será de 12 meses desde la formalización del mismo, contando siempre a partir de la finalización de la licitación anterior (2 de mayo de 2023) , con la posibilidad de una prórroga por 12 meses, y una segunda prórroga por otros 12 meses.

3. SITUACIÓN ACTUAL

La CISJUFI tiene implantadas licencias del software antivirus Kaspersky, con una vigencia hasta el 2 de mayo de 2023.

La infraestructura actual se compone de una consola de administración subdividida en varios grupos para gestionar equipos adscritos a diferentes políticas de seguridad (como servidores, equipos de formación, equipos de trabajo portátiles, etc ….). Desde cada una de esas administraciones encargadas del mantenimiento del antivirus se realizan, entre otras, las siguientes tareas:

- Administración de la consola
- Distribución de nuevas firmas de antivirus
- Revisión de los logs.

• Desinfección remota de los equipos.
• Análisis y estudio de posibles infecciones, falsos positivos, etc.

Debido al aumento de equipos que se integran en la Consejería, y en base a la experiencia de uso de dicha consola, hemos de adaptarnos a un aumento de licencias (llegando a una estimación de 8.000) y al uso de la solución de antivirus Kaspersky para un aprovechamiento de los servicios configurados y la base de conocimiento generada en los últimos años.

El parque de microordenadores se compone fundamentalmente de Windows 10, si bien todavía quedan muchos equipos con Windows XP y Windows 7 que se están sustituyendo progresivamente por Windows 10. También hay equipos, especialmente en aulas de formación, con Guadalinex. Sobre servidores también existen diferentes versiones: Windows Server 2000, 2003, 2012 y 2019.

4. PRESCRIPCIONES TÉCNICAS

- Características Principales del Suministro
    - Suministro de 8.000 licencias de antivirus. La empresa adjudicataria gestionará el suministro y registro de las licencias de antivirus a fin de que la CISJUFI adquiera la condición de licenciataria de las mismas por los años de duración del contrato, para lo que deberá realizar todas las gestiones documentales, telemáticas y materiales necesarias, incluida la subsanación de cualquier incidencia que surja.
    - Deberá, asimismo, organizar un calendario de formación para los administradores de la consola de los diferentes grupos, tratándose todas las configuraciones y políticas aplicables sobre el sistema de antivirus, así como todos los procedimientos necesarios para realizar las tareas de mantenimiento de los sistemas. Esta formación tendrá la duración suficiente para que el personal de la consejería pueda adquirir efectivamente los conocimientos a traspasar, estableciéndose un mínimo de 20 horas, pudiéndose dividir en varias convocatorias si se observa un número excesivo de asistentes para una sola.
    - De igual manera, las actualizaciones del software de gestión del antivirus (Servidor principal y consolas) deberán ser cubiertas por la adjudicataria, a razón de una sesión anual para ejecutar y coordinar dicha actualización y dar soporte frente a posibles incidencias en las diferentes consolas de administración usadas. Dicha sesión deberá tener la duración necesaria para cubrir las necesidades planteadas.
    - Posibilidad de gestión de equipos con diferentes políticas de seguridad: Servidores, aulas de formación equipos portátiles de trabajo, de sobremesa, etc ...
    - Suscripción del derecho de actualizaciones de versiones de software, de firmas y de patrones de virus para el servidor de antivirus y los equipos protegidos durante el plazo de garantía del contrato.
    - Suscripción de soporte y mantenimiento 24x7 para todas las licencias ofertadas durante el plazo de garantía del contrato. El soporte será proporcionado en castellano.

UNIÓN EUROPEA

- Administración centralizada en los servicios centrales con la posibilidad de administración delegada para cada una cada una de las provincias en su ámbito de competencia.
- La solución ofertada debe de estar ejecutada y operativa en un plazo máximo de un mes desde la firma del contrato.
- Todos los licitadores deben de ser partners oficiales de la solución antivirus Kaspersky, y esta condición se debe mantener durante la duración del contrato.
- En previsión de que la Agencia Digital de Andalucía sea el organismo que asuma la gestión de los sistemas antivirus corporativos para la Junta de Andalucía, las licencias aportadas por el adjudicatario han de poder reasignarse para cambiar la titularidad entre CISJUFI y la ADA, sin coste adicional.

- Requisitos Técnicos
  - Se debe tener una arquitectura que garantice la robustez de la solución en términos de disponibilidad, tolerancia a fallos y seguridad.
  - Soporte de funciones de supervisión y gestión centralizada.
  - Visibilidad y administración centralizada: consola con vista de panel único que permita gestionar la seguridad en el entorno corporativo, ya sea en la nube, en máquinas físicas o virtuales.
  - Gestión de políticas y amenazas.
  - Asignación de responsabilidades diferentes a diversos administradores.
  - Gestión de forma remota de las funciones de seguridad básicas a través de consola web.
  - Protección de endpoints, tanto físicos como virtualizados, con los siguientes sistemas operativos:
    - Windows XP, 7, 8, 10
    - Windows Server 2000, 2003, 2012 y 2019
    - GNU/Linux: Ubuntu, Guadalinex
  - Compatible con plataformas de virtualización como VMWare.
  - Cifrado de datos: archivos, carpetas, discos y dispositivos extraíbles, gestionado desde la consola de gestión centralizada.
  - Posibilidad de analizar unidades USB y extraíbles.
  - Posibilidad de analizar servidores de ficheros.
  -

- Posibilidad de bloquear comunicaciones de tipo comando y control (Command and Control – C&C).
- Posibilidad de detección y eliminación del malware, spyware, adware y otras amenazas, que permita aplicar múltiples opciones según el tipo de amenaza parada (limpiar el fichero, ponerlo en cuarentena, eliminar un correo o solamente el adjunto, reemplazarlo, insertar X-headers, tags, etc.)
- Método de escaneo inteligente, que no necesite la descarga continua de ficheros de patrones completos, sino que usando la información de sus cabeceras, pueda decidir si usar un patrón u otro de manera más rápida y eficiente.
- Métodos de escaneo basados en patrones tradicionales (toda la información del patrón reside en el endpoint) o escaneo inteligente (la información del patrón reside en una BBDD de reputación centralizada y accesible por los endpoints). La BBDD deberá estar ubicada en la nube y ser actualizada varias veces al día o en el momento de conocerse una nueva amenaza.
- Vulnerabilidades no parcheadas: parcheo virtual (bloqueando tráfico que intenten explotar una determinada vulnerabilidad) de las vulnerabilidades tanto de sistema operativo como de aplicativos. Escaneo previo del equipo para identificación de versiones del sistema operativo y de los aplicativos para aplicar únicamente y de manera automática los parches virtuales necesarios para proteger dicho equipo. Reportes individuales por equipos de las vulnerabilidades.
- Motor de reputación Web: detección y bloqueo de Amenazas web permitiendo la personalización de URLs a bloquear/permitir así como ajustar el nivel de agresividad de dicho motor. Dicho motor deberá permitir establecer configuraciones diferentes en función de la ubicación del endpoint (red corporativa u otra).
- Posibilidad de efectuar escaneo de archivos:
  - En tiempo real.
  - Programados.
  - Inmediatos (a demanda).
- Cada método de escaneo debe permitir excluir ficheros del mismo de manera independiente del resto de métodos de escaneo.
- Control de uso dispositivos: control de acceso a dispositivos mediante la asignación de permisos por endpoint, pudiendo configurar los dispositivos que se permiten o no se permiten utilizar al usuario.
- Aislamiento del endpoint en caso de infección latente (“Out Break”). Con capacidad de configurar umbrales de infección en el endpoint (Virus/Malware, Spyware/Grayware, Firewall blocks, Shared folder Session y comunicaciones reportadas como Command and control), para su posterior notificación y aislamiento de los equipos.

- Actualizaciones programables del producto y de los ficheros de patrones.
- Deberán poder establecerse configuraciones y políticas de escaneo distintas en función de la ubicación del endpoint (red corporativa u otra).
- Actualizaciones de la base de datos de amenazas de al menos 2 veces al día.
- Detección de equipos no gestionados por rango de redes, dominios de Windows y Active Directory
- Política de control de aplicaciones, que permita detectar y bloquear aplicaciones que no suponen una amenaza para la seguridad, pero cuyo uso no considere adecuado en la organización.

- Servicios Requeridos
  - Se deberá auditar la implantación actual y adaptarla al modelo propuesto de administración centralizada con administraciones delegadas.
  - El adjudicatario será responsable de realizar la configuración de los diferentes grupos de administración que se usarán en las diferentes delegaciones.
  - Se deberán realizar todas las pruebas que permitan validar el cumplimiento de todos y cada uno de los requerimientos técnicos de este PPT.
- Documentación entregable del proyecto
  - Documento de suministro en el que aparezca claramente recogido:
    - Denominación comercial de las licencias suministradas
    - Cantidad de licencias suministradas
    - Procedimiento detallado que debe seguirse para la instalación de las licencias
    - Fechas de inicio y de fin del mantenimiento de las licencias suministradas
  - Documento de cumplimiento del Esquema Nacional de Seguridad (ENS): documento que relacione las medidas de seguridad del ENS con las funcionalidades del producto suministrado, identificado claramente en qué contribuye cada funcionalidad del producto al cumplimiento de cada medida del ENS.
  - Documentación técnica completa de la solución ofertada, documentación técnica de la implantación y configuraciones realizadas y documentación de la formación impartida.
  - Toda la documentación debe entregarse en castellano.

5. FORMA DE PAGO

Pago único una vez suministradas las licencias.

6. IMPORTE

El importe máximo de la contratación se establece en 48.400 € (CUARENTA Y OCHO MIL CUATROCIENTOS EUROS), IVA incluido. Esa cantidad procede de la estimación del número de licencias necesarias, multiplicado por el coste estimado del precio de cada licencia anual, calculado el año de contrato:

8.000 licencias * 5 €/licencia * 1 año= 40.000 €, IVA excluido (48.400 €, IVA incluido)

El valor estimado del contrato se establece en 120.000 € (CIENTO VEINTE MIL EUROS), IVA excluido. Esa cantidad procede de la estimación del número de licencias necesarias, multiplicado por el coste estimado del precio de cada licencia anual, calculado el año inicial de contrato, más las dos posibles prórrogas:

8.000 licencias * 5 €/licencia * (1 año + 1 año + 1 año) = 120.000 €

En Sevilla, en la fecha de la firma electrónica

El Jefe del Servicio de Sistemas de Información

UNIÓN EUROPEA