ACTUALIZACIÓN LICENCIAS MCAFEE

PLIEGO DE BASES TÉCNICAS

TABLA DE CONTENIDOS

1. INTRODUCCIÓN 3
2. OBJETO DEL EXPEDIENTE 3
3. APLICACIÓN DE LAS LICENCIAS DE SOFTWARE 3
4. SOFTWARE ANTIVIRUS MCAFEE 4
5. PRESENTACIÓN DE LA OFERTA ECONOMICA 4
6. EJECUCIÓN DE LAS PRESTACIONES 5
7. CONDICIONES DE SEGURIDAD 5

1. INTRODUCCIÓN

El Decreto 6/2021, de 19 de enero, por el que se establece la estructura orgánica y funcional del Departamento de Seguridad del Gobierno Vasco, en su artículo 13, establece que corresponde a la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos (DGTSI) lo referente a la planificación, gestión y mantenimiento de los sistemas destinados a actividades de seguridad pública. Es en virtud de dicha competencia que se acomete el presente expediente.

En desarrollo de este precepto y para hacer frente a las actuales necesidades la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos precisa la actualización de las licencias de los productos de software antivirus vigentes en el departamento.

2. OBJETO DEL EXPEDIENTE

El objeto de este expediente es la actualización de licencias de software Antivirus McAfee tanto en dimensionamiento como en las prestaciones que ofrecen. Estas licencias son utilizadas por los servicios y unidades del Departamento de Seguridad.

Se pretende de esta manera proporcionar un salto de calidad al disponer de licencias con unas mayores prestaciones, así como disponer de la última versión del fabricante con soporte técnico sobre el producto, y utilizar los productos en compatibilidad con las versiones disponibles en el mercado.

3. APLICACIÓN DE LAS LICENCIAS DE SOFTWARE

El Departamento de Seguridad cuenta, entre otras medidas de seguridad desplegadas tanto en EndPoints como en servidores con una plataforma de protección basada en la solución de la empresa McAfee (ahora Trellix por la fusión de McAfee Enterprise y FireEye). Se trata de un conjunto de tecnologías de prevención que incluyen el antivirus, la prevención de intrusiones y la prevención de pérdida de datos. Se entiende como “endpoint” cualquier dispositivo informático conectado a una red.

La gestión de dicha plataforma se realiza de forma centralizada a través de la consola conocida como ePO (ePolicy Orchestrator) garantizando que antivirus y otras herramientas de seguridad funcionen juntos con controles orquestados, información compartida y flujos de trabajo automatizados.

La evolución de las amenazas de ciberseguridad y el aumento creciente de la superficie de exposición de sistemas y servicios hace que el enfoque de protección tradicional basado en la protección del endpoint, conocido como EPP no sea suficiente. Los ataques utilizan mecanismos que no son detectables por los antivirus tradicionales ya que:

- No utilizan archivos por lo cual no se pueden detectar firmas en ellos.
- Utilizan vulnerabilidades de día cero, cuentas comprometidas
- Utilizan ingeniería social e información obtenida por los infiltrados.
- Utilizan Software malicioso o especialmente diseñado, software único.

- Los ataques volátiles y dirigidos se pueden generar por los ciberdelincuentes con un coste muy bajoy mucha facilidad. Su volatilidad hace que el antivirus tradicional no los pueda detectar.
- Las técnicas de infiltración son cada vez más sofisticadas y su detección únicamente puede hacerse utilizando mecanismos de inteligencia artificial en los endpoints.

En consecuencia, es interesante completar la protección de los endpoints con mecanismos de detección y respuesta orientados a las amenazas avanzadas. La compañía Trellix cuenta con el software Mvision que complementa la solución actualmente desplegada en el Departamento de Seguridad integrándose en la misma consola de gestión, ePO. La adopción de MVision será simple ya que los agentes de McAfee están desplegados en todos los equipos del Departamento de Seguridad.

Por otra parte, se desea completar el despliegue del componente de prevención de pérdida de datos (DLP) a todos los equipos de la Organización. Una fuga de datos o Data Leakage es la pérdida de confidencialidad de la información de una organización, empresa o individuo, mediante la obtención de la misma o el conocimiento del contenido de ésta por parte de personas no autorizadas para ello.

El componente DLP permite aplicar los controles disminuyendo al máximo el riesgo de una fuga de información.

Se deberán incluir en la oferta las jornadas necesarias para la adaptación de los productos licenciados al entorno concreto del Departamento de Seguridad.

4. SOFTWARE ANTIVIRUS MCAFEE

La descripción de las licencias que se deben ofertar, incluyendo su mantenimiento, actualización y soporte durante la vigencia del contrato, es la siguiente:

DESCRIPCION	FABRICANTE	TIPO ADQUISICION	CANTIDAD
DLP: Trellix Data Loss Prevention Endpoint:	Trellix-McAfee	24 meses	2501
EDR+EDR: Trellix Protect plus EDR for Endpoint	Trellix-McAfee	24 meses	2501
Mobile: Trellix Mobile Security Advanced (Hasta 5 dispositivos por usuario)	Trellix-McAfee	24 meses	501

5. PRESENTACIÓN DE LA OFERTA ECONOMICA

La oferta económica se presentará de acuerdo con el modelo de proposición económica correspondiente.

Los importes totales de la oferta, no podrán exceder el importe máximo (Sin IVA).

6. EJECUCIÓN DE LAS PRESTACIONES

De cara al Servicio de Actualizaciones y Soporte Técnico se requerirá la entrega de la siguiente documentación:

- Documento del Certificado de Titularidad de los Productos, que acredite la disponibilidad del Servicio de Actualizaciones y Soporte Técnico de los productos de Software durante el periodo de cobertura contratado.
- Documento descriptivo del detalle de todas las prestaciones incluidas en el Servicio de Actualizaciones y Soporte Técnico de los productos de Software contratados, proporcionando los medios a emplear (Claves de activación de las licencias vía telemática, etc.) en cada producto para obtener tanto las actualizaciones de versión como su soporte técnico.

7. CONDICIONES DE SEGURIDAD

El adjudicatario se compromete a cumplir la política de Seguridad de la Información del Departamento de Seguridad del Gobierno Vasco y todas las normativas y procedimientos aplicables en el contexto del suministro.

El Departamento de Seguridad del Gobierno Vasco tendrá derecho a llevar a cabo auditorías para asegurarse de que el suministro se realiza de acuerdo a lo establecido en el presente pliego. Todo el material e información requerida para dichas inspecciones estará disponible sin restricciones.

La información facilitada para abordar los trabajos no se aplicará ni utilizará con una finalidad diferente a la que es objeto de este pliego ni el prestador del suministro la comunicará, ni siquiera a efectos de su conservación a terceros.

El adjudicatario y el personal a su cargo están obligados a guardar secreto y absoluta confidencialidad respecto de la información que les sea confiada en virtud del suministro prestado.

El adjudicatario deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de la información y eviten su alteración, pérdida, sustracción, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.

Al finalizar el contrato, y una vez haya sido transferida la información al Departamento de Seguridad del Gobierno Vasco, el adjudicatario se compromete a destruir toda la información, teniendo en cuenta los distintos soportes o documentos donde esta pueda constar: bases de datos en discos, ficheros temporales, copias de seguridad, soportes en papel, etc. A tal efecto, una vez realizada la operación descrita, entregará una declaración por escrito al Departamento de Seguridad donde conste que así se ha realizado.