



SEGURTASUN SAILA

Babes Zibileko Sailburuordetza
Telekomunikazioak eta Sistema Informatikoak
Kudeatzeko Zuzendaritza

DEPARTAMENTO DE SEGURIDAD

Viceconsejería de Protección Civil
Dirección de Gestión de Telecomunicaciones
y Sistemas Informáticos

ACTUALIZACIÓN LICENCIAS TRELLIX

PLIEGO DE BASES TÉCNICAS

TABLA DE CONTENIDOS

1.	INTRODUCCIÓN.....	3
2.	OBJETO DEL EXPEDIENTE.....	4
3.	DETALLE DE SUMINISTROS Y SERVICIOS.....	5
A)	SOFTWARE TRELLIX	6
B)	SERVICIOS	6
4.	PRESENTACIÓN DE LA OFERTA ECONOMICA	7
5.	EJECUCIÓN DE LAS PRESTACIONES	8
6.	CONDICIONES DE SEGURIDAD	9

1. INTRODUCCIÓN

El Decreto 318/2024, de 29 de octubre, por el que se establece la estructura orgánica y funcional del Departamento de Seguridad del Gobierno Vasco, en su artículo 18, establece que corresponde a la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos (DGTSI) lo referente a la planificación, elaboración, desarrollo, ejecución, gestión y mantenimiento de los sistemas de información y telecomunicaciones 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.

La evolución de las ciberamenazas requiere de una adaptación continua de las tecnologías utilizadas para mitigar los riesgos presentes en cualquier sistema IT. En este sentido, la criticidad de los servicios prestados por el Departamento de Seguridad requiere adoptar medidas específicas y rigurosas que minimicen la exposición de los activos y permitan una respuesta rápida mediante la detección avanzada de incidentes tanto derivados de ataques externos como de posibles errores de operación de los usuarios.

2. OBJETO DEL EXPEDIENTE

El Departamento de Seguridad cuenta con un sistema de protección del EndPoint basado en la solución del fabricante Trellix. Dicha plataforma se encuentra perfectamente integrada tanto en sus procedimientos de instalación y gestión como en la monitorización de la seguridad llevada a cabo por el COSSIP mediante el software de SIEM desplegado a tal efecto.

Ligada a dicho software se encuentra la solución de Data Leak Protection (DLP) que permite la detección de movimiento de ficheros cuya información pueda estar sujeta a regulación especial bien por motivos de privacidad o de confidencialidad.

Sustituir este producto por otro equivalente generaría varios inconvenientes:

- Migración de un producto a otro, lo cual supone pagar licencias de ambos productos durante un tiempo hasta que se consigue finalizar la migración. En experiencias previas con migraciones de antivirus (producto de características similares) este proceso de migración supone varios años de trabajo.
- Durante el tiempo de convivencia hay que gestionar dos plataformas, con las implicaciones que tiene a nivel de recursos humanos (técnicos que dominen ambos entornos) y de calidad del servicio (los equipos no migrados no contarán con las diferentes novedades hasta no estar en el nuevo entorno).
- La migración constituiría un proyecto en sí mismo, con una dedicación y un coste difícil de dimensionar.

El objeto de este expediente, como consecuencia de lo indicado anteriormente, es la renovación y actualización de licencias de software Trellix (fusión de McAfee Enterprise y FireEye) adaptando tanto su dimensionamiento con sus funcionalidades al estado de la tecnología.

Se pretende de esta manera proporcionar continuidad en el salto de calidad que supuso 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.

Además, se incluye dentro del objeto la migración de la solución EDR desde la plataforma SAAS ofrecida anteriormente por Trellix a un despliegue en servidores dentro del perímetro de seguridad de las comunicaciones gestionado por la DGTSI.

3. DETALLE DE SUMINISTROS Y SERVICIOS

El Departamento de Seguridad cuenta, entre otras medidas de seguridad desplegadas tanto en EndPoints –entendiendo como tal cualquier dispositivo informático conectado a una red–, como en servidores con una plataforma de protección basada en la solución de la empresa Trellix –anteriormente McAfee–. Al conjunto de tecnologías de prevención que incluyen el antivirus, la prevención de intrusiones y la prevención de pérdida de datos.

La gestión de dicha plataforma se realiza de forma centralizada a través de la consola ePO (ePolicy Orchestrator) que permite monitorizar y garantizar que tanto el antivirus como 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 ya que los ataques utilizan mecanismos que no son detectables por los antivirus tradicionales EPP por los siguientes motivos:

- 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 bajo y 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.

Por ello, se procedió a completar la protección de los endpoints con mecanismos de detección y respuesta orientados a las amenazas avanzadas con el software Mvision complementando la solución del Departamento de Seguridad integrándose en la misma consola de gestión, ePO.

Por otra parte, se ha desplegado en los equipos el componente de prevención de pérdida de datos (DLP) en 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. Esto se puede complementar, en determinados casos con la gestión del cifrado de los dispositivos extraíbles o la automatización de la clasificación de la información en determinadas carpetas objetivos que se busca conseguir con la inclusión de la suscripción de la suite “Trellix Data Security Endpoint Protection”.

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

A) SOFTWARE TRELLIX

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
<i>Endpoint Security Virtual Appliance</i>	Trellix	36 meses	1
<i>Trellix Endpoint Security Suite - Upgrade</i>	Trellix	36 meses	2501
<i>Trellix Mobile Security Advanced (Hasta 5 dispositivos por usuario)</i>	Trellix	36 meses	501
<i>Trellix Data Loss Prevention Endpoint Complete – Subscription</i>	Trellix	36 meses	2401
<i>Trellix Data Security Endpoint Protection Suite – Subscription</i>	Trellix	36 meses	100

Se entenderán como mejoras el aumento en el número de licencias ofertado tanto para “Trellix Mobile Security Advanced” como para “Trellix Data Security Endpoint Protection”.

B) SERVICIOS

Se incluirán en el expediente los siguientes servicios:

- al menos 40 jornadas de servicios profesionales para acometer la implantación y la migración entorno on-premise del Servidor que de soporte al producto EDR en modalidad virtual en la infraestructura del Departamento de Seguridad (Licenciamiento, Configuración, Integración con ePO del cliente, piloto, despliegue, etc.).
- jornadas necesarias para la puesta en marcha de los nuevos componentes software incluidos en la solución.
- jornadas para la revisión periódica de los diferentes módulos desplegados en la EPO, actualizaciones, ajustes de políticas, evolución de DLP, identificación de áreas de mejora, etc.

Estos servicios se realizarán por un perfil consultor con experiencia en proyectos de software del fabricante Trellix.

4. 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).

5. 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.

6. 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.