

**PLIEGO DE PRESCRIPCIONES TÉCNICAS
PARTICULARES PARA LA CONTRATACIÓN DEL
SUMINISTRO Y DEL SOPORTE TÉCNICO DE LAS
LICENCIAS ANTIMALWARE DE LOS PC ´S,
PORTÁTILES, SERVIDORES Y TABLETS
MEDIANTE PROCEDIMIENTO ABIERTO**



EXPEDIENTE: 2023.73

27/07/2023 (Versión 0)



INDICE

1.	OBJETO	3
2.	REQUISITOS MÍNIMOS DE LA SOLUCIÓN TÉCNICA	3
3.	PLAN DE FORMACIÓN	5
4.	CONDICIONES DE SUMINISTRO	5
5.	SERVICIOS DE SOPORTE TÉCNICO	6
6.	VALIDACIÓN Y VERIFICACIÓN PRESENCIAL DE PROPUESTA	6
7.	PENALIZACIONES.....	7
8.	DOCUMENTACIÓN A PRESENTAR POR LAS ENTIDADES LICITADORAS.....	7
8.1	SOBRE C.- DOCUMENTACIÓN RELATIVA A LOS CRITERIOS DE ADJUDICACIÓN VALORADOS MEDIANTE JUICIO DE VALOR.....	7
8.2	SOBRE B.- DOCUMENTACIÓN RELATIVA A LA OFERTA EVALUABLE AUTOMÁTICAMENTE A TRAVÉS DE FÓRMULAS.	7



1. OBJETO

El objeto del contrato al que se refiere el presente pliego lo constituye el suministro y el posterior soporte técnico de las licencias antimalware de los PC's de usuario, portátiles, servidores y tablets de EITB MEDIA, S.A.U. (en adelante, **EITB MEDIA, Entidad Contratante o EC**, indistintamente).

La prestación de los servicios se deberá efectuar con arreglo a los requerimientos y condiciones que se estipulan en este Pliego de Prescripciones Técnicas Particulares (PPTP), así como el correspondiente Pliego de Cláusulas Administrativas Particulares (en adelante, PCAP), relativas a la presente contratación, de los que se derivan los derechos y obligaciones de las partes contratantes.

2. REQUISITOS MÍNIMOS DE LA SOLUCIÓN TÉCNICA

La solución objeto de la presente contratación deberá cumplir con, al menos, los siguientes requerimientos y condiciones mínimas de integración con el sistema de seguridad o SIEM (acrónimo de *Security Information and Event Management*):

- Las licencias serán compatibles con los sistemas operativos de los PC's, portátiles, tabletas y servidores físicos y virtuales (con VMWARE 7) de la EC: Microsoft (Windows 2008 / 2012 / 2016 / 2019 y 2022, Windows 7 (residual) y Windows 10 y 11 en versiones servidor y cliente en cada caso); SUSE Linux Enterprise 12 [x64] y Oracle Linux 6, 7 y 8 [x64]; macOS 10 / Monterrey / Ventura; y Android 9.
- Será requisito disponer de una API que permita desencadenar acciones en el sistema antivirus (AV) desde SIEM, cortafuegos, u otros elementos de seguridad y viceversa. Esta funcionalidad es opcional desde el punto de vista del AV, pero deberá estar disponible para facilitar la integración y la realización de acciones automatizadas.
- La solución técnica propuesta deberá estar activa permanentemente, analizando y protegiendo los procesos en ejecución en los equipos.

También deberá permitir lanzar análisis personalizables bajo demanda.

- Deberá integrarse con el Directorio Activo de la EC.
- Deberá ser ligera y no sobrecargar los sistemas individuales ni la red.
- Deberá permitir la actualización continua y automática a las últimas versiones de las licencias.
- Deberá permitir que cualquier PC que tenga o no conectividad con Internet se actualice automáticamente sin necesidad de acceso a la consola.
- Deberá dar protección de todo tipo de Malware, incluyendo virus, troyanos, spyware, rootkits, Adware, vigilancia de contenido Web (http, cachés, etc.), Correo, Aplicaciones, por comportamiento, etc.
- La solución técnica propuesta incluirá DLP y EDR en la solución de puesto, permitiendo notificaciones y trazas.



- Deberá permitir definir y aplicar reglas proactivas sobre tipos de archivos y directorios.

También deberá poder definir exclusiones.

- Deberá tener políticas de distribución y configuración de puestos personalizables.
- Deberá controlar y gestionar los dispositivos periféricos tales como USB´s, lectora de tarjetas y otros periféricos que sean susceptibles de ser conectados.

Además, deberá integrar en el SIEM los eventos registrados por los agentes.

Concretamente, los eventos que deberán incluir son los siguientes:

- Detecciones de virus y malware: envío de alertas al SIEM cuando se detecten y bloqueen amenazas en el sistema.
- Escaneo de archivos: envío de registros de los archivos escaneados, así como los resultados del análisis, incluyendo si se encontró alguna amenaza.
- Actualizaciones de antivirus: envío de alertas al SIEM cuando se descargue e instale una actualización de definiciones de virus o una actualización del software antivirus.
- Acciones del usuario: envío de eventos al SIEM cuando un usuario realice una acción que pueda comprometer la seguridad, como descargar un archivo sospechoso o hacer clic en un enlace malicioso.
- Otros tipos de eventos:
 - Creación o eliminación de procesos: envío de alertas cuando se creen o eliminen procesos en el sistema, lo que puede indicar actividad maliciosa.
 - Cambios en el registro: envío de alertas cuando se realicen cambios en el registro del sistema, lo que puede indicar actividad maliciosa.
 - Conexiones de red: envío de registros de las conexiones de red establecidas por procesos en el sistema, lo que puede indicar actividad maliciosa.
 - Cambios en archivos de sistema: envío de alertas cuando se realicen cambios en archivos de sistema críticos, lo que puede indicar actividad maliciosa.
 - Autenticación de usuarios: envío de registros de los intentos de autenticación de usuarios, lo que puede indicar intentos de intrusión.

En relación a los requisitos mínimos del sistema de gestión de la solución (consola de gestión) deberá contar con:

- ✓ Administración centralizada. Existirá la posibilidad de distribución por las Sedes.
- ✓ Gestión completa del sistema desde la consola.
- ✓ Informes personalizables por la EC.
- ✓ Autodiscover.



- ✓ Deberá mostrar información relacionada con el usuario logeado, IP y la versión del S.O. de la estación, servidor, portátil o tablet.
- ✓ En cualquiera de los equipos protegidos se deberá podrá llevar a cabo una desinstalación/instalación manual basada en Scripts o comandos del agente y protección.

En relación a los requisitos de la solución en cuanto a distribución de protecciones deberá:

- ✓ La distribución del software de la solución deberá ser modular personalizable.
- ✓ Permitir la desinstalación de antivirus de terceros.
- ✓ Permitir la creación de paquetes MSI o EXE para su posterior distribución, tanto del agente como de la protección.

De conformidad con el ESQUEMA NACIONAL DE SEGURIDAD y el Plan de adaptación de EITB, la solución deberá necesariamente estar incluida en el "*Catálogo de productos de seguridad de las tecnologías de la información y la comunicación*" (cpstic) publicado por el CCN (Centro Criptográfico Nacional) en [HTTPS://WWW.CCN-CERT.CNI.ES/SEGURIDAD-AL-DIA/COMUNICADOS-CCN-CERT/5524-CATALOGO-DE-PRODUCTOS-DE-SEGURIDAD-TIC-CPSTIC-RECOMENDADOS-POR-EL-CENTRO-CRIPTOLOGICO-NACIONAL.HTML](https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/5524-catalogo-de-productos-de-seguridad-tic-cpstic-recomendados-por-el-centro-criptologico-nacional.html), dentro de la familia de protección del puesto de trabajo cualificado con al menos ENS ALTA.

Asimismo, de conformidad con los criterios de adjudicación definidos en el PCAP, en relación a la solución técnica se valorarán en los términos las siguientes funcionalidades adicionales, de valor añadido:

- El control y la protección de vulnerabilidades conocidas del S.O. y aplicaciones.
- La realización de análisis de vulnerabilidades y envío de informes con los resultados al SIEM.
- La posibilidad de configurar las notificaciones en los puestos (*Popup*, email, opcionalmente SNMP, etc.) con otros idiomas al original del producto.
- La posibilidad de integración con los sistemas SYSLOG y SNMP de la EC.
- La posibilidad de interactuar desde soluciones perimetrales hacia los puestos ejecutando acciones preventivas y/o reactivas. (análisis del puesto, etc.)

3. PLAN DE FORMACIÓN

La presente contratación comprenderá la realización por la adjudicataria de, al menos, UN (1) curso de formación sobre la solución técnica para CUATRO (4) personas de:

- ✓ Mínimo una jornada de SIETE (7) horas.

4. CONDICIONES DE SUMINISTRO

La presente contratación comprenderá el suministro de licencias en las siguientes condiciones:



- Número de licencias para PC's, portátiles, servidores y tablets hasta un máximo de 1800 unidades (actualmente se disponen de 1550 equipos).
- El plazo de suministro y su instalación en los diferentes PC's, portátiles, servidores y tablets no podrá exceder del plazo de QUINCE (15) días laborales a contar desde el día siguiente a la formalización del contrato.

La EC indicará a la adjudicataria, aquellos equipos que excepcionalmente por razones de operativa y producción no pueden ser instalados en los plazos indicados. En estos casos, la planificación se realizará de común acuerdo con la EC.

- La adjudicataria deberá ejecutar la migración a la nueva solución y para todos los equipos desde la sede de Bilbao en colaboración con el responsable de la EC dentro de las siguientes franjas horarias:
 - ✓ De 09:00 a 17:00 horas.

En algunos casos teniendo en cuenta la criticidad de las aplicaciones que corren sobre los servidores de la EC, la instalación de las licencias en los mismos deberá realizarse fuera del horario anterior según indicaciones de la EC.

5. SERVICIOS DE SOPORTE TÉCNICO

La presente contratación comprenderá, al menos, la realización de los siguientes servicios de soporte técnico:

- Atención telefónica las 24 horas del día los 7 días de la semana en euskera y castellano.
- UNA (1) asistencia mensual "in situ" de 6 horas en la Sede de la EC en Bilbao.
- DOS (2) asistencias de emergencia como máximo al año. La EC podrá utilizar las asistencias mensuales como asistencias de emergencia.

(Nota: En atención a las necesidades la EC se reserva la facultad de compensar, sin superar en número descrito, las asistencias de emergencia a utilizar con las asistencias mensuales).

Asimismo, de acuerdo con los trabajos y términos de prestación objeto de la presente contratación, las candidatas deberán contar y acreditar las siguientes condiciones NECESARIAS:

- Ser fabricante o distribuidor autorizado del equipamiento objeto de la presente contratación, así como, de los servicios de soporte en los términos solicitados en este pliego y el PCAP.

6. VALIDACIÓN Y VERIFICACIÓN PRESENCIAL DE PROPUESTA

A fin de verificar y valorar en los términos previstos en el PCAP, cada una de las soluciones técnicas propuestas la comisión técnica constituida al efecto procederá a



efectuar a cada una de las entidades candidatas una “prueba de concepto, valoración y verificación técnica” (en lo sucesivo, Prueba).

Esta prueba tendrá por objeto la validación, verificación y evaluación por la comisión técnica de la solución propuesta.

A efectos de valorar la solución ofertada, la EC, previa convocatoria, realizará una prueba a cada producto ofertado. Para ello, la EC creará una infraestructura física (maqueta) de las siguientes características:

- a) VEINTE (20) equipos de la EC conectados en red y de diferentes usuarios de diferentes áreas del Grupo EITB.
- b) Consola o consolas en función de la arquitectura propuesta por el ofertante.

Las candidatas deberán indicar la plataforma necesaria para el despliegue de la maqueta. La EC dotará a la maqueta de los elementos hardware necesarios para la implementación de la misma. Esta maqueta podrá llegar a convertirse en el entorno productivo.

De todo lo actuado se dejará constancia en el correspondiente expediente. La no consecución de la puesta en marcha de la maqueta implicará de forma automática la exclusión de los ofertantes que hayan propuesto el producto.

Las Pruebas se efectuarán en la Sede de la EC en Bilbao en un periodo comprendido entre el 2 de octubre y el 3 de noviembre de 2023.

Estas fechas podrán ser modificadas en función del número de candidatas. En dicho caso, se procederá a publicar el correspondiente anuncio de modificación de fechas.

7. PENALIZACIONES

Serán las establecidas en el Punto **13.- PENALIDADES** del apartado Cláusulas Específicas del Pliego de Cláusulas Administrativas Particulares (PCAP).

8. DOCUMENTACIÓN A PRESENTAR POR LAS ENTIDADES LICITADORAS

Las entidades licitadoras deberán de acuerdo con lo dispuesto en el cláusula 24 de las cláusulas específicas del PCAP.

8.1 SOBRE C.- DOCUMENTACIÓN relativa a los criterios de adjudicación valorados mediante juicio de valor

De conformidad con los criterios de valoración fijados en el PCAP, las entidades candidatas deberán incluir en el **SOBRE C**, una propuesta que contenga la documentación señalada en el en el **ANEXO IV.1** del PCAP.

8.2 SOBRE B.- DOCUMENTACIÓN relativa a la oferta evaluable automáticamente a través de fórmulas.



Las entidades presentarán sus ofertas ajustándose al modelo de tabla indicado en el **ANEXO III.1** del Pliego de Cláusulas Administrativas Particulares: FÓRMULAS MATEMÁTICAS.