

Pliego de prescripciones técnicas

DOUE-2026-125

Plataforma de Ciberseguridad: SIEM + SOC + EDR/XDR

1 Objeto del contrato

El objeto del presente pliego es la contratación de una solución integral de ciberseguridad basada en una plataforma de protección del endpoint y gestión de eventos (capacidades EPP/EDR/XDR y SIEM), la cual contemplará los siguientes requisitos:

- **Plataforma Nativa y Unificada:** El componente de protección del endpoint (EPP/EDR/XDR) y el componente de gestión y correlación de eventos (Next-Gen SIEM) deberán ser herramientas nativas del mismo fabricante. Ambas capacidades se operarán, visualizarán e investigarán obligatoriamente desde una única interfaz web de gestión (consola centralizada), descartándose propuestas basadas en la integración de plataformas independientes o de distintos fabricantes.
- **Arquitectura Cloud Nativa:** Toda la infraestructura tecnológica asociada a la plataforma unificada deberá estar basada en un modelo de arquitectura 100% Cloud Nativa bajo modalidad SaaS (Software as a Service).
- **Despliegue de tecnología de protección avanzada:** Suministro y configuración de licencias EPP/EDR/XDR para la protección de los activos de la organización corporativa.
- **Gestión inteligente de eventos:** Recogida, correlación, enriquecimiento, almacenamiento, explotación y análisis automatizado de logs y eventos de seguridad a través del SIEM.
- **Servicio Gestionado de Operaciones de Seguridad (SOC) 24x7x365:** Monitorización continua, detección proactiva de amenazas, análisis experto de alertas y gestión integral de incidentes de seguridad en tiempo real.
- **Capacidades avanzadas de respuesta:** Contención, aislamiento de amenazas y remediación activa de incidentes sobre los entornos afectados.
- **Integración tecnológica:** Conexión e interoperabilidad nativa con los sistemas, aplicaciones y plataformas existentes en la organización.
- **Ciclo de vida del servicio:** Soporte técnico especializado, seguimiento de Niveles de Servicio (SLAs), gobernanza y mejora continua durante toda la vigencia del contrato.
- **Cualificación en el Catálogo CPSTIC (ENS):**

La solución de protección de Endpoint (EPP/EDR/XDR) deberá disponer de cualificación vigente en el Catálogo CPSTIC del CCN para sistemas ENS Categoría **Alta**. Este requisito tiene como finalidad garantizar que la solución propuesta ha sido sometida a procesos de evaluación independientes y dispone de las garantías de seguridad exigidas por el CCN para su despliegue en entornos de alta exigencia.
- La solución propuesta deberá facilitar el cumplimiento de los controles aplicables del Esquema Nacional de Seguridad (ENS) en Categoría Media, especialmente en materia de:
 - Monitorización continua.
 - Gestión de incidentes.
 - Registro y conservación de eventos.
 - Trazabilidad de acciones.
 - Control de accesos.
 - Generación de evidencias para auditoría.

2 Infraestructura actual

Para el correcto dimensionamiento técnico y económico de la solución SaaS, así como para la estimación de las capacidades de monitorización del servicio de SOC, se detalla a continuación el parque informático y los sistemas perimetrales activos de la organización:

Puestos de Trabajo (Endpoints):

- 140 Endpoints (Puestos de Trabajo): Equipos portátiles y de sobremesa corporativos que operan en modalidad presencial y en modalidad de teletrabajo.
- **Servidores de Infraestructura Central** (6 servidores): Servidores basados en sistema operativo Windows Server que alojan los servicios e infraestructura centralizados de la organización (incluyendo Controladores de Dominio / Active Directory).
- **Dispositivos Móviles Corporativos (87 unidades):** 80 dispositivos Android (Samsung) distribuidos en modalidad COPE (*Corporate-Owned Personally-Enabled*) y 7 dispositivos iOS (iPhone). Se dispone de 80 licencias Antivirus para los dispositivos Android.

Seguridad de Red Perimetral:

- 2 x FortiGate 201E en HA.
- CDN (Content Delivery Network) para la WEB.
- Proxy inverso Apache.

Identidad: Entorno híbrido compuesto por un Directorio Activo Local (Active Directory On-Premise) sincronizado de forma nativa con Microsoft Entra ID (Azure AD) bajo licenciamiento corporativo Microsoft 365 (110 usuarios bajo perfil Business Basic / Standard) con capacidades Entra ID P1.

Plataforma SIEM actual (A sustituir):

- **Plataforma SIEM y SOC de procedencia:** Servicio prestado actualmente por la herramienta MonICA SIEM.
- **Fuentes de Logs e Integraciones Activas:** El nuevo componente SIEM deberá asumir de manera nativa la ingesta de eventos de las siguientes fuentes actuales:
 - Directorio Activo Local (Active Directory On-Premise).
 - Microsoft Entra ID.
 - Eventos y tráfico perimetral de la infraestructura de Firewalls FortiGate (2 equipos FortiGate en alta disponibilidad).
 - Apache (Proxy Reverse).
- **Volumen actual de eventos de seguridad:** La plataforma SIEM actualmente procesa aproximadamente entre 17 y 22 millones de eventos semanales (datos obtenidos del informe semanal del SIEM actual desde 26-04-2026 al 18/07/2026)

La distribución aproximada por tipología de fuente es la siguiente:

- Auditoría e identidades (AU): entre 10 y 15 millones de eventos semanales.
- Firewalls y seguridad perimetral (FW): entre 4 y 6,5 millones de eventos semanales.
- Aplicaciones y servicios corporativos (APPS): entre 300.000 y 550.000 eventos semanales.
- Apache: entre 2.000 y 11.000 eventos semanales.
- VPN: entre 2.000 y 3.500 eventos semanales.

Estos valores se facilitan únicamente a efectos orientativos para el dimensionamiento de la solución y podrán variar durante la vigencia del contrato en función de la evolución de la infraestructura y de las fuentes de información monitorizadas.

Las propuestas deberán contemplar la capacidad necesaria para asumir el crecimiento de las fuentes de información y del volumen de eventos durante la vigencia del contrato

3 Alcance de la solución

El adjudicatario deberá proveer una solución integral "llave en mano" en modalidad de servicio gestionado que articule de manera nativa los siguientes tres bloques operativos fundamentales, cuyas especificaciones detalladas se desarrollan en el apartado de Funcionalidades Obligatorias de este pliego:

3.1. Plataforma Tecnológica Unificada (SaaS): Suministro, despliegue y configuración en la nube de las licencias necesarias para cubrir la totalidad de la infraestructura declarada en este pliego, integrando de forma nativa las capacidades de Protección Avanzada del Endpoint (EPP/EDR/XDR) y la Gestión de Eventos de Seguridad SIEM bajo una misma consola de gestión del mismo fabricante.

3.2. Servicio Operativo de SOC Gestionado (24x7x365): Operación humana ininterrumpida de la plataforma tecnológica por parte de un equipo de analistas de seguridad especializado. El alcance del servicio cubrirá la monitorización continua, la clasificación y priorización de alertas, el escalado protocolizado de incidentes y el acompañamiento técnico a la organización en procesos de auditoría del Esquema Nacional de Seguridad (ENS).

3.3. Capacidades Avanzadas de Respuesta y Proactividad (MDR): Ejecución de tareas proactivas de caza de amenazas (*Threat Hunting*), enriquecimiento mediante inteligencia de fuentes de amenazas corporativas y, fundamentalmente, la capacidad de ejecutar de manera delegada acciones inmediatas de respuesta ante incidentes críticos (tales como el aislamiento remoto de activos afectados corporativos y tareas de remediación).

4 Funcionalidades obligatorias

La solución deberá proporcionar las siguientes capacidades:

a. Inventario de software

- Descubrimiento automático.
- Inventario centralizado.
- Identificación de software no autorizado.
- Informes de cumplimiento.

b. Control de dispositivos USB

- Bloqueo por defecto.
- Listas blancas.
- Gestión centralizada de excepciones.
- Auditoría de uso.

c. Control de aplicaciones

- Application Control.
- Listas blancas y listas negras.
- Restricción de ejecución de aplicaciones no autorizadas.

5 Integraciones requeridas para el SIEM

La solución deberá integrar, como mínimo:

a. Integración obligatoria

- Active Directory On-Premise.
- Microsoft 365: integración nativa con sus principales servicios, incluyendo como mínimo Microsoft Entra ID, SharePoint, OneDrive y Exchange.
- FortiGate.
- Proxy Reverse Apache.
- Estaciones de trabajo y Servidores.

Deberá permitir:

- Correlación de eventos de seguridad procedentes de Microsoft 365.
- Detección de accesos anómalos.
- Detección de comportamientos sospechosos.
- Generación de alertas e incidentes para el SOC.
- Consulta y análisis histórico de eventos.

6 Requisitos de arquitectura

La solución deberá:

- Minimizar infraestructuras on-premise.
- Evitar dependencias de VPN específicas para la recogida de eventos cloud.
- Utilizar conectores nativos cuando sea posible.
- Garantizar alta disponibilidad.
- Garantizar continuidad del servicio.

7 Objetivos principales

- Implantar solución **SaaS**
- **Unificación en una única plataforma**
- Ampliación de fuentes de log.

Permitir la incorporación de nuevas fuentes de información sin costes adicionales de licenciamiento por el uso de conectores estándar.

- Mejora de la correlación y detección.

8 Objetivos específicos

- SOC gestionado **24x7x365**
- Eliminación de costes adicionales de ingesta.
- Mejora del análisis de:
 - SharePoint.
 - Servidores de datos.

9 Requisitos funcionales

a. Capacidades de seguridad endpoint (EDR/XDR)

Obligatorio:

- Inventario de software.
- Control de dispositivos USB, con capacidad de crear listas blancas.

- Protección anti-malware avanzada.
- Control de aplicaciones (Listas blancas y negras).
- Capacidad de detección y respuesta XDR.
- Capacidades de bloqueo, contención y respuesta integradas de forma nativa en la solución, utilizando el mismo agente y la misma consola de gestión, sin requerir herramientas adicionales de terceros, plataformas externas de orquestación ni desarrollos específicos para su ejecución.

b. SIEM / Plataforma de monitorización

- Integración de múltiples fuentes:
 - Plataforma EPP/EDR/XDR incluida en la oferta.
 - Active Directory On-Premise.
 - Firewalls (FortiGate).
 - Endpoints.
 - Proxy Apache.
 - Microsoft 365: integración nativa con sus principales servicios, incluyendo como mínimo: Microsoft Entra ID, SharePoint, OneDrive y Exchange, permitiendo la recogida de eventos de auditoría y seguridad mediante conectores o APIs oficiales del fabricante, sin requerir infraestructuras adicionales para la captura de los eventos.
- Dashboards e informes orientados a auditoría y cumplimiento ENS.
- Capacidades de ingesta y correlación de eventos: Deberá permitir la recopilación, normalización, enriquecimiento, almacenamiento y correlación de eventos de seguridad procedentes tanto de la solución EDR/XDR como de sistemas, aplicaciones, servicios cloud y dispositivos de terceros.
Deberá cumplir:
 - Correlación avanzada de eventos
 - Integración de fuentes de información mediante mecanismos estándar, incluyendo Syslog, APIs REST, conectores nativos, formatos estándar de intercambio de eventos y otros métodos equivalentes.
 - Permitir la incorporación de nuevas fuentes de información sin necesidad de desarrollos complejos ni de infraestructuras adicionales, utilizando preferentemente conectores o APIs soportadas por el fabricante.
 - Almacenar y correlacionar de forma conjunta la información procedente de la plataforma EDR/XDR y de las fuentes externas integradas.
 - Permitir la creación de reglas de correlación, casos de uso, automatizaciones y alertas combinando información procedente de cualquier fuente integrada.
 - Permitir la incorporación de nuevas fuentes de información sin costes adicionales de licenciamiento por el uso de conectores estándar.
- Retención de logs: Deberá disponer de una capacidad de retención mínima de eventos de seguridad de 12 meses, permitiendo su consulta, explotación e investigación durante todo el periodo de conservación.

9.1 SOC (Security Operations Center)

9.1.1 Cobertura del servicio

El servicio SOC deberá prestarse de forma continua durante las 24 horas del día, 7 días a la semana y 365 días al año (24x7x365).

La prestación del servicio deberá realizarse por analistas especializados en ciberseguridad, encargados de la supervisión continua de la plataforma, la validación de alertas, la investigación y gestión de incidentes de seguridad.

El servicio deberá prestarse en idioma castellano o euskera.

9.1.2 Capacidades mínimas

El servicio deberá incluir como mínimo:

- Monitorización continua.
- Análisis y validación de alertas.
- Clasificación y priorización de incidentes.
- Escalado a los responsables designados por BEC.
- Investigación de incidentes.
- Inteligencia de amenazas (Threat Hunting).
- Recomendaciones de mitigación y remediación.
- Elaboración de informes periódicos.
- Apoyo en investigaciones forenses básicas cuando resulte necesario.

El adjudicatario deberá acreditar la participación activa de su Centro de Operaciones de Seguridad (SOC) en la Red Nacional de SOC (RNS) promovida por el Centro Criptológico Nacional (CCN) o en aquellas iniciativas de colaboración oficiales que la sustituyan durante la vigencia del contrato.

Asimismo, deberá describir el nivel de participación de su SOC, indicando, como mínimo:

- Modalidad de adhesión o pertenencia.
- Años de participación.
- Actividades de colaboración realizadas.
- Mecanismos de intercambio de información e inteligencia de amenazas.
- Procedimientos de coordinación con organismos públicos de ciberseguridad.

9.1.3 Niveles de Servicio SLA

Los tiempos comenzarán a computarse desde la validación de la alerta por parte del SOC.

Severidad Incidentes	Tiempo máximo de notificación
Crítica	30 minutos
Alta	1 hora
Media	4 horas
Baja	1 día laborable

9.1.4 Canales de comunicación

El adjudicatario deberá disponer de mecanismos de comunicación con la organización mediante:

- Correo electrónico.
- Plataforma de ticketing.
- Teléfono para incidencias críticas.

9.1.5 Reporting

El servicio deberá proporcionar:

- Informe mensual de actividad.
- Informe individual de cada incidente de severidad alta o crítica.
- Reuniones periódicas de revisión del servicio.

El adjudicatario deberá colaborar con la organización durante los procesos de auditoría ENS, proporcionando evidencias, informes, registros e información técnica relacionada con el servicio prestado. El servicio SOC deberá estar prestado por personal especializado del adjudicatario, no siendo suficiente la mera provisión de herramientas automatizadas de monitorización.

El servicio deberá incluir capacidades MDR, contemplando acciones de investigación, contención y apoyo a la remediación de incidentes de seguridad.

10 Requisitos técnicos

- Arquitectura **100% SaaS**.
- Consola única de gestión.
- APIs para integración.
- Alta disponibilidad.
- Cumplimiento RGPD.
- Datacenters en UE.

11 Requisitos de cumplimiento (ENS)

La solución deberá facilitar el cumplimiento de los controles aplicables al **ENS Nivel Medio**, los licitadores deberán describir:

- Certificaciones de seguridad disponibles.
- Procedimientos de gestión de incidentes.
- Medidas de trazabilidad y auditoría.
- Mecanismos de control de acceso.
- Gestión de evidencias.
- Ubicación de los datos.
- Cumplimiento RGPD.

12 Criterio de valoración por juicio valor: Plan de implantación (10 puntos)-A INCLUIR EN SOBRE 2

El adjudicatario deberá incluir un plan de implantación detallado que garantice la puesta en marcha de la solución minimizando el impacto sobre los servicios de producción y asegurando la continuidad de las capacidades de monitorización y respuesta durante todo el proceso de transición, también se deberá detallar los plazos previstos para cada una de las fases del proyecto.

Deberá contemplar:

- Análisis y toma de requisitos.
- Diseño de la arquitectura propuesta.
- Despliegue de la plataforma SaaS.
- Integración de las fuentes de eventos.
- Puesta en servicio del SIEM.
- Activación del SOC.
- Implantación de la solución EPP/EDR.
- Periodo de validación y ajuste.

La documentación técnica presentada por el licitador deberá ser clara, estructurada y suficiente para acreditar el cumplimiento de los requisitos establecidos en el presente pliego. Tendrá una extensión máxima de 60 páginas, excluyéndose del cómputo:

- Portada e índice.
- Anexo I de cumplimiento de requisitos.
- Fichas técnicas oficiales de fabricante.
- Certificaciones.
- Documentación acreditativa de CPSTIC.

La información que exceda del límite establecido podrá no ser tenida en consideración durante el proceso de evaluación.

Los requisitos técnicos mínimos se evaluarán tomando como base la información aportada por el licitador en el "Anexo I" -A INCLUIR EN SOBRE 2- así como en la documentación técnica complementaria presentada para acreditar los requisitos declarados

12.1 Enfoque

Implantación progresiva:

- Fase 1: Despliegue de la plataforma SaaS.
- Fase 2: SIEM + SOC.
- Fase 3: Endpoints.

12.2 Consideraciones

- Debe coexistir temporalmente con las herramientas actuales.
- Minimizar impacto en producción.
- Fecha límite para la implantación de los EPP/EDR 08/01/2027.
- Fecha límite para la implantación de las fuentes en el SIEM 31/01/2027.

13. Formación

El adjudicatario deberá impartir formación técnica a los administradores designados por BEC sobre:

- Uso de la consola.
- Investigación de incidentes.
- Consulta de eventos.
- Generación de informes.
- Operación básica de la plataforma.

14. Otros criterios de valoración por formula (25 puntos)-A INCLUIR EN SOBRE 3

Quedarán excluidas aquellas propuestas que no cumplan con el mínimo requerido en este pliego.

Puntuación máxima por categoría:

Concepto	Puntuación máxima
Capacidades básicas DLP	5
Threat Hunting	5
Experiencia y madurez SOC	5
Asistencia presencial: Tiempo de respuesta	5
Asistencia presencial: Precio por hora	5
Total	25

14.1. Criterios de valoración técnica

Los licitadores deberán indicar para cada requisito si cumplen o no cumplen, identificando la funcionalidad, módulo o componente de la solución que proporciona dicho cumplimiento y la referencia documental correspondiente.

BEC podrá requerir a los licitadores la realización de una demostración funcional de la solución ofertada, con el objeto de verificar las funcionalidades declaradas en la documentación técnica. La demostración no podrá modificar la oferta presentada ni incorporar funcionalidades no incluidas en la misma.

14.2. Capacidades básicas DLP

Se valorará la incorporación de capacidades básicas de supervisión y protección de la información que permitan:

- Detectar descargas masivas desde SharePoint o OneDrive.
- Detectar accesos anómalos a información corporativa.
- Identificar comportamientos potencialmente asociados a exfiltración de información.
- Generar alertas e incidentes para su análisis por el SOC.

Criterio	Puntos
No dispone de capacidades de supervisión en entornos de colaboración en la nube	0
Supervisión de SharePoint	1
Supervisión de SharePoint, OneDrive y Exchange	3
Correlación con SIEM y generación automática de incidentes al SOC , a partir de eventos detectados en SharePoint, o Exchange relacionados con accesos anómalos, descargas masivas, transferencias de información o comportamientos potencialmente asociados a fuga de datos	5

14.3. Threat Hunting

Se valorarán las capacidades adicionales del servicio Threat Hunting sobre los requisitos mínimos exigidos, los licitadores deben presentar las evidencias del servicio para la valoración de puntos.

Criterio	Puntos
Cumple el mínimo obligatorio	0
Threat Hunting proactivo periódico	2
Threat Hunting continuo basado en inteligencia de amenazas	5

14.4. Experiencia y madurez SOC

Criterio	Puntos
Miembro de la Red Nacional de SOC - Categoría Bronce	1
Miembro de la Red Nacional de SOC - Categoría Plata	3
Miembro de la Red Nacional de SOC - Categoría Oro	5

14.5. Asistencia presencial ante incidentes críticos

Se valorará la capacidad del adjudicatario para proporcionar asistencia técnica presencial en las instalaciones de BEC ante incidentes de ciberseguridad clasificados como críticos que requieran intervención inmediata.

Se considerarán incidentes críticos aquellos que impliquen la indisponibilidad de servicios esenciales, el compromiso de sistemas críticos, ataques de ransomware, la exfiltración de información sensible o cualquier otra situación que requiera una intervención presencial.

El licitador deberá indicar el tiempo máximo garantizado de llegada desde la activación del servicio, valorándose especialmente tiempos inferiores a 2 horas.

El licitador deberá indicar:

- Tiempo máximo garantizado de llegada a las instalaciones.
- Horario de prestación del servicio.
- Perfil técnico del personal desplazado.
- Precio por hora de asistencia presencial.

La valoración se realizará de la siguiente forma:

- Tiempo de respuesta: hasta 5 puntos.
- Precio de la hora de asistencia: hasta 5 puntos.

La puntuación económica se calculará mediante la fórmula:

$$P = (P_{\text{mín}} / P_{\text{of}}) \times 5$$

Donde:

P = puntuación obtenida.

P_{mín} = precio hora más bajo admitido.

P_{of} = precio hora ofertado por el licitador.

Asimismo, deberá especificar las tarifas aplicables a los servicios de asistencia presencial, incluyendo coste horario y posibles gastos asociados.

Tiempo de respuesta in situ	Puntos
No ofrece servicio	0
Superior a 4 horas	1
Entre 2 y 4 horas	2
Igual o inferior a 2 horas	5

Precio hora asistencia especializada	Puntos
Mejor oferta económica	5
Resto proporcional	Según fórmula

El tiempo de respuesta ofertado tendrá carácter contractual y será considerado un Acuerdo de Nivel de Servicio (SLA). Su incumplimiento reiterado podrá dar lugar a la aplicación de penalizaciones previstas en el contrato.

ANEXO I

La ausencia de respuesta, la respuesta incompleta o la falta de acreditación documental de cualquiera de los requisitos declarados como cumplidos podrá ser considerada como incumplimiento del requisito correspondiente.

Matriz de Cumplimiento de Requisitos Técnicos				
Requisito	Obligatorio	Cumple (Sí/No)	Descripción de la solución propuesta	Referencia documental
Plataforma 100% SaaS	Sí			
Consola de gestión única	Sí			
Plataforma EPP/EDR/XDR y SIEM del mismo fabricante	Sí			
Servicio SOC 24x7x365	Sí			
Capacidades MDR	Sí			
SIEM Integración con Active Directory On-Premise	Sí			
SIEM Integración con Microsoft 365	Sí			
SIEM Integración con Firewall FortiGate	Sí			
SIEM Integración con Proxy Apache	Sí			
Integración con endpoints y servidores Windows	Sí			
Inventario de software	Sí			
Control de dispositivos USB	Sí			
Control de aplicaciones	Sí			
Protección antimalware avanzada	Sí			
Capacidades EDR/XDR	Sí			
Correlación avanzada de eventos	Sí			
Retención mínima de logs de 12 meses	Sí			
Consulta histórica durante todo el periodo de retención	Sí			
Soporte a auditorías ENS	Sí			
Generación de evidencias para auditoría	Sí			
Cumplimiento RGPD	Sí			
Alojamiento de datos en la Unión Europea o adecuación legal equivalente	Sí			
CPSTIC ENS Alto para la solución EPP/EDR/XDR	Sí			

Matriz de Cumplimiento del Servicio SOC/MDR				
Requisito	Obligatorio	Cumple (Sí/No)	Descripción	Referencia documental
SOC 24x7x365	Sí			
Monitorización continua	Sí			
Clasificación y priorización de alertas	Sí			
Gestión de incidentes	Sí			
Escalado a responsables designados por BEC	Sí			
Informes mensuales	Sí			
Informes de incidentes críticos	Sí			
Threat Hunting	Sí			
Inteligencia de amenazas integrada	Sí			
Capacidades MDR	Sí			
Apoyo en auditorías ENS	Sí			
Servicio prestado por analistas especializados	Sí			
Participación en la Red Nacional de SOC (RNS)	Sí			

SLA del SOC		
Concepto	SLA mínimo exigido	SLA ofertado
Cobertura SOC	24x7x365	
Notificación incidente crítico	≤ 30 minutos	
Notificación incidente alta severidad	≤ 1 hora	
Notificación incidente media severidad	≤ 4 horas	
Notificación incidente baja severidad	≤ 1 día laborable	
Disponibilidad portal SOC	≥ 99,5 %	
Informe mensual	Incluido	
Informe incidente crítico	Incluido	