TRACTAMENT I SELECCIÓ DE RESIDUS, S.A.

PLIEGO DE PRESCRIPCIONES TÉCNICAS

SERVICIO DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD (SIEM) PARA GRUP TERSA

NÚMERO DE EXPEDIENTE CTTE1126

1. OBJETO.

El objeto del presente pliego de prescripciones es el de establecer las condiciones de carácter técnico para la contratación de un Sistema de Gestión de Eventos e Información de Seguridad (SIEM) y un Centro de Operaciones de Seguridad (SOC) para GRUP TERSA. El objetivo es garantizar la protección efectiva de los activos digitales de la organización mediante un servicio integral que aborde todos los elementos técnicos, organizativos y de gestión necesarios para la seguridad de la información.

A tal efecto, la prestación deberá efectuarse con arreglo a los requerimientos y condiciones que se estipulan en este pliego, de los que se derivan los derechos y obligaciones de las partes contratantes.

2. DURACIÓN DEL CONTRATO.

El plazo previsto es dos (2) años o hasta el consumo total del importe presupuestado, sin posibilidad de prórroga.

Se estima que el contrato se iniciará en fecha 1 de junio de 2025.

3. PLAZO DE EJECUCIÓN

El plazo de ejecución del servicio comprenderá la totalidad de las actuaciones durante el periodo de vigencia del contrato.

El alcance específico y contenido de cada uno de los servicios se detalla en el punto 4 del presente pliego.

4. DESCRIPCIÓN Y ALCANCE DE LOS SERVICIOS

4.1. Descripción del servicio

Se requiere la implantación, puesta en marcha y prestación de un servicio continuo 24x7 de monitorización, detección en tiempo real, gestión y respuesta a incidentes, inteligencia y caza de amenazas basado en SIEM. La prestación del servicio comprenderá el período estipulado en el apartado correspondiente. También dará cobertura al licenciamiento del SIEM en ese período.

La disponibilidad de estos servicios permite a la entidad pública cumplir con la normativa, mejorar su capacidad de detección y respuesta ante incidentes, y optimizar los recursos disponibles, garantizando una seguridad integral y una gestión eficiente de los riesgos.

4.2. Alcance del servicio

Se demanda un servicio de gestión, administración y alerta temprana de eventos de seguridad IT que asegure una monitorización experta y diligente, en la ventana horaria 24x7 y con un SIEM que cumpla con lo establecido a continuación. Aplicará a los siguientes activos:

- 2 Firewall en HA de Sophos (se estima que a partir del 1 de junio de 2025 serán sustituidos por 2 Firewall en HA de Fortinet).
- 1 vCenter de WMware
- 3 Host ESXI
- 10 servidores
- Hasta un máximo de mil (1000) cuentas de correo electrónico Microsoft 365, incluyendo sus respectivos entornos de SharePoint Online y OneDrive.
- 1 servidor de ficheros.
- 1 servidor de antivirus Sophos (en servicio hasta diciembre de 2025), que actualmente se está migrando al servicio de antivirus Microsoft Defender

CENTRO DE OPERACIONES DE SEGURIDAD (SOC):

La empresa adjudicataria deberá disponer de la infraestructura suficiente y de equipos de analistas especializados (seguridad defensiva, ofensiva, analistas de seguridad y de respuesta ante incidentes), para acometer una monitorización 24/7, análisis experto y respuesta rápida a incidentes.

El servicio SOC debe realizar las siguientes funciones:

1. Monitorización y Detección en Tiempo Real
   - Supervisión continua 24x7 de todos los activos de TI descritos en el alcance, incluyendo la protección de datos, sistemas Cloud y aplicaciones.
   - Detección temprana de amenazas mediante herramientas SIEM y UEBA.

2. Gestión y Respuesta a Incidentes (CSIRT/CERT)
   - Capacidad de respuesta inmediata ante incidentes de seguridad cibernética.
   - Implementación de planes de contención, erradicación y recuperación.
   - Coordinación con equipos internos y externos en incidentes de alta criticidad.

3. Inteligencia de Amenazas y Caza de Amenazas (Threat Hunting)
   - Identificación proactiva de amenazas ocultas mediante técnicas de Threat Hunting.
   - Uso de frameworks como MITRE ATT&CK para rastrear tácticas de atacantes.

4. Seguridad en Cloud y Protección de SaaS
   - Monitorización y protección de entornos M365.
   - Integración con un amplio espectro de productos de ciberseguridad de terceros (fabricantes).
   - Análisis de actividad sospechosa en servicios SaaS como Microsoft 365, SharePoint, OneDrive y Teams.

5. Análisis de vulnerabilidades
   - Identificación y corrección de posibles brechas de seguridad.
   - Reducción de riesgos de explotación, mantenimiento de la integridad del sistema.

6. Cumplimiento y Forense Digital
   - Generación de informes y evidencias digitales para auditorías y procesos legales.
   - Preservación de registros de incidentes con integridad asegurada.

7. Seguimiento del servicio e informes
   - Seguimiento de indicadores de seguridad y del nivel de servicio.
   - Informes y reunión de seguimiento periódicas.

- Propuestas de mejoras de seguridad conforme a las conclusiones obtenidas del desarrollo del servicio.

Servicio CSIRT respuesta a incidentes

El SOC será responsable de recrear potenciales escenarios de ataque para, a partir de ello, elaborar los Planes de Respuesta a Incidentes (IRP).

Deberán para ello considerarse, al igual que en el resto de los servicios, las guías, buenas prácticas y en general cualquier directriz que el Centro Criptológico Nacional (CCN) establezca para ello.

Los planes de respuesta llevarán el detalle de las acciones a todos los niveles que deberán llevarse a cabo en caso de sufrir un incidente de seguridad.

En los planes también se definirán las acciones que deberán estar catalogadas según sus plazos de forma inmediata, en el corto, medio y largo plazo.

Análisis de vulnerabilidades

El SOC será responsable de implantar y ejecutar una herramienta de evaluación de vulnerabilidades para actuar en los activos críticos y proporcionar la información necesaria para evaluar las vulnerabilidades desde la perspectiva de un atacante. Debe incorporar las siguientes funcionalidades:

- Analizar y descubrir vulnerabilidades en los activos automáticamente.
- Detección de vulnerabilidades en base a los CVSS.
- Categorización del nivel de riesgo de los activos.
- Monitorización de la capacidad de explotación y el nivel de impacto.
- Obtención de información detallada como la tendencia de vulnerabilidad.
- Auditoría de software de alto riesgo.

SIEM

El núcleo del sistema de correlación de eventos de seguridad debe llevarse a cabo a través de una solución SIEM (Security Information and Event Management).

La arquitectura del SIEM deberá permitir adaptarse sin esfuerzos adicionales a exigencias futuras en cuanto a necesidades de procesamiento y almacenamiento (escalado horizontal).

Una solución SIEM unificada con funciones DLP y CASB integradas para poder detectar, priorizar, investigar y responder a amenazas de seguridad. Disponer de inteligencia de análisis de amenazas, detección de anomalías basadas en machine learning, técnicas de detección de ciberataques basadas en reglas, ofreciendo una consola de gestión de incidentes para la remediación efectiva.

El SIEM debe ir más allá de la simple recopilación y correlación de logs, integrando tecnologías avanzadas para detección y respuesta ante amenazas.

1. Recolección y Normalización de Datos
   - Integración con múltiples fuentes de datos (logs de sistemas, firewalls, endpoints, aplicaciones en la nube, etc.).
   - Capacidad para normalizar y enriquecer datos en tiempo real para mejorar el análisis de eventos.

2. Correlación de Eventos y Detección de Amenazas
   - Motor de correlación basado en reglas y machine learning para identificar patrones anómalos.
   - Capacidad para detectar amenazas avanzadas, ataques persistentes (APT) y técnicas MITRE ATT&CK.
   - Generación de alertas priorizadas según criticidad y contexto.

3. Inteligencia de Amenazas (Threat Intelligence)
   - Integración con fuentes de inteligencia de amenazas (TI) en tiempo real.
   - Detección de indicadores de compromiso (IoC) y tácticas de adversarios conocidos.

4. Análisis de Comportamiento y Detección de Anomalías (UEBA)
   - Incorporación de User and Entity Behavior Analytics (UEBA) para detectar comportamientos sospechosos.
   - Análisis basado en IA y machine learning para identificar desviaciones en el tráfico de red, acceso a datos y actividad de usuarios.

5. Respuesta Automatizada y Orquestación (SOAR)
   - Integración con plataformas SOAR (Security Orchestration, Automation and Response) para respuestas automatizadas.
   - Ejecución de playbooks de seguridad ante amenazas detectadas.

6. Cumplimiento Normativo y Auditoría
   - Generación de informes automáticos para cumplimiento de ENS, ISO 27001, GDPR (RGPD), NIST, PCI DSS, entre otros.
   - Almacenamiento seguro de logs con retención configurable para auditorías forenses.

Detalle de las funcionalidades que deben incluir y aplicarse en el servicio:

- Centralización de Eventos de Seguridad
- UEBA
- Monitorización IDS e IPS
- DLP
- SOAR
- Servicio de Inteligencia de Amenazas

<u>Centralización de Eventos de Seguridad para Correlación y Análisis</u>

- Objetivo: Agregar eventos de seguridad para análisis centralizado.
- Logros: Identificación de patrones, mejora en la detección y respuesta a incidentes.

La infraestructura de TI genera una enorme cantidad de datos de log a diario. Estos logs contienen información vital que suministra información e inteligencia sobre la seguridad de la red sobe los comportamientos de los usuarios, anomalías en la red, inactividad del sistema, violaciones de políticas, amenazas internas, cumplimiento regulatorio, etc.

No obstante, la tarea de analizar manualmente estos logs de eventos y syslogs sin una herramienta automatizada que analice logs puede ser tedioso y difícil.

Administración de registros:

- Recopilar registros de diversos orígenes, tales como dispositivos de usuarios finales, servidores, dispositivos de red, cortafuegos y sistemas antivirus y de prevención de intrusiones.
- Analizar registros fácilmente en paneles de control que muestran información gráfica e informes intuitivos, y ayudan a detectar ataques, detectar comportamientos sospechosos de los usuarios y detener amenazas potenciales.
- Valorar el efecto de los incidentes de seguridad realizando análisis posteriores al ataque e identifique el patrón de ataque para detener los ataques en curso a través del análisis forense de registros.
- Monitorización de los cambios críticos, detección el robo de datos, identificación los ataques y supervisión del tiempo de inactividad de las aplicaciones críticas para el negocio, como las bases de datos y los servidores web, mediante la auditoría de los logs de las aplicaciones.

Revisión y Gestión de Alertas o Eventos Anormales en Registros de Auditoría

- Objetivo: Identificación y respuesta a eventos inusuales.
- Logros: Mejora en la capacidad de reacción ante posibles amenazas, optimización de la seguridad.

UEBA (User and Entity Behaviour Analytics):

Una solución UEBA hace un seguimiento de la conducta de los usuarios y las entidades de una organización, para distinguir el comportamiento normal del anormal. En el contexto de la ciberseguridad, un usuario o una entidad pueden ser cualquier sistema informático, proceso empresarial u organización (incluida una organización de la administración).

La solución UEBA supervisa a estos usuarios y entidades, revisando y analizando constantemente sus datos para determinar si una actividad o conducta concretas son anómalas y, por lo tanto, potencialmente peligrosas, debido a que podrían desembocar en un ciberataque.

- Analíticas de comportamiento de usuarios y hosts mediante machine learning.
- Agrupamientos dinámicos, detectando anomalías granulares en grupos de usuarios para los que se establece una línea base.
- Gestión de riesgos integrado.
- Detección de amenazas.

Monitorización IDS y IPS:

- Propósito: Garantizar la detección temprana y defensa contra amenazas.
- Logros: Identificación y respuesta proactiva ante intrusiones, correlación de eventos y gestión centralizada de registros de auditoría.

Detección de amenazas:

- Inteligencia de amenazas: bloqueo de intrusos maliciosos utilizando fuentes de amenazas.
- Búsqueda de amenazas: alertar de actores maliciosos y ataques potenciales ocultos que se hayan deslizado a través de las defensas iniciales de seguridad aprovechando las analíticas avanzadas de amenazas.
- Mitigación de amenazas externas: utilizar fuentes de amenazas para descubrir IPs, dominios, y URLs maliciosos.

- Mitigación de amenazas internas: alertar y bloquear tráfico malicioso a o desde IPs, dominios y URLs en lista negra y ofrece recomendaciones para remediar las amenazas con reglas predefinidas de workflow.

Detección de ataques:

- Inteligencia de amenazas: bloqueo de intrusos maliciosos utilizando fuentes de amenazas.
- Correlación en tiempo real basado en reglas.
- Alertas basadas en firmas de MTRE ATT&CK.

Sistema de Prevención de Pérdida de Datos (DLP):

- Objetivo: Evitar la fuga de información sensible.
- Logros: Protección de datos confidenciales, cumplimiento de normativas de privacidad.

DLP integrado:

- Data risk assesment: Protección de la información empresarial sensible, evalúación las localizaciones donde se almacenan los datos críticos y garantía de la seguridad del dato
- Protección según contenido de la información sensible almacenada en la red.
- Monitorización de integridad de ficheros: creación, modificación, acceso, renombrado y borrado.
- Supervisión de accesos no autorizados de ficheros y carpetas con notificación de alertas.

SOAR:

Se requiere la implementación de un sistema SOAR (Security Orchestration, Automation, and Response) que permita mejorar la eficiencia en la gestión de incidentes de seguridad mediante las siguientes funcionalidades clave:

- Auditoría en tiempo real del Directorio Activo, permitiendo un monitoreo continuo y detallado de cambios y actividades críticas.
- Respuesta automatizada ante incidentes, con generación de alertas en tiempo real y ejecución de workflows para una mitigación eficiente.
- Optimización de la gestión de incidentes, reduciendo el Tiempo Medio de Detección (MTTD) y el Tiempo Medio de Resolución (MTTR) a través de la detección, categorización, análisis y resolución de amenazas.
- Integración con herramientas de ticketing externas, asegurando una orquestación completa y una respuesta estructurada ante incidentes de seguridad.

Este sistema garantizará una mayor capacidad de respuesta, optimización de recursos y reducción del impacto de incidentes en la infraestructura de TI.

Servicio de inteligencia de amenazas:

Con el objeto de gestionar las amenazas externas, se solicita el servicio de Cybersecurity Threat Intelligence, que proporcione visibilidad y alertas de todos los elementos que viajan por las redes públicas o privadas, y que, además no se encuentran bajo el control de GRUP TERSA

Para llevar a cabo la detección y descubrimiento de esta información, se solicita el empleo de decenas de fuentes que se alimentan desde redes como Darkweb, Deepweb, foros, social media, etc.

Se pretende de este modo minimizar al menos los siguientes riesgos:

- Protección del dominio
- Cuentas y contraseñas filtradas
- Malware
- Exfiltración de datos
- Monitorización de Phishing en tiempo real

FORMACIÓN:

Se solicita 1 sesión anual en formato presencial en la sede de GRUP TERSA.

A través de este servicio se pretende fortalecer las capacidades del personal de GRUP TERSA a dos niveles:

- Alineación con los nuevos requisitos de la directiva europea NIS2 y resto de normativa (ENS) y marcos estándares (ISO 27001) que aplican en GRUP TERSA.
- Gobernanza de la Seguridad de la Información de GRUP TERSA.

Durante la duración del contrato, el responsable del contrato acordará con el adjudicatario el alcance concreto de esta formación, no superando ninguna de las sesiones anuales las cuatro (4) horas.

4.3. Responsabilidades del Adjudicatario

Se establece las siguientes responsabilidades del adjudicatario

- La empresa adjudicataria deberá estar certificada como mínimo en ENS categoría MEDIA.

- La empresa adjudicataria deberá estar dentro de la Red Nacional de SOC.

- La Solución SIEM deberá estar certificada como mínimo en ENS categoría MEDIA.

- La Solución SIEM deberá disponer de soporte por parte del fabricante y poder abrir casos, consultas o incidencias mediante email o sistema de ticketing.

- La empresa adjudicataria deberá disponer de al menos dos Centros de Operaciones de Seguridad en España, configurados en modo activo/activo, y operando 24 horas al día, 7 días a la semana, para garantizar que la detección y respuesta ante incidentes de seguridad, así como que el soporte se preste sin interrupción.

- Todos los trabajos y servicios requeridos en el presente pliego deberán prestarse conforme a los requisitos establecidos tanto por el Esquema Nacional de Seguridad en su categoría mínima de MEDIA, así como por el estándar internacional ISO 27001. Si durante la vigencia del contrato se identificaran no conformidades a través de procesos de auditoría interna, externa o cualquier otro proceso de control, la empresa adjudicataria deberá resolverlas en los plazos establecidos por dichas normas y sin que la resolución implique coste alguno para GRUP TERSA.

- Acuerdos exigidos de Nivel de Servicio (SLA) referidos a los tipos de alarmas que el SIEM genere y referidos a sucesos imputables a la empresa prestataria del servicio:

Tipología	Tiempo de respuesta máximo
Apertura de incidencias	24x7x365
Tiempo de respuesta en incidencias de seguridad de prioridad ALTA, o que afecten a la totalidad del servicio	1 hora
Tiempo de actuación en incidencias de seguridad de prioridad MEDIA, o que afecten gravemente al servicio	4 horas naturales (servicio 24x7x365)
Tiempo de actuación en incidencias de seguridad de prioridad BAJA, o que no afecten gravemente al servicio	24 horas naturales (servicio 24x7x365)
Tiempo de actuación en cambios y solicitudes	24 horas naturales (servicio 24x7x365) Si bien estas intervenciones deberán ser programadas con GRUP TERSA para minimizar el impacto de cambios en la red.
Disponibilidad del SIEM y sus componentes.	Disponibilidad ≥99,95 %.

Para ello, se establece la descripción de cada prioridad:

- Prioridad ALTA: evento de riesgo alto que requiere de la intervención de los técnicos del SOC, y que podría requerir la activación del servicio CSIRT incluido en este contrato.
- Prioridad MEDIA: detección de situación de potencial riesgo, pero del que aún no se dispone de toda la información para identificarlo como prioridad ALTA por lo que el evento debe ser analizado por los técnicos del SOC.
- Prioridad BAJA: evento de riesgo bajo que no requiere una respuesta, pero sobre el que se abre un ticket a modo informativo y de registro documental.

4.4. Subcontratación

El Adjudicatario no podrá en ningún caso ceder a terceros la subcontratación de ninguna parte del alcance establecido en los pliegos sin el previo consentimiento escrito de TERSA.

TERSA podrá pedir al Adjudicatario la documentación que sea necesaria para dar su consentimiento.

El Adjudicatario deberá aplicar un plan específico para las empresas subcontratadas por él para que éstas cumplan con las disposiciones contenidas en la Ley de Prevención de Riesgos Laborales, además de cualquier normativa vigente de seguridad existente en relación a la naturaleza de la acción que se deba desarrollar en la empresa contratista, y será responsable de que los montajes se ajusten a lo establecido en este PPT.

5. RESPONSABLES DEL CONTRATO

5.1. Responsable del contrato por parte de la empresa adjudicataria

El contratista deberá nombrar un responsable del contrato, que actuará como interlocutor delante de Grup Tersa, y que será el responsable de la correcta ejecución del servicio.

El responsable deberá realizar las reuniones de seguimiento del servicio e informes correspondientes que sean requeridos conforme a los requerimientos técnicos establecidos o las solicitudes específicas del responsable de TERSA.

5.2. Responsable del contrato por parte de Grup Tersa

Por parte del Grup Tersa, se designará un responsable del contrato, que será el interlocutor principal con el adjudicatario.

6. RETRIBUCIÓN DEL SERVICIO

El adeudo de los servicios se realizará mediante pago de cuota mensual conforme se indica en el Pliego de Cláusulas Administrativas, de acuerdo con la cuota mensual que se refleje en la formalización del contrato.

Mensualmente el Adjudicatario procederá a la realización de un albarán de servicio donde consten:

- Nº de pedido.
- Concepto, deberá indicar el nº de expediente.
- Alcance realizado junto con su valor económico.

El albarán deberá ser revisado y aprobado por TERSA. Una vez aprobado, el Adjudicatario emitirá una factura con los cargos o adeudos que procedan en concepto de servicios efectuados.