

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE UNA “PLATAFORMA DE PROTECCIÓN DEL ENDPOINT (EDR/XDR) PARA EGARSAT, MUTUA COLABORADORA CON LA SEGURIDAD SOCIAL Nº 276”.

1. Objeto del contrato

El objeto del presente pliego de prescripciones técnicas es definir y establecer las condiciones técnicas que regirán la adjudicación, por parte de EGARSAT, del contrato para la implantación de una plataforma de protección del endpoint en la nube 100% SaaS de última generación con capacidades avanzadas de prevención, detección y respuesta (EDR/XDR), gestión de vulnerabilidades, protección de identidades y replicación de telemetría para almacenamiento extendido, que deberá cubrir la totalidad de identidades, de servidores y de estaciones de trabajo. Deberán proporcionarse todos los elementos software y licencias que resulten necesarios para que la solución sea totalmente funcional y operativa, y todas las funcionalidades ofertadas deberán estar disponibles, sin pagos adicionales, durante toda la vigencia del contrato.

Esta evolución tecnológica debe garantizar la continuidad, la actualización y el soporte experto necesario para mantener la operatividad, la seguridad y la disponibilidad de las infraestructuras TI de EGARSAT, asegurando así el correcto funcionamiento de los servicios esenciales para el desarrollo de las actividades de la entidad.

El alcance del presente pliego comprende:

- Suministro de licencias de plataforma de seguridad endpoint con todas las capacidades funcionales y técnicas requeridas.
- Servicios profesionales de configuración inicial de la plataforma.
- Servicios de apoyo técnico durante el despliegue de la solución.
- Formación del personal técnico de EGARSAT.
- Servicios de soporte en tiempo de operación durante toda la vigencia del contrato.

Volumetrías actuales a efectos de que los licitadores puedan realizar su propuesta:

- Número de equipos a proteger: 875 (aproximadamente 150 servidores y 725 estaciones de trabajo)
- Número de usuarios activos en el Directorio Activo de Microsoft que EGARSAT tiene instalado: 1.050

Solo se aceptarán aquellas propuestas que incluyan en su oferta softwares que figuren como líderes en los análisis correspondientes al año 2025 de plataformas de protección del endpoint de los principales analistas mundiales independientes del sector, como pueden ser “Gartner Magic Quadrant” y/o “Forrester Wave”.

Del mismo modo, solo se aceptarán aquellas propuestas que incluyan en su oferta una solución que esté incluida en el ‘Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información (guía CCN STIC 105) del CCN-CERT, siendo tipificado como producto “Cualificado” y Categoría ENS “Media” como mínimo, en el momento de la presentación de la oferta. Dicha certificación deberá estar vigente durante toda la vigencia del contrato. Se valorará en oferta técnica una mejora en este apartado.

Por último, todos los elementos que componen la solución ofertada deberán estar ubicados en Europa y, por extensión, bajo el cumplimiento del RGPD de la Unión Europea.

En cuanto al contratista, éste deberá disponer de la certificación que acredite el cumplimiento de lo dispuesto en el Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad, comprometiéndose a aplicar las medidas correspondientes al nivel MEDIO, cuando el acceso o tratamiento de información así lo exija, y a colaborar en las auditorías o actuaciones de verificación que se determinen. Se aceptará la acreditación de dicho requisito mediante la aportación de certificaciones equivalentes, tales como la certificación ISO 27001:2022 sobre Sistemas de Gestión de Seguridad de la

Información objeto de este contrato. La certificación o certificaciones presentadas deberán estar vigentes durante toda la vigencia del contrato. Se valorará en oferta técnica una mejora en este apartado.

Los licitadores deberán presentar dentro del SOBRE B una **memoria técnica** que detalle la solución propuesta. Esta memoria técnica deberá incorporar, como mínimo, los siguientes aspectos:

- En cuanto a la plataforma ofertada: el licitador deberá describir las características de los distintos componentes y funcionalidades de la solución propuesta destacando y justificando el cumplimiento de todos los aspectos indicados en los puntos 2 y 3 del presente pliego de prescripciones técnicas, la cual deberá cumplir de manera exacta y verificable todos y cada uno de los requisitos técnicos detallados en este pliego. Cualquier propuesta de solución deberá aportar evidencias técnicas documentadas, pruebas independientes verificables (como evaluaciones MITRE ATT&CK), documentación oficial del fabricante y, si EGARSAT lo requiere, demostraciones en entorno real que validen cada capacidad específica requerida.
- En cuanto a los Servicios relacionados con la implantación y puesta en marcha de la solución el licitador deberá incluir una descripción detallada sobre su propuesta de ejecución de las tareas relacionadas en el punto 4 del presente pliego de prescripciones técnicas.
- En cuanto a los Servicios de soporte en tiempo de operación el licitador deberá incluir una descripción detallada sobre las características del soporte ofertado y el cumplimiento de los requisitos mínimos relacionadas en el punto 6 del presente pliego de prescripciones técnicas.
- Otra información que las empresas licitadoras estimen necesario incluir para facilitar la comprensión de la oferta presentada y acreditar su adecuación a lo dispuesto en el presente pliego, así como toda aquella documentación que resulte precisa para permitir la valoración de las propuestas conforme a los criterios de adjudicación evaluables mediante juicio de valor establecido en el Anexo 9 del Pliego de Cláusulas Administrativas Particulares.

No deberá incluirse en esta memoria ninguna información objeto de valoración en la oferta técnica valorable automáticamente (SOBRE C). Cualquier referencia podrá ser motivo de exclusión de la oferta presentada.

EGARSAT podrá rechazar la oferta cuando, de la información aportada según lo exigido en este apartado, se desprenda que la solución ofertada no cumple con los requisitos definidos en el presente pliego, o a juicio del personal técnico de Egarsat, no sea apta para el objeto de licitación.

Serán excluidas de la licitación aquellas empresas que no presenten toda la documentación exigida en este apartado y con el nivel de detalle requerido, dada la necesidad de comprobación de la adecuación de la solución ofertada a las exigencias técnicas incluidas en el presente pliego técnico.

2. Características globales de la solución

La decisión de EGARSAT de evolucionar una plataforma de seguridad del endpoint de última generación responde a la necesidad de EGARSAT de fortalecer significativamente su postura de ciberseguridad mediante capacidades avanzadas de prevención, detección, respuesta y visibilidad integral del entorno. Es por este motivo que la plataforma ofertada deberá proporcionar, como mínimo:

- Protección de última generación: motor de prevención basado en inteligencia artificial y machine learning, capaz de defender contra todo tipo de amenazas incluyendo malware conocido, amenazas de zero-day, ransomware y ataques sin archivos (fileless), con actualizaciones automáticas sin necesidad de firmas y con impacto no apreciable en el rendimiento de los sistemas protegidos.
- Capacidades de detección y respuesta en endpoints (EDR): capacidades de visibilidad completa

y continua de la actividad en endpoints mediante telemetría en tiempo real, permitiendo investigaciones forenses detalladas, análisis de comportamiento con indicadores de ataque (IOA) alineados con el framework MITRE ATT&CK, y capacidades de respuesta remota para contención y remediación de incidentes de seguridad.

- Descubrimiento y gestión de activos: identificación automática de todos los dispositivos presentes en la red corporativa, incluyendo equipos no gestionados o no autorizados (shadow IT), proporcionando un inventario actualizado en tiempo real del perímetro de seguridad.
- Gestión continua de vulnerabilidades: evaluación continua de vulnerabilidades sin necesidad de escaneos intrusivos, credenciales de administrador o impacto en el rendimiento de los sistemas, priorizando riesgos según criticidad, exposición real y disponibilidad de exploits activos.
- Protección de identidades: capacidades especializadas de detección de movimientos laterales, uso indebido de credenciales, ataques de elevación de privilegios en Active Directory y técnicas avanzadas de compromiso de identidades corporativas.
- Replicación y retención extendida de telemetría de seguridad: capacidad de replicación automática y continua de la telemetría completa generada por los endpoints protegidos hacia repositorios de almacenamiento externos existentes en EGARSAT, permitiendo la retención de datos de seguridad a largo plazo, análisis forenses retrospectivos, auditorías regulatorias y actividades avanzadas de threat hunting sobre históricos de varios años y sin impacto en el rendimiento de los sistemas.

El licenciamiento suministrado deberá ser de nueva adquisición, original del fabricante, no reutilizado ni reciclado, no remanufacturado ni de segunda mano ni procedente de transferencias previas, procediendo de canal autorizado por el fabricante de la plataforma ofertada y apto para su alta directa en el portal de licenciamiento y/o de gestión correspondiente.

3. Requisitos técnicos y operativos detallados

3.1. Arquitectura y diseño de la plataforma

La plataforma ofertada deberá cumplir de manera obligatoria con los requisitos técnicos y operativos que se detallan a continuación, como mínimo:

- Deberá estar basada en una arquitectura cloud-native 100% SaaS sin requerir ningún componente on-premise. No se admitirán soluciones que requieran, directa o indirectamente, el despliegue de componentes on-premise, appliances virtuales, recolectores de logs, forwarders, gateways, proxies, sensores intermedios, ni ningún tipo de infraestructura on-premise gestionada por EGARSAT para el funcionamiento completo de la solución.
- Deberá utilizar una base de datos de telemetría correlacionada en tiempo real que permita análisis de comportamiento cruzado entre millones de endpoints a nivel global, con garantía de almacenamiento exclusivamente en datacenters bajo el cumplimiento del RGPD.
- Deberá permitir consultas de telemetría en tiempo real con respuesta en menos de 5 segundos sobre conjuntos de datos de más de 90 días de antigüedad sin degradación de rendimiento ni necesidad de sistemas SIEM externos.
- Todos los requisitos de seguridad demandados en el presente pliego deberán ser cubiertos íntegramente por un único fabricante de seguridad y mediante una única tecnología nativa, diseñada, desarrollada y operada de forma unificada por dicho fabricante y gestionada desde una única interfaz o consola web, sin necesidad de integraciones de terceros, módulos adicionales o componentes externos para completar alguna de las funcionalidades requeridas. No se

considerará fabricante único aquel que requiera la utilización conjunta de varios productos, servicios, licencias, consolas, dominios, portales web, data lakes o modelos de datos independientes, aunque pertenezcan al mismo grupo empresarial o proveedor tecnológico. Todos los módulos funcionales deberán operar de forma nativa sobre una única base de datos de telemetría común, generada directamente por el sensor del endpoint, sin mecanismos de ingestión de logs, sincronización diferida, replicación entre bases de datos independientes, correlación posterior ni dependencia de plataformas SIEM, SOAR o data lakes externos para alcanzar las funcionalidades requeridas. No se considerarán válidas aquellas soluciones que requieran vincular, enlazar o integrar distintas plataformas, aplicaciones web, dominios o consolas para cubrir las funcionalidades requeridas.

- Deberá implementar una arquitectura cloud native multi-tenant con aislamiento lógico completo entre clientes, utilizando microservicios containerizados distribuidos geográficamente con arquitectura de alta disponibilidad (HA) activo-activo en múltiples zonas de disponibilidad dentro de la región europea. Deberá garantizar objetivos de recuperación cercanos a tiempo real (RPO $\approx$ 0) y tiempos de recuperación inferiores a 60 segundos ante fallos de la infraestructura.
- Deberá ofrecer una disponibilidad tanto del servicio cloud como de la consola de administración de un 99,9% mensual, como mínimo, excluyendo ventanas de mantenimiento planificadas y comunicadas previamente.
- Deberá implementar una base de datos de telemetría de gran escala que le permita ser capaz de ingestar y procesar más de 1 billón de eventos de seguridad diarios a nivel global, con capacidad de correlación en tiempo real entre eventos de diferentes endpoints, regiones geográficas y periodos temporales. Deberá utilizar indexación distribuida con capacidad de búsqueda en menos de 5 segundos sobre conjuntos de datos de más de 90 días y millones de endpoints simultáneos.
- Deberá implementar una arquitectura de sensor ligero unificado, esto es, un binario único multiplataforma con firma digital de código (Code Signing) validada por autoridad certificadora reconocida internacionalmente que proporcione todas las capacidades requeridas sin necesidad de múltiples agentes o módulos independientes. El tamaño del sensor deberá ser reducido y optimizado, no superando aproximadamente los 50 MB en Windows, 35 MB en macOS y 30 MB en Linux. Deberá implementar autoprotección mediante driver en modo kernel con certificación WHQL para Windows y notaría oficial de Apple para macOS. Las capacidades de protección de identidades deberán integrarse en el mismo ecosistema de sensores y telemetría de la plataforma, admitiéndose únicamente un sensor adicional específico para controladores de dominio, gestionado desde la misma consola y base de datos.
- Respecto al consumo de recursos y optimización del rendimiento, el sensor deberá mantener un uso promedio de CPU inferior al 5% durante operaciones normales y picos máximos no superiores al 15% durante operaciones de escaneo bajo demanda. El consumo de memoria RAM deberá mantenerse entre 200-500 MB en configuración estándar. El tráfico de red deberá ser optimizado mediante compresión y deberá consumir menos de 10 MB por día y por endpoint en promedio para sincronización de políticas, envío de telemetría y actualización de inteligencia de amenazas.
- Toda comunicación entre sensores y la plataforma cloud deberá realizarse mediante protocolos de comunicación segura, utilizando cifrado TLS 1.2 o superior con Perfect Forward Secrecy (PFS), validación mutua de certificados, y resistencia a ataques de man-in-the-middle. El protocolo deberá ser resiliente ante interrupciones de red con capacidades de buffer local de hasta 7 días de telemetría en caso de desconexión prolongada, y sincronización automática sin pérdida de datos al restablecimiento de la conectividad.
- La plataforma deberá soportar despliegue automatizado mediante la herramienta de distribución de software corporativa, así como permitir el despliegue mediante scripts de instalación silenciosa. Las actualizaciones del sensor deben realizarse de forma automática y silenciosa sin requerir reinicios del sistema operativo (se permitirá requerir el reinicio el sistema operativo en

casos puntuales de cambios mayores de versión que afecten al driver kernel), con rollout gradual configurable y capacidad de rollback automático en caso de detección de incompatibilidades.

- La infraestructura cloud deberá implementar arquitectura de alta disponibilidad con redundancia geográfica dentro de la región europea, desplegada en múltiples zonas de disponibilidad independientes o múltiples datacenters dentro de la Unión Europea
- La plataforma ofertada deberá incorporar de forma nativa un sistema avanzado de gestión de incidentes y eventos de seguridad, integrado en la propia plataforma, que permita cubrir todo el ciclo de vida del incidente, desde su detección hasta su cierre definitivo. En particular, deberá permitir, como mínimo:
 - La visualización centralizada, correlación y priorización de incidentes y eventos de seguridad, con información suficiente para su análisis técnico, evaluación del impacto y toma de decisiones.
 - La asignación obligatoria de incidentes y/o eventos a técnicos concretos, identificados de forma unívoca, así como la reasignación controlada cuando proceda.
 - La gestión completa del estado del incidente (abierto, en análisis, en mitigación, resuelto, cerrado), garantizando la coherencia y trazabilidad de los cambios de estado.
 - La documentación estructurada de todas las actuaciones realizadas, quedando constancia, como mínimo, del técnico responsable, fecha y hora de cada acción, descripción de la actuación y resultado obtenido.
- La plataforma ofertada deberá garantizar la trazabilidad completa de los incidentes y eventos, de forma que sea posible reconstruir de manera inequívoca quién ha realizado cada actuación y en qué momento, dando cumplimiento a los principios de responsabilidad, no repudio y registro de actividad exigidos por el Esquema Nacional de Seguridad.
- Asimismo, la solución deberá disponer de cuadros de mando (dashboards) avanzados y configurables, orientados tanto a perfiles técnicos como a perfiles de supervisión y gestión, que permitan en todo momento una visión global y en tiempo real del estado de la seguridad, incluyendo como mínimo:
 - Incidentes abiertos, en curso y cerrados.
 - Incidentes y/o eventos pendientes de asignación.
 - Técnico responsable de cada incidente y estado de las actuaciones.
 - Evolución temporal de los incidentes y carga de trabajo por técnico.Estos cuadros de mando deberán facilitar la supervisión del servicio, el control operativo, la toma de decisiones y la generación de evidencias, contribuyendo al cumplimiento de las medidas del Esquema Nacional de Seguridad, en particular las relativas a monitorización, gestión de incidentes, registro de actividad y supervisión continua, así como a los requisitos de control y seguimiento establecidos en la norma ISO/IEC 27001.
- Deberá disponer de un sistema parametrizable de notificaciones por correo electrónico para que avise al personal técnico de EGARSAT de todas aquellas detecciones y/o eventos que EGARSAT determine.
- En cuanto al rendimiento del portal de gestión centralizada, deberá ofrecer los umbrales mensuales de P95 de tiempos de carga < 5 segundos en procedimiento de login y acceso a las distintas pantallas de la plataforma, < 5 segundos en vistas de detalle.
- Deberá ser 100% compatible con el resto de plataformas de seguridad instaladas en servidores y estaciones de trabajo de EGARSAT, sin tener que deshabilitar ninguna funcionalidad ni en la plataforma ofertada ni en las plataformas de seguridad existentes en EGARSAT para su total compatibilidad y normal funcionamiento de todas ellas.

El detalle de las plataformas de seguridad existentes actualmente en EGARSAT no se aporta como información pública al considerarse información sensible de seguridad. Esta información

se facilitará bajo demanda y para ello, deberá enviarse un correo electrónico a licitaciones@egarsat.es indicando CIF y nombre de la empresa solicitante.

3.2. Capacidades de detección y respuesta

La plataforma ofertada deberá cumplir de manera obligatoria con los requisitos operativos y técnicos que se detallan a continuación, como mínimo:

- Deberá incorporar tecnología de prevención mediante inteligencia artificial para la defensa contra amenazas avanzadas conocidas y desconocidas, entrenada con al menos 1 billón de eventos de seguridad diarios a nivel global, sin utilizar firmas tradicionales ni definiciones de malware.
- Deberá implementar un conjunto de modelos de machine learning entrenados con más de 10 años de datos históricos de malware y comportamientos maliciosos, incluyendo más de 100 mil millones de muestras únicas. Los modelos deberán actualizarse automáticamente cada 5-10 minutos mediante aprendizaje. Deberá ser capaz de detectar malware zero-day en menos de 60 segundos desde su primera aparición global.
- Deberá ser capaz de prevenir y detectar ataques fileless, living-off-the-land (LOLBins), técnicas de process injection, exploits de memoria, ransomware, ataques de supply chain y amenazas de zero-day sin necesidad de actualizaciones de definiciones.
- Deberá implementar detección basada en indicadores de ataque (IOA) basados en comportamiento con mapeo completo y nativo al framework MITRE ATT&CK, mostrando automáticamente la táctica, técnica y subtécnica específica utilizada en cada detección, en lugar de indicadores de compromiso (IOC) estáticos.
- Deberá implementar detección de técnicas de evasión avanzadas incluyendo process hollowing, process doppelganging, process injection (reflective DLL injection, APC injection, AtomBombing), exploits de memoria (heap spray, ROP chains, DEP/ASLR bypass) y ataques fileless (PowerShell encoded commands, WMI abuse, MSHTA, regsvr32 squiblydoo, CMSTP bypass).
- La solución deberá haber demostrado resultados verificables en las evaluaciones MITRE ATT&CK Evaluations con una tasa de detección igual o superior al 95% de pasos de ataque, priorizando detecciones con alta visibilidad y baja tasa de falsos positivos.
- La plataforma deberá capturar y correlacionar un mínimo de 400 tipos diferentes de eventos de telemetría por endpoint, incluyendo como mínimo ejecución de procesos con árbol completo mostrando relaciones padre/hijo de hasta 10 niveles de profundidad, hash SHA256 de ejecutables, líneas de comando con argumentos, conexiones de red con IP origen/destino y geolocalización, modificaciones de registro de Windows con valores antes/después, accesos y modificaciones de archivos con timestamps precisos, cambios en scheduled tasks, modificaciones WMI, eventos de autenticación local y de dominio, servicios de Windows instalados/modificados, actividad de drivers y módulos kernel, eventos DNS con resolución completa, conexiones RDP y sesiones remotas, conexiones SMB, actividad PowerShell con scripts completos, carga dinámica de DLLs, inyecciones de código entre procesos, modificaciones de AMSI, eventos de firma digital, modificaciones de drivers, cambios en certificados y actividad de navegadores web. Deberá identificar visualmente los procesos sospechosos incluyendo un scoring de riesgo automático
- Deberá implementar protección antiransomware con rollback, monitorizando en tiempo real las operaciones de escritura masiva en disco, cifrado de archivos, y modificación de extensiones de archivo, con capacidad de revertir automáticamente todos los cambios realizados por

ransomware antes de la detección. Deberá proteger contra ransomware conocido (WannaCry, Ryuk, LockBit, BlackCat, Akira) y variantes desconocidas mediante análisis de comportamiento.

- Deberá detectar y bloquear exploits de vulnerabilidades conocidas y zero-day mediante análisis de comportamiento de explotación, incluyendo protección contra buffer overflows, heap corruption, use-after-free, null pointer dereference, integer overflow, format string attacks, y técnicas de escalado de privilegios en kernel.
- El sensor deberá implementar autoprotección mediante driver en modo kernel firmado, con protección contra su desinstalación no autorizada, terminación de procesos del sensor, modificación de archivos del agente, manipulación de configuración mediante registro, eliminación de servicios de Windows, y ataques de driver tampering. Deberá mantener la conectividad con la plataforma cloud incluso cuando el sistema operativo está comprometido.
- Deberá ofrecer cobertura multiplataforma unificada, con soporte completo para Windows 10 Professional y Windows 11 Professional, Windows Server 2012 R2 o superior, macOS 15 o superior, y distribuciones Linux principales (RHEL, CentOS, Ubuntu, SUSE) tanto en arquitecturas x86_64 como ARM64, todo con el mismo motor de prevención y políticas centralizadas.
- Deberá ofrecer un impacto en CPU inferior al 5% promedio durante operaciones normales, picos máximos no superiores al 15% durante escaneos bajo demanda, consumo de memoria RAM entre 200-500 MB y sin degradación perceptible en aplicaciones de usuario según benchmarks estándar como PCMark, SPECint y/o Geekbench.
- La solución deberá incorporar capacidades de respuesta remota en tiempo real permitiendo acceso remoto a endpoints para la ejecución de acciones de respuesta como comandos de shell, captura de archivos específicos para análisis forense, cálculo de hash de archivos, terminación forzada de procesos maliciosos, eliminación de archivos, quarantine de malware, extracción de configuración de red, consulta de registro de Windows, captura de memoria de proceso específico, listado de procesos activos con detalles, historial de comandos ejecutados, y transferencia bidireccional de archivos, todo sin necesidad de RDP, SSH, VNC o herramientas de administración remota de terceros.
- Deberá mantener conectividad con endpoints aislados de red para permitir remediación incluso cuando el equipo está en cuarentena. El aislamiento de red deberá ser instantáneo (<1 segundo), bloqueando todo tráfico entrante y saliente excepto conectividad con la plataforma cloud de gestión. Deberá soportar aislamiento selectivo donde se puede permitir tráfico específico hacia servicios críticos (ej: Domain Controller, DNS) mientras se bloquea todo lo demás. Durante el aislamiento, el sensor deberá mantener comunicación activa con la consola para permitir investigación forense y remediación sin necesidad de reconectar el equipo a la red.
- Deberá soportar creación de consultas de threat hunting personalizadas en lenguaje de consulta específico o mediante interfaz de búsqueda avanzada, con capacidad de ejecutar búsquedas complejas sobre telemetría histórica, guardar consultas para reutilización, programar ejecución periódica de búsquedas, y recibir alertas automáticas cuando una consulta devuelva resultados positivos.
- Deberá incorporar capacidades de análisis forense de memoria RAM en tiempo real sin necesidad de crear memory dumps completos, sin reiniciar el sistema operativo y sin impacto perceptible para el usuario. Deberá detectar rootkits en memoria, bootkits, inyecciones de código malicioso, proceso hiding y hooks en funciones de sistema operativo.

3.3. Descubrimiento y gestión de activos

La plataforma ofertada deberá proporcionar un inventario automático, continuo y en tiempo real de

todos los dispositivos y aplicaciones presentes en la red corporativa, debiendo cumplir de manera obligatoria con los requisitos técnicos y operativos que se detallan a continuación, como mínimo:

- Deberá detectar automáticamente cualquier dispositivo conectado a la red corporativa en menos de 5 minutos desde su conexión, utilizando técnicas pasivas de análisis de tráfico (sin generación de paquetes de escaneo activo) complementadas con la información reportada por los endpoints gestionados. Deberá identificar equipos con el agente instalado, equipos sin el agente instalado, dispositivos IoT, impresoras de red, puntos de acceso WiFi, switches gestionados, cámaras IP y cualquier otro dispositivo con dirección IP asignada.
- Deberá realizar un inventario exhaustivo de aplicaciones con detección de obsolescencia, manteniendo dicho inventario actualizado automáticamente de todas las aplicaciones instaladas en cada endpoint, incluyendo el nombre completo de la aplicación, la versión específica (incluidos build numbers), el editor/fabricante, la ruta de instalación, su tamaño en disco, la fecha de instalación y de última actualización, su arquitectura (x86/x64/ARM) y método de instalación (MSI, EXE, package manager). Deberá identificar automáticamente aplicaciones que no han recibido actualizaciones en más de 90 días, aplicaciones que han alcanzado fin de soporte (EOL) del fabricante, y aplicaciones con vulnerabilidades conocidas críticas o altas.
- Deberá detectar y generar alertas automáticas de dispositivos conectados a la red corporativa que no están autorizados o gestionados, incluyendo endpoints personales y/o no corporativos, máquinas virtuales no registradas, contenedores en ejecución no autorizados, dispositivos IoT no corporativos, rogue access points y cualquier sistema que no cumpla con las políticas de seguridad corporativas. Deberá clasificar automáticamente dichos dispositivos por tipo (workstation, servidor, móvil, IoT, red) y nivel de riesgo, como mínimo.
- Deberá monitorizar continuamente el estado de protección de todos los endpoints gestionados, generando alertas automáticas cuando el agente de seguridad se encuentre desinstalado, el servicio esté detenido, la protección en tiempo real esté deshabilitada, las políticas no se hayan aplicado correctamente, el endpoint no se haya conectado con la plataforma durante más de 48 horas, o el sensor no esté operando al 100% de sus funcionalidades por conflictos con algún otro software de seguridad existente en el endpoint.
- Deberá realizar un inventario de hardware de cada endpoint incluyendo, como mínimo, fabricante y modelo exacto, número de serie, tipo de CPU y número de cores, cantidad de RAM instalada, capacidad sus discos duros y SSDs, tipo y versión de BIOS/UEFI, tarjetas de red con direcciones MAC, versión de firmware de componentes críticos y estado de características de seguridad hardware (TPM, Secure Boot, DEP, ASLR).
- Deberá proporcionar APIs REST para exportación automática del inventario de activos actualizado hacia sistemas CMDB y/o herramientas de gestión de activos corporativas, incluyendo webhooks para notificaciones de cambios en el inventario. Deberá también poder nutrir sistemas de ticketing con actualización incremental en tiempo real.
- Deberá identificar automáticamente software duplicado o redundante instalado en los endpoints (por ejemplo, múltiples navegadores, varias herramientas de compresión, aplicaciones similares de diferentes fabricantes), con recomendaciones de consolidación para optimizar licenciamiento y reducir superficie de ataque.

3.4. Gestión de vulnerabilidades:

La plataforma ofertada deberá evaluar de forma continua las posibles vulnerabilidades sin impactar en el rendimiento de los dispositivos ni en las operaciones de red, con priorización inteligente en tiempo real, cumpliendo de manera obligatoria con los requisitos operativos y técnicos que se detallan a continuación, como mínimo:

- El módulo de gestión de vulnerabilidades deberá operar mediante inventario continuo y correlación del inventario de aplicaciones instaladas con bases de datos CVE sin realizar escaneos activos de red, la evaluación de vulnerabilidades no deberá implicar la ejecución de procesos adicionales en el endpoint ni generar consumo adicional de CPU, siendo este incremento 0% verificable mediante herramientas estándar de monitorización del sistema operativo,
-
- sin requerir credenciales de administrador, sin generar tráfico de escaneo, sin necesidad de programar ventanas de escaneo y sin impacto apreciable en el rendimiento de los endpoints (0% de CPU adicional para la función de evaluación de vulnerabilidades).
- Deberá proporcionar evaluación continua 24x7 de equipos tanto conectados como desconectados de la red, con actualización inmediata al reconectar el endpoint.
- Deberá implementar un sistema de priorización de vulnerabilidades multifactor basada en riesgo real, que considere simultáneamente múltiples factores de riesgo: CVSS base score (v3.x), CVSS temporal score con ajustes por disponibilidad de exploit público, CVSS environmental score según exposición del activo (internet-facing vs interno), evidencia de explotación activa en campañas de ransomware o APT documentadas, facilidad de explotación (weaponization), impacto potencial en confidencialidad/integridad/disponibilidad, criticidad del activo afectado según clasificación corporativa, y presencia de controles compensatorios activos. Deberá asignar un risk score unificado de 0-100 para facilitar priorización.
- La base de datos de CVE deberá estar actualizada en menos de 24 horas desde la publicación oficial de nuevos CVE, manteniendo sincronización con bases de datos públicas de vulnerabilidades (NVD National Vulnerability Database, MITRE CVE, vendor advisories). Deberá correlacionar automáticamente CVEs con información de exploit público verificado, mencionando referencias a Exploit-DB, Metasploit modules, proof-of-concept publicados en GitHub, y análisis de vendors de seguridad.
- Deberá realizar la detección de exploits activos en campañas reales cruzando vulnerabilidades detectadas con inteligencia de amenazas en tiempo real, identificando específicamente aquellas vulnerabilidades que están siendo explotadas activamente en campañas de ransomware (LockBit, BlackCat, ClOp, Akira), operaciones APT documentadas (grupos PANDA, BEAR, KITTEN, SPIDER), ataques masivos de botnet, o campañas de cryptomining, con contexto detallado de TTPs utilizadas por atacantes en la explotación.
- Deberá ofrecer cobertura completa de plataformas y aplicaciones, evaluando vulnerabilidades en sistemas operativos (Windows todas las versiones, Windows Server, macOS y distribuciones Linux), aplicaciones de Microsoft (Microsoft Office principalmente), navegadores web (Chrome, Firefox, Edge, Safari), Java Runtime Environment, Adobe Reader, aplicaciones de terceros populares (7-Zip, VLC, WinRAR, Notepad++), drivers de hardware, y componentes de infraestructura instalados en endpoints (Python, Node.js, .NET Framework y OpenSSL, como mínimo).
- Deberá generar informes detallados de remediación para cada vulnerabilidad incluyendo, como mínimo, la descripción técnica de la vulnerabilidad, versión vulnerable instalada vs versión parcheada disponible, instrucciones paso a paso para aplicar el parche, enlaces directos a descargas de actualizaciones del fabricante, impacto esperado de la actualización (si requiere reinicio, si puede causar incompatibilidades y/o cambios en la funcionalidad), y opciones de mitigación alternativas si el parche no pudiera aplicarse inmediatamente.
- Deberá realizar un seguimiento de SLAs de remediación y compliance, permitiendo establecer SLAs de remediación diferenciados por criticidad de vulnerabilidad (por ejemplo: críticas en 7 días, altas en 30 días, medias en 90 días), con tracking automático del estado de cumplimiento, generación de alertas ante incumplimientos, y reporting ejecutivo de métricas de gestión de

vulnerabilidades incluyendo el tiempo medio de remediación (MTTR), la tasa de cierre de vulnerabilidades, el porcentaje de cumplimiento de SLAs, las tendencias temporales y comparativas por área, departamento o tipo de activo.

3.5. Protección de identidades y Active Directory

La plataforma ofertada deberá incluir capacidades nativas de protección de identidades mediante sensores que detecten, como mínimo, las siguientes 12 técnicas avanzadas de compromiso de identidad:

- Técnicas de Lateral Movement y Credential Theft:
 - Pass-the-Hash (PtH)
 - Pass-the-Ticket (PtT)
 - Mimikatz y herramientas de credential dumping
 - Ataques a LSASS para extracción de credenciales
- Técnicas de Persistencia y Escalación:
 - Golden Ticket
 - Silver Ticket
 - Privilege escalation attacks
 - Modificaciones no autorizadas en cuentas privilegiadas
- Técnicas de Reconnaissance:
 - LDAP enumeration
 - BloodHound y SharpHound reconnaissance
 - Kerberoasting
 - Unusual service logins y accesos anómalos

Adicionalmente, deberá usar técnicas avanzadas de compromiso de identidad, detección de movimientos laterales y ataques a Active Directory mediante análisis de comportamiento y machine learning, cumpliendo de manera obligatoria con los requisitos operativos y técnicos que se detallan a continuación, como mínimo:

- La detección deberá realizarse mediante análisis en tiempo real con latencia inferior a 5 segundos desde la ejecución de la técnica de ataque y con impacto <5% en los recursos de CPU durante operaciones normales (incluyendo picos de autenticación masiva en horarios de entrada de empleados), sin afectar los tiempos de autenticación de usuarios con latencia adicional máxima de 50 milisegundos, sin requerir modificaciones en el esquema de Active Directory, sin requerir de permisos de administrador del dominio para su instalación y sin generar tráfico adicional de replicación entre controladores de dominio. Las capacidades de detección de compromiso de identidades deberán basarse en análisis directo del tráfico de autenticación, replicación y comportamiento en memoria, sin depender exclusivamente de Windows Event Logs, sistemas SIEM externos ni configuraciones avanzadas de auditoría del sistema operativo.
- Deberá realizar análisis de comportamiento con machine learning de usuarios y entidades (UEBA) mediante modelos de machine learning que establezcan automáticamente líneas base de comportamiento normal para cada cuenta, especialmente cuentas privilegiadas y administrativas. Deberá detectar de anomalías en tiempo real, analizando horarios habituales de inicio de sesión con detección de accesos en horarios anómalos, ubicaciones geográficas típicas con alertas de accesos desde países inesperados, recursos y servidores accedidos normalmente con detección de accesos a sistemas fuera del scope habitual, aplicaciones y servicios utilizados regularmente, volumen de datos transferidos, número de intentos de autenticación, y cambios en patrones de navegación

- Deberá detectar técnicas de movimiento lateral y pivoting, incluyendo: Remote Desktop Protocol (RDP) desde equipos no habituales, PsExec y ejecución remota de comandos, uso de Windows Remote Management (WinRM), accesos SMB anómalos a recursos compartidos administrativos (C\$, ADMIN\$, IPC\$), uso de Windows Management Instrumentation (WMI) para ejecución remota, abusos de PowerShell Remoting, y propagación de credenciales mediante logon interactivo en múltiples sistemas.
- Deberá monitorizar continuamente cambios en permisos y membresías de grupos privilegiados, detectando adiciones a Domain Admins, Enterprise Admins, Schema Admins, o grupos personalizados con permisos elevados, modificaciones en permisos de GPO (Group Policy Objects), delegación de permisos Kerberos sospechosa, cambios en ACLs de objetos críticos de Active Directory, creación de cuentas de servicio con privilegios excesivos e intentos de escalación de privilegios local a SYSTEM o root.
- Deberá detectar intentos de acceso al proceso LSASS (Local Security Authority Subsystem Service) para extracción de credenciales en memoria, incluyendo el uso de herramientas como Mimikatz, ProcDump, Comsvcs.dll, o técnicas de process injection para leer memoria de LSASS, detección de volcados de memoria de LSASS mediante Task Manager o debug privileges, y protección contra técnicas de evasión como direct syscalls o unhooking.
- Deberá correlacionar detecciones de compromiso de identidad con inteligencia de amenazas sobre grupos APT conocidos, identificando TTPs específicas utilizadas por actores como APT28 (Fancy Bear), APT29 (Cozy Bear), APT41, Lazarus Group, FIN7, y otros grupos que utilizan técnicas avanzadas de ataques a Active Directory, con contexto sobre campañas recientes, sectores objetivo, y recomendaciones específicas de mitigación.
- Deberá realizar detección mediante análisis directo de tráfico de autenticación Kerberos y NTLM, inspección de consultas LDAP, y monitorización de replicación de Active Directory, sin depender únicamente de Windows Event Logs (que pueden ser deshabilitados o manipulados por atacantes), y sin requerir forwarding de logs a SIEM externo para detección básica.
- No se considerarán válidas aquellas soluciones cuya detección de compromiso de identidades dependa, total o parcialmente, de Windows Event Logs, Azure AD / Entra ID Logs, sistemas SIEM externos, recolección de logs mediante agentes genéricos ni configuraciones avanzadas de auditoría del sistema operativo para alcanzar el nivel de detección requerido.

3.6. Integración con otros sistemas: replicación y retención de telemetría

La plataforma ofertada deberá cumplir de manera obligatoria con los requisitos operativos y técnicos que se detallan a continuación:

- La plataforma deberá contar con integraciones certificadas y soportadas oficialmente por el fabricante con soluciones de terceros incluyendo SIEM, SOAR, ticketing, threat intelligence, firewalls y cloud security platforms., y deberá proporcionar APIs públicas documentadas (REST) para extracción de telemetría, gestión de configuración, automatización de respuesta y consultas de detecciones. Concretamente deberá poder integrarse con tecnologías existentes actualmente en EGARSAT. *El detalle de dichas tecnologías existentes actualmente en EGARSAT no se aporta como información pública al considerarse información sensible de seguridad. Esta información se facilitará bajo demanda y para ello, deberá enviarse un correo electrónico a licitaciones@egarsat.es indicando CIF y nombre de la empresa solicitante.*
- Deberá poder realizar replicación automática y desatendida, continua y fiable de telemetría de seguridad generada por los endpoints protegidos, permitiendo su almacenamiento a largo plazo, análisis forense retrospectivo, auditorías regulatorias y actividades avanzadas de threat hunting sobre históricos de varios años. Dicha funcionalidad deberá ser nativamente en arquitectura

cloud, sin necesidad de agentes adicionales ni infraestructura intermedia gestionada por EGARSAT,

- Deberá ofrecer una latencia máxima entre evento y disponibilidad en destino ≤ 15 minutos, así como garantizar la no pérdida de eventos incluso ante picos de generación de telemetría.
- Deberá tener independencia del entorno de destino, permitiendo replicación simultánea hacia uno o varios destinos.
- La telemetría extraída deberá preservar íntegramente, como mínimo todos los campos originales del evento, timestamps con precisión de milisegundos, relaciones y contexto entre eventos y el enriquecimiento de inteligencia de amenazas aplicado por la plataforma. No se admitirán soluciones que exporten datos resumidos, agregados o transformados de forma irreversible.
- Deberá garantizar que los datos replicados sean accesibles para búsquedas retrospectivas mediante herramientas especializadas de consulta sobre datalakes o sistemas de log management, con tiempo de respuesta inferior a 60 segundos para consultas sobre conjuntos de datos de varios años. Los datos históricos almacenados deberán ser accesibles sin requerir procesos manuales de restauración o rehidratación desde almacenamiento frío (cold storage).
- Mediante herramientas especializadas de consulta, deberá ser posible realizar búsquedas avanzadas con correlación temporal entre eventos históricos, soportando consultas complejas tipo: "Identificar todos los endpoints que ejecutaron PowerShell con encoding en las 2 horas previas a conexión hacia dominios .ru, y que además modificaron scheduled tasks en las 24 horas posteriores". Las consultas deberán soportar operadores booleanos avanzados (AND, OR, NOT, XOR), expresiones regulares, wildcards, agregaciones estadísticas y joins entre diferentes tipos de eventos.
- Deberá soportar exportación automática de telemetría en formatos estándar de la industria incluyendo: JSON estructurado (formato nativo detallado), CSV para análisis en hojas de cálculo o herramientas BI, Parquet para data lakes y análisis big data, XML para integración con sistemas legacy, CEF (Common Event Format) para SIEMs, SYSLOG RFC 5424 para log management, como mínimo. La configuración del formato de exportación deberá ser flexible y adaptable a las necesidades de consumo de cada sistema de destino.
- Deberá permitir exportaciones masivas de telemetría histórica de más de 1 TB de datos sin impacto perceptible en el rendimiento de la plataforma productiva de seguridad. Las exportaciones deberán poder programarse en horarios de bajo uso mediante jobs automáticos, con capacidad de reintento ante fallos de conectividad y verificación de integridad de datos exportados mediante checksums (MD5, SHA256).
- Deberá garantizar integridad criptográfica de datos almacenados mediante hashing SHA-256 de eventos individuales, timestamping criptográfico con precisión de milisegundos, y firma digital de archivos de exportación para verificación de cadena de custodia. Los datos en tránsito deberán cifrarse mediante TLS 1.2 o superior, y los datos en reposo deberán soportar cifrado mediante claves gestionadas o cifrado server-side del proveedor de almacenamiento.
- Deberá facilitar cumplimiento de regulaciones de retención extendida de logs de seguridad como es RGPD/GDPR (Artículo 5 sobre conservación de datos) Deberá proporcionar capacidad de generación de informes automáticos de cumplimiento demostrando disponibilidad y accesibilidad de los logs requeridos.

4. Servicios relacionados con la implantación y puesta en marcha de la solución

Todas las tareas desde el inicio de las mismas y hasta la puesta en marcha de la solución deberán ser

realizadas sin que suponga ningún corte en el servicio que se ofrece actualmente a los usuarios de EGARSAT y de forma totalmente transparente para ellos, y se realizarán en horario laborable de lunes a viernes, preferiblemente en horario de mañana. Para dichas tareas, el licitador deberá tener en cuenta en todo momento las indicaciones de EGARSAT, de tal forma que se prepare todo el entorno de forma consensuada. Las tareas incluidas en este apartado serán las siguientes:

- Configuración inicial:
 - Configuración y parametrización del entorno siguiendo la documentación de buenas prácticas aportada por el fabricante de la solución.
 - Diseño de las políticas de prevención y respuesta diferenciadas por tipo de endpoint.
 - Integración con Active Directory de EGARSAT para la automatización del despliegue.
 - Configuración de roles y permisos para el equipo de TI.
 - Diseño de dashboards personalizados tanto para los perfiles técnicos para su operación diaria de gestión de incidentes y eventos de seguridad, como para perfiles de supervisión de los trabajos realizados y su seguimiento.
- Despliegue de la solución:
 - Planificación de la migración desde la solución actual y del despliegue de forma faseada.
 - Acompañamiento en fase piloto y despliegue masivo: en este apartado en adjudicatario será el encargado, conjuntamente con los Administradores de Sistemas de EGARSAT, del despliegue en el 50% de los servidores corporativos y en el 20% de las estaciones de trabajo. El resto de despliegue será efectuado por EGARSAT, tutelado en todo momento por el adjudicatario. Se valorará en oferta técnica una mejora en este apartado.
 - Tareas de tuning para la optimización de las parametrizaciones de la plataforma para su correcta adaptación a la red, sistemas y aplicaciones ya existentes en EGARSAT.
 - Validación post-despliegue de instalación y validación de correcta conectividad del endpoint con la plataforma central, y validación de correcta aplicación de políticas definidas: se usarán los mismos criterios porcentuales para los servidores y estaciones de trabajo que en el punto anterior.
 - Realización de informes periódicos de progreso con métricas de cobertura.
- Colaboración para la integración de la plataforma con sistemas ya existentes en EGARSAT (plataformas de monitorización y/o NGSIEMs).
- Formación técnica y de gestión a los Administradores de Sistemas y a los Técnicos de Sistemas de EGARSAT sobre la solución implantada de 4 horas de duración, como mínimo. Esta formación deberá realizarse en horario laboral y mediante videoconferencia. Esta formación deberá realizarse posterior a la puesta en marcha del punto anterior. Aspectos mínimos a incluir en la formación:
 - Formación en administración de la consola de gestión.
 - Dimensionamiento y aprovechamiento al máximo la plataforma.
 - Análisis e interpretación de detecciones de seguridad.
 - Uso de capacidades de respuesta remota.
 - Técnicas de threat hunting proactivo
 - Casos de uso prácticos con simulaciones de escenarios reales.
 - Gestión de los eventos de seguridad (detecciones) generados por la plataforma a revisar por EGARSAT, asignación de dichos eventos a técnicos de EGARSAT para su seguimiento y respuesta, cierre de eventos.
 - Aspectos no incluidos en esta relación y que la empresa adjudicataria considere adecuada su inclusión en la formación.

Las tareas de formación no deberán demorarse más de 15 días naturales después de la finalización de la puesta en marcha. EGARSAT considerará finalizada la puesta en marcha cuando se haya desplegado la solución en el 100% de servidores y estaciones de trabajo con éxito y con todas las medidas y políticas de seguridad 100% operativas

Todas las tareas relacionadas en este apartado deberán ser realizadas por perfiles que dispongan de conocimientos, habilidades y destrezas específicos del ámbito de la seguridad. Deberán disponer de certificación técnica del fabricante de la solución ofertada para las tareas a realizar y contar con al menos 1 año de experiencia en implantación de la solución ofertada. Dicha certificación deberá estar vigente durante toda la vigencia del contrato.

Los servicios relacionados con la implantación y puesta en marcha de la solución (a excepción de las tareas de formación) no deberán demorarse más de 30 días naturales desde la fecha de inicio del contrato. Se valorará en oferta técnica una mejora en este apartado.

A la finalización de la formación y durante los 15 días naturales siguientes, como máximo, el adjudicatario deberá hacer entrega de la siguiente documentación:

- Documento de Configuración y parametrización del entorno que refleje las políticas, parámetros, ajustes aplicados a la plataforma, dashboards configurados y sus criterios, e configuración de las integraciones con otros sistemas existentes en EGARSAT.
- Guía de administración de la plataforma para los Administradores de Sistemas de EGARSAT.
- Guía de uso para casos habituales de análisis, interpretaciones de detecciones y gestión incidentes y eventos de seguridad para los Técnicos de Sistemas de EGARSAT.
- Inventario de Endpoints protegidos al cierre del despliegue, incluyendo estado de protección y conectividad
- Informe final de Despliegue.
- Material de Formación completo.

Todos los entregables deberán proporcionarse en su formato digital editable y mantenerse alineados con la configuración final desplegada en producción.

El incumplimiento en las mejoras ofertadas en los servicios relacionados con la implantación y puesta en marcha de la solución otorgará a EGARSAT la potestad para la aplicación de penalizaciones, tal y como se especifica en el Anexo 11 del Pliego de Cláusulas Administrativas Particulares.

5. Gestión del proyecto de implantación y puesta en marcha de la solución

Para garantizar la correcta puesta en marcha de la solución, la empresa adjudicataria designará un Jefe de Proyecto que actuará como interlocutor único con EGARSAT en esta fase de implantación. Deberá disponer de certificación técnica de gestión de la plataforma del fabricante de la solución ofertada para las tareas a realizar (la cual deberá estar vigente durante toda la vigencia del contrato), que serán las siguientes:

- Organizar, dirigir, representar y coordinar al equipo de trabajo que preste los servicios relacionados.
- Asegurar el nivel de calidad de las tareas realizadas.
- Proporcionar a EGARSAT la información periódica necesaria para el seguimiento de la implantación.

6. Servicios de mantenimiento y soporte en tiempo de operación de la nueva plataforma

Para garantizar la correcta ejecución de la prestación, el contrato contempla también los servicios de soporte técnico sobre la solución ofertada durante toda la vigencia del contrato. Estos servicios de soporte técnico deberán incluir, como mínimo:

- Horario 10x5 (de lunes a viernes de 8h a 18h).
- Forma de contacto con el soporte técnico (portal web, correo electrónico, chat en vivo y/o teléfono).

- Forma de contacto telefónica en horario 24x7 para casos críticos.
- Incidencias: asistencia ante averías y/o incidencias de funcionamiento de los servicios y apoyo en investigación de incidentes complejos, sea cual fuere su naturaleza, hasta su resolución.
- Consultas: asistencia ante consultas relacionadas con el funcionamiento de la plataforma, definición y aplicación de políticas, configuraciones, parametrizaciones, optimizaciones y asesoramiento sobre integración con otras herramientas existentes en EGARSAT.
- Actualizaciones sin sobre coste: cualquier componente que llegue al final de su ciclo de vida de forma no programada, o que presente una vulnerabilidad crítica, deberá ser actualizado por la empresa adjudicataria y colaborar con los Administradores de Sistemas de EGARSAT a su despliegue en la totalidad de equipos afectados (si dicha actualización lo requiriera) sin ningún coste adicional para EGARSAT.

SLA's de tiempos máximos de respuesta a incidencias y consultas:

Prioridad	Tiempos de respuesta
Incidencia Prioridad Crítica (notificación telefónica)	Inmediato
Incidencia Prioridad Alta	2h laborables
Incidencia Prioridad Normal	4h laborables
Consulta	8h laborables

El horario laboral se estipula de lunes a viernes de 8h a 18h. Se valorará en oferta técnica una mejora en los SLAs de tiempos máximos de respuesta a incidencias y consultas.

Adicionalmente, la empresa adjudicataria deberá ofrecer de forma anual 2 jornadas trabajo de 2 horas cada una de ellas (en horario laboral), destinadas a la revisión y mejora de la plataforma de forma conjunta y consensuada con los Administradores de Sistemas de EGARSAT. Se valorará en oferta técnica la inclusión de horas adicionales destinadas a la revisión y mejora de la plataforma.

Tanto las tareas de mantenimiento y soporte como las jornadas de trabajo deberán ser realizados por perfiles que dispongan de conocimientos, habilidades y destrezas específicos del ámbito de la seguridad. Deberán disponer de certificación técnica del fabricante de la solución ofertada para las tareas a realizar (la cual deberá estar vigente durante toda la vigencia del contrato) y contar con al menos 1 año de experiencia en la gestión de la solución ofertada.

A la finalización de cada jornada de trabajo y durante los siguientes 7 días naturales (a más tardar), el adjudicatario deberá entregar a EGARSAT un informe técnico que refleje:

- El detalle de las tareas realizadas, así como posibles propuestas de mejora motivadas.
- El % de disponibilidad mensualizado tanto del servicio cloud como de la consola de administración, de los últimos 6 meses.
- La relación de tickets abiertos por EGARSAT al soporte técnico del adjudicatario. Dicha relación deberá incluir, como mínimo: fecha/hora de apertura del ticket, descripción, prioridad asignada, fecha/hora de respuesta, fecha/hora de resolución, texto de resolución.

El incumplimiento en las mejoras ofertadas en este apartado otorgará a EGARSAT la potestad para la aplicación de penalizaciones, tal y como se especifica en el Anexo 11 del Pliego de Cláusulas Administrativas Particulares.

7. Gestión del servicio en tiempo de operación y transferencia tecnológica

Para garantizar la calidad de los servicios en tiempo de operación, la empresa adjudicataria designará un Jefe de Servicio que actuará como interlocutor único con EGARSAT. Deberá disponer de certificación técnica de gestión de la plataforma del fabricante de la solución ofertada para las tareas a realizar (la cual deberá estar vigente durante toda la vigencia del contrato), que serán las siguientes:

- Dirigir, representar y coordinar al equipo de trabajo que preste los servicios.

- Organizar la ejecución de la prestación del servicio.
- Asegurar el nivel de calidad de la prestación de los servicios.
- Proporcionar a EGARSAT la información periódica necesaria para el seguimiento de los servicios.

Durante toda la vigencia del contrato el adjudicatario, a través del Jefe de Servicio, se compromete a facilitar al responsable de supervisión de tareas designado por EGARSAT, toda la información y documentación que éste solicite para disponer de un pleno conocimiento técnico de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos, y herramientas utilizadas para resolverlos. Deberá asistir a aquellas reuniones que EGARSAT considere necesarias para el buen desarrollo del servicio, y quedará a potestad de EGARSAT decidir si a dichas reuniones deben acudir también los técnicos asignados al servicio.

8. Finalización del servicio

A la finalización del servicio, el licitador deberá realizar una jornada de trabajo conjuntamente con los Administradores de Sistemas de EGARSAT a modo de guía y acompañamiento para la retirada de los sensores de todos los equipos corporativos.

9. Medio ambiente

El proveedor será responsable de cumplir con la legislación medioambiental comunitaria, estatal, autonómica y local vigente durante toda la vigencia del contrato.

EGARSAT podrá requerir justificantes al adjudicatario que acrediten la adecuada gestión medioambiental de los residuos, reservándose el derecho de repercutir sobre el adjudicatario las acciones y gastos que haya incurrido EGARSAT por la falta de diligencia de la empresa adjudicataria en materia de residuos.

10. Precio

Servicios al inicio de proyecto. Desglose de precios:

Descripción	Importe máximo (SIN IVA)
Servicios relacionados con la implantación y puesta en marcha de la solución	15.000,00 €

Suministros y servicios anuales. Desglose de precios:

Descripción	Importe máximo anual (SIN IVA)
Suministro de licencias	53.000,00 €
Servicios de mantenimiento y soporte en tiempo de operación	3.500,00 €
TOTAL	56.500,00 €

Duración inicial del contrato: 3 años.

Prórrogas previstas: 2 prórrogas de 1 año de duración cada una de ellas.

Forma de pago:

A la finalización de las tareas incluidas en “Servicios al inicio de proyecto” se abonará:

- el importe ofertado correspondiente al ítem “Servicios relacionados con la implantación y puesta en marcha de la solución”
- el importe ofertado correspondiente al ítem “Suministro de licencias” para la totalidad de la duración inicial del contrato (es decir, “Suministro de licencias” multiplicado por 3)
- el importe anual ofertado correspondiente al 1er año del ítem “Servicios de mantenimiento y soporte en tiempo de operación”

Al inicio de la 2ª anualidad y posteriores, el importe correspondiente al ítem “Servicios de mantenimiento y soporte en tiempo de operación”.

Al inicio de cada una de las prórrogas se abonarán los importes anuales ofertados correspondientes a los ítems “Suministro de licencias” y “Servicios de mantenimiento y soporte en tiempo de operación”.

Firmado digitalmente por Jordi Trabal (Jefe del Departamento de Producción y Operaciones TI de EGARSAT).

Jordi
Trabal
Esquerda

Firmado
digitalmente por
Jordi Trabal
Esquerda
Fecha: 2026.02.26
15:25:53 +01'00'