

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE LA “RENOVACIÓN DEL LICENCIAMIENTO Y DE LOS SERVICIOS MANTENIMIENTO Y SOPORTE DEL SISTEMA DE CORTAFUEGOS EXISTENTE PARA EGARSAT, MUTUA COLABORADORA CON LA SEGURIDAD SOCIAL Nº 276”.

1. Antecedentes y situación actual

EGARSAT dispone actualmente de una plataforma corporativa de seguridad plenamente implantada y en explotación, concebida como un entorno integrado que articula de forma coordinada la protección perimetral, la monitorización, el análisis de eventos, la gestión de endpoints y la administración de los sistemas. Esta plataforma no responde a soluciones aisladas, sino a un modelo operativo consolidado basado en la integración funcional entre sus distintos componentes y en la gestión centralizada de las capacidades de seguridad. Dentro de este esquema, la infraestructura de seguridad de red desempeña un papel fundamental como elemento de protección del perímetro corporativo, interrelacionándose de forma directa con los sistemas de análisis y registro de eventos, así como con las herramientas de gestión y control del entorno. Asimismo, la organización dispone de mecanismos de supervisión centralizada que permiten mejorar la visibilidad operativa, reforzar la trazabilidad de las actuaciones y facilitar la gestión continua de la seguridad, así como de una plataforma de protección del puesto de trabajo integrada en la operativa diaria del área técnica.

La arquitectura existente presenta un elevado grado de interdependencia entre sus componentes, de modo que su eficacia no depende únicamente de las capacidades individuales de cada elemento, sino de su integración, del intercambio de información de seguridad y del mantenimiento de un modelo homogéneo de administración. Esta realidad ha dado lugar a la consolidación de procedimientos, configuraciones y prácticas operativas alineadas con dicha arquitectura, constituyendo un entorno estable, conocido y plenamente integrado en el funcionamiento ordinario de la organización.

Esta arquitectura constituye una solución integrada, certificada y soportada por el fabricante, implantada conforme a buenas prácticas del sector y alineada con los requisitos del Esquema Nacional de Seguridad (ENS) - Nivel Medio. Es por este motivo que el contratista 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. La certificación presentada deberá estar vigente durante toda la vigencia del contrato. Se valorará en oferta técnica una mejora en este apartado.

El detalle de los componentes actualmente en servicio, así como el detalle del módulo adicional de análisis y centralización de registros y el detalle del módulo de control de endpoints 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.

Todos estos elementos se encuentran plenamente integrados en el modelo operativo vigente y forman parte esencial del funcionamiento ordinario del entorno de seguridad.

La necesidad que motiva la presente contratación se enmarca en la evolución de esta plataforma existente, y no en la implantación de un nuevo modelo de seguridad. El objeto es garantizar la continuidad operativa del entorno, renovar determinados componentes cuya adecuación tecnológica lo requiere, reforzar capacidades existentes y ampliar funcionalidad en áreas específicas, manteniendo la coherencia técnica y operativa del conjunto. En particular, resulta necesario abordar la renovación de los licenciamientos de las funcionalidades de la infraestructura de seguridad de red actualmente contratadas, renovar los equipos que por su antigüedad están próximos a su obsolescencia tecnológica y adecuar las capacidades tanto de la plataforma de análisis de eventos como de la plataforma de gestión de endpoints actualmente implantadas. Estas actuaciones deben entenderse como una evolución del entorno existente y no como una sustitución desvinculada de su arquitectura actual.

La experiencia operativa demuestra que el valor de la plataforma reside en su integración funcional, que

permite una administración eficiente, una mayor coherencia en la aplicación de políticas, una mejor capacidad de respuesta y una reducción de la complejidad técnica. En consecuencia, cualquier actuación sobre este entorno debe preservar dicha lógica de plataforma, evitando soluciones que impliquen ruptura del modelo existente, pérdida de capacidades de integración o incremento innecesario de la complejidad operativa. En este sentido, la contratación deberá contemplarse no solo desde la perspectiva de la capacidad individual de los componentes, sino desde su compatibilidad e integración con la arquitectura existente. EGARSAT ha realizado una inversión tecnológica y organizativa significativa, incluyendo no solo infraestructura y licencias, sino también procedimientos, configuraciones y conocimiento técnico, cuya preservación responde a criterios de eficiencia, buena administración y minimización de riesgos. Por ello, la evolución de la plataforma deberá garantizar la continuidad tecnológica del entorno, evitando la introducción de soluciones que requieran rediseños sustanciales, la incorporación de herramientas adicionales de gestión o integración, o la generación de dependencias técnicas no alineadas con el modelo actual. Asimismo, deberá prevenirse cualquier fragmentación del ecosistema de seguridad o pérdida de visibilidad y control centralizado.

En definitiva, la presente contratación responde a la necesidad de asegurar una evolución coherente de la plataforma corporativa de seguridad, preservando su integración, su modelo de operación y su capacidad funcional, y garantizando que cualquier mejora o renovación se realice sin degradación del entorno existente ni incremento desproporcionado de la complejidad técnica u organizativa.

2. Objeto y alcance del contrato

La presente contratación tiene como finalidad asegurar la adecuación de la plataforma corporativa de seguridad a las necesidades actuales de EGARSAT, tanto desde el punto de vista tecnológico como operativo, garantizando su evolución de forma coherente con el entorno existente y con los requerimientos de seguridad, gestión y explotación propios de la organización, todo ello en el marco de la arquitectura tecnológica actualmente implantada y en explotación

En este sentido, la actuación persigue, en primer lugar, la actualización de aquellos componentes cuya capacidad, ciclo de vida o adecuación funcional requieren una revisión, permitiendo disponer de una infraestructura alineada con las exigencias actuales en términos de rendimiento, capacidad de tratamiento de información y sostenibilidad del servicio en el tiempo. Asimismo, el contrato tiene como objetivo reforzar la visibilidad y la capacidad de análisis sobre el entorno de seguridad, facilitando una gestión más eficiente de los eventos, una mejor comprensión del comportamiento del sistema y una mayor capacidad de supervisión por parte del área técnica. De igual modo, se requiere adecuar a las nuevas necesidades volumétricas las capacidades de protección del puesto de trabajo ya implantadas, asegurando la continuidad de los mecanismos actualmente en uso y su correcta integración dentro del conjunto de la plataforma de seguridad.

Junto a lo anterior, constituye un objetivo esencial de la contratación asegurar que la evolución de la plataforma permita mantener un modelo de gestión eficiente, homogéneo y sostenible, evitando incrementos innecesarios de complejidad técnica, reduciendo la carga operativa asociada a la administración del entorno y facilitando la prestación del servicio por parte del equipo técnico. Finalmente, la contratación persigue garantizar que la solución resultante se integre de manera efectiva dentro del ecosistema tecnológico de EGARSAT, permitiendo una explotación coordinada de sus distintos componentes y una gestión unificada de las capacidades de seguridad, en condiciones de estabilidad operativa y con un nivel adecuado de soporte y mantenimiento durante todo el periodo de vigencia del contrato.

La contratación se concibe como una actuación integral orientada a garantizar la adecuación tecnológica y la mejora funcional de dicha plataforma, comprendiendo tanto la renovación de aquellos componentes que así lo requieren como la continuidad y adaptación de capacidades ya existentes, manteniendo en todo caso la coherencia técnica y operativa del entorno. En particular, el alcance del contrato incluye, de forma conjunta y no independiente:

- la renovación de la infraestructura de seguridad de red actualmente en servicio mediante el suministro de 2 nuevos equipos

- los servicios profesionales para la implantación efectiva de la solución, incluyendo la planificación, instalación, configuración, parametrización, migración desde la situación actual, realización de pruebas, validación y puesta en producción, así como el soporte inicial durante la fase de arranque y estabilización
- la adecuación de la capacidad de la plataforma de análisis y registro de eventos de seguridad existente
- la adecuación de la volumetría de equipos protegidos en la plataforma de gestión de endpoints existente
- todo el licenciamiento necesario para el correcto funcionamiento de la solución durante toda la vigencia del contrato, con el mismo nivel de soporte oficial del fabricante que el que se dispone actualmente
- los servicios profesionales de mantenimiento y soporte de toda la plataforma tanto a nivel de hardware como de software por parte del adjudicatario durante toda la vigencia del contrato, garantizando su disponibilidad, actualización y correcto funcionamiento, tanto en lo relativo a los elementos objeto de renovación o ampliación como a aquellos cuya continuidad forma parte de la plataforma corporativa de seguridad

La ejecución del contrato deberá asegurar que todos los elementos suministrados y los servicios asociados configuren un entorno plenamente operativo, integrado y alineado con la arquitectura existente y con el modelo de gestión de EGARSAT. A estos efectos, no se considerará suficiente la mera entrega de equipamiento o licencias, sino que se requerirá la provisión efectiva de una solución implantada, funcional y adaptada a los requerimientos operativos de la organización. Todas las actuaciones deberán ejecutarse de forma coordinada, asegurando su correcta integración en el entorno existente y su funcionamiento conjunto como una solución única.

Los licitadores deberán presentar, dentro del SOBRE B, una memoria técnica que detalle la solución propuesta y que deberá ajustarse al contenido previsto en el Anexo 9 del Pliego de Cláusulas Administrativas Particulares.

La información contenida en la memoria técnica será utilizada para verificar el cumplimiento de los requisitos y prescripciones establecidos en presente pliego, pudiendo dar lugar la falta de adecuación a los mismos, así como la falta de presentación de la información exigida, a la exclusión de la oferta. Asimismo, el contenido de la memoria servirá para la valoración de los criterios evaluables.

Toda la documentación requerida para la evaluación de las ofertas deberá entregarse en idioma español (sin perjuicio de que la documentación técnica oficial del fabricante pueda aportarse en inglés cuando no exista versión disponible en español ni en catalán).

Toda la documentación requerida durante toda la vigencia del contrato deberá entregarse en idioma español (sin perjuicio de que la documentación técnica oficial del fabricante pueda aportarse en inglés cuando no exista versión disponible en español ni en catalán), en formato electrónico, editable y reutilizable por EGARSAT.

Toda la interacción con personal de EGARSAT durante toda la vigencia del contrato deberá realizarse en idioma español o catalán.

3. Descripción y requisitos técnicos de la solución e integración con la arquitectura existente

La solución objeto del presente contrato deberá configurarse como una evolución de la plataforma corporativa de seguridad actualmente implantada, proporcionando un conjunto integrado de capacidades orientadas a la protección de red, la supervisión y análisis de eventos, la gestión de endpoints y la administración centralizada del entorno, todo ello alineado con la arquitectura existente y con el modelo operativo de EGARSAT.

La solución deberá articularse como un entorno unificado en el que sus distintos componentes operen de

forma coordinada, permitiendo una gestión centralizada, una visibilidad global del estado del sistema y una explotación homogénea del conjunto. En este sentido, se exige que la funcionalidad de la solución derive tanto de las capacidades individuales de cada elemento como de su capacidad de integrarse de forma efectiva y de compartir información relevante de seguridad de manera automatizada. A tal efecto, la solución deberá basarse en un modelo de integración nativa entre sus componentes, permitiendo el intercambio de información de seguridad, la correlación de eventos y la aplicación coherente de políticas, sin necesidad de desarrollos específicos, mecanismos intermedios o herramientas ajenas al modelo existente.

En el ámbito de la seguridad de red, la solución deberá proporcionar capacidades avanzadas de protección del perímetro, incluyendo mecanismos de inspección del tráfico, control de accesos, segmentación y detección y prevención de amenazas, garantizando al mismo tiempo niveles adecuados de rendimiento, disponibilidad y resiliencia acordes con las necesidades del entorno.

En relación con la supervisión y análisis de eventos, la solución deberá permitir la recogida, almacenamiento, tratamiento y explotación de la información generada por los distintos componentes de la plataforma, proporcionando una visión centralizada que facilite la monitorización, el análisis y la gestión de la seguridad. Dichas capacidades deberán estar adecuadamente dimensionadas y permitir su evolución sin necesidad de rediseñar la arquitectura global.

Por su parte, la gestión de la seguridad en los endpoints deberá mantenerse como un elemento plenamente integrado en la solución, adecuando el volumen de equipos protegidos a las nuevas necesidades, asegurando la continuidad de las capacidades existentes y su correcta interoperabilidad con el resto de los componentes, permitiendo la aplicación de políticas de seguridad coherentes y el intercambio de información relevante con la infraestructura de seguridad de red.

La solución deberá proporcionar asimismo capacidades integradas de monitorización, registro y trazabilidad, que permitan el seguimiento de la actividad del sistema y la auditoría de las actuaciones realizadas, sin depender de soluciones externas no alineadas con el entorno principal.

En todo caso, la solución ofertada deberá integrarse en la arquitectura existente de forma directa y efectiva, garantizando su correcto funcionamiento desde el punto de vista técnico y operativo, permitiendo mantener los procedimientos, configuraciones y dinámicas de gestión actualmente en uso. Adicionalmente, deberá poder integrarse con otra infraestructura existente en EGARSAT.

El detalle de la infraestructura existente 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.

Los licitadores deberán acreditar el cumplimiento de los requisitos establecidos, demostrando de forma objetiva la compatibilidad de la solución propuesta con el entorno de EGARSAT y su capacidad para integrarse en el mismo sin introducir complejidad adicional, duplicidad de herramientas o dependencias técnicas no justificadas.

4. Condiciones técnicas específicas de los componentes incluidos en la solución

Los componentes que integren la solución objeto del contrato deberán cumplir, con carácter mínimo y obligatorio, las condiciones técnicas establecidas en el presente apartado. Todos los requisitos recogidos en este epígrafe tendrán la consideración de prescripciones técnicas esenciales, de modo que su incumplimiento, su acreditación insuficiente o su contradicción con la documentación aportada determinarán la no conformidad de la oferta con el presente Pliego.

La solución ofertada deberá responder a una arquitectura plenamente operativa, homogénea e integrada, compatible con los componentes actualmente implantados en EGARSAT cuya continuidad forma parte del objeto del contrato. No se admitirán soluciones que, para alcanzar el cumplimiento de los requisitos

exigidos, precisen la sustitución de elementos no incluidos expresamente en el alcance contractual, ni aquellas que requieran la incorporación de plataformas adicionales, herramientas intermedias, conectores específicos o desarrollos a medida para obtener los niveles de integración requeridos.

Los equipos propuestos como referencia funcional y prestacional a integrarse en la plataforma de seguridad con el fin de garantizar la continuidad tecnológica, la compatibilidad operativa y la integración nativa con los componentes cuya continuidad forma parte del contrato, no se aportan 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 acreditarse de forma suficiente el cumplimiento íntegro de todos los requisitos técnicos, funcionales, de rendimiento, conectividad, integración y operación establecidos en el presente Pliego.

4.1. Infraestructura de seguridad de red

La solución deberá incluir el suministro de dos (2) equipos físicos de seguridad de red de nueva adquisición a través de los canales oficiales para la comercialización de estos equipos en España. Los equipos deben ser nuevos sin haber tenido ninguna titularidad anterior, e iguales entre sí. Con el fin de asegurar que no habrá riesgo de obsolescencia tecnológica, no se aceptarán equipos o componentes respecto de los cuales el fabricante haya anunciado, con anterioridad a la fecha límite de presentación de ofertas, la finalización de su comercialización, su retirada del catálogo para nuevas adquisiciones, o cuyo fin de soporte oficial por parte del fabricante tenga lugar durante el periodo de ejecución del contrato, incluidas sus posibles prórrogas.

A efectos de cumplimiento del Esquema Nacional de Seguridad (ENS), los equipos ofertados deberán estar incluidos en el Catálogo STIC-105 (CPSTIC) con Categoría ENS “Alta”, según lo establecido por el Centro Criptológico Nacional. En caso de que los equipos ofertados no estén incluidos en el Catálogo STIC-105 (CPSTIC) con Categoría ENS “Alta”, también se aceptarán dichos equipos si acreditan certificación Common Criteria (ISO/IEC 15408) válida, de conformidad con lo previsto en el artículo 19 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Los equipos ofertados estarán destinados a operar como infraestructura principal de protección perimetral de EGARSAT en configuración de alta disponibilidad, con sincronización nativa y completa de estado, sesiones y configuración. Cada uno de los equipos ofertados deberá reunir, como mínimo, las siguientes características técnicas, acreditadas mediante documentación oficial del fabricante:

- arquitectura Next Generation Firewall (NGFW) para entornos corporativos
- formato appliance físico para instalación en CPD
- configuración nativa en alta disponibilidad activo/pasivo. No obstante, se requiere que los equipos permitan adicionalmente una configuración en alta disponibilidad activo/activo para cubrir posibles necesidades futuras
- soporte de inspección de tráfico a nivel de aplicación
- detección y prevención de intrusiones (IPS)
- filtrado web y control de contenidos
- control de aplicaciones
- inspección de tráfico cifrado SSL/TLS
- soporte de VPN IPsec y SSL VPN
- capacidades de segmentación, control entre redes internas y zonas DMZ, y aplicación de políticas basadas en múltiples criterios de red, usuario, servicio y aplicación.
- configuración de políticas de capa 7

Adicionalmente, cada equipo, considerado individualmente y sin agregación de capacidades entre nodos del cluster, deberá acreditar los siguientes valores de capacidad y rendimiento:

- rendimiento IPS no inferior a 9 Gbps
- rendimiento NGFW no inferior a 7 Gbps
- rendimiento de protección frente a amenazas no inferior a 6 Gbps
- rendimiento de control de aplicaciones (HTTP 64K) no inferior a 27 Gbps
- rendimiento Isec VPN (512 bytes / AES256-SHA256) no inferior a 36Gbps:
 - número de túneles Gateway-to-Gateway soportados no inferior a 2000
 - número de túneles Client-to-Gateway soportados no inferior a 16.000
- número de políticas configurables no inferior a 10.000
- firewall IPv4 y IPv6 (1518 / 512 / 64 byte, UDP) no inferior a 39 / 39 / 26,5 Gbps
 - latencia firewall (64 bytes, UDP): 5 µs como máximo
 - paquetes por segundo como firewall no inferior a 39 Mpps
- capacidad de sesiones concurrentes no inferior a 11.000.000
- capacidad de nuevas sesiones por segundo no inferior a 390.000

En cuanto a características de los componentes físicos de cada equipo:

- tamaño máximo de 1RU en armario rack estándar (no superior)
- doble fuente de alimentación redundante e integrada, diseñada conforme a criterios de alta eficiencia energética, minimizando el consumo eléctrico y la generación de calor en condiciones normales de funcionamiento. A estos efectos, se considerará adecuado el cumplimiento de certificaciones reconocidas de eficiencia energética, tales como 80 PLUS o equivalentes, o bien la acreditación, mediante documentación técnica oficial del fabricante, de niveles de eficiencia energética comparables y adecuados a entornos de operación continua en CPD
- módulo TPM integrado

En cuanto a conectividad, cada equipo deberá disponer, como mínimo, de:

- dos (2) puertos 1GbE RJ45 dedicados a gestión y HA
- ocho (8) puertos 1GbE RJ45
- ocho (8) puertos RJ45 multigigabit 5/2,5/1 GbE
- ocho (8) puertos 10 GbE SFP+/SFP
- cuatro (4) puertos 1 GbE SFP o puertos SFP/SFP+ compatibles con operación a 1 GbE
- un (1) puerto de consola
- un (1) puerto USB

Los requisitos de conectividad indicados deberán entenderse referidos a puertos físicos integrados y simultáneamente disponibles en cada appliance ofertado, sin que pueda considerarse cumplimiento válido la reasignación excluyente de puertos, la suma alternativa de interfaces de distinta naturaleza o de ambos nodos del clúster (debiendo alcanzarse los mínimos indicados por cada appliance individualmente considerado) o la necesidad de módulos, equipos o elementos externos no incluidos expresamente en la oferta base.

En cuanto a funcionalidades de software, todas las funcionalidades de seguridad indicadas deberán estar incluidas, licenciadas y disponibles (para cualquiera de los 2 equipos) para su uso efectivo durante todo el periodo de vigencia del contrato, sin que se admitan funcionalidades parciales y/o incompletas:

- Protección Antimalware: esta funcionalidad deberá proteger contra la transmisión de código malicioso, referido normalmente como malware (troyanos, virus, gusanos, exploits de puerta trasera, spyware, etc.). Para ello deberá incluir perfiles de seguridad antivirus de forma integrada contra una variedad de amenazas, incluyendo códigos conocidos o desconocidos (malware), y también APTs (Advanced Persistent Threats). Deberá permitir configurar que

el firewall aplique la protección antivirus a las sesiones HTTP, FTP, IMAP, POP3, SMTP, NNTP, HTTPS, IMAPS, POP3S, SMTPS, y FTPS.

El motor de escaneo antimalware deberá utilizar una base de datos de firmas de virus (signature database) en la que se detallen los atributos únicos de cada infección. El escáner de antimalware deberá buscar en estas firmas y si localiza un patrón en la red, el firewall deberá determinar si el fichero está infectado y tomar la acción configurada en su política (por ejemplo, impedir la descarga, bloquear la sesión, etc.). Las técnicas que deberá usar este motor de antimalware deberán ser, como mínimo, escaneo de virus, protección grayware, escaneo heurístico, protección de conexión a botnets conocidas y a sitios que incluyan phishing.

La actualización de la base de datos donde se conecte el firewall para obtener información de nuevas amenazas deberá ser automática (descarga e instalación) y con una frecuencia diaria, como mínimo. Esta base de datos deberá ser facilitada por el fabricante de los equipos de forma globalmente distribuida, garantizando que el servicio de actualizaciones no se vea interrumpido y que los equipos siempre tengan acceso a la última definición de amenazas.

- **Filtrado URLs:** esta funcionalidad deberá permitir proteger de URLs y contenidos web no apropiados. Los filtros deberán filtrar, como mínimo, en base a URLs, categorías, contenidos, scripts web y escaneo antimalware.

En cuanto al filtrado URL, éste deberá bloquear o permitir URLs específicas añadiéndolas a listas de filtrado. Para añadir las URLs deberán poder utilizarse patrones de texto, comodines o expresiones regulares. El sistema deberá permitir configurar listas blancas y listas negras. Además de permitir y bloquear, deberá poderse configurar monitorización y crear excepciones. En caso de bloquear el acceso a un usuario, deberá mostrarle un mensaje para su información.

En cuanto al filtrado de contenidos, éste deberá bloquear el acceso a webs que contengan patrones determinados de contenido. Estos patrones deberán poder configurarse específicamente mediante palabras, frases, comodines y expresiones regulares. Este filtrado deberá detectar scripts y códigos maliciosos, así como bloquear contenido web inseguro, tal como Java Applets, Cookies y ActiveX. Se deberán poder escoger categorías a filtrar en base a bases de datos del fabricante que ya haya pre-categorizado contenido web.

- **Control de aplicaciones:** esta funcionalidad deberá determinar qué aplicaciones pueden operar en la red en función de políticas, y restringir el uso de estas aplicaciones según las configuraciones de políticas de seguridad. Permitirá por tanto que el entorno de firewall detecte y tome decisiones sobre el tráfico de la red en función de la aplicación que lo haya generado. El sistema deberá detectar dichas aplicaciones, aunque el tráfico generado por las mismas no use los puertos y los protocolos estándar de dicha aplicación.

El sistema deberá disponer de un catálogo de aplicaciones pre-identificadas por parte del fabricante, así como los servicios y protocolos que éstas utilizan, de forma que sea fácil para los equipos detectar las aplicaciones de uso más común y poder aplicar las políticas configuradas. Este catálogo deberá disponer de conocimiento de al menos 2000 aplicaciones identificables, y deberá ser actualizado desde la nube de forma automática por el fabricante de los equipos sin necesidad de intervención por parte de los Administradores de Sistemas de EGARSAT.

Este catálogo deberá facilitar información útil sobre las aplicaciones incluidas para las que se permitan configurar distintas acciones (permitir, denegar, monitorizar y poner en cuarentena, como mínimo) de manera sencilla. Para ello deberá facilitar al menos la siguiente información sobre cada aplicación:

- nombre de la aplicación
- categoría (Business, Botnet, Collaboration, Audio/Video, etc.)
- tecnología (Browser, Client to Server, P2P, etc.)
- popularidad (mediante una puntuación que al menos permita la comparación con el resto de las aplicaciones del catálogo)
- riesgo que supone (si se trata de un malware, si pertenece a una red botnet, si consume

un ancho de banda alto, etc.)

- Prevención de intrusiones: esta funcionalidad deberá proteger la red de actividades o comportamientos que concuerden con técnicas de intrusión en la red. Los equipos deberán ser capaces de detectar dichas técnicas y bloquear la intrusión. La detección deberá realizarse tanto mediante firmas como mediante patrones de comportamiento anómalo. Por tanto, esta funcionalidad deberá incluir decodificadores de protocolo que analicen el tráfico por protocolo, pudiendo comparar con las firmas de dicho protocolo concreto y facilitando la eficiencia en el uso de recursos de la máquina.

La funcionalidad de prevención de intrusiones deberá poderse configurar de varias formas:

- mediante identificación basada en patrones (Pattern-Based), seleccionando los atributos asociados con el tipo de ataque: aplicación afectada por el ataque, sistema operativo, protocolo (usado como vector de ataque), severidad (nivel de amenaza) y objetivo (target)
- mediante identificación basada en puntuación (Rate-Based). En la base de datos de firmas IPS, deberán existir unas firmas por defecto con la acción asociada
- configuradas a mano, mediante especificación manual que pudieran requerir los Administradores de Sistemas de EGARSAT

Las acciones que se deben poder configurar cuando se detecta una concordancia con una firma IPS, es decir, un intento de intrusión en la red, deben ser:

- permitir (permite el tráfico)
- monitorizar (permite el tráfico y registra la actividad de éste)
- bloquear (descarta el tráfico)
- reiniciar (cierra la sesión que originó el tráfico)
- cuarentena (rechaza el tráfico de esa IP origen durante un tiempo. Dicho tiempo deberá ser configurable)

Esta base de datos deberá ser actualizada desde la nube de forma automática por el fabricante de los equipos sin necesidad de intervención por parte de los Administradores de Sistemas de EGARSAT.

Otras funcionalidades requeridas:

- los equipos deberán permitir crear instancias lógicas de firewall, es decir, permitir disponer de distintos entornos de firewall segmentados entre sí que se ejecuten en el mismo hardware. Cada una de estas instancias deberá poder permitir asignación de interfaces propias (físicas o lógicas/VLAN), disponer de su propia colección de objetos, políticas de filtrado, tablas de enrutamiento y configuraciones de VPN. Esta funcionalidad por tanto debe posibilitar una segmentación total dentro del firewall, permitiendo un mínimo de 10 instancias lógicas de firewall en cada dispositivo. Este número de instancias deberá poder crecer a futuro, aunque para ello se requieran de softwares y/o licencias adicionales (no objeto de este pliego).
- los equipos deberán disponer de capacidades nativas de gestión o integración centralizada con elementos de red y acceso del mismo ecosistema tecnológico, incluyendo switches, puntos de acceso inalámbrico y mecanismos de autenticación multifactor, debiendo acreditarse documentalmente los límites máximos soportados por el fabricante.
- los equipos deberán incorporar mecanismos de seguridad física que garanticen que únicamente firmware autorizado y validado por el fabricante de los mismos pueda ser instalado en los mismos.

Los equipos ofertados deberán ser, además, plenamente compatibles con la plataforma de análisis y centralización de registros actualmente implantada en EGARSAT cuya continuidad forma parte del contrato, así como con la plataforma de gestión de endpoints y acceso remoto actualmente desplegada, debiendo permitir, como mínimo:

- el envío nativo de logs y eventos de seguridad
- la correlación de eventos con la plataforma de análisis y registros
- la recepción y explotación de telemetría de endpoint
- su integración deberá permitir la utilización directa de la información de estado de los endpoints por parte de la infraestructura de seguridad de red, sin mecanismos intermedios de traducción, exportación o tratamiento externo de dicha información
- la aplicación de políticas o controles de acceso en función del estado del endpoint
- la operación coordinada del entorno sin recurrir a soluciones de terceros

No se considerará suficiente, a estos efectos, la mera interoperabilidad genérica mediante syslog estándar, integraciones parciales, conectores de terceros o desarrollos específicos no soportados oficialmente por el fabricante. En ningún caso se considerará válido el cumplimiento mediante soluciones que requieran la sustitución, desactivación o bypass de los componentes actualmente implantados cuya continuidad forma parte del objeto del contrato.

4.2. Plataforma de análisis, centralización de registros y explotación de eventos

La solución deberá incluir la adecuación de la plataforma de análisis y centralización de registros actualmente implantada, manteniendo dicha plataforma y ampliando su capacidad hasta un mínimo agregado equivalente a 6 GB/día, conservando la compatibilidad y continuidad del ecosistema actualmente existente. La plataforma resultante deberá permitir, como mínimo:

- la recepción centralizada de logs y eventos generados por la infraestructura de seguridad de red
- el almacenamiento estructurado y consultable de la información
- la explotación de registros mediante búsquedas, filtros, informes y análisis
- la correlación de eventos de seguridad
- la generación de alertas
- la visibilidad centralizada del comportamiento del entorno

No se admitirán propuestas que, para alcanzar el dimensionamiento requerido, supongan la sustitución de la plataforma actualmente existente por una herramienta distinta no contemplada en el objeto del contrato, ni aquellas que basen el cumplimiento en plataformas externas ajenas al ecosistema actual.

La integración entre la infraestructura de seguridad de red y la plataforma de análisis y registros deberá ser nativa, directa y soportada oficialmente por el fabricante, debiendo quedar acreditado que la solución permite la explotación conjunta de la información de seguridad sin desarrollos complementarios ni componentes intermedios no previstos. En ningún caso se considerará válido el cumplimiento mediante soluciones que requieran la sustitución, desactivación o bypass de los componentes actualmente implantados cuya continuidad forma parte del objeto del contrato.

4.3. Plataforma de gestión y protección de endpoints

La solución deberá contemplar la continuidad del licenciamiento, con el mismo nivel de soporte oficial del fabricante que el que se dispone actualmente, y operativa de la plataforma de protección de endpoints actualmente implantada, adecuando el volumen de equipos a cubrir hasta 250 dispositivos, manteniendo sus capacidades funcionales y su integración con el resto de la plataforma de seguridad. La solución deberá permitir, como mínimo:

- la gestión centralizada de los endpoints protegidos mediante plataforma a tal efecto
- la aplicación de políticas de seguridad sobre los dispositivos
- la continuidad de las funcionalidades de acceso remoto seguro actualmente utilizadas
- la telemetría de endpoint y supervisión de su estado de seguridad

- la interoperabilidad con la infraestructura de seguridad de red
- la aplicación de controles o políticas en función del estado del endpoint
- la integración con la plataforma de análisis y registros

No se admitirán propuestas que, para dar cumplimiento al contrato, requieran la sustitución, la desactivación o el bypass de la plataforma de gestión de endpoints actualmente implantada cuya continuidad forma parte del objeto del contrato, ni aquellas que basen la interoperabilidad exigida en mecanismos externos al fabricante, conectores no nativos o integraciones no soportadas oficialmente.

4.4. Licenciamiento, suscripciones, mantenimiento y soporte del fabricante

Todos los componentes incluidos en la solución deberán suministrarse con el licenciamiento, suscripciones y mantenimiento y soporte técnico oficial del fabricante necesarios para su funcionamiento completo durante toda la vigencia del contrato. Dicho alcance deberá incluir, como mínimo:

- soporte técnico oficial del fabricante con el mismo nivel de soporte que el que se dispone actualmente
- acceso a actualizaciones de software y firmware
- acceso a actualizaciones de firmas, motores y bases de datos asociadas a las funcionalidades de seguridad contratadas
- derecho de uso de todas las funcionalidades requeridas en el presente Pliego
- mantenimiento de la compatibilidad operativa entre los componentes de la solución

No se admitirán ofertas que limiten el uso de funcionalidades esenciales mediante licenciamiento parcial, condicionado o insuficiente para dar cumplimiento íntegro a las prescripciones técnicas del Pliego.

4.5. Requisitos de compatibilidad, integración y acreditación del cumplimiento

Todos los componentes ofertados deberán ser plenamente compatibles entre sí y con la arquitectura actualmente existente en EGARSAT, de manera que la solución pueda operar como un entorno único, coherente y funcionalmente integrado. En particular, la oferta deberá acreditar de forma expresa y suficiente:

- la compatibilidad de la solución de seguridad de red con la plataforma de análisis y centralización de registros actualmente implantada, cuya continuidad y adecuación forman parte del contrato
- la compatibilidad de la solución de seguridad de red con la plataforma de gestión de endpoints actualmente implantada, cuya continuidad forma igualmente parte del contrato;
- la existencia de integración nativa entre dichos componentes
- la ausencia de necesidad de incorporar plataformas de terceros, desarrollos específicos, conectores externos o sustituciones adicionales de productos no previstos en el objeto contractual
- la posibilidad de mantener la operativa requerida por EGARSAT con una arquitectura técnica homogénea y coherente

La acreditación del cumplimiento de los requisitos establecidos en este apartado deberá realizarse mediante documentación oficial del fabricante de los productos ofertados. A estos efectos, los licitadores deberán aportar, como mínimo:

- fichas técnicas oficiales de los equipos, licencias y componentes ofertados
- documentación oficial del fabricante que acredite de forma expresa las capacidades de integración exigidas

- una matriz de cumplimiento requisito a requisito, con referencia concreta a la documentación justificativa aportada
- descripción técnica de la arquitectura propuesta
- identificación detallada de cualquier componente adicional que, en su caso, resultara necesario para el funcionamiento de la solución

La integración exigida se considerará acreditada únicamente cuando exista soporte nativo y oficialmente documentado por el fabricante entre los componentes ofertados y las plataformas actualmente implantadas, mediante funcionalidades propias del fabricante, debidamente documentadas en fichas técnicas o documentación oficial, y que permita el funcionamiento conjunto de los componentes sin requerir plataformas adicionales, productos intermedios ni componentes distintos de los incluidos en el objeto del contrato, no considerándose suficiente la interoperabilidad basada en protocolos estándar (como syslog, API genéricas o exportación de logs), ni integraciones mediante herramientas intermedias, plataformas externas o mecanismos de correlación ajenos al ecosistema principal de la solución. Por el contrario, no se considerará acreditado el cumplimiento mediante meras declaraciones del licitador, documentación comercial genérica, presentaciones no vinculantes o referencias imprecisas sin respaldo técnico oficial del fabricante. La falta de acreditación suficiente, la aportación de documentación contradictoria, o la constatación de que el cumplimiento exige sustituciones, herramientas o desarrollos no previstos en el contrato, determinarán la no conformidad técnica de la oferta.

4.6. Condiciones de equivalencia técnica

El detalle de las condiciones de equivalencia técnica de los dispositivos requeridos 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.

La acreditación de la equivalencia deberá realizarse exclusivamente mediante documentación oficial del fabricante de la solución ofertada, no considerándose válida la mera declaración del licitador ni la aportación de documentación comercial genérica sin respaldo técnico suficiente.

EGARSAT se reserva el derecho de requerir cuanta información adicional considere necesaria, incluyendo demostraciones técnicas, pruebas de concepto o validaciones adicionales, para verificar el cumplimiento efectivo de los requisitos de equivalencia.

La falta de acreditación suficiente, la aportación de documentación incompleta o ambigua, o la constatación de que el cumplimiento de los requisitos exige la introducción de elementos adicionales, desarrollos específicos o alteraciones del modelo operativo existente, determinarán la no conformidad técnica de la oferta.

5. Servicios relacionados con la implantación y puesta en producción de los equipos

El adjudicatario deberá ejecutar todos los trabajos necesarios para la correcta implantación, configuración, migración de parametrizaciones y configuraciones, y puesta en marcha de la solución objeto del contrato, garantizando su completa operatividad en el entorno de EGARSAT y su adecuada integración con la arquitectura existente. Estos servicios tendrán carácter integral, no limitándose a la mera instalación o suministro de equipamiento o licencias, sino comprendiendo la provisión efectiva de una solución plenamente implantada, funcional y adaptada a los requerimientos técnicos y operativos de EGARSAT.

A tal efecto, el adjudicatario será responsable de la planificación, ejecución y supervisión de todas las actuaciones necesarias, incluyendo, como mínimo, el suministro, instalación física y lógica de los equipos, la configuración de todos los componentes, la adecuación de parámetros y políticas de seguridad, la integración con los sistemas existentes, la migración desde la situación actual y la puesta en producción de la solución.

Para ello, los licitadores deberán definir y aportar en sobre B un plan de implantación detallado que contemple las distintas fases del proyecto, incluyendo, al menos, las actividades de auditoría inicial, diseño de la solución, preparación del entorno, instalación, configuración, migración, validación y puesta en producción, así como los mecanismos de control y seguimiento necesarios para garantizar su correcta ejecución. Los trabajos de implantación deberán realizarse en horario laborable de lunes a viernes, preferiblemente en horario de mañana, minimizando el impacto sobre la operativa habitual de EGARSAT y garantizando en todo momento la continuidad del servicio. A estos efectos, el adjudicatario deberá contemplar la realización de aquellas actuaciones necesarias fuera del horario establecido, cuando así se requiera por razones operativas o de disponibilidad del servicio; en este escenario las actuaciones deberán ser realizadas de lunes a viernes a partir de las 20h o en fin de semana (de forma consensuada con EGARSAT). La migración desde la infraestructura actualmente en servicio deberá ejecutarse de forma controlada y planificada, asegurando la preservación de la configuración, políticas de seguridad y funcionalidades existentes, así como la integridad de la información relevante para la operación del sistema. En ningún caso se admitirán actuaciones que impliquen pérdida de funcionalidad, degradación del servicio o alteración no justificada del modelo operativo existente.

La solución deberá quedar completamente instalada, configurada, integrada y validada en entorno productivo, incluyendo la correcta operación en configuración de alta disponibilidad, la verificación de la sincronización entre nodos, la validación del tratamiento de tráfico en condiciones reales de operación y la comprobación de la correcta generación, envío y explotación de logs y eventos de seguridad. Asimismo, deberá verificarse de forma expresa la correcta integración con las plataformas actualmente implantadas cuya continuidad forma parte del objeto del contrato, incluyendo la validación del intercambio de información de seguridad, la recepción de telemetría de endpoint y la aplicación de políticas en base a dicha información, sin recurrir a mecanismos intermedios no previstos, así como las integraciones tecnológicas ya existentes en EGARSAT.

El detalle de las tecnologías existentes 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.

El adjudicatario deberá llevar a cabo todas las pruebas necesarias para garantizar el correcto funcionamiento de la solución, incluyendo pruebas funcionales, de rendimiento, de integración y de conmutación en escenarios de alta disponibilidad, debiendo documentarse adecuadamente los resultados obtenidos. La puesta en producción de la solución no se considerará finalizada hasta que se haya verificado, de manera satisfactoria por parte de EGARSAT, el correcto funcionamiento conjunto de todos los componentes, su integración efectiva en el entorno existente, el cumplimiento de los requisitos establecidos en el presente Pliego y la desconexión de la red de los equipos actuales.

La fase de implantación y puesta en marcha de la solución deberá ser finalizada, a más tardar, durante los 30 días naturales siguientes a la fecha de inicio del contrato. Se valorará en oferta técnica una mejora en este apartado.

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 la máxima certificación técnica del fabricante de la solución ofertada para las tareas a realizar y contar con al menos 2 años de experiencia en implantación de la solución ofertada. Dicha certificación deberá estar vigente durante toda la vigencia del contrato.

El incumplimiento en los requerimientos y/o 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.

6. Gestión del proyecto de implantación y puesta en producción de los equipos

Para garantizar la correcta puesta en marcha de los equipos, la empresa adjudicataria designará un jefe

de Proyecto que actuará como interlocutor único con EGARSAT en esta fase de implantación. Deberá disponer de conocimientos para la realización de las tareas encomendadas y un mínimo de 2 años de experiencia en trabajos similares a los requeridos. Tareas a realizar:

- 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.

7. Documentación, entregables y transferencia de conocimiento

El adjudicatario deberá proporcionar toda la documentación, entregables y acciones de transferencia de conocimiento necesarias para garantizar una correcta explotación, administración y mantenimiento de la solución por parte de EGARSAT, asegurando su autonomía operativa una vez finalizada la fase de implantación. La documentación deberá ser completa, clara, estructurada y adaptada al entorno específico de EGARSAT, no considerándose suficiente la aportación de documentación genérica del fabricante que no refleje la configuración y arquitectura real implantada.

En particular, el adjudicatario deberá entregar, como mínimo, la siguiente documentación:

- descripción detallada de la arquitectura de la solución implantada, incluyendo la relación entre los distintos componentes y su integración en el entorno existente
- inventario completo de los elementos suministrados, incluyendo equipamiento, licencias, versiones de software y suscripciones asociadas
- documentación de configuración de todos los componentes, incluyendo parámetros relevantes, políticas de seguridad aplicadas y estructura de funcionamiento del entorno
- documentación de la configuración de alta disponibilidad, incluyendo mecanismos de conmutación, sincronización y validación del estado del sistema
- documentación de integración con las plataformas actualmente implantadas cuya continuidad forma parte del contrato;
- procedimientos de operación habituales, incluyendo tareas de administración, monitorización y gestión básica del sistema
- procedimientos de actuación ante incidencias, incluyendo identificación, análisis y medidas de respuesta
- procedimientos de aplicación de actualizaciones, cambios de configuración y medidas de mantenimiento preventivo
- cualquier otra documentación necesaria para garantizar la correcta operación del sistema en condiciones reales
- grabaciones y material usado en la transferencia de conocimiento

Deberán incluirse en sobre B ejemplos de cada uno de los entregables solicitados, a excepción de las grabaciones y material usado en la transferencia de conocimiento.

Toda la documentación deberá mantenerse actualizada por el adjudicatario durante la ejecución del contrato en aquellos aspectos que puedan verse afectados por modificaciones o actuaciones realizadas sobre la solución. El adjudicatario deberá garantizar la coherencia entre la documentación entregada y la configuración real del sistema, no admitiéndose discrepancias que dificulten la explotación o administración del entorno por parte de EGARSAT.

Asimismo, el adjudicatario deberá llevar a cabo las actuaciones necesarias de transferencia de conocimiento hacia el personal técnico de EGARSAT, con el objetivo de asegurar la correcta comprensión del funcionamiento de la solución y su explotación autónoma.

Dichas actuaciones deberán incluir, al menos, 2 sesiones de 2 horas cada una de ellas de carácter práctico orientadas a:

- la administración de la infraestructura de seguridad de red
- la gestión y explotación de la plataforma de análisis y registros
- la utilización y administración de la plataforma de gestión de endpoints
- la gestión de incidencias y resolución de problemas habituales
- la aplicación de cambios y operaciones de mantenimiento
- la interpretación de logs, eventos y alertas de seguridad

La transferencia de conocimiento deberá estar basada en la solución realmente implantada, utilizando el entorno operativo de EGARSAT o un entorno equivalente, no considerándose suficiente la formación genérica sobre productos o tecnologías desvinculada de la implantación realizada. El adjudicatario deberá aportar los materiales necesarios para dichas sesiones, incluyendo documentación de apoyo, guías de operación y ejemplos prácticos, quedando dichos materiales a disposición de EGARSAT para su uso posterior.

La solución no se considerará plenamente entregada mientras no se haya completado la entrega de toda la documentación requerida y la ejecución efectiva de las acciones de transferencia de conocimiento, debiendo quedar acreditado que el personal técnico de EGARSAT dispone de los conocimientos necesarios para su explotación básica. En todo caso, EGARSAT deberá disponer, al finalizar estas actuaciones, de la capacidad suficiente para operar, supervisar y administrar la solución sin dependencia continua del adjudicatario para las tareas ordinarias. Dicha fase de documentación, entregables y transferencia de conocimiento deberá ser finalizada, a más tardar, durante los 15 días naturales siguientes a la fecha de finalización de la fase de implantación y puesta en marcha de la solución.

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 la máxima certificación técnica del fabricante de la solución ofertada para las tareas a realizar y contar con al menos 2 años de experiencia en implantación de la solución ofertada. Dicha certificación deberá estar vigente durante toda la vigencia del contrato.

El incumplimiento en los requerimientos de 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.

8. Servicios de mantenimiento y soporte en tiempo de operación

El adjudicatario deberá garantizar la prestación de los servicios de mantenimiento, soporte técnico y actualización de todos los componentes que integran la solución durante todo el periodo de vigencia contractual, asegurando su correcto funcionamiento, disponibilidad y adecuación continua a las necesidades operativas de EGARSAT. El mantenimiento deberá comprender tanto el soporte correctivo como el soporte evolutivo y preventivo, incluyendo la resolución de incidencias, la aplicación de actualizaciones, la revisión del funcionamiento de la solución y la adopción de las medidas necesarias para garantizar su estabilidad y rendimiento en condiciones reales de operación.

El servicio de soporte técnico deberá permitir la apertura, seguimiento y resolución de incidencias de forma continua, disponiendo de los mecanismos necesarios para la gestión integral del ciclo de vida de las mismas, desde su notificación hasta su resolución definitiva. Las incidencias deberán ser atendidas con niveles de servicio adecuados a su criticidad, garantizando tiempos de respuesta y resolución acordes con la naturaleza de los sistemas, debiendo el adjudicatario establecer procedimientos de escalado adecuados, tanto internos como hacia el fabricante, cuando así resulte necesario. 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 o correo electrónico o teléfono (mínimo 2 de ellos).
- Horario 24x7 para casos críticos. Contacto con el soporte técnico de forma telefónica.

- Incidencias: asistencia ante averías y/o incidencias de funcionamiento, sea cual fuere su naturaleza, hasta su resolución.
- Peticiones de servicio: 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 de firmware debidos a la necesidad de inclusión de nuevas funcionalidades, o ante vulnerabilidades detectadas en el firmware actual (en un escenario de no detección de vulnerabilidades en el firmware instalado, se estiman un máximo de 2 actualizaciones anuales). Las actualizaciones deberán ser evaluadas previamente por el adjudicatario, valorando su impacto en el entorno de EGARSAT, y aplicadas de forma planificada, evitando afectaciones no controladas al servicio. En aquellos casos en que la actualización implique riesgo potencial, deberá contemplarse la existencia de mecanismos de reversión que permitan recuperar la situación anterior en caso necesario.

SLA's de tiempos máximos de resolución de incidencias, peticiones y actualizaciones:

Prioridad	Tiempos de resolución
Prioridad Crítica (comunicación telefónica)	4 horas naturales
Prioridad Alta	4h laborables
Prioridad Media	8h laborables
Prioridad Baja	De mutuo acuerdo

Donde:

- Tiempo máximo de resolución: tiempo transcurrido desde que se comunica la incidencia/petición al servicio de soporte propuesto, hasta que se soluciona la incidencia/petición.
- Prioridad Crítica:
 - Incidencias de fallo total de alguno de los servicios ofrecidos (o gravemente afectados), no disponiendo de alternativas de funcionamiento.
- Prioridad Alta:
 - Incidencias de fallo parcial de alguno de los servicios ofrecidos, no disponiendo de alternativas de funcionamiento.
 - Peticiones de servicio prioritarias
- Prioridad Media:
 - Incidencias de fallo total o parcial de alguno de los servicios ofrecidos (o gravemente afectados), disponiendo de alternativas de funcionamiento.
 - Peticiones de servicio tipificadas como cambio menor, entendiendo como cambio menor aquel que requiera una dedicación menor o igual a 2 horas y que no se consideren urgentes ni prioritarias.
 - Preguntas / dudas.
- Prioridad Baja:
 - Peticiones de servicio tipificadas como cambio mayor, entendiendo como cambio mayor aquel que requiera una dedicación mayor a 2 horas y que no se consideren urgentes ni prioritarias.
 - Actualizaciones de firmware

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 resolución 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 de configuraciones, capacidad, rendimiento y estado de los componentes, así como a la 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.

Informes de servicio:

- el contratista deberá enviar un informe de servicio semestral en formato editable (durante los 15 primeros días naturales después de la finalización del semestre) que incluya una relación detallada de las actuaciones realizadas (incidencias, consultas, actualizaciones) así como la descripción de las tareas, fecha/hora inicio, fecha hora/fin, prioridad asignada, solución adoptada, y el cumplimiento de los SLAs para cada una de las tareas relacionadas.
- el contratista deberá enviar, durante los 15 primeros días naturales después de la finalización de cada jornada de trabajo, un informe en formato editable que refleje las tareas realizadas en dicha jornada de trabajo, un detalle del estado general del servicio, y recomendaciones y mejoras aplicables y/o nuevas funcionalidades susceptibles de ser habilitadas sin coste adicional para EGARSAT. En el supuesto de que EGARSAT considere factibles las recomendaciones/mejoras/nuevas funcionalidades reportadas por el contratista, EGARSAT las petitionará a los servicios de soporte a modo de peticiones de servicio.

Deberán incluirse en sobre B ejemplos de cada uno de los entregables solicitados.

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 la máxima certificación técnica del fabricante de la solución ofertada para las tareas a realizar y contar con al menos 2 años de experiencia en implantación de la solución ofertada. Dicha certificación deberá estar vigente durante toda la vigencia del contrato

El incumplimiento en los requerimientos y/o 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.

9. 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 conocimientos para la realización de las tareas encomendadas y un mínimo de 2 años de experiencia en trabajos similares a los requeridos. Tareas a realizar:

- 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.

10. 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.

11. Precio

Servicios y suministros para la duración inicial del contrato. Desglose de precios:

Descripción	Importe máximo (SIN IVA)
a) Suministro de 2 equipos con mantenimiento y soporte oficial del fabricante durante 3 años	48.000,00 €
b) Servicios profesionales relacionados con la implantación y puesta en producción de los equipos, documentación, entregables y transferencia de conocimiento, por parte del adjudicatario	10.000,00 €
c) Renovación y adecuación de la plataforma de análisis y centralización de registros ampliando su capacidad hasta un mínimo agregado equivalente a 6 GB/día, con mantenimiento y soporte oficial del fabricante durante 3 años (desde el 31/01/2027 al 30/01/2030)	6.000,00 €
d) Renovación y adecuación de la plataforma de protección de endpoints actualmente implantada, adecuando el volumen de equipos a cubrir hasta 250 dispositivos, con mantenimiento y soporte oficial del fabricante durante el periodo que comprende desde el 01/08/2027 hasta el 30/01/2030	12.500,00 €
e) Servicios profesionales de mantenimiento y soporte en tiempo de operación de toda la plataforma tanto a nivel de hardware como de software durante 3 años, por parte del adjudicatario	15.000,00€
TOTAL	91.500,00 €

Servicios anuales para cada una de las prórrogas. Desglose de precios:

Descripción	Importe máximo anual (SIN IVA)
f) Renovación anual del mantenimiento y soporte oficial del fabricante para los 2 equipos	9.000,00 €
g) Renovación anual del mantenimiento y soporte oficial del fabricante para la plataforma de análisis y centralización de registros con capacidad hasta un mínimo agregado equivalente a 6 GB/día	2.000,00 €
h) Renovación anual del mantenimiento y soporte oficial del fabricante para la plataforma de protección de endpoints actualmente implantada con capacidad para cubrir hasta 250 dispositivos	5.000,00 €
i) Servicios profesionales de mantenimiento y soporte en tiempo de operación de toda la plataforma tanto a nivel de hardware como de software, por parte del adjudicatario	5.000,00 €
TOTAL	21.000,00 €

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 correspondientes al apartado “7. Documentación, entregables y transferencia de conocimiento” del Pliego de Prescripciones Técnicas, los importes ofertados correspondientes a los ítems “a”, “b”, “c”, “d”, y la tercera parte del importe ofertado correspondiente al ítem “e”.
- Al inicio del 2º y del 3er año de contrato, la tercera parte del importe ofertado correspondiente al ítem “e”.
- Al inicio de cada prórroga, los importes ofertados correspondientes a los ítems “f”, “g”, “h” e “i”.

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: 2026.07.15
09:59:11 +02'00'

