PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE "IMPLEMENTACIÓN DE UN NGSIEM Y SERVICIOS DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC) PARA EGARSAT MUTUA COLABORADORA CON LA SEGURIDAD SOCIAL Nº 276"

1. Introducción

Durante los últimos años EGARSAT no ha cesado en sus procesos de mejora continua en cuanto a materias de seguridad tecnológica con la finalidad de potenciar las capacidades de resiliencia, protección y defensa de la compañía frente al creciente número y sofisticación de las amenazas provenientes del ciberespacio a fin de:

- Reducir el riesgo de interrupción de las operaciones de la organización a causa de ataques malintencionados o por causas accidentales, limitar su impacto potencial y reforzar la capacidad de resiliencia y recuperación de la compañía en caso de llegar a verse afectada.

- Garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, tanto aquella generada por la actividad propia, como la recibida en custodia por parte de ciudadanos, empleados y terceras partes.

- Asegurar el cumplimiento de las obligaciones legales de la compañía en materia de seguridad de la información y ciberseguridad.

El continuo aumento y complejidad de las amenazas, ataques e incidentes en materia de seguridad de la información y ciberseguridad, así como la entrada en vigor de nuevas obligaciones legales relativas a la necesidad de la monitorización continua y comunicación de los incidentes de seguridad, hace necesario la implementación de un NGSIEM y la contratación de servicios de un Centro de Operaciones de Seguridad (SOC).

El incumplimiento de cualquiera de los requisitos solicitados en este pliego por parte de la empresa adjudicataria dará lugar a la resolución del contrato, tal y como se especifica en el Anexo 14.

2. Objeto del contrato

El objeto del contrato es la implementación de un NGSIEM y la contratación de los servicios de un Centro de Operaciones de Seguridad (SOC) que incluya la prestación de los servicios de monitorización, vigilancia y respuesta a incidentes. Son objeto de licitación los siguientes elementos y servicios:

- Suministro de todos los equipos y licencias necesarias, instalación, configuración, parametrización, puesta en marcha, entrega del sistema en producción, formación a los Administradores de Sistemas de EGARSAT y servicios de mantenimiento y soporte asociados de un NGSIEM para la recolección, análisis y correlación de eventos e información de seguridad para la detección de posibles incidentes de ciberseguridad.

- Servicios de Centro de Operaciones de Seguridad (SOC) que incluya la monitorización en formato 24x7, servicio de alertas a los técnicos de EGARSAT de todos aquellos eventos que puedan ser indicativos de la existencia de un ciberincidente, así como

los correspondientes servicios de remediación. Adicionalmente deberán incluirse servicios de remediación para equipos Windows que permitan la recuperación ante ataques de ransomware.

El objetivo principal de la presente contratación es el de garantizar la monitorización 24x7 de los sistemas informáticos, comunicaciones y sistemas de seguridad perimetral de EGARSAT, con la implantación de una herramienta NGSIEM y su supervisión correspondiente que mejore la seguridad de las infraestructuras, comunicaciones y servicios digitales prestados por EGARSAT, y ampliar sus capacidades de prevención, detección y respuesta ante incidentes de ciberseguridad. Adicionalmente y en caso de producirse un ciberincidente, los servicios de SOC incluirán la alerta y las todas las tareas de remediación necesarias para restablecer los servicios TI de EGARSAT afectados.

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 al proyecto global:
  - Detalle de elementos hardware y software incluidos, y descripción general de las herramientas, tecnologías y servicios y procedimientos propuestos.
  - Cronograma en el que se ordenen en el tiempo las tareas del proyecto con sus dependencias, así como los hitos principales del proyecto.
  - Guión del plan de formación.
  - Relación de entregables del proyecto, tanto en fase de implantación como en tiempo de operación (ejemplos de informes solicitados en el presente Pliego de Prescripciones Técnicas) y de devolución del servicio.
  - Descripción detallada de los procedimientos de gestión del proyecto, tanto en fase de implantación como en tiempo de operación.
  - Descripción detallada de los procedimientos de devolución del servicio a la finalización del contrato.

- En cuanto al NGSIEM propuesto:
  - Arquitectura completa e interconexión con los elementos existentes.
  - Descripción detallada de sus capacidades y de sus funcionalidades técnicas.
  - Descripción detallada de fuentes externas de enriquecimiento del sistema que se aportan (excepto la sonda SAT INET del Centro Criptológico Nacional (CCN-CERT) en caso de aportarse, por ser objeto de valoración en la oferta técnica valorable automáticamente (SOBRE C)) de forma adicional a las mínimas requeridas en Pliego de Prescripciones Técnicas.
  - Descripción de los procedimientos asociados a sus servicios de soporte (mantenimientos correctivos, mantenimientos evolutivos, cambios en configuraciones y actualizaciones periódicas del NGSIEM, como mínimo).

- En cuanto a los servicios de SOC propuestos:
  - Descripción detallada de casos de uso propuestos.
  - Descripción detallada de los procedimientos para la gestión de alertas.
  - Descripción detallada de los procedimientos para la remediación de ciberincidentes, incluyendo aquellos procedimientos específicos para la remediación de ataques de ransomware.
  - Descripción detallada de los procedimientos para el seguimiento del servicio.

- Otra información que las empresas licitadoras estimen necesario incluir para facilitar

la comprensión de la oferta presentada

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

Las tareas de suministro, instalación, configuración, parametrización, puesta en marcha, entrega del sistema en producción y formación a los Administradores de Sistemas de EGARSAT no deberán demorarse más de 120 días desde la fecha de inicio del contrato.

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.

3. Características de la solución

3.1. NGSIEM: alcance

Se requiere del suministro e implantación de un NGSIEM en formato appliance físico para la recolección, análisis y correlación de eventos e información de seguridad. Este NGSIEM deberá ser implementado en el CPD que EGARSAT tiene en sus instalaciones de Sant Cugat del Vallés.

EGARSAT dotará al/los equipos de fluido eléctrico, conectividad de red y un máximo de 6U en el rack existente. Adicionalmente, el/los equipos deberán ser integrados en la red de EGARSAT siguiendo los criterios de seguridad de redes que los técnicos de EGARSAT determinen, de forma consensuada con el adjudicatario.

Será imprescindible una arquitectura en la que toda la información que salga de la red de EGARSAT (en el supuesto que hubiera información saliente) deberá transferirse mediante protocolos seguros, y deberá ser almacenada garantizando la integridad y la confidencialidad de la misma. Adicionalmente, dicha información saliente deberá tener como origen un contenedor/colector intermedio incluido en la propuesta, quedando totalmente prohibido el envío de información hacia el exterior desde cada uno de los sistemas desde los que se debe realizar la ingesta de datos.

Deberán estar incluidas en la oferta todas las licencias necesarias durante toda la vigencia del contrato (estando éstas de forma obligatoria a titularidad de EGARSAT), así como el mantenimiento y soporte del NGSIEM en horario 8x5 (de lunes a viernes de 9:00h a 17:00h).

Deberá realizarse ingesta de logs, como mínimo, de los siguientes sistemas:

- Firewall perimetral (la marca y modelo del / de los equipos ya existentes en EGARSAT no se aportan como información pública al considerarse información sensible de seguridad. Esta información se facilitará bajo demanda)

- Antivirus y/o EDR (la marca y funcionalidades de dichos softwares ya existentes en EGARSAT no se aportan como información pública al considerarse información sensible de seguridad. Esta información se facilitará bajo demanda)

- Active Directory de Microsoft

- Servidores DNS de Microsoft

- Servidores Windows (50 aproximadamente)

- Servidores Linux (50 aproximadamente)

Se valorará en oferta técnica la inclusión en el NGSIEM propuesto de la ingesta de información que provee el CCN-CERT mediante su sonda SAT INET, para la alerta temprana del tráfico de internet.

La capacidad de ingesta de la herramienta deberá ser la suficiente para disponer de una retención de datos para su gestión y análisis en tiempo real de 90 días para cada una de las fuentes de ingesta de información, como mínimo.

El tamaño del histórico de datos deberá ser de 365 días para cada una de las fuentes de ingesta de información, como mínimo.

3.2. NGSIEM: características principales y requisitos mínimos

El sistema deberá recopilar información en tiempo real sobre los eventos de seguridad generados por la red de EGARSAT, procesarla y generar informes y/o alertas que puedan ayudar a la organización en la toma de decisiones. Deberá contemplar, como mínimo:

- La gestión centralizada de los registros y eventos de seguridad generados por los sistemas.

- El análisis y la monitorización en tiempo real de los eventos de seguridad de múltiples fuentes.

- La consolidación de la información.

- La generación de acciones para la notificación, contención y remediación.

Requisitos mínimos que deberá cumplir el sistema NGSIEM:

- Deberá estar incluido en el apartado de sistemas de gestión de eventos de seguridad en la guía CCN-STIC- 105 con categoría “Media” como mínimo, y con fecha de validez no sobrepasada a fecha de publicación del expediente.

- Deberá disponer de un conjunto suficiente de conectores, reglas de correlación y alertas para integrar, como mínimo, los siguientes sistemas:

    - Firewall perimetral (la marca y modelo del / de los equipos ya existentes en EGARSAT no se aportan como información pública al considerarse información sensible de seguridad. Esta información se facilitará bajo demanda).

- Antivirus y/o EDR (la marca y funcionalidades de dichos softwares ya existentes en EGARSAT no se aportan como información pública al considerarse información sensible de seguridad. Esta información se facilitará bajo demanda).
- Active Directory de Microsoft.
- Servidores DNS de Microsoft.
- Servidores Windows (50 aproximadamente).
- Servidores Linux (50 aproximadamente).
- Sonda SAT INET del CCN-CERT (en el supuesto que se haya ofertado su ingesta como mejora técnica).

Deberán estar incluidas en oferta todas las tareas para la integración de aquellos sistemas que, ya estando integrados en el NGSIEM, EGARSAT decida sustituir durante la vigencia del contrato (ejemplos: cambio de firewall, cambio de antivirus y/o EDR, cambio/upgrade de controladores de dominio, o cambios similares)

- En lo relativo a la retención de datos, deberá ofrecer un mínimo de 90 días de datos sobre los que pueda trabajar en tiempo real. Además, deberá permitir el almacenamiento de datos históricos hasta una antigüedad de 365 días, como mínimo.

- Deberá ofrecer una arquitectura robusta y escalable que permita el crecimiento para adecuarse a las necesidades de EGARSAT. Es por este motivo que, al margen de los sistemas mínimos a integrar descritos, el NGSIEM propuesto debe contar con una arquitectura robusta y escalable que permita el crecimiento según las necesidades de EGARSAT. El NGSIEM propuesto deberá permitir crecer, como mínimo, en los siguientes conceptos:

  - Tipo de fuentes conectadas. Deberá permitir un crecimiento de 2 tipos de fuentes anuales (adicionales a la sonda SAT INET, en el supuesto que se haya ofertado su ingesta como mejora técnica). Se valorará en oferta técnica crecimientos anuales superiores en cuanto a tipos de fuentes de ingesta de información durante la vigencia del contrato

  - Número de fuentes conectadas. Deberá poderse incrementar el número de servidores Windows y Linux que sean fruto del crecimiento vegetativo de los servicios TI de EGARSAT. Se estima un crecimiento vegetativo en el número de servidores Windows y Linux a incluir no superior al 5% anual. Se valorará en oferta técnica la inclusión de un número de fuentes de ingesta de información superior a este 5% anual durante la vigencia del contrato.

  - Capacidad de ingesta de la herramienta. Como consecuencia de los dos puntos anteriores, la capacidad de ingesta de la herramienta deberá adecuarse a los crecimientos en tipo y número de fuentes máximos ofertados.

  - Retención de datos, tanto de datos en tiempo real como de datos históricos. Pese al posible crecimiento estimado, deberán mantenerse los días de retención de los

datos en tiempo real y de los datos históricos para todos los tipos de fuentes y para todo el número de fuentes.

- Deberá estar adecuadamente dimensionado para la ingesta de información descrita en el apartado anterior, pudiendo soportar picos puntuales de ingesta de mayor magnitud sin pérdida de servicio.

- Deberá ofrecer funcionalidades de correlación de eventos en tiempo real.

- Deberá ofrecer casos de uso ya predefinidos, mantenidos y documentados.

- Deberá ofrecer informes ya predefinidos, mantenidos y documentados.

- Deberá incluir reglas que permitan detectar anomalías en tiempo real.

- Deberá ser capaz de agrupar incidentes relacionados en un único incidente, aunque los eventos estén separados en el tiempo por horas o incluso días.

- Deberá ser personalizable, permitiendo crear, como mínimo, vistas, gráficos, filtros y cuadros de mando personalizados adecuados a las necesidades de EGARSAT

- Deberá permitir analizar el comportamiento del usuario (UEBA según Gartner, SUBA según Forrester Research) de manera nativa y sin soluciones de terceros adicionales.

- Deberá permitir realizar consultas avanzadas mediante listas desplegables y mediante lenguaje estructurado tipo SQL.

- Deberá incorporar de manera nativa y sin soluciones de terceros adicionales capacidades de detección de anomalías y funcionalidades XDR.

- Deberá permitir la incorporación de LUCIA como plataforma de gestión de tickets bidireccional con el CCN-CERT.

- Deberá permitir la incorporación de REYES como plataforma de feeds de inteligencia con datos sobre amenazas de seguridad que utilice posteriormente en sus correlaciones y búsquedas de eventos de seguridad.

- Deberá permitir la recolección de logs utilizando diferentes protocolos (syslog, TLS syslog, syslog multilínea, SNMPv3, SMB, SCP/SFTP, WMI, MSRPC, y API, como mínimo).

- Deberá detectar y reconocer automáticamente las fuentes syslog más comunes.

- Deberá permitir incorporar fuentes personalizadas o no soportadas por defecto.

- Deberá proporcionar soporte para el intercambio de información de ciberseguridad basado en estándares abiertos como STIX, indicadores abiertos de compromiso (OpenIOC), o TAXII.

- Deberá ofrecer una cónsola web en formato HTML5 que permita su ejecución en cualquier plataforma compatible, sin necesidad de sistemas propietarios de fabricante.

- Desde la perspectiva de licenciamiento, deberá permitir crecer en EPS y/o en usuarios que utilicen la consola sin coste adicional para EGARSAT.

- Deberá integrar la información en tiempo real y la información forense de manera nativa y sin necesidad de elementos y/o componentes adicionales, para la óptima interacción con la información en tiempo real y la información forense.

- Deberá ofrecer capacidades para la implementación de desarrollos a medida para la integración con aplicaciones propietarias, herramientas de ticketing, soluciones EDR u otras integraciones que EGARSAT pudiera precisar.

- Deberá disponer de la certificación de seguridad "Common Criteria" mínimo EAL2.

3.3. NGSIEM: servicios de formación, mantenimiento y soporte asociados

La oferta deberá incluir servicios de formación, y servicios de mantenimiento y soporte asociados sobre el NGSIEM implantado. Como mínimo:

- A la finalización de la puesta en marcha de la solución, deberá procederse a la formación a los Administradores de Sistemas de EGARSAT sobre la configuración, procedimientos básicos de acceso y gestión de la herramienta implantada. En dicha formación, que podrá realizarse indistintamente de forma presencial o por videoconferencia, deberá entregarse un documento detallado que incluya arquitectura de la solución, parámetros de configuración del sistema e integración con la infraestructura de EGARSAT. Duración mínima de la formación: 8 horas.

- Durante toda la vigencia del contrato, servicios de mantenimiento correctivo integral de la solución (hardware y software).

- Durante toda la vigencia del contrato, servicios de mantenimiento evolutivo. Deberán implementarse todas las actualizaciones de software recomendadas por el fabricante. Adicionalmente y a efectos de disponer de una plataforma mínimamente actualizada, se deberá aplicar una actualización de software anual (como mínimo). Será potestad de EGARSAT decidir si debe realizarse más de una actualización anual del software de la solución.

- Durante toda la vigencia del contrato, actualizaciones de aquellos casos de uso predefinidos de fabricante que se adapten a la realidad de EGARSAT a medida que sean publicados.

- Durante toda la vigencia del contrato, actualizaciones de aquellos casos de uso que se estimen oportunos en base a la experiencia del adjudicatario en otros clientes similares a EGARSAT.

- Durante toda la vigencia del contrato, integración en la herramienta de inteligencia proveniente de fuentes externas que pudieran mejorar la capacidad en la detección de incidentes.

- Durante toda la vigencia del contrato, cambios en configuraciones y/o parametrizaciones de la herramienta. El adjudicatario deberá realizar los cambios que EGARSAT solicite. En el supuesto que dichos cambios impliquen ampliaciones de

hardware y/o de licenciamiento no incluidas en la propuesta del adjudicatario, éstas se contemplarán como "Modificaciones contractuales previstas".

- La propuesta deberá incluir actualizaciones periódicas (mínimo 1 actualización anual) de la plataforma en las que estén incluidas nuevas reglas de correlación que pueda ofrecer la herramienta, nuevos casos de uso, y nuevos informes y alertas predefinidos y documentados.

Características de los servicios de mantenimiento y soporte asociados:

- Deberán ser efectuados por técnicos especializados. Se considerará técnico especializado aquél que disponga de la máxima certificación técnica oficial del fabricante del NGSIEM propuesto.

- Horario 8x5, de lunes a viernes de 9:00h a 17:00h.

- Forma de contacto: portal web, correo electrónico y/o teléfono.

- Idioma: catalán y/o castellano.

- Asistencia ante incidencias de funcionamiento de la solución (mantenimiento correctivo).

- Asistencia ante peticiones de servicio: configuraciones, peticiones de cambio, mejoras, upgrades de software, resolución de dudas… (mantenimiento evolutivo, cambios en configuraciones).

- Forma de resolución de los casos abiertos: mediante conexión remota por VPN que EGARSAT facilitará. En el supuesto que no se pueda efectuar la resolución del caso de forma remota, el adjudicatario deberá desplazar a un técnico a las instalaciones que EGARSAT tiene en Sant Cugat del Valles.

- 1 jornada anual de 4 horas laborables como mínimo, para la revisión global de la plataforma conjuntamente con los Administradores de Sistemas de Egarsat. Estas jornadas se podrán realizar mediante videoconferencia, y deberán centrarse especialmente en:

    - Revisión y validación global del correcto funcionamiento de la solución
    - Revisión global para mejora continua de las configuraciones existentes
    - Propuestas y aplicación de mejoras consensuadas
    - Resolución de dudas

    Se valorará en oferta técnica la inclusión 1 jornada anual de 4 horas laborables adicional para la revisión global de la plataforma.

    Durante los 15 días siguientes a dicha jornada/s anual/es, el adjudicatario deberá confeccionar y entregar por correo electrónico a la persona que Egarsat designe, un informe (a modo de acta) que refleje las tareas, propuestas y acuerdos sucedidos durante la jornada de trabajo.

Para la realización de cualquier tipo de tarea que requiera de la intervención del fabricante de los equipos y/o de los softwares implantados, el soporte técnico especializado mencionado

actuará como SPOC (single point of contact) entre EGARSAT y el fabricante dichos equipos y/o softwares.

Con el objetivo de disponer de métricas del servicio de soporte que permitan a Egarsat una valoración empírica de la calidad de los servicios prestados por parte del adjudicatario, se aplicarán SLA's sobre las incidencias y peticiones de servicio que EGARSAT reporte a dicho soporte. Los SLA's variarán en función de la prioridad asignada a cada uno de los casos, la cual será asignada por EGARSAT de forma consensuada con el adjudicatario para cada uno de ellos.

Prioridades:

- Crítica:
    - Incidencias de fallo total de alguno de los servicios ofrecidos (o gravemente afectados), no disponiendo de alternativas de funcionamiento.
    - Peticiones de servicio urgentes.
- Alta:
    - Incidencias de fallo parcial de alguno de los servicios ofrecidos, no disponiendo de alternativas de funcionamiento.
    - Peticiones de servicio prioritarias.
- Media:
    - Incidencias de fallo total de alguno de los servicios ofrecidos (o gravemente afectados), disponiendo de alternativas de funcionamiento.
    - Incidencias de fallo parcial de alguno de los servicios ofrecidos, 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 4 horas y que no se consideren urgentes ni prioritarias.
    - Preguntas / dudas.
- Baja :
    - Peticiones de servicio tipificadas como cambio mayor, entendiendo como cambio mayor aquel que requiera una dedicación mayor a 4 horas.

SLA's de tiempos máximos de resolución de incidencias y peticiones de servicio (en horas laborables, en horario de lunes a viernes de 9:00h a 17:00h):

Prioridad	Tiempo de resolución
Crítica	8h
Alta	12h
Media	16h
Baja	De mutuo acuerdo

Se valorará en oferta técnica una reducción en los tiempos de resolución de las incidencias y peticiones de servicio.

El adjudicatario entregará a EGARSAT durante los 15 primeros días del trimestre, un informe que refleje los tiempos de resolución de incidencias y peticiones de servicio correspondientes al trimestre anterior. Dicho informe deberá incluir una relación de los casos acontecidos durante el trimestre anterior, incluyendo:

- Fecha y hora de comunicación del caso.
- Explicación detallada del caso.
- Aceptación (si/no) del caso por tener que ver con los servicios ofertados.
- Prioridad aplicada.
- Fecha y hora de primera respuesta.
- Fecha y hora de resolución del caso.
- Solución adoptada.

En el supuesto de que el adjudicatario proponga enriquecer las fuentes de ingesta de datos del NGSIEM por medio de sondas, herramientas, dispositivos o similares que deban instalarse en la red corporativa de EGARSAT:

- Estas mejoras de la solución deberán realizarse de forma consensuada con los técnicos de EGARSAT.

- En caso de llevarse a cabo dichas propuestas, EGARSAT dotará al/los equipos de fluido eléctrico, conectividad de red y espacio en rack existente, así como cualquier recurso de tipo servidor físico y/o virtual, y también la adquisición del software que fuese necesario.

- El adjudicatario correrá con todos los gastos de instalación, configuración, parametrización y explotación.

3.4. Centro de Operaciones de Seguridad (SOC): alcance

El servicio de Centro de Operaciones de Seguridad (SOC) deberá monitorizar (24x7) los eventos de seguridad alojados en el NGSIEM implantado, con el objetivo de detectar y alertar lo antes posible de la materialización de un ciberincidente o de acciones/situaciones/comportamientos sospechosos que pudieran desembocar en un ciberincidente.

Se deberán monitorizar los eventos de seguridad de los siguientes sistemas:

- Firewall perimetral (la marca y modelo del / de los equipos ya existentes en EGARSAT no se aportan como información pública al considerarse información sensible de seguridad. Esta información se facilitará bajo demanda).

- Antivirus y/o EDR (la marca y funcionalidades de dichos softwares ya existentes en EGARSAT no se aportan como información pública al considerarse información sensible de seguridad. Esta información se facilitará bajo demanda).

- Active Directory de Microsoft.

- Servidores DNS de Microsoft.

- Servidores Windows (50 aproximadamente).

- Servidores Linux (50 aproximadamente).

- Sonda SAT INET del CCN-CERT (en el supuesto que se haya ofertado su ingesta como mejora técnica).

- Todos aquellos tipos de fuentes y/o número de fuentes añadidos al sistema durante toda la vigencia del contrato.

Deberá estar incluida en oferta la monitorización de aquellos sistemas que, ya estando integrados en el NGSIEM, EGARSAT decida sustituir durante la vigencia del contrato (ejemplos: cambio de firewall, cambio de antivirus y/o EDR, cambio/upgrade de controladores de dominio, o cambios similares).

3.5. Centro de Operaciones de Seguridad (SOC): características principales y requisitos mínimos

El SOC propuesto deberá formar parte de la Red Nacional de Centros de Operaciones de Ciberseguridad y en consecuencia, la coordinación de los centros integrados en esta red nacional se llevará a cabo a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes. Los requisitos mínimos del SOC propuesto serán los siguientes:

- Servicio en horario 24x7

- Monitorización: monitorización permanente de los eventos de seguridad alojados en el NGSIEM implantado.

- Alerta: cuando el adjudicatario detecte un ciberincidente o una acción/situación/comportamiento susceptible desembocar en ciberincidente, este hecho será notificado de forma inmediata a los técnicos de EGARSAT de acuerdo con el procedimiento que se acuerde para ello. Todas las alertas generadas por el NGSIEM deberán ser revisadas por un técnico de seguridad del adjudicatario como paso previo a su notificación a los técnicos de EGARSAT. Este requisito deberá permitir un elevado nivel de acierto que minimizará el porcentaje de falsos positivos en la identificación de incidentes. El tiempo máximo de respuesta (entendiendo por tiempo de respuesta el transcurrido entre la detección del evento que genera la alerta por parte del adjudicatario hasta que se efectúa la comunicación con los técnicos de EGARSAT no deberá superior a 1 hora natural). Se valorará en oferta técnica una reducción en el tiempo de respuesta.

- Remediación: el servicio de remediación consistirá en la puesta a disposición de EGARSAT de personal experto en ciberseguridad y de todas las herramientas que se precisen para la contención, análisis, mitigación y posterior investigación de posibles ciberincidentes tras la activación del servicio por parte de los técnicos de EGARSAT, a través de los procedimientos que se acuerden entre el adjudicatario y EGARSAT. Una vez activado dicho servicio de remediación por parte de los técnicos de EGARSAT, los técnicos del adjudicatario conjuntamente con los técnicos de EGARSAT, procederán a la actuación sobre la infraestructura tecnológica de EGARSAT hasta el restablecimiento de los servicios TI afectados.

- Remediación ante ransomware: adicionalmente deberán incluirse servicios de remediación para equipos Windows que permitan la recuperación ante ataques de ransomware, hasta el restablecimiento de los servicios TI afectados.

4. Seguimiento del servicio

Con carácter semestral, el adjudicatario deberá asistir a una reunión con EGARSAT (preferiblemente mediante videoconferencia) durante los primeros 15 días posteriores al semestre finalizado, donde deberá entregar y se analizará un informe de servicio que refleje los principales eventos acontecidos en el semestre finalizado, tanto en cuanto al funcionamiento del NGSIEM como a los servicios de SOC prestados. Dicho informe deberá incluir una valoración global del servicio motivada, así como propuestas de mejora detalladas y priorizadas.

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 y que realizará las siguientes tareas:

- Organizar, dirigir, representar y coordinar al equipo de trabajo que preste los servicios de instalación, configuración, parametrización, puesta en marcha, entrega del sistema en producción y formación a los administradores de sistemas de EGARSAT.
- Asegurar el nivel de calidad de las tareas realizadas.
- Proporcionar a EGARSAT la información periódica necesaria para el seguimiento de la implantación.
-

Será potestad de EGARSAT decidir, en cada una de las tareas a realizar, si éstas se ejecutan en horario laboral común (entre las 8:30h y las 17:30h) o bien deberán realizarse en horario nocturno y/o fines de semana.

6. Servicios de en tiempo de operación de la nueva plataforma

Para garantizar la correcta ejecución del contrato, la empresa adjudicataria designará un Jefe de Servicio que actuará como interlocutor único con EGARSAT y que realizará las siguientes tareas:

- 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.

7. Transferencia tecnológica

Durante toda la vigencia del contrato el adjudicatario 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 utilizados para resolverlos.

8. Devolución del servicio

A la finalización del contrato, la empresa adjudicataria:

- Dejará en propiedad de EGARSAT todos los suministros y licencias necesarios para la continuidad del servicio que finaliza.
- Mantendrá en el NGSIEM todas las configuraciones y parametrizaciones realizadas.
- Retirará aquellas herramientas de su propiedad que se hubieren utilizado durante la vigencia del contrato para el enriquecimiento del servicio.
- Realizará las tareas de formación suficientes en el funcionamiento y configuraciones del NGSIEM a los técnicos de EGARSAT para que sean autónomos en la gestión del servicio. Estas tareas de formación consistirán en 1 jornada de 8 horas de formación, como mínimo.
- Hará entrega a los técnicos de EGARSAT de:
    - documentación detallada y actualizada sobre la arquitectura en funcionamiento y los elementos que la componen
    - documentación detallada sobre las configuraciones actuales
    - documentación de uso de la herramienta (manuales de uso)
- Hará entrega a quien EGARSAT designe de un informe final de seguimiento del servicio.

9. Precio y forma de pago

Desglose de precios para el 1er año:

Descripción	Importe máximo
a) NGSIEM: suministro en formato appliance físico y licencias necesarias, mantenimiento y soporte 1er año	24.000,00 €
b) NGSIEM: servicios de instalación, configuración, parametrización, puesta en marcha, entrega del sistema en producción	14.400,00 €
c) NGSIEM: formación a Administradores de Sistemas de EGARSAT	1.200,00 €
d) Servicios de SOC anual 24x7 (monitorización, alerta, remediación) y servicios asociados	73.750,00 €
TOTAL	**113.350,00 €**

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 la entrega de todos los elementos que componen el ítem ‘a’ se abonará la

totalidad del importe correspondiente a dicho ítem.

A la finalización de la realización de las tareas correspondientes a los ítems b y c se abonará la totalidad de los importes correspondientes a los ítems b y c, y el importe unitario anual correspondiente al ítem d, prorrateado al número de meses de servicio que se va a ofrecer durante el primer año (se restará, a los 12 meses del 1er año, los meses destinados a las tareas correspondientes a los ítems a, b y c).

Al inicio del 2º año de contrato (y de forma anual durante la vigencia inicial del contrato y de las correspondientes prórrogas en caso de ejecutarse) se abonará el importe correspondiente que figura en la tabla siguiente (desglose de precios para el 2o año y siguientes):

Descripción	Importe máximo anual
a) NGSIEM: mantenimiento y soporte anual appliance físico y licencias necesarias	14.000,00 €
b) Servicios de SOC anual 24x7 (monitorización, alerta, remediación) y servicios asociados	73.750,00 €
TOTAL	**87.750,00 €**

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

Jordi Trabal Esquerda

Firmado digitalmente por Jordi Trabal Esquerda
Fecha: 2022.09.30 10:52:10 +02'00'