PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE LOS "SERVICIOS DE MONITORIZACIÓN EXTERNA, ANÁLISIS DE VULNERABILIDADES Y TESTS DE INTRUSIÓN DE LOS SISTEMAS TI DE EGARSAT, MUTUA COLABORADORA CON LA SEGURIDAD SOCIAL Nº 276"

1. Introducción

EGARSAT es una entidad que gestiona información sensible que requiere de una protección adecuada. Esto es especialmente importante en el creciente ambiente de negocios interconectados por redes de datos en el que la información está expuesta a un mayor rango de amenazas y vulnerabilidades.

En este contexto, EGARSAT, al estar dotada de una importante infraestructura tecnológica que gestiona varios servicios ofrecidos a través de Internet, desea contratar la realización de servicios de monitorización externa, análisis de vulnerabilidades y tests de intrusión de los sistemas TI por parte de un proveedor externo.

2. Objeto

Los servicios objeto del presente contrato serán los siguientes:

- Monitorización externa de disponibilidad de fluido eléctrico en el CPD que EGARSAT tiene en la provincia de Barcelona.
- Monitorización externa de los elementos y/o servicios TI que EGARSAT tiene publicados desde su CPD (o pueda publicar, durante toda la vigencia del contrato) en la red pública de internet.
- Análisis de vulnerabilidades de:
    - Los elementos y/o los servicios TI que EGARSAT tiene publicados desde su CPD (o pueda publicar, durante toda la vigencia del contrato) en la red pública de internet.
    - Los elementos que componen los servicios de WiFi que EGARSAT tiene instalados (o pueda instalar, durante toda la vigencia del contrato) en sus distintas sedes ubicadas en todo el territorio nacional.
- Realización de tests de intrusión a través de las vulnerabilidades detectadas en el análisis de vulnerabilidades que, por su naturaleza, pudieran comportar una posterior intrusión no deseada.
- Asesoría y soporte especializado en materias de ciberseguridad

El servicio debe incluir todos aquellos elementos (hardware y software) para la prestación del servicio: recursos de computación, almacenamiento, acceso a Internet, softwares configuraciones, parametrizaciones y cualquier otro elemento necesario para el cumplimiento del objeto del contrato. La totalidad de dichos elementos deberán ofrecerse alojados de forma remota sin que EGARSAT deba aportar ningún elemento para la correcta prestación del servicio.

Cualquiera de los análisis, accesos, intrusiones y/o ataques a la seguridad de los sistemas de información de EGARSAT que con motivo del desarrollo de los trabajos del presente pliego deba llevarse a cabo por el adjudicatario, serán realizados con la máxima diligencia y con el único fin de analizar el estado de la seguridad de los sistemas de información, entornos de operaciones, y elementos de comunicaciones de EGARSAT de acuerdo con los objetivos señalados en el presente pliego.

En ningún caso la ejecución de las tareas a realizar deberá impedir el normal funcionamiento de los servicios TI que EGARSAT ofrece en producción, ni desde el punto de vista funcional, ni de su rendimiento ni de la disponibilidad de los mismos.

Los licitadores deberán presentar dentro del sobre único una **memoria técnica** que detalle su propuesta

para cada uno de los servicios solicitados en el presente pliego de prescripciones técnicas, softwares y herramientas a utilizar, metodologías empleadas, ejemplos de informes periódicos a entregar y toda aquella información que ayude a la comprensión por parte de EGARSAT de la solución ofertada.

La puesta en marcha de la solución no deberá demorarse más de 30 días naturales desde la fecha de inicio del contrato. Se valorará en oferta técnica una mejora en este apartado.

La no presentación de la documentación solicitada 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, podrá comportar la exclusión de la empresa incumplidora. EGARSAT podrá solicitar aclaración tantas veces sea necesario para comprobar dicho cumplimiento, excluyéndose de la licitación a las empresas que no lo acrediten.

3. Características de cada uno de los servicios solicitados

3.1. Servicios de monitorización externa de disponibilidad de fluido eléctrico en el CPD

Se deberá monitorizar, desde el exterior, que el CPD de EGARSAT dispone de fluido eléctrico proveniente de la empresa suministradora del mismo (no alimentación proveniente de los SAIs de la compañía).
Esta monitorización deberá realizarse en continuo (24x7x365).
Ante caídas de fluido eléctrico que afecten al CPD de EGARSAT, el sistema deberá notificar la incidencia vía correo electrónico y con un desfase máximo de 2 minutos desde el inicio del incidente a los Administradores de Sistemas de EGARSAT. En el supuesto que la incidencia afectara a elementos que impidieran la entrega del correo electrónico o la recepción del mismo por parte de los destinatarios, la notificación de dicha incidencia deberá realizarse por SMS (sin costes adicionales para EGARSAT). La utilización de canales alternativos a los propuestos para la notificación de dichas incidencias deberá ser consensuada con EGARSAT.

3.2. Servicios de monitorización externa de los servicios TI publicados

Se deberá monitorizar, desde el exterior, la disponibilidad de los elementos y/o servicios TI que EGARSAT tiene publicados desde su CPD (o pueda publicar, durante toda la vigencia del contrato), en la red pública de internet. El detalle de los elementos y/o servicios TI que EGARSAT tiene publicados desde su CPD actualmente no se aporta como información pública al considerarse información sensible de seguridad. Esta información se facilitará bajo demanda.
Las empresas interesadas en la licitación podrán solicitar aclaraciones al respecto a través del correo electrónico licitaciones@egarsat.es y en todo caso, deberán respetar el carácter confidencial de la información a la que tengan acceso, de acuerdo con lo previsto en el artículo 133 de la LCSP.
Esta monitorización deberá realizarse en continuo (24x7x365).
Ante caídas de alguno de los elementos y/o servicios TI que EGARSAT tiene publicados desde su CPD (o pueda publicar, durante toda la vigencia del contrato) en la red pública de internet, el sistema deberá notificar la incidencia vía correo electrónico y con un desfase máximo de 2 minutos desde el inicio del incidente a los Administradores de Sistemas de EGARSAT. La notificación deberá especificar el servicio o servicios afectados. En el supuesto que la incidencia afectara a elementos que impidieran la entrega del correo electrónico o la recepción del mismo por parte de los destinatarios, la notificación de dicha incidencia deberá realizarse por SMS (sin costes adicionales para EGARSAT). La utilización de canales alternativos a los propuestos para la notificación de dichas incidencias deberá ser consensuada con EGARSAT.

3.3. Análisis de vulnerabilidades

Se deberá realizar un análisis de vulnerabilidades con periodicidad semestral, como mínimo. Se valorará en oferta técnica la realización del análisis de vulnerabilidades con periodicidad trimestral.

Alcance de los análisis de vulnerabilidades a realizar desde el exterior:

- Los elementos y/o servicios TI que EGARSAT tiene publicados desde su CPD (o pueda publicar, durante toda la vigencia del contrato) en la red pública de internet.

- Los elementos que componen los servicios de WiFi que EGARSAT tiene instalados (o pueda instalar, durante toda la vigencia del contrato) en sus distintas sedes. El detalle de los elementos que componen los servicios de WiFi que EGARSAT tiene instalados actualmente y las sedes donde están ubicados no se aporta como información pública al considerarse información sensible de seguridad. Esta información se facilitará bajo demanda. Estos análisis de vulnerabilidades a realizar desde el exterior para los elementos que componen los servicios WiFi que EGARSAT tiene instalados (o pueda instalar, durante toda la vigencia del contrato) en sus distintas sedes, son los únicos servicios que están sujetos a posible subcontratación. ***Las empresas interesadas en la licitación podrán solicitar aclaraciones al respecto a través del correo electrónico licitaciones@egarsat.es y en todo caso, deberán respetar el carácter confidencial de la información a la que tengan acceso, de acuerdo con lo previsto en el artículo 133 de la LCSP.***

El análisis de vulnerabilidades (para todos los elementos y servicios descritos en el párrafo anterior "Alcance de los análisis de vulnerabilidades a realizar desde el exterior") deberá realizarse mediante técnicas de caja negra y, como mínimo, deberá incluir los siguientes tipos y categorías de ataques para buscar vulnerabilidades:

- Obtención de información sobre servicios no publicados.
- Obtención de información sobre tráfico de información.
- Obtención de información sobre equipos conectados a la red interna de la organización.
- Conexión a servicios no publicados.
- Conexión remota a equipos de la red interna de la organización.
- Conexión remota a equipos de la red interna con acceso de administración.
- Vulnerabilidades de tipo "deface".
- Vulnerabilidades de tipo "cross-site scripting".
- Vulnerabilidades de tipo "spoofing".
- Vulnerabilidades de tipo inyección de SQL.
- Vulnerabilidades de tipo inyección de código.
- Vulnerabilidades derivadas de la validación de entrada/salida.
- Vulnerabilidades derivadas de análisis de tiempos.
- Vulnerabilidades de sincronización.
- Vulnerabilidades de tipo desbordamiento de memoria.
- Vulnerabilidades basadas en secuestro de sesiones.
- Vulnerabilidades en las redes WiFi.

En el caso particular de los sitios Web de la organización la lista de vulnerabilidades deberá incluir, como mínimo, estudios para los siguientes diez tipos (OWASP TOP 10 2021):

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery (SSRF)

Quedarán fuera de alcance las vulnerabilidades relacionadas con ataques de denegación de servicio e ingeniería social. En la memoria técnica a presentar, el licitador podrá proponer mejoras sobre los tipos y categorías mínimos descritos en el presente apartado con el objetivo de aumentar el nivel de calidad de los servicios a ofertar.

En el supuesto que durante la vigencia del contrato y debido a la evolución tecnológica aparezcan nuevos tipos y categorías de ataques y/o nuevos documentos OWASP TOP 10, estos deberán ser incluidos en los posteriores análisis a realizar.

3.4. Tests de intrusión

Como resultado del análisis de vulnerabilidades periódico del punto anterior y en el supuesto que se detectaran vulnerabilidades que por su naturaleza pudieran comportar una posterior intrusión no deseada y que se hubieren categorizado con riesgo alto, se realizará inmediatamente a continuación un test de intrusión para cada una de dichas vulnerabilidades. Por tanto, los tests de intrusión deberán efectuarse con la misma frecuencia que la frecuencia ofertada para los análisis de vulnerabilidades descritos en el apartado anterior.

El alcance de los tests de intrusión a realizar desde el exterior incluirá tanto las vulnerabilidades detectadas en los elementos y/o servicios TI que EGARSAT tiene publicados desde su CPD (o pueda publicar, durante toda la vigencia del contrato) en la red pública de internet, como aquellas detectadas en los elementos que componen los servicios de WiFi que EGARSAT tiene instalados (o pueda instalar, durante toda la vigencia del contrato) en sus distintas sedes.

3.5. Asesoría y soporte técnico especializado en materias de ciberseguridad

A demanda de EGARSAT, el adjudicatario deberá ofrecer servicios de asesoría y soporte técnico especializado en materias de ciberseguridad. Estos servicios se podrán ofrecer de forma telefónica o a través de videoconferencia (no será necesario que se ofrezca de forma presencial). Se estima una necesidad máxima de 4 horas mensuales en este apartado.

4. Metodologías a utilizar e informes de servicio

El proveedor presentará y realizará sus servicios siguiendo alguna de las metodologías habituales en el campo de las tecnologías de seguridad de redes y sistemas y del hacking ético. Por ejemplo, para la actividad específica de verificación de seguridad de los sistemas de información podrán utilizarse las recomendaciones NIST 800-42, NIST 800-115, así como manuales o procedimientos técnicos, recomendaciones y sistemas de puntuación de vulnerabilidades del SANS Institute, ISAF, ISECOM, ISACA, EC-Council, OWASP, CVSS, OSSTMM e ISSAF. En el supuesto de usar metodologías, manuales, procedimientos técnicos, recomendaciones y/o sistemas de puntuación no explicitados en este párrafo, éstos deberán ser previamente autorizados por EGARSAT.

Deberán relacionarse en la memoria técnica las herramientas comerciales empleadas para la realización de las pruebas de seguridad, las cuales deberán estar adecuadamente licenciadas. Dichas licencias podrán ser solicitadas por el responsable de EGARSAT únicamente a efectos de comprobación del correcto licenciamiento de las herramientas utilizadas en la ejecución de los servicios objeto de este contrato. La utilización de cualquier herramienta no incluida en la oferta tendrá que ser aprobada por el responsable de EGARSAT.

Los informes sobre los análisis de vulnerabilidades y sobre los tests de intrusión descritos a continuación deberán presentarse al personal técnico de EGARSAT en reunión de seguimiento mediante sistemas de videoconferencia, a más tardar 7 días naturales después de su entrega a través de correo electrónico.

4.1. Informes sobre los servicios de monitorización externa de disponibilidad de fluido eléctrico en el CPD

Como resultado de la monitorización externa de disponibilidad de fluido eléctrico en el CPD de

EGARSAT el adjudicatario enviará por correo electrónico y con periodicidad mensual un informe de servicio que refleje las caídas de fluido eléctrico del mes anterior. Dicho informe deberá contener, como mínimo:

- Fecha/hora de inicio de la caída de fluido eléctrico.
- Fecha/ hora fin de la caída de fluido eléctrico.
- % de disponibilidad de fluido eléctrico en el mes anterior.
- % de disponibilidad de fluido eléctrico acumulada del año en curso.

4.2. Informes sobre los servicios de monitorización externa de los servicios TI publicados

Como resultado de la monitorización externa de los servicios TI publicados el adjudicatario enviará por correo electrónico y con periodicidad mensual un informe de servicio que refleje las caídas de los elementos y/o servicios TI que EGARSAT tiene publicados desde su CPD (o pueda publicar, durante toda la vigencia del contrato), en la red pública de internet del mes anterior. Dicho informe deberá contener, como mínimo:

- Nombre del servicio.
- Fecha/hora de inicio de la caída del servicio.
- Fecha/ hora fin de la caída del servicio.
- % de disponibilidad de cada uno de los servicios en el mes anterior.
- % de disponibilidad de cada uno de los servicios acumulada del año en curso.

4.3. Informes sobre los análisis de vulnerabilidades

Como resultado del análisis de vulnerabilidades a realizar con la frecuencia ofertada , el adjudicatario enviará por correo electrónico y dentro de los 7 días naturales siguientes a la realización dicho análisis un informe en formato Word y/o Excel editables (nivel de seguridad mínimo: ZIP con contraseña compleja) que refleje los resultados de dicho análisis y que constará, como mínimo, de 3 grandes apartados:

- Relación de vulnerabilidades encontradas
- Relación de recomendaciones a aplicar para la minimización y/o a ser posible extinción, de las vulnerabilidades encontradas
- Conclusiones

Las vulnerabilidades encontradas se clasificarán siguiendo el sistema de puntuación de la metodología CVSS (Common Vulnerability Scoring System) versión 4.0. En el supuesto que durante la vigencia del contrato y debido a la evolución tecnológica aparezcan nuevas versiones de la metodología CVSS, estas deberán ser incluidas en los posteriores análisis a realizar, siempre que EGARSAT así lo comunique al adjudicatario.

Para facilitar la visualización e interpretación de dichas vulnerabilidades encontradas, el informe deberá etiquetar cada puntuación numérica de CVSS, tal y como se observa en la siguiente tabla (o de forma similar):

RIESGO	CVSS SCORE
CRÍTICO	9,0 – 10
ALTO	7,0 – 8,9
MODERADO	4,0 - 6,9
BAJO	0,0 - 3,9

En caso de que la vulnerabilidad identificada no tenga impacto o sea informativa, no se incluirá Score ni Vector de CVSS.

La relación de vulnerabilidades deberá mostrar, como mínimo:

- identificación del elemento y/o servicio afectado
- el CVE de la vulnerabilidad

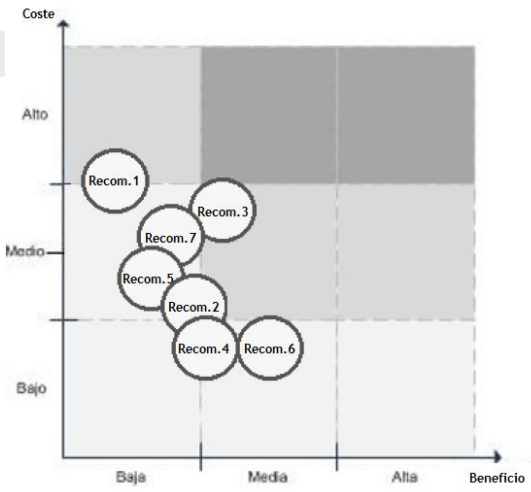
- el CVSS vector
- una descripción de la vulnerabilidad (o un hipervínculo de acceso a información más detallada)
- el CVSS Score
- la categorización del riesgo asociado tal y como refleja la tabla anterior

En cuanto a las recomendaciones y para facilitar su visualización e interpretación, éstas se categorizarán según su propuesta de prioridad de implantación sugerida por el adjudicatario (desde la perspectiva de la seguridad de los servicios TI objeto del análisis de vulnerabilidades) utilizando la siguiente leyenda (o similar):

Prioridad	Icono
ALTA	
MEDIA	
BAJA	

La relación de recomendaciones deberá mostrar, como mínimo:
- identificación de la vulnerabilidad a la que hace referencia
- descripción detallada de la recomendación. Esta descripción detallada deberá ser lo más específica posible y redactada de forma personalizada adecuándose de forma concreta al escenario de EGARSAT (deberán evitarse textos genéricos). Podrá complementarse dicha información con hipervínculos con información más genérica que ayuden a implementación de la recomendación
- propuesta de prioridad de implantación sugerida por el adjudicatario tal y como refleja la tabla anterior

Se valorará en oferta técnica la inclusión de una valoración de coste/beneficio de cada una de las recomendaciones propuestas, siguiendo el siguiente esquema (o similar):



Por último, el informe periódico deberá recoger las conclusiones técnicas que el adjudicatario considere necesarias para la mejora de la seguridad de los servicios objeto de análisis.

4.4. Informes sobre los tests de intrusión

Como resultado de los tests de intrusión el adjudicatario enviará por correo electrónico conjuntamente con el informe de vulnerabilidades del punto anterior, un informe en formato Word y/o Excel editables (nivel de seguridad mínimo: ZIP con contraseña compleja) sobre los tests de intrusión realizados. Dicho informe deberá contener, como mínimo:

- Identificación de la vulnerabilidad que por su naturaleza pudiera comportar una posterior intrusión no deseada y que se hubiera categorizado con riesgo crítico y/o alto.
- Relación de herramientas utilizadas en el intento de intrusión a través de esta vulnerabilidad.
- Descripción detallada de las tareas realizadas en dicho test: estrategias, vías de ataque planteadas y objetivos deseados, exploraciones realizadas, datos y/o información obtenida, resultado (éxito o fracaso) del intento de intrusión y niveles de intrusión conseguidos.

5. Tareas post-presentación de informes

Una vez presentados los informes y realizada cada reunión de seguimiento periódica, EGARSAT podrá implementar las medidas que considere oportunas para la mitigación total o parcial de las vulnerabilidades detectadas en los informes presentados. En el supuesto que EGARSAT aplique dichas medidas tendrá potestad para solicitar al adjudicatario, sin coste adicional, la realización de un nuevo análisis de vulnerabilidades y posterior informe de resultados adicional a los análisis periódicos ya establecidos (en este caso, sin necesidad de reunión de presentación del informe adicional).

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

Todas las tareas relacionadas con la implantación del servicio desde el inicio de las mismas y hasta la puesta en marcha de la solución deberán realizarse sin que éstas supongan un impedimento para el normal funcionamiento de los servicios TI que EGARSAT ofrece en producción, ni desde el punto de vista funcional, ni de su rendimiento ni de la disponibilidad de los mismos.

Para los servicios relacionados con la implantación se estiman 2 reuniones con la empresa adjudicataria de 3 horas de duración máxima cada una de ellas, donde se realizarán tareas de recogida de datos y de adecuación de la solución de forma consensuada con los Administradores de Sistemas de EGARSAT. A efectos de garantizar la correcta ejecución de dichas tareas, la empresa adjudicataria designará un Jefe de Proyecto que actuará como interlocutor único con EGARSAT y que se encargará de:

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

7. Seguimiento del servicio en tiempo de operación

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

- Realizar tareas de coordinación entre los técnicos de la empresa adjudicataria y el contacto de EGARSAT para determinar el calendario de ejecución de cada uno de los servicios solicitados, en especial los análisis de vulnerabilidades, tests de intrusión y reuniones de seguimiento periódicas.

- Proporcionar a EGARSAT la información periódica necesaria para el seguimiento del servicio, así como resolver todas aquellas cuestiones que EGARSAT pudiera plantear durante toda la vigencia del contrato.

8. Precio

Servicios anuales. Desglose de precios:

Descripción	Importe máximo anual (SIN IVA)
Monitorización externa de disponibilidad de fluido eléctrico en el CPD de EGARSAT, en modo continuo (24x7x365)	60,00 €
Monitorización externa de los elementos y/o servicios TI que EGARSAT tiene publicados desde su CPD (o pueda publicar, durante toda la vigencia del contrato) en la red pública de internet, en modo continuo (24x7x365)	1.050,00 €
Análisis de vulnerabilidades, con la periodicidad ofertada, de los elementos y/o los servicios TI que EGARSAT tiene publicados desde su CPD (o pueda publicar, durante toda la vigencia del contrato) en la red pública de internet, y de los elementos que componen los servicios de WiFi que EGARSAT tiene instalados (o pueda instalar, durante toda la vigencia del contrato) en sus distintas sedes. Realización y presentación de los informes correspondientes	4.840,00 €
Realización de tests de intrusión a través de las vulnerabilidades detectadas en el análisis de vulnerabilidades que, por su naturaleza, pudieran comportar una posterior intrusión no deseada, realización y presentación de los informes correspondientes con la periodicidad que oferte la empresa adjudicataria	770,00 €
Servicios de asesoría y soporte técnico especializado en materias de ciberseguridad	2.640,00 €
TOTAL	9.360,00 €

Duración inicial del contrato: 2 años.
Prórrogas previstas: 3 prórrogas de 12 meses de duración cada una de ellas.

Forma de pago: al inicio de cada mensualidad se abonará el importe ofertado anual dividido por 12 meses.

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: 2025.02.06 13:42:32 +01'00'