Expediente: 2024/018 PA

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA LA CONTRACIÓN DEL SERVICIO DE GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD PARA LA AUTORIDAD INDEPENDIENTE DE RESPONSABILIDAD FISCAL, AAI (AIReF)

1. Introducción

La Autoridad Independiente de Responsabilidad Fiscal, AAI (en lo sucesivo AIReF) tiene instaladas varias soluciones hardware y software para garantizar la ciberseguridad de sus sistemas de información.

Dada la complejidad que supone la monitorización y análisis de los eventos generados por estas soluciones, se hace necesario integrar todos y cada uno de los mecanismos de protección en un sistema global.

La AIREF no dispone de los recursos necesarios para realizar esta integración y la posterior gestión de los incidentes de ciberseguridad, por lo que se necesita contratar un servicio de ciberseguridad gestionada SOC (Security Operations Center), con la finalidad de mejorar la situación de seguridad y gestionar las amenazas que se puedan derivar del análisis de los eventos de los sistemas de la AIREF.

2. Objeto del contrato

Los servicios objeto de este contrato serán los siguientes:

1. Prevención frente a ciberincidentes.
    a. Protección de puestos de trabajo, servidores y dispositivos móviles mediante el uso de tecnologías de Endpoint Detection and Response (EDR) para un total de 200 dispositivos y/o 150 usuarios.
    b. Plataforma para el intercambio de indicadores de compromiso (IoCs), que permita agregar fuentes públicas, privadas y propias de ciber inteligencia como, por ejemplo, REYES, y posteriormente, crear subconjuntos que puedan distribuir esos indicadores a los distintos elementos de protección disponibles en la organización (EDR, NGFW, filtrado de correo electrónico, filtrado de navegación web, etc.).
    c. Administración y operación de la solución, en modalidad 24x7. La AIReF también dispondrá de usuarios administradores de la plataforma y, en particular, de la solución de protección de puestos de trabajo.

2. Detección de ciberincidentes.
    a. Plataforma de recolección de eventos de seguridad en modalidad nube, que permita recoger información, al menos, de las siguientes fuentes de información:
        - Puestos de trabajo y servidores (EDR).
        - Dispositivos de seguridad de red (NGFW) y otros.

- Identidad de los usuarios (MS-AD, etc).
- Servicios en nube pública: Azure, AWS, Google cloud, etc.
- Otras fuentes de información, actuales o futuras, que la AIReF determine que deban ser integradas.

b. Plataforma de recolección con capacidad de aplicar reglas de correlación y detección, y analíticas de comportamiento, con el objeto de detectar amenazas que las plataformas individuales de prevención no hayan detectado.
c. Plataforma con capacidades para integrar los IoCs desde distintos ámbitos, incluyendo el entorno descrito anteriormente.
d. Administración y operación de la solución en lo que se refiere a la detección de incidentes por parte del proveedor, en modalidad 24x7. La AIReF también dispondrá de usuarios administradores de la plataforma y, en particular, de la solución de protección de puestos de trabajo.

3. Servicio de respuesta frente a incidentes de ciberseguridad.
   a. Asistencia técnica para la respuesta a ciberincidentes, optimizando los tiempos de detección y de respuesta ante incidentes.
   b. El sistema deberá permitir la agregación y correlación de fuentes de inteligencia de amenazas (IoCs), con objeto de mejorar las capacidades de investigación.
   c. Posibilidad de integración con distintas plataformas de ticketing y, entre ellas, las propias de la AIReF, la del propio proveedor (para la gestión de ciberincidentes) y con LUCIA del CCN-CERT.
   d. Disponibilidad de un espacio unificado para la investigación de ciberincidentes para múltiples usuarios que puedan trabajar concurrentemente en un caso.
   e. Documentación automática de la gestión completa del ciberincidente (bitácora de acciones realizadas) e informes personalizados.
   f. Como parte del servicio, el adjudicatario deberá incluir:
      i. Soporte en la gestión de crisis frente a ciberincidentes, colaborando con el personal responsable de la AIReF y siguiendo las directrices de la guía CCN-STIC 817.
      ii. Capacidad de realizar, en caso de necesidad, análisis forense con validez legal, que pueda ser utilizado por la AIReF frente a posibles reclamaciones de todo tipo.
      iii. Integración del equipo del proveedor en los procesos y procedimientos a los que la AIReF está obligada, dentro del marco del ENS y otras normativas (por ejemplo, RGPD y LOPDGDD), en cuanto a notificaciones y comunicaciones con los organismos reguladores pertinentes.

3. Requisitos técnicos

Los requisitos técnicos que deberán cumplir los servicios mencionados en el punto anterior se detallan a continuación:

3.1.Gestión de inteligencia de seguridad

Los requisitos específicos para el sistema de gestión de inteligencia de seguridad son los especificados a continuación:

- Requisitos generales:
  - RQ-TI-1. La plataforma de inteligencia de amenazas (Threat Intel) del fabricante debe incluir feeds propios de inteligencia.
  - RQ-TI-2. La plataforma debe incluir una plataforma para investigación de amenazas y threat hunting con todo tipo de IoCs (direcciones IP, dominios, hashes, URLs, etc), donde se pueda, además de consultar en segundos la información de la amenaza, analizar el contexto de creación, uso, datos y características del dominio o IP asociado al incidente.
  - RQ-TI-3. La plataforma debe incluir un componente para la gestión de la inteligencia de amenazas, con la capacidad de añadir más feeds de otros proveedores terceros (por ejemplo, REYES del CCN-CERT) o desde un marketplace integrado, con capacidades de contexto y políticas de tiempo para los indicadores.
  - RQ-TI-4. Además, el componente de gestión debe permitir la exportación de la inteligencia a otros dispositivos de seguridad (MRTI – Machine Readable Threat Intelligence).
- Servicio asociado:
  - RQ-TI-5. Despliegue, instalación, puesta en marcha y configuración de la plataforma en el entorno de la AIReF, realizado por perfiles certificados en la solución.
  - RQ-TI-6. Operación de la plataforma por el proveedor, en modalidad 24x7. El proveedor prestará asistencia técnica a la AIReF en la administración de la plataforma, con los siguientes acuerdos de nivel de servicio:
    - Tiempo máximo de respuesta del servicio frente a incidencias: 30 minutos. El proveedor comunicará a los administradores de la AIReF la necesidad de intervención en los sistemas frente a las alertas detectadas en un plazo máximo de 30 minutos. El proveedor colaborará con los interlocutores de la AIReF para resolver la incidencia en el menor tiempo posible.
    - Tiempo máximo de respuesta del servicio frente a peticiones: 2 horas, dentro del horario establecido para el servicio.

3.2.Seguridad del puesto

Los requisitos específicos para los mecanismos de seguridad de los puestos de trabajo son los detallados a continuación:

- Requisitos generales:
  - RQ-EDR-1. Suministro, instalación y configuración, con base en las especificaciones de la AIReF, de 200 licencias de la tecnología seleccionada,

sobre los distintos dispositivos de la AIReF, que pueden ser puestos de trabajo y estaciones de trabajo, servidores (físicos o virtuales), tabletas o dispositivos móviles, soportando las siguientes versiones:

- Linux:
  - CentOS 6, 7 y 8
  - Debian 8, 9 y 10
  - Oracle linux server
  - Red Hat Enterprise Linux 6, 7, 8, 9
  - SUSE Linux Enterprise Server
  - Ubuntu
- Mac versiones con ciclo de vida
- Windows:
  - Windows 7
  - Windows 10 (versiones con ciclo de vida de soporte o en soporte extendido)
  - Windows Server (versiones con ciclo de vida de soporte o en soporte extendido)
  - Windows 11 (versiones con ciclo de vida de soporte o en soporte extendido)
- Android 9 o superior
- iOS 15.0 o superior

- RQ-EDR-2. El agente de puesto deberá ser único, de forma que todas las acciones de detección y respuesta puedan ser realizadas con ese único agente. El agente debe incluir capacidades de prevención avanzada frente a malware/exploits, tanto conocidos como desconocidos (zero day).
- RQ-EDR-3. La solución debe basarse en una plataforma 100% nativa en cloud.
- RQ-EDR-4. Los servicios en cloud pública del fabricante (su proveedor de infraestructura en nube) deben estar alojados en datacenters de la Unión Europea y disponer de la certificación de ENS nivel ALTO.
- RQ-EDR-5. Todos los requisitos de seguridad exigidos en el presente pliego deben ser cubiertos por un único fabricante de seguridad, una única tecnología y una única interfaz o consola. Es decir, la solución propuesta debe facilitar el acceso a todas las funcionalidades demandadas, preferentemente desde una única interfaz o consola, entendiéndose esta como un único portal web en el que se recojan todas las capacidades. No se considerarán válidas aquellas soluciones que requieran vincular, enlazar o integrar distintas plataformas o aplicaciones web, dominios o consolas para cubrir las funcionalidades requeridas o aquellas que integren estas consolas en un portal de aplicaciones.

- Capacidades de detección:
    - RQ-EDR-6. El servicio de detección debe recolectar información y datos de telemetría que lleguen a nivel de hilo (thread) de un proceso.
    - RQ-EDR-7. Motor de análisis de comportamiento: debe estar activo de manera predeterminada y supervisar todos los eventos de los endpoints para identificar cadenas de ataque.
    - RQ-EDR-8. Protección frente al ransomware basada en el comportamiento y técnicas de engaño o honeypots.
    - RQ-EDR-9. Debe permitir la puesta en cuarentena de malware detectado y ofrecer la posibilidad de restaurar o poner en lista blanca los archivos de cuarentena directamente desde la plataforma de gestión.
    - RQ-EDR-10. La solución propuesta debe ser una plataforma de seguridad de última generación que utilice técnicas de aprendizaje automático/machine learning para la prevención previa a la ejecución de malware conocido y desconocido.
    - RQ-EDR-11. La solución debe disponer de las capacidades de detección y prevención que incluya la detección de técnicas, tácticas y procedimientos y los indicadores de ataque (IoAs) susceptibles de ser utilizados por agentes maliciosos.
    - RQ-EDR-12. Prevención de exploits basada en técnicas: debe evitar que aparezcan vulnerabilidades conocidas, de día cero y sin actualizar bloqueando las técnicas de explotación que emplean los atacantes para manipular aplicaciones.
    - RQ-EDR-13. La plataforma debe proporcionar capacidades de detección basadas en el análisis de comportamiento posterior a la ejecución de un malware, permitiendo la protección contra las actividades habituales del ransomware (cifrado de archivos, eliminación de archivos sombra, etc.).
    - RQ-EDR-14. La solución debe facilitar acciones de respuesta que incluyan el aislamiento del endpoint de la red (persistiendo la desconexión tras un reinicio) o la conexión remota interactiva con el endpoint. Durante esta conexión, los administradores deben poder realizar acciones de análisis, contención, respuesta y remediación.
    - RQ-EDR-15. La solución debe ofrecer detección de amenazas basada en comportamiento e inteligencia de amenazas que permita alertar y bloquear amenazas y que adicionalmente ofrezca información relativa a:
        - Vector de entrada utilizado por el atacante.
        - Comprensión de las tácticas y técnicas utilizadas por el atacante.
        - Periodo temporal en el que se enmarca la amenaza.
        - Activos comprometidos.
        - Contextualización de los procesos seguidos por el atacante a lo largo de la cadena de ataque.

- RQ-EDR-16. Proporcionará una detección y prevención basada en el comportamiento posterior a la ejecución, basada en el Indicador de Ataque (IoA) mapeado según el marco MITRE ATT&CK. Este tipo de reglas de detección debe soportar reglas relacionadas con procesos (hasta 3 niveles de procesos y líneas de comando asociadas), ficheros y comunicaciones. En todos los casos debe ofrecerse la posibilidad de ofrecer detección y bloqueo.
- RQ-EDR-17. La solución propuesta debe tener capacidades de detección y respuesta de amenazas relacionadas con la identidad. Debe ser capaz de detectar, prevenir y responder eficazmente a amenazas internas, filtración de datos, movimientos laterales sospechosos, modificación de permisos, exfiltración de dispositivos físicos, recopilación y manipulación de archivos confidenciales, etc (ITDR, Identity Threat Detection and Response).
- RQ-EDR-18. La solución propuesta deberá disponer de un panel o dashboard de Identidad para revisar la postura de riesgo de la organización con el fin de ayudar a la toma de decisiones. Deberá permitir la visualización de riesgo por usuario/equipo, proporcionando información adicional sobre el activo, incluyendo la tendencia sobre eventos notables, comparación entre afines y alertas e información adicional asociadas a activos para descubrir fácilmente las amenazas ocultas.
- RQ-EDR-19. La solución realizará una clasificación automatizada de roles de usuarios y puestos, basada en un análisis constante de la actividad.
- RQ-EDR-20. La solución debe incluir asistentes y lenguaje de búsquedas para analizar la información de telemetría disponible. Los asistentes deben permitir al menos buscar, para un conjunto de host, procesos y rango de fechas:
  - Procesos
  - Ficheros
  - Red
  - Imágenes cargadas
  - Registro
  - Log de eventos
  - Todos los tipos de eventos combinados
- RQ-EDR-21. La solución debe poder inspeccionar el tráfico (DPI) en tiempo real para detectar amenazas relacionadas con la Identidad.
- RQ-EDR-22. Las capacidades de seguridad contra ataques basados en identidad (ITD- Identity Threat Detection) deben utilizar el mismo agente único que en el resto de las funcionalidades solicitadas. No serán válidas soluciones que requieran el despliegue de soluciones adicionales que requieran la instalación de servicios, servidores o entornos adicionales.

- <u>Capacidades forenses:</u>
  - RQ-EDR-23. La solución debe poder incluir, opcionalmente, la capacidad de recoger información forense histórica, permitiendo analizar el origen y alcance de un ataque, desde un único agente EDR.

- RQ-EDR-24. La telemetría extraída de los endpoints, así como los detalles forenses, deben poder enviarse a la plataforma cloud en tiempo real. En caso de que no exista conectividad entre la consola cloud y el endpoint para el envío de telemetría, el agente instalado se encargará de guardar y custodiar esta información hasta que se retome esta conectividad y pueda realizarse el envío a la plataforma cloud.
- RQ-EDR-25. Mediante la solución ofertada, se debe poder hacer triaje de datos de ficheros, registro, logs, historial del navegador, sesiones de red, puertos escuchando, procesos escuchando, descriptores y configuraciones.
- RQ-EDR-26. La solución debe tener integrada una herramienta de inteligencia de amenazas para la identificación y clasificación del malware.
- RQ-EDR-27. La solución debe proporcionar la capacidad de conectarse remotamente a los sistemas de destino con el fin de recopilar pruebas forenses adicionales (volcados de memoria completos, registro, archivos, etc).
- RQ-EDR-28. La consola de gestión debe poder proporcionar al analista, al menos, la siguiente información:
  - Visor de eventos con prioridad.
  - Cadena de actividad / causalidad.
  - Timeline del ataque.
  - Visualización de la actividad y contexto para la investigación y detección de ataques.
  - Dashboard de Incidentes y gravedad incluyendo la asignación de incidentes por parte de los analistas, bloc de notas y panel de discusión. Consultas personalizadas sobre los datos durante una investigación, incluyendo búsquedas de IOCs.
  - Integración con herramienta de inteligencia de amenazas que enriquezca la información de contexto de los incidentes aportando información útil para su análisis.
- RQ-EDR-29. La solución se gestionará a partir de una interfaz gráfica basada en Web (GUI).
- RQ-EDR-30. La solución debe permitir las búsquedas en la información generada por toda la base instalada sin producir afectación a los endpoints o incrementar los consumos de recursos hardware del agente instalado.
- RQ-EDR-31. La solución debe admitir el control de acceso basado en roles

- <u>Generación de informes:</u>
  - RQ-EDR-32. La solución debe tener capacidad para generar informes incluidos nativamente para poder monitorizar la postura de seguridad y la salud de los equipos en la organización, incluyendo al menos:
    - Dashboard de eventos de seguridad.
    - Panel de amenazas detallado.
    - Dashboard de errores de seguridad (logs).
    - Panel del estado de los equipos.
    - Historial de cambio de políticas sobre los equipos.

        - Panel para revisión del historial de estado del servicio.
        - Panel de Ingestión de Datos.
        - Paneles customizados en base a los datos de telemetría a partir del lenguaje de queries.
    - RQ-EDR-33. La solución debe admitir alertas por correo electrónico para proporcionar notificaciones inmediatas a los equipos relevantes.
    - RQ-EDR-34. La solución debe generar informes para proporcionar un resumen de eventos de seguridad y estado de la implementación.
    - RQ-EDR-35. La solución deberá soportar el registro de acciones permitiendo la monitorización de tareas tales como las actualizaciones, desinstalación, scans, recuperación de datos críticos (eventos de seguridad, ficheros de soporte técnico) y restauración de ficheros en cuarentena, proporcionando visibilidad de los fallos o errores ocurridos.
    - RQ-EDR-36. La solución propuesta es capaz de proporcionar una visualización, a través del navegador, de amenazas y malware, pudiendo realizar la exportación de los datos de amenazas o la salud de los equipos en formato CSV.
- Servicio asociado:
    - RQ-EDR-37. Despliegue, instalación, puesta en marcha y configuración de la solución, realizado por perfiles certificados en la solución y siguiendo las directrices del personal de la AIReF para acompasar la puesta en marcha con las necesidades específicas que serán planteadas al inicio del proyecto y durante la vigencia del contrato.
    - RQ-EDR-38. Monitorización, detección y comunicación de alertas por incidencias, en modalidad 24x7. El proveedor prestará asistencia técnica a la AIReF en la administración de la solución, con los siguientes acuerdos de nivel de servicio:
        - Tiempo máximo de respuesta del servicio frente a incidencias: 30 minutos. El proveedor comunicará a los administradores de la AIReF la necesidad de intervención en los sistemas frente a las alertas detectadas en un plazo máximo de 30 minutos. El proveedor colaborará con los interlocutores de la AIReF para resolver la incidencia en el menor tiempo posible.
        - Tiempo máximo de respuesta del servicio frente a peticiones: 2 horas, dentro del horario establecido para el servicio.

3.3.Monitorización de la seguridad

Los requisitos específicos para la monitorización y detección de incidentes de seguridad son los detallados a continuación:

- Repositorio de información:
    - RQ-MON-1. El repositorio proporcionado para la ingesta de eventos de seguridad debe permitir la integración de los logs de endpoint propuestos para realizar la correlación.

- RQ-MON-2. El servicio de recolección de la información debe ser capaz de recolectar datos a gran escala, estando preparado para su aplicación en el análisis matemático y el big data.
- RQ-MON-3. La solución debe ser autoescalable y basada en Cloud, sin necesidad de almacenamiento físico en las instalaciones del cliente. Se valorará positivamente que la ampliación de almacenamiento sea transparente para la organización y que no requiera parada de servicio.
- RQ-MON-4. Se requiere que todas las comunicaciones sean cifradas entre los componentes que forman parte del servicio de base de datos (tanto los de ingesta de logs como los de reenvío, con Syslog sobre TLS). Es necesario que los datos en tránsito sean encriptados utilizando, al menos, el método de encriptación TLS 1.2.
- RQ-MON-5. La base de datos que soporta el repositorio debe poder registrar toda la información de los eventos recibidos, independiente de la fuente, creando los datasets correspondientes que podrán ser consultados en raw o parseados.
- RQ-MON-6. El servicio debe proporcionar las capacidades de:
  - Almacenamiento en caliente en la nube del fabricante al menos 30 días.
- RQ-MON-7. La plataforma debe permitir utilizar y crear reglas de parseo, que permitan:
  - Eliminar datos no necesarios para analíticas, hunting o regulación.
  - Reducir los costes de almacenamiento de datos.
  - Añadir etiquetas a los datos recolectados como parte del flujo de recolección.
- RQ-MON-8. La solución debe incorporar un agente de recolección para la recogida on-premise en sistemas Windows y Linux.

  RQ-MON-9. La solución debe permitir no solo visualizar los logs en crudo sino agregar, parsear y correr analíticas sobre la información recogida, enriqueciendo la información dada por la solución.

- <u>Servicio asociado:</u>
  - RQ-MON-10. Despliegue, instalación, puesta en marcha y configuración de la solución, realizado por perfiles certificados en la solución.
  - RQ-MON-11. Monitorización y detección de incidentes y comunicación de alertas por parte del proveedor en modalidad 24x7. El proveedor prestará asistencia técnica a la AIReF en la administración de la solución, con los siguientes acuerdos de nivel de servicio:
    - Tiempo máximo de respuesta del servicio frente a incidencias: 30 minutos. El proveedor comunicará a los administradores de la AIReF la necesidad de intervención en los sistemas frente a las alertas detectadas en un plazo máximo de 30 minutos. El proveedor colaborará con los interlocutores de la AIReF para resolver la incidencia en el menor tiempo posible.
    - Tiempo máximo de respuesta del servicio frente a peticiones: 2 horas.

3.4.Respuesta de seguridad

Los requisitos específicos para los servicios de respuesta frente a incidentes de seguridad son los indicados a continuación:

- Requisitos generales:
  - RQ-RESP-1. La plataforma propuesta debe permitir medir la disminución paulatina en los tiempos de respuesta frente a ciberincidentes, y para ello debe disponer de indicadores cuantitativos relacionados con la respuesta.
  - RQ-RESP-2. La plataforma propuesta debe disponer de la capacidad de agregar y correlacionar fuentes de inteligencia de amenazas, incluyendo, al menos, las propias del proveedor, de terceros (REYES) y de la plataforma de inteligencia de amenazas que se debe incluir en la propuesta.
  - RQ-RESP-3. La plataforma debe ser capaz, de forma autónoma, de establecer puntuaciones sobre las amenazas, combinando las distintas fuentes de información de entrada con las fuentes de inteligencia de seguridad integradas, ofreciendo a los analistas de seguridad del proveedor valoraciones que maximicen la eficacia en las investigaciones y en la respuesta.
  - RQ-RESP-4. La plataforma debe permitir la personalización de la visualización, de manera que el procesamiento de posibles incidentes y la aplicación de inteligencia se ajuste a las capacidades y necesidades de cada analista de seguridad.
  - RQ-RESP-5. La plataforma debe permitir que las integraciones con los distintos elementos puedan ser ampliables y que sean abiertas, pudiendo por tanto modificar integraciones existentes y/o añadir nuevas integraciones.
  - RQ-RESP-6. La plataforma debe permitir la convergencia de datos sobre incidentes e indicadores: la plataforma registrará y capturará automáticamente todos los indicadores presentes en los incidentes recibidos.
- Requisitos específicos:
  - RQ-RESP-9. Deben generarse registros de acceso para cada acción y acceso realizado, permitiendo incluir esos registros de auditoría en el proceso de monitorización de seguridad.
  - RQ-RESP-10. Integración con diferentes plataformas de ticketing para la recepción de tickets, generación de tickets, complementar la información de tickets. Especialmente relevantes los casos de LUCIA y de la propia plataforma de ticketing de la AIReF.
  - RQ-RESP-11. La solución deberá permitir el establecimiento de pesos de riesgos asociado a cada dato para la toma de decisiones basadas en el nivel del riesgo.
  - RQ-RESP-12. El producto debe incluir un panel de administración con información sobre tendencias de incidentes por tipología, siendo este personalizable.
  - RQ-RESP-13. La plataforma debe permitir a los operadores acceder a una historia gráfica del incidente en su trabajo diario, incluyéndose:

        - Ver y acceder fácilmente a todos los artefactos, notas y archivos adjuntos recopilados en un incidente.
        - Ver los aspectos más destacados de la investigación hasta el momento.
        - Designar fácilmente artefactos como importantes o como evidencia.
        - Interactuar con fuentes de inteligencia externa a través de IoCs.
    - RQ-RESP-14. Los analistas deben poder ejecutar comandos o tareas ad-hoc mientras investigan incidentes.
    - RQ-RESP-15. La solución debe permitir el establecimiento tanto de notificación por correo electrónico, como recordatorios para tareas pendientes, parametrizables según criticidad y tiempo.
    - RQ-RESP-16. La solución debe permitir agrupar incidentes por tipología.
    - RQ-RESP-17. La solución debe incluir capacidades de búsqueda (por ejemplo, para incidentes pasados). A tal fin, todos los objetos clave, como datos de investigación, indicadores, chats, etc., estarán indexados pudiéndose buscar en tiempo real.
- Generación de informes:
    - RQ-RESP-18. Disponibilidad de paneles e informes flexibles y personalizables, tanto acumulativos como acciones de incidentes en movimiento. La plataforma deberá proporcionar informes predefinidos y también permitir la creación de informes propios. La exportación de los informes podrá ser realizada en formatos PDF, CSV y HTML. Se deberá permitir generar informes de forma periódica.
    - RQ-RESP-19. Capacidad para generar informes de Threat Intel que incluya los resultados de la investigación Threat Intel realizada por los analistas del proveedor y/o de la AIReF.
    - RQ-RESP-20. Integración con servicios de correo electrónico, como Microsoft EWS, Gmail o servicios SMTP para el envío de informes automatizados.
- Servicio asociado:
    - RQ-RESP-21. El proveedor prestará asistencia técnica para la resolución de incidencias, en modalidad 24x7, y con los siguientes acuerdos de nivel de servicio:
        - Tiempo máximo de respuesta del servicio frente a incidencias: 30 minutos. El proveedor comunicará a los administradores de la AIReF la necesidad de intervención en los sistemas frente a las alertas detectadas en un plazo máximo de 30 minutos. El proveedor colaborará con los interlocutores de la AIReF para resolver la incidencia en el menor tiempo posible.
        - Tiempo máximo de respuesta del servicio frente a peticiones: 2 horas, dentro del horario establecido para el servicio.

4. Plazo de implantación de la solución, comienzo del servicio y horario de servicio

La solución -con todas las mejoras ofertadas, en su caso, por el adjudicatario- deberá estar totalmente implantada y operativa en el plazo máximo de 4 semanas a contar desde el día siguiente a la formalización del contrato, salvo que el adjudicatario haya ofertado un plazo inferior (tres semanas).

El horario de prestación del servicio será:

- 24x7 para los servicios de monitorización y detección de incidencias;
- de 9:00 a 19:00 de lunes a viernes y de 9:00 a 18:00 en fines de semana para la asistencia técnica para solución de incidencias.

La Presidenta de la Autoridad Independiente
de Responsabilidad Fiscal, AAI
P.D.(Resolución de 28/7/2014)
El Director de la División Jurídico-Institucional

Diego Pérez Martínez

Fecha:
2024.02.29
14:14:37 +01'00'

Diego Pérez Martínez

POR EL ADJUDICATARIO:

Firmado

D.N.I.