Junta de Andalucía

Consejería de la Presidencia, Interior,
Diálogo Social y Simplificación Administrativa
Agencia Digital de Andalucía

PLIEGO DE PRESCRIPCIONES TÉCNICAS

Suministro y servicios asociados de plataforma de monitorización, y de servicios recurrentes y bajo demanda, para apoyo al Centro de Operaciones de Seguridad de la Junta de Andalucía (AndalucíaCERT)

Expte. CONTR 2023 642838

LOTE 1 - SUMINISTRO Y SERVICIOS ASOCIADOS DE PLATAFORMA DE MONITORIZACIÓN PARA APOYO AL CENTRO DE OPERACIONES DE SEGURIDAD DE LA JUNTA DE ANDALUCÍA (ANDALUCÍACERT)

LOTE 2 – SERVICIOS RECURRENTES Y BAJO DEMANDA PARA APOYO AL CENTRO DE OPERACIONES DE SEGURIDAD DE LA JUNTA DE ANDALUCÍA (ANDALUCÍACERT)

Cofinanciado por la Unión Europea

Contenido

Cofinanciado por la Unión Europea

1. Antecedentes

El Centro de Operaciones de Seguridad de Andalucía, conocido como AndalucíaCERT e integrado dentro del centro de ciberseguridad de Andalucía es la capacidad de respuesta a incidentes de seguridad TIC de la Junta de Andalucía. AndalucíaCERT se puso en marcha en el marco del Plan Director de Seguridad de los Sistemas de Información y Telecomunicaciones de la Administración de la Junta de Andalucía para el periodo 2010- 2013. Dicho Plan incluía entre sus proyectos el despliegue y explotación del centro de seguridad TIC de Andalucía, AndalucíaCERT, como instrumento de referencia para la prevención, detección y respuesta a incidentes y amenazas de seguridad digital en el ámbito de la administración autonómica andaluza.

El Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, en su modificación por el Decreto 70/2017, de 12 de junio, indica en su artículo 12 que se desarrollarán acciones centralizadas de prevención, detección y respuesta a incidentes en el ámbito de la Administración de la Junta de Andalucía a través de AndalucíaCERT, centro especializado y orientado a la prevención, detección y respuesta a incidentes y amenazas de seguridad.

El organismo competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones es la Agencia Digital de Andalucía (en adelante, "ADA") que, en su Plan Inicial de Actuación, recogido en la Orden del 3 de mayo de 2022, por la que se aprueba el Plan Inicial de Actuación de la Agencia Digital de Andalucía, contempla (línea de actuación 3.1. Desarrollo del Centro de Ciberseguridad de Andalucía) la mejora de la protección, detección y respuesta de incidentes.

Con fecha 21 de octubre de 2022 se publica el Acuerdo de 18 de octubre de 2022, del Consejo de Gobierno, por el que se aprueba la Estrategia Andaluza de Ciberseguridad 2022-2025. Dicha Estrategia, con el objetivo de conseguir una hoja de ruta que permita avanzar hacia una sociedad digital segura y confiable, define líneas de actuación (LA) para alcanzar los objetivos estratégicos de fortalecimiento de las estructuras de gobierno; refuerzo de las capacidades de prevención, detección y respuesta a incidentes; cooperación y colaboración; impulso de Andalucía como referente en ciberseguridad; mejora de las capacidades de ciberseguridad en las empresas andaluzas; desarrollo de una industria de ciberseguridad; potenciación del talento y la competencias de ciberseguridad; y mejora de la cultura y buenas prácticas de ciberseguridad.

De acuerdo con la línea de actuación LA2, "Definición e implantación de un plan de desarrollo y mejora continua de las capacidades de prevención, detección y respuesta a incidentes de AndalucíaCERT", este centro debe dotarse de los medios necesarios para asegurar la seguridad y la resiliencia de los sistemas y servicios proporcionados por los organismos incluidos en el ámbito de su competencia.

Cofinanciado por la Unión Europea

2. El nuevo marco FEDER 21-27

La situación excepcional derivada de la pandemia de la COVID-19 ha acelerado el proceso de digitalización, poniendo de relieve las fortalezas y también las carencias tanto desde el punto de vista económico como social y territorial.

En este contexto, la Comisión Europea ha presentado la comunicación "*Dar forma al futuro digital de Europa*". La estrategia europea contiene un conjunto de medidas para una Transformación Digital que redunde en beneficio de todos, y refleje lo mejor de Europa: abierta, justa, diversa, democrática y con confianza en sí misma.

España Digital 2025 recoge un conjunto de medidas, reformas e inversiones, articuladas en diez ejes estratégicos, alineados a las políticas digitales marcadas por la Comisión Europea para el nuevo periodo. Las acciones de la Agenda están orientadas a impulsar un crecimiento más sostenible e inclusivo, impulsado por las sinergias de las transiciones digital y ecológica, que llegue al conjunto de la sociedad y concilie las nuevas oportunidades que ofrece el mundo digital con el respeto de los valores constitucionales y la protección de los derechos individuales y colectivos.

El eje 4 tiene como objetivo *"reforzar la capacidad española en ciberseguridad, consolidando su posición como uno de los polos europeos de capacidad empresarial (meta 2025: 20.000 nuevos especialistas en ciberseguridad, IA y Datos)"* y consta de cinco medidas. La medida 17 del eje 4. Ciberseguridad se denomina "*Despliegue y operación del Centro de Operaciones de Ciberseguridad*".

El objetivo específico 1.2. "*Aprovechamiento de las ventajas de la digitalización para los ciudadanos, las empresas, las organizaciones de investigación y las administraciones públicas*" del nuevo marco FEDER 21-27 recoge en su Línea Estratégica de actuación 1.2.4 una serie de Actuaciones para garantizar la ciberseguridad y protección de datos, entre ellas "*Reforzar las capacidades de prevención, detección y respuesta a incidentes en la Administración de la Junta de Andalucía a través de servicios avanzados de ciberseguridad*".

En este contexto, el objeto de este contrato viene a proporcionar una solución para la prevención, detección, gestión y respuesta ante incidentes de seguridad, así como dotar a AndalucíaCERT de las capacidades técnicas y operativas precisas para evaluar el estado de seguridad y establecer líneas de mejora.

3. Entorno tecnológico actual

La Red Corporativa de la Junta de Andalucía (RCJA) integra el conjunto de servicios avanzados de telecomunicaciones para los organismos de la Administración autonómica, reduciendo así los costes globales en comunicaciones, mejorando la prestación de los servicios y optimizando su gestión. Con objeto

de compartir servicios y recursos, se encuentra, además, interconectada a otras redes externas, pertenecientes a otras Administraciones, Organismos Públicos de Andalucía no adscritos a RCJA o a entidades y empresas privadas, entre las que destacan sin ánimo de ser exhaustivo:

- Red NEREA. Red interadministrativa de Andalucía, donde se ponen en contacto las administraciones públicas presentes en el territorio andaluz (Entidades Locales, Administración Autonómica y Administración General del Estado).
- Red SARA. Red de interconexión de las comunidades autónomas con la Administración General del Estado.
- Accesos Externos, donde resaltan hospitales concertados, pasarela de usuarios en movilidad, o entidades bancarias.

Los Nodos de Interconexión de RCJA ofrecen los servicios de seguridad perimetral y control de acceso necesarios para minimizar el nivel de riesgo en seguridad, monitorizando todo el tráfico desde y hacia RCJA, e incluyen un conjunto de servicios de valor añadido sobre servicios portadores de la RCJA.

La infraestructura está desplegada en la actualidad en dos centros de proceso de datos (CPD) ubicados en la provincia de Sevilla:

- El primer CPD “Zoco”, ubicado en el municipio de Tomares, y uno de los nodos de interconexión.
- El segundo CPD “Cica”, ubicado en Sevilla capital, donde se encuentra el otro nodo de interconexión.

Esta configuración podrá variar en el futuro conforme a la evolución de las infraestructuras tecnológicas de la Junta de Andalucía. En caso de que la arquitectura del sistema sufriera modificaciones respecto a la descrita anteriormente, el adjudicatario deberá adaptar la prestación de sus servicios a los cambios producidos, con objeto de dar cumplimiento a lo establecido en la documentación de la presente licitación y en la oferta presentada. Por este motivo, los requisitos descritos en el presente pliego han sido especialmente diseñados para permitir su eventual adaptación a las posibles evoluciones de RCJA.

AndalucíaCERT con presencia en Sevilla y Málaga cuenta actualmente con un Sistema de Gestión de Información y Eventos de Seguridad (en adelante “SIEM”, siglas de su designación en lengua inglesa “Security Information and Event Management”) de arquitectura distribuida. Desde este SIEM se realiza la gestión de la información y de los eventos de seguridad procedentes de distintas fuentes que incluyen principalmente el tráfico de red e infraestructuras de cada uno de los dos Nodos de Interconexión de RCJA, y entre otras, las correspondientes a los sistemas horizontales de la Junta de Andalucía, así como otros sistemas de gestión de eventos pertenecientes a distintos organismos.

Por otro lado, AndalucíaCERT se integra en el Sistema de Alerta Temprana (SAT) de Internet, un servicio desarrollado e implantado por el Equipo de Respuesta ante Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT) que procesa los datos relativos a los eventos detectados y remite

información procesada de inteligencia sobre ciberamenazas a los organismos adscritos. Para ello, utiliza sondas que deben ser instaladas en las redes de los organismos adscritos y que, tras recoger y depurar la información relevante, envía los eventos al sistema central de CCN-CERT.

Adicionalmente, AndalucíaCERT cuenta con un conjunto de medios que le permiten realizar tareas de detección de riesgos y amenazas, en algunos casos con herramientas proporcionadas por el CCN-CERT, como Reyes, Rocío o Ana. Otros son servicios como Trillion o Shodan.

Además, se están desarrollando los mecanismos para disponer de una solución para la detección y respuesta a ciberincidentes en equipo final (EDR) desde AndalucíaCERT.

En el Anexo I se relacionan las características principales de la solución actual en cuanto a la tecnología y a las diferentes fuentes de eventos a integrar.

4. Objeto del contrato

El objeto de este contrato es proveer de servicios de soporte a las actividades de Prevención, Detección y Respuesta a incidentes realizadas por AndalucíaCERT.

El amplio espectro de actividades y el hecho de promover la concurrencia ha motivado la división en diferentes lotes que se relacionan a continuación:

- Lote 1: Suministro y servicios asociados de plataforma de monitorización para apoyo al Centro de Operaciones de Seguridad de la Junta de Andalucía (AndalucíaCERT)
- Lote 2: Servicios recurrentes y bajo demanda para apoyo al Centro de Operaciones de Seguridad de la Junta de Andalucía (AndalucíaCERT)

Las finalidades comunes a los dos lotes son las siguientes:

1. Reforzar la ciberseguridad en el ámbito de los organismos que forman parte del ámbito de actuación de AndalucíaCERT mediante la implantación de **infraestructuras de ciberseguridad para mejorar la detección y respuesta ante incidentes**.
2. Avanzar en la implantación del CSIRT autonómico AndalucíaCERT como **Centro de Operaciones de Seguridad (SOC) de la Junta de Andalucía** en el ámbito arriba mencionado.
3. Prestar apoyo al **cumplimiento del Esquema Nacional de Seguridad** (Real Decreto 311/2022, de 3 de mayo) en los organismos del grupo atendido de AndalucíaCERT. Esto supone aproximadamente 85 organismos, aunque podrá ampliarse en base a convenios de colaboración con otras entidades. En concreto, se dará soporte al principio básico de "Prevención, detección, respuesta y conservación" (art. 8.3) y al de "Vigilancia continua" (art. 10), así como a los requisitos mínimos de "Prevención ante otros sistemas de información interconectados" (artículo 23) e "Incidentes de seguridad" (art. 25), y a las medidas de seguridad op.mon.1 (detección de intrusión), op.mon.3 (vigilancia) y, particularmente, op.mon.3.1 (se dispondrá de un sistema automático de recolección de eventos de seguridad).
4. Avanzar en la **ejecución de la Estrategia Andaluza de Ciberseguridad 2022-2025**, en concreto de las Líneas de Actuación LA2 (Definición e implantación de un plan de desarrollo y mejora continua de las capacidades de prevención, detección y respuesta a incidentes de AndalucíaCERT) y LA4 (Creación y desarrollo de un plan de promoción de Andalucía, posicionándola como territorio de referencia en materia de ciberseguridad.)

Cofinanciado por la Unión Europea

5. Lote 1: Suministro y servicios asociados de plataforma de monitorización para apoyo al Centro de Operaciones de Seguridad de la Junta de Andalucía (AndalucíaCERT)

En los siguientes epígrafes se describirán los suministros y servicios incluidos en el presente lote. Los requisitos establecidos en el presente Pliego de Prescripciones Técnicas tienen la consideración de mínimos exigibles a cumplir en todo momento por el adjudicatario, cuya oferta podrá incluir mejoras y características adicionales.

Salvo indicación en sentido contrario:

- Los medios humanos adscritos a estos servicios lo harán con dedicación completa.
- El personal destinado por el adjudicatario para realizar servicios prestados de forma localizada y de forma continuada en el tiempo trabajará, en colaboración con el equipo de AndalucíaCERT, en las instalaciones de este organismo, ubicadas en Málaga y en Sevilla.

5.1. Objeto

El objeto de este lote es dotar a AndalucíaCERT de:

- El suministro, instalación, integración, soporte y mantenimiento de una plataforma de monitorización de eventos y detección de incidentes de seguridad en las infraestructuras TI de la Junta de Andalucía, que sustituirá y mejorará la existente. Dicha plataforma deberá contar con capacidades y características que permitan:
  - Capturar y analizar tráfico de red.
  - Recoger y normalizar eventos de seguridad y flujos de distintas fuentes.
  - Realizar correlación y generar alarmas, gestionables a través de una consola de operación integrada, con capacidad para generar informes.
- Equipos para la actualización de sondas del Sistema de Alerta Temprana (SAT) de CCN-CERT.
- Servicio de gestión y respuesta a incidentes de seguridad y de incidencias, peticiones y consultas de AndalucíaCERT.

Las finalidades que se persiguen con la contratación de estos servicios son las siguientes:

1. Obtener una solución global de monitorización acorde al estado del arte en materia de detección de amenazas de ciberseguridad basada en análisis de logs, eventos de seguridad y tráfico de red.

2. Permitir el crecimiento del ámbito de actuación y de los servicios de AndalucíaCERT mediante un sistema escalable, adaptable y con alto grado de operatividad, mejorando los servicios que se prestan actualmente.

Si durante la vigencia del contrato y sus posibles prórrogas AndalucíaCERT cambiara de denominación o alguna de sus funciones relacionadas con el objeto del presente lote fueran asumidas por otro organismo o entidad, las menciones a AndalucíaCERT contenidas en este documento deberán considerarse como referidas a la nueva denominación o al organismo o entidad que asuma dichas funciones.

5.2. Suministro

Con carácter general y en relación con el suministro se considerarán los siguientes requisitos:

- REQ-SUM-1: Todos los elementos deberán contar con medidas de redundancia ante fallos y, los elementos hardware, de gestión remota fuera de banda.
- REQ-SUM-2: Se requiere que todos los componentes, hardware y software, necesarios para el correcto funcionamiento del equipamiento objeto del suministro no se encuentren incluidos en procesos de discontinuidad, descatalogación o fin de vida del fabricante. En el caso de que los equipos o el software objeto de la licitación entren en un proceso de descatalogación durante la duración del contrato y sus posibles prórrogas, el licitador está obligado a sustituir el equipamiento o el software por otros de características similares sin coste para la Junta de Andalucía antes del vencimiento del fin de vida del producto, previa autorización por parte de la Junta de Andalucía. El retraso en la sustitución de los productos dará lugar a la aplicación de las penalizaciones establecidas en el Pliego de Cláusulas Administrativas Particulares, llegando a constituir causa de rescisión del contrato.
- VAL-SUM-1: Mediante este criterio se verificará y valorará con carácter general la idoneidad, calidad y flexibilidad de la arquitectura de las soluciones propuestas y cómo estas dan cumplimiento a los requisitos enumerados. (SOBRE 2).

5.2.1. Plataforma de monitorización

El adjudicatario deberá proporcionar los elementos hardware y software y los servicios necesarios para implementar una Plataforma de monitorización de eventos y detección de incidentes de seguridad en las infraestructuras TI de la Junta de Andalucía y mantenerla operativa durante la vigencia del contrato y sus posibles prórrogas conforme a lo establecido en este pliego.

5.2.1.1. Componentes y arquitectura de la plataforma de monitorización

La plataforma de monitorización tendrá una arquitectura flexible que permita integrar tanto elementos ubicados en las instalaciones de la Junta de Andalucía (*on-premise*), tanto físicos como virtualizados, y servicios prestados en la nube (*cloud*) en cualquier modalidad SaaS, PaaS, IaaS.

Deberá, además, ofrecer la posibilidad de incrementar o disminuir su capacidad de proceso de forma simple.

Se compondrá de componentes instalados *on-premise* y de elementos ubicados en la nube, con la siguiente estructuración, en la que se indica en qué ubicación deberán residir (*on-premise* o en la nube):

- Componentes de captura de información y eventos (ubicados *on-premise*)
    - **Sensor recolector de tráfico de red** o **sensor de red**: elemento encargado de capturar y analizar el tráfico de red y detectar indicadores de actividad maliciosa en primera instancia. Incluye las funciones propias de un sistema de detección de intrusión de red (NIDS). No requiere capacidad de prevención.
    - **Agente**: elemento software opcional que, instalado en un sistema, recoge información sobre eventos en el mismo, los cuales son remitidos a otro elemento de la plataforma de monitorización, generalmente un recolector de logs, o, en un escalón superior, el propio servidor de gestión (SIEM).
    - **Recolector de logs**: elemento encargado de recoger información de los diferentes dispositivos de la red, sistemas y aplicaciones, así como de filtrar, consolidar y normalizar los eventos y flujos de red recogidos (capacidad de almacenamiento). Una vez hecho esto, podrá reenviar todos o algunos de los eventos o flujos al servidor de gestión (SIEM) o también tener la posibilidad de almacenarlos localmente para su consulta posterior. En función de la respuesta ofrecida en el criterio de adjudicación basado en fórmulas "*VAL-RECOL-1: Se valorará que los recolectores de logs puedan estar ubicados en la nube u on-premise según necesidades*" alguno/s de estos recolectores podrían estar en la nube.
- Componentes de consolidación de información y eventos (ubicados en la nube)
    - **Servidor de gestión (SIEM)**: elemento encargado de normalizar, priorizar y recolectar información procedente de los elementos de captura de información y eventos, así como de realizar evaluaciones del riesgo, enriquecimiento, contextualización y correlación de eventos. El servidor de gestión podrá recibir información y eventos de seguridad desde elementos situados en su mismo nivel o bien en capas inferiores. Además, soportará la ejecución de tareas de mantenimiento del sistema y de tareas externas, como las copias de respaldo.
    - **Repositorio de logs**: elemento en el que se realizará el almacenamiento de todos los eventos recogidos. Incluye mecanismos de indexado para agilizar las búsquedas de eventos. La capacidad de almacenamiento, rapidez de acceso y retención son sus características clave.
    - **Base de datos de gestión**: elemento en el cual se almacenarán los eventos representativos de seguridad recogidos, alarmas generadas, informes, inventario de activos e información útil

para la gestión del sistema. Deberá permitir realizar consultas de forma sencilla y proporcionar un tiempo de respuesta adecuado.

- **Consola de administración y operación centralizada**: herramienta centralizada para la operación, visualización y gestión de eventos, alarmas e informes. Constituye la interfaz entre el SIEM central y el personal que lo administra y utiliza.

Estos componentes deben entenderse como de carácter conceptual. No será obligatorio que, en las descripciones de la plataforma de monitorización ofertada, se asocie unívocamente un dispositivo físico o un módulo software a cada componente. Bastará indicar cuáles de ellos son implementados por cada uno de los servicios o productos utilizados.

5.2.1.2. Sensores de red

El suministro constará de elementos con los requisitos indicados en el siguiente subapartado "Requisitos". Un conjunto de estos elementos estará comprometido, y se suministrará al inicio del proyecto (fase II). Por otra parte, otro grupo de elementos será suministrado e integrado bajo demanda a lo largo de la ejecución del proyecto, no estando comprometidos. Se reflejan unos y otros en el apartado "Elementos y dimensionamiento" y en el "Catálogo de Elementos Unitarios".

5.2.1.2.1. Requisitos

Los sensores de red estarán ubicados en diversas ubicaciones (*on-premise*) para analizar los flujos de tráfico de red entrada y salida de acceso a redes externas (Internet y otras) antes y después del segmento o zona de red desmilitarizada (DMZ). Adicionalmente se analizará el tráfico de red de la red troncal y de otras sedes.

Estas sondas, de forma general, no estarán en el camino seguido por el tráfico real (*inline*), sino que recibirán una copia (*mirror*) del tráfico a analizar y actuarán, en principio, como IDS (detección) y no como IPS (prevención).

Los requisitos mínimos son:

Generales

- REQ-IDS-1: Se deberán suministrar los elementos necesarios para dar cobertura a los puntos de monitorización y las capacidades de análisis que se recogen en el apartado "Elementos y Dimensionamiento" desarrollado abajo.
- REQ-IDS-2: El hardware y software utilizado para los sensores de red deberá estar dimensionado conforme a las especificaciones de su fabricante para ofrecer las características demandadas y atender a los requisitos de volumen de tráfico mencionados en el apartado siguiente.

- REQ-IDS-3 Capacidades de:
    - Detección de amenazas de ciberseguridad en base al análisis del tráfico de red, hasta la capa 7 “aplicación” según el modelo OSI.
    - Generación de flujos de red con formato interpretable por el SIEM.
    - Captura del contenido de los paquetes de red que generan los eventos para análisis forense.

Inteligencia/reglas

- REQ-IDS-4: Se incluirán en el suministro fuentes de inteligencia, que proporcionen reglas, indicadores, etc., que se integrarán en los sensores y estarán actualizadas durante todo el período de vigencia del contrato, así como sus posibles prórrogas.
- REQ-IDS-5: Capacidad de modificación de reglas de detección existentes y creación de reglas nuevas a medida.
- VAL-IDS-1: Se valorará la compatibilidad con reglas de detección de tráfico de red de formato SNORT. (SOBRE 3, NO INCLUIR EN SOBRE 2).
- VAL-IDS-2: Se valorará la utilidad y calidad de las fuentes de inteligencia suscritas. (SOBRE 2).

Interconexión

- REQ-IDS-6: Capacidad de cifrado del envío de eventos desde el equipo sensor al recolector de logs o, si procede, directamente al SIEM.
- REQ-IDS-7: Por cada punto de captura de tráfico de red dimensionado en la solución, se deben proporcionar a la ADA dos (2) transceptores para la interconexión con la electrónica de red de captura del tráfico (10G o 1G, según aplique).

Soporte y mantenimiento

- REQ-IDS-8: Asociado al suministro, y durante la duración del contrato y sus posibles prórrogas, se prestará un soporte y mantenimiento para los elementos integrantes del suministro, incluyendo al menos:
    - Acceso a actualizaciones y parches del producto.
    - Acceso a actualizaciones de indicadores y otras características actualizables del producto.
    - Acceso a bases de datos de conocimientos del producto.
    - Atención a consultas e incidencias en la web del fabricante.
    - Mantenimiento correctivo sobre las plataformas ante incidencia o mal funcionamiento de estas.

- Atención de consultas en horario 8x5 sobre el producto/servicio vía telefónica y/o la herramienta de tickets (ticketing) que se acuerde entre las partes.

- REQ-IDS-9: La capacidad agregada de procesado de tráfico de red asciende a (10+10+10+10+10+10+5 Gbps) 65 Gbps.
- VAL-IDS-3: Dado que el sistema recibirá tráfico de múltiples puntos de monitorización (ver apartado siguiente), se valorará que se trate de sondas dedicadas a los puntos de monitorización, o que permita identificar el origen de las alarmas según los puntos de monitorización. (SOBRE 3, NO INCLUIR EN SOBRE 2).
- VAL-IDS-4: Se valorará la posibilidad de aplicar configuraciones (reglas de detección, indicadores, generación de flujos…) diferentes para puntos de monitorización diferentes. (SOBRE 3, NO INCLUIR EN SOBRE 2).

5.2.1.2.2. Elementos y Dimensionado

Puntos de monitorización comprometidos:

- ELEM-IDS-PPAL: Equipamiento para la monitorización del tráfico actual en los siguientes puntos:
    - Nodo de interconexión 1 - tráfico Externo: 10Gbps
    - Nodo de interconexión 2 - tráfico Externo: 10Gbps
    - Nodo de interconexión 1 - tráfico RCJA: 10Gbps
    - Nodo de interconexión 2 - tráfico RCJA: 10Gbps
    - Nodo de interconexión 1 - Interconexión sedes troncal: 10Gbps
    - Nodo de interconexión 2 - Interconexión sedes troncal: 10Gbps
    - Servicios Horizontales: 5 Gbps

Puntos de monitorización bajo demanda:

- ELEM-IDS-1 (no comprometidos, bajo demanda): Equipamiento para la monitorización sede pequeña (1Gbps)
- ELEM-IDS-5 (no comprometidos, bajo demanda): Equipamiento para la monitorización de sede mediana (5Gbps)
- ELEM-IDS-10 (no comprometidos, bajo demanda): Equipamiento para la monitorización de sede grande (10Gbps)

5.2.1.3. Recolectores de logs

Adicionalmente a los recolectores de logs que se consideren necesarios para dar soporte a las necesidades del SIEM, y que estarán incluidos en el despliegue del mismo, este elemento de suministro contempla las unidades que sean necesarias, bajo demanda, para dar soporte a fuentes de nueva creación o no contempladas anteriormente.

El suministro constará de elementos con los requisitos indicados en el subapartado "Requisitos". El dimensionado de los recolectores de logs queda a discreción del proveedor según la solución adoptada, sin perjuicio de que pudieran demandarse unidades para nuevos despliegues según lo indicado en el subapartado "Elementos y dimensionamiento".

5.2.1.3.1. Requisitos

- REQ-RECOL-1: Capacidad para filtrar, agregar, etiquetar y normalizar los eventos recogidos y reenvío al SIEM.
- REQ-RECOL-2: Capacidad para almacenar temporalmente (buffer) los eventos recogidos.
- VAL-RECOL-1: Se valorará que los recolectores de logs puedan estar ubicados en la nube u on-premise según necesidades. (SOBRE 3, NO INCLUIR EN SOBRE 2).
- VAL-RECOL-2: Se valorará que la solución de recolección de logs sea en alta disponibilidad y sin intervención manual. (SOBRE 3, NO INCLUIR EN SOBRE 2).

5.2.1.3.2. Elementos y dimensionamiento

ELEM-RECOL-LOG-ADICIONAL: Unidad de recolector de logs.

5.2.1.4. Componentes de consolidación y de gestión

En los siguientes apartados se empleará el término general "SIEM" (o "solución") para referirnos a estos componentes, aunque particularizaremos (consola, repositorio de logs, BD de gestión…) si es necesario.

El suministro constará de elementos, con los requisitos indicados en el apartado "Requisitos". De estos elementos, unos estarán comprometidos, y se suministrarán al inicio del proyecto (fase II) y otros se suministrarán bajo demanda, no estando comprometidos, y su suministro se podrá solicitar a lo largo de la ejecución del proyecto. Se reflejan unos y otros en el apartado "Elementos y dimensionamiento" y en el "Catálogo de Elementos Unitarios".

El suministro incluirá los recolectores de logs que se consideren necesarios para dar soporte a las necesidades del SIEM.

5.2.1.4.1. Requisitos

La solución proporcionada deberá poseer las siguientes características:

Generales

- REQ-SIEM-1: La solución de SIEM propuesta debe ser 100% en nube y no debe requerir la instalación de ningún elemento físico o virtual en las instalaciones de la Junta de Andalucía para ofrecer todas sus funcionalidades, salvo la instalación de los elementos del suministro descritos como on-premise. (Ver apartado “Componentes y arquitectura de la plataforma de monitorización”).
- REQ-SIEM-2: Los servicios de infraestructura en nube que presten el servicio deben estar alojados en datacenters de la Unión Europea y disponer de la certificación de ENS nivel ALTO.
- REQ-SIEM-3: La solución propuesta se debe prestar en modalidad 24x7x365.
- REQ-SIEM-4: Será necesario que la solución propuesta por el licitador, a nivel de producto, esté incluida, a fecha de formalización de contrato, y mantenga su inclusión durante toda la duración del contrato, en el Catálogo de Productos de Seguridad de las TIC (Catálogo CPSTIC) recogido en la Guía de Seguridad de las TIC CCN-STIC-105 “Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación”, con Categoría ENS “ALTA” para la familia SISTEMAS DE GESTIÓN DE EVENTOS DE SEGURIDAD (SIEM). Los licitadores deberán indicar el producto y versión ofertada.
- REQ-SIEM-5: La solución debe disponer de control de acceso con doble factor de autenticación, soportar SSO (SAML 2.0) para su integración con los sistemas de gestión de identidades de la Junta de Andalucía, múltiples usuarios y diferentes roles para permitir el acceso a diferentes ámbitos o funcionalidades.
- REQ-SIEM-6: Las tareas de gestión, mantenimiento y actualizaciones de la plataforma deben realizarse de forma transparente para el servicio, sin ninguna indisponibilidad del servicio o inactividad total o parcial.
- REQ-SIEM-7: La solución debe permitir escalar ante futuras demandas (EPS y almacenamiento).
- VAL-SIEM-1: Se valorará la provisión por el licitador de transporte de los eventos entre la Red Corporativa de Telecomunicaciones de la Junta de Andalucía y el SIEM, habilitando una línea dedicada entre ambos. (SOBRE 3, NO INCLUIR EN SOBRE 2).

Consola

- REQ-SIEM-8: Consola de administración, configuración y operación accesible remotamente mediante protocolos seguros (por ejemplo, https) soportado en sistemas Linux.
- REQ-SIEM-9: La plataforma debe ser accesible desde un navegador web.

- REQ-SIEM-10: Capacidad de restringir el acceso a la información según activos involucrados o sensores origen de los eventos basada en roles, usuarios o grupos de usuarios.
- REQ-SIEM-11: La solución propuesta debe poder ofrecer una configuración de tipo multi-organismo (multi-tenant) que a su vez permita ofrecer visibilidad completa y capacidades de actuación globales desde el "tenant" principal (tenant padre).
- REQ-SIEM-12: La plataforma debe proporcionar un registro de auditoría de la actividad de los usuarios, incluyendo tareas administrativas (creación de usuarios, asignación de roles, etc.) y de operación. Esta información de auditoría debe ser accesible desde la propia interfaz o a través de API.

Recepción de eventos

- REQ-SIEM-13: Capacidad base de ingesta diaria mínima licenciada de 3 TB, ampliable bajo demanda (y reducible) según los escalones indicados en "Elementos y dimensionamiento".
- REQ-SIEM-14: Capacidad para rechazar, agregar, etiquetar y normalizar los eventos recibidos.
- REQ-SIEM-15: Mecanismos disponibles para evitar la pérdida de eventos en caso de superación puntual del límite de la capacidad máxima soportada o licenciada.
- REQ-SIEM-16: Monitorización, control y ajuste de la capacidad usada.
- REQ-SIEM-17: Capacidad de integración con eventos/alarmas de seguridad de principales fabricantes y sus casos de uso conforme al apartado "Fuentes de eventos e inteligencia".

Inteligencia

- REQ-SIEM-18: Se incluirán en el suministro fuentes de inteligencia que proporcionen reglas de correlación, indicadores… que se integrarán en la plataforma y estarán actualizadas durante todo el período de vigencia del contrato, así como sus posibles prórrogas.
- REQ-SIEM-19: Disponibilidad de una librería de casos de uso alineados con el esquema MITRE ATT&CK.
- REQ-SIEM-20: Clasificación de los eventos y alarmas según el esquema MITRE ATT&CK.
- REQ-SIEM-21: Capacidad de integración con fuentes de inteligencia externas conforme al apartado "Fuentes de eventos e inteligencia".
- REQ-SIEM-22: Capacidad de integración con fuentes de inteligencia basadas en estándares STIX/TAXII.
- REQ-SIEM-23: Capacidad de ofrecer información de contexto (información histórica de DNS, geolocalización, reputación de dirección IP, etc.) durante el análisis del evento.

- VAL-SIEM-2: Se valorará la utilidad y calidad de las fuentes de inteligencia suscritas. (SOBRE 2).

Análisis

- REQ-SIEM-24: Capacidad de correlación empleando operaciones lógicas sobre los eventos detectados.
- REQ-SIEM-25: Capacidad de correlación relacionando los eventos detectados y la información contenida en la base de datos de conocimiento (por ejemplo, inventario de activos e información sobre los mismos).
- REQ-SIEM-26: Capacidad de correlación empleando técnicas de inteligencia artificial y aprendizaje máquina.
- REQ-SIEM-27: Capacidad de modificación y ajuste de las reglas de correlación existentes y creación de reglas de correlación nuevas a medida.
- REQ-SIEM-28: Capacidad de correlación de fuentes de flujos de red.
- REQ-SIEM-29: Capacidad de correlación basada en datos históricos.
- REQ-SIEM-30: Capacidad de correlación basada en vulnerabilidades.
- REQ-SIEM-31: Capacidad de detección por anomalías.
- REQ-SIEM-32: Capacidad de analizar el comportamiento de usuarios y entidades (UEBA, *User and Entity Behavior Analytics*).
- REQ-SIEM-33: Capacidad de reducción en la detección de falsos positivos mediante ajuste de los umbrales de detección.
- REQ-SIEM-34: Capacidad de crear casos de uso mediante pasos guiados (*playbook*).
- REQ-SIEM-35: Capacidad de priorización de eventos basada en distintos criterios (valoración del activo, el tipo o taxonomía del evento, la fiabilidad del evento, reputación de la dirección IP, etc.).
- REQ-SIEM-36: Capacidad de filtrado y aplicación de políticas en la detección de eventos según las necesidades del entorno (modificación de la prioridad, eliminación del panel de eventos, notificación de eventos, activación/desactivación de la opción de correlación, etc.) que se den en ciertos activos.
- VAL-SIEM-3: Se valorará la capacidad de visualización del contenido de los paquetes de red de los eventos de red para análisis forense. (SOBRE 2).
- VAL-SIEM-4 Se valorará la cantidad, calidad, utilidad y adecuación al tipo de organización de los casos de uso base ofertados por el licitador. (SOBRE 2).

Alertas y reporte

- REQ-SIEM-37: La plataforma debe facilitar la comunicación de alertas de detección en tiempo real y proporcionar informes y cuadros de mando en tiempo real.
- REQ-SIEM-38: Notificación automática de alarmas de seguridad por diversos medios. Al menos, se deberá ofrecer: alarma en la consola de operación, correo electrónico y *syslog*.
- REQ-SIEM-39: Capacidad de definición de políticas de notificación diferentes según distintos criterios: grupo de activos, propietario de activos, sensores de detección, taxonomías, etc.
- VAL-SIEM-5: Se valorará la inclusión de capacidades de automatización y orquestación de respuestas a incidentes (SOAR, Security Orchestration, Automation, and Response), preferentemente en la misma consola o interfaz, siendo valorables aquellas soluciones que propongan una simplificación en una única interfaz o consola, entendiéndose ésta el portal web único en el que se recojan todas las capacidades (SOBRE 2).

Repositorio de logs

- REQ-SIEM-40: Búsqueda rápida y flexible.
- REQ-SIEM-41: Retención de logs en caliente (accesibles para búsquedas sin degradación del tiempo de acceso a los logs más antiguos y sin necesidad de operaciones adicionales para su recuperación, ni manuales ni automáticas): mínimo 180 días.
- REQ-SIEM-42: Capacidad de búsquedas avanzadas que faciliten la caza de amenazas (*threat hunting*).
- REQ-SIEM-43: Capacidad de firma y sellado de tiempo de los logs y eventos almacenados en formato original.
- VAL-SIEM-6: Se valorará la ampliación del tiempo de retención de los logs en caliente (misma definición que en REQ-SIEM-41). (SOBRE 3, NO INCLUIR EN SOBRE 2).

Gestión

- REQ-SIEM-44: Capacidad de gestión centralizada de los elementos que componen la solución: agentes, sensores, fuentes de datos de monitorización, motores de correlación, interfaces de gestión o consulta, etc.
- REQ-SIEM-45: Generación de informes personalizados según distintos criterios (sensor, grupo de activos, propietario de activos, taxonomía, rangos temporales, activos, geolocalización, etc.).
- REQ-SIEM-46: Capacidad de paneles informativos personalizados y configurables con datos estadísticos de los eventos y demás información sobre amenazas recogidas por la plataforma.

- REQ-SIEM-47: Capacidad de generación de mapas de riesgo en tiempo real.
- REQ-SIEM-48: Capacidad de exportar datos en diferentes formatos de salida, al menos CSV.
- REQ-SIEM-49: Capacidad de configuración y gestión de realización de copias de seguridad de la información albergada en la solución.

Integración

- VAL-SIEM-7: Se valorará que la solución proporcione una API rica y robusta para integración con herramientas de terceros. (SOBRE 2).
- VAL-SIEM-8: Se valorarán las integraciones y casos de uso con las herramientas del CCN-CERT (REYES, LUCIA). (SOBRE 2).

Soporte y mantenimiento

- REQ-SIEM-50: Asociado al suministro, y durante la duración del contrato y sus posibles prórrogas, se prestará un soporte y mantenimiento para los elementos integrantes del suministro, incluyendo al menos:
    - Acceso a actualizaciones y parches del producto.
    - Acceso a actualizaciones de indicadores y otras características actualizables del producto.
    - Acceso a bases de datos de conocimientos del producto.
    - Atención a consultas e incidencias en la web del fabricante.
    - Mantenimiento preventivo y correctivo sobre las plataformas ante posibles incidencias o mal funcionamiento.
    - Atención de consultas en horario 8x5 sobre el producto/servicio vía telefónica y/o la herramienta de tickets (ticketing) que se acuerde por las partes.
    - Atención en horario 24x7 de incidencias que se reporten en relación a la plataforma y/o el servicio que ésta presta.

El adjudicatario deberá garantizar, por sí mismo o a través de los correspondientes fabricantes y proveedores, que, durante todo el periodo de vigencia del contrato y sus posibles prórrogas:

- REQ-SIEM-51: Se lleva a cabo una actualización continuada conforme a los cambios de los formatos de eventos, de forma que se asegure la integración de la plataforma con las diferentes evoluciones del software.
- REQ-SIEM-52: Se lleva a cabo una actualización continuada conforme a los cambios de las bases de datos de firmas de los sistemas de seguridad, de forma que se asegure la integración de la

plataforma con las diferentes evoluciones del software de los dispositivos y sistemas externos (identificadores/firmas de virus, vulnerabilidades, prevención de ataques...).

- REQ-SIEM-53: Para la prestación de este soporte, será requisito que el fabricante de la solución ofertada acredite al adjudicatario como partner oficial o, en su defecto, se disponga de carta emitida por el fabricante en la que se comprometa a ofrecer al licitador soporte oficial de la solución ofertada. Esta certificación debe estar vigente durante toda la ejecución del contrato. En el caso de uso de componentes de software libre, este requisito se aplicará sobre los mismos si el desarrollador del componente proporciona soporte oficial.
- VAL-SIEM-9: Se valorará la disponibilidad de un gestor técnico de cuentas (TAM – Technical Account Manager) que ayude con los casos en curso y la transferencia de conocimiento. (SOBRE 3, NO INCLUIR EN SOBRE 2).

5.2.1.4.2. Fuentes de eventos e inteligencia

El SIEM propuesto debe integrarse, para la recepción de eventos y alarmas, con los sensores de red propuestos por la solución. El SIEM debe estar adaptado a estos sensores de red para obtener el mayor de los beneficios en la correlación y contextualización de los eventos.

Además, deberá integrarse con los servicios de infraestructura de los principales fabricantes empleados por la Junta de Andalucía y otras entidades y organismos adscritos a AndalucíaCERT. El listado detallado de las fuentes de eventos a integrar se indica en el Anexo I.

En caso de que los productos utilizados no soportaran de forma nativa alguna de las fuentes mencionadas en la anterior lista, el adjudicatario deberá proporcionar un mecanismo alternativo de integración de las mismas. Este mecanismo deberá proporcionar un adecuado nivel de eficacia y eficiencia y no necesitar de recursos adicionales ni mantenimiento por parte de AndalucíaCERT.

El sistema deberá soportar como mínimo los siguientes protocolos de intercambio de fuentes de eventos y de inteligencia:

- Protocolo SNMP: SYSLOG.
- Fuentes de eventos en formatos XML, TXT, CSV, CEF o JSON.
- Fuentes de inteligencia en estándares STIX/TAXII.
- Flujos de red en formato NetFlow o IPFIX.

5.2.1.4.3. Elementos y dimensionamiento

ELEM-SIEM-BASE (comprometido): Tres meses de licencia ingesta 3 TB/día.

ELEM-SIEM-AMPL1 (bajo demanda): Tres meses de AMPLIACIÓN de ELEM-SIEM-BASE en 0,5 TB/día. No sustituye a ELEM-SIEM-BASE, sino que lo complementa para ampliarlo.

ELEM-SIEM-AMPL2 (bajo demanda): Tres meses de AMPLIACIÓN de ELEM-SIEM-AMPL1 en 0,5 TB/día. No sustituye a ELEM-SIEM-BASE, sino que lo complementa para ampliarlo.

ELEM-SIEM-AMPL3 (bajo demanda): Tres meses de AMPLIACIÓN de ELEM-SIEM- AMPL2 en 0,5 TB/día. No sustituye a ELEM-SIEM-BASE, sino que lo complementa para ampliarlo.

ELEM-SIEM-AMPL4 (bajo demanda): Tres meses de AMPLIACIÓN de ELEM-SIEM- AMPL3 en 0,5 TB/día. No sustituye a ELEM-SIEM-BASE, sino que lo complementa para ampliarlo. Una vez alcanzado los 5TB /día (con las 4 ampliaciones), las siguientes ampliaciones de 0,5 TB/día se facturará al mismo precio de ELEM-SIEM-AMPL4.

5.2.1.5. Sondas SAT

5.2.1.5.1. Requisitos

El adjudicatario deberá suministrar dos (2) servidores con los que se reemplazarán las sondas del Sistema de Alerta Temprana (SAT) del CCN-CERT desplegadas actualmente en las instalaciones de la Junta de Andalucía, con objeto de evitar su obsolescencia y así prestar un servicio de mantenimiento y soporte de los mismos que garantice su correcto funcionamiento durante la duración del contrato y sus posibles prórrogas. Se podrán requerir, bajo demanda, hasta dos (2) servidores adicionales.

Estas sondas del CCN-CERT se despliegan sobre servidores dedicados de alto rendimiento que incorporan varias herramientas de detección y monitorización. El suministro de los servidores, el despliegue de las sondas (con imágenes proporcionadas por CCN-CERT) y su configuración forman parte de este elemento del suministro.

Se suministrarán también elementos de conexión de red para la captura de tráfico. Para facilitar la conexión de estos equipos con la electrónica de red de captura del tráfico, se suministrarán los transceptores necesarios.

Los requisitos mínimos de los servidores para el SAT son los siguientes:

Generales

REQ-SAT-1: Las características técnicas mínimas de los servidores a suministrar son las siguientes (siempre deberán ser conforme con las especificaciones que establece el CCN):

Procesadores	2 procesadores multinúcleo. 20 cores por procesador Intel o 28 cores por procesador AMD.
RAM	32 GB.

Discos duros	2 discos duros 146GB SAS, con redundancia en RAID-1.
Interfaces de red para el análisis	2 puertos de red de velocidad mínima de 10 Gigabit/segundo, Ethernet SFP de tecnología Intel (driver e1000e o igb).
Interfaces de red para la gestión	2 puertos de red de velocidad mínima de 1 Gigabit/segundo, Ethernet con distinto driver que las interfaces de red de análisis. Debe incluirse cableado para una toma de red (3 metros).
Interfaces para la gestión fuera de banda (IPMI o similar)	1 puerto de red de velocidad mínima de 1 Gigabit/segundo, Ethernet, con funcionalidad de acceso a consola KVM remota. Debe incluirse cableado para una toma de red (3 metros). Puede ser una interfaz compartida con la red de gestión. En caso de requerirse licenciamiento para la funcionalidad de acceso a consola KVM remota, correrá por cuenta de la persona adjudicataria.
Medios extraíbles	Soporte para CD, DVD y medios USB físicos o virtuales. El lector de CD – DVD será requerido únicamente durante la instalación, no siendo un requisito del suministro.
Fuentes de alimentación	2 fuentes de alimentación y cableado PDU.
Compatibilidad	Todo el hardware de la sonda debe ser compatible con CentOS en sus versiones 7.3 superiores.

Instalación

REQ-SAT-2: Se incluirá la entrega en las sedes establecidas por AndalucíaCERT, la instalación física, la instalación de software, la configuración y la puesta en marcha de la plataforma de monitorización y las sondas SAT, así como las operaciones necesarias para la transición desde la plataforma preexistente, conforme a lo establecido en el apartado “Fase IV: Transición e integración de sistemas preexistentes”. La persona responsable del servicio proporcionará al adjudicatario el instalador software y las instrucciones necesarias para realizar el despliegue del software SAT y su integración con el nodo central.

Soporte y mantenimiento

REQ-SAT-3: Tras la recepción del suministro e instalación y configuración del mismo, y durante la duración del contrato, incluida su prórroga, se prestarán servicios de soporte y mantenimiento para los elementos integrantes del suministro. Se prestarán en modalidad de siguiente día laborable (NBD, Next Business Day) en horario 8x5, por la empresa adjudicataria, apoyándose en los servicios especializados en la tecnología del fabricante, con asistencia in-situ en caso necesario. El soporte y mantenimiento incluirán:

- Reposición e instalación de piezas averiadas o sustitución de equipos, en modalidad de soporte 8x5 de siguiente día laborable, por otros de iguales o superiores características, sin coste.

- Acceso a las bases de datos de conocimiento de los productos adquiridos.
- Acceso a los parches y alertas de seguridad.
- Acceso ilimitado a nuevos lanzamientos y versiones del software y firmware.
- Acceso, en modalidad de 24x7, al centro de soporte del fabricante para realizar consultas técnicas, abrir incidencias, acceder a bases de datos de conocimiento, parches, nuevos lanzamientos y versiones de software y firmware. El acceso podrá ser bien telefónico o bien vía Web.
- El servicio deberá ser proporcionado por el integrador o el fabricante, debiendo garantizar:
    - Que la Junta de Andalucía pueda acceder a las incidencias abiertas con el fabricante del equipamiento, y seguir dichas consultas en directo. Para ello, dispondrá de una cuenta en la cual se dará de alta el equipamiento suministrado.
    - Que el fabricante o el integrador serán los responsables de tramitar las incidencias detectadas proactivamente o notificadas por la Junta de Andalucía, y la sustitución efectiva de piezas de las piezas averiadas sin coste adicional para la Junta de Andalucía, y todas las acciones necesarias para la correcta resolución de las averías.

5.2.1.5.2. Elementos y Dimensionado

ELEM-SAT-SONDA: Equipo para el despliegue de sondas SAT-INET del CCN-CERT, con las características mínimas indicadas.

5.3. Servicios asociados

A continuación, se desglosan los servicios asociados a la plataforma de monitorización para dar soporte al Centro de Operaciones de Seguridad de la Junta de Andalucía (AndalucíaCERT).

El adjudicatario asignará a estos servicios personal cuyos perfiles profesionales deberán cumplir como mínimo los requisitos descritos en los apartados "Jefatura de Proyecto", y "Requisitos de cualificación para el personal del equipo del proyecto" según corresponda en cada servicio.

Ante necesidades puntuales o permanentes, se podrá solicitar por el responsable del servicio, previo acuerdo con el jefe de proyecto, un incremento de la dotación/dedicación de perfiles a estos servicios.

5.3.1. Despliegue inicial de la plataforma de monitorización

5.3.1.1. Descripción del servicio

Este servicio abarca la instalación física, la instalación de hardware (incluyendo las sondas SAT, etc.) y software, la configuración y la puesta en marcha de la plataforma de monitorización en las sedes establecidas por la Dirección del proyecto como las operaciones necesarias para la transición desde la plataforma preexistente, conforme a lo establecido en el apartado "Plan de ejecución del proyecto principal".

5.3.1.2. Condiciones de prestación

Este servicio se prestará, como mínimo, en modalidad 8x5 con dedicación completa.

5.3.1.3. Elementos y Dimensionado

ELEM-DESPLIEGUE: Trabajos para el despliegue inicial.

5.3.2. Servicio de mantenimiento de la plataforma

5.3.2.1. Descripción del servicio

El servicio permitirá ejecutar las características requeridas de soporte y mantenimiento de todos los elementos de suministro, y formarán parte de él los siguientes tipos de tareas y operaciones:

- Soporte hardware y software, incluyendo la gestión (reposición e instalación) de piezas averiadas o sustitución de equipos.
- Monitorización de la disponibilidad y el correcto funcionamiento de la plataforma.
- Atención a las incidencias de indisponibilidad de la plataforma.

- Administración de la plataforma de monitorización:
    - Gestión de incidencias.
    - Gestión de cambios.
    - Gestión de parches y actualizaciones
    - Gestión de control de acceso, usuarios y permisos.
    - Gestión de *tenants* o particiones.

5.3.2.2. Condiciones de prestación

El servicio será prestado durante todo el periodo del contrato y sus posibles prórrogas de forma deslocalizada en horario 24x7, salvo necesidades que requieran la prestación localizada, según la naturaleza de los elementos implicados.

5.3.2.3. Elementos y Dimensionado

ELEM-TRIMES-SYM: Trimestre de prestación del servicio.

5.3.3. Monitorización

5.3.3.1. Descripción

Este servicio comprende la monitorización de incidentes de seguridad basados en alarmas y alertas generadas por la plataforma de monitorización, así como labores propias de la operación de la plataforma, incluyendo:

- Uso de la plataforma de monitorización para detección de incidentes de seguridad.
- Monitorización de otras consolas en la Junta de Andalucía.
- Atención a las detecciones y alarmas en sistemas auxiliares.
- Notificación de los incidentes de seguridad en la plataforma LUCÍA de AndalucíaCERT, para su gestión por el servicio de respuesta a incidentes.
- Identificación y reporte de posibles falsos positivos al servicio avanzado.
- Identificación y reporte al servicio avanzado de posibles errores o desajustes en las reglas de detección, casos de uso y otros procedimientos o configuraciones.

- En caso de producirse incidencias con la plataforma de monitorización, interlocución con el servicio de soporte y mantenimiento de la plataforma de monitorización, así como con los fabricantes de los productos y los proveedores de servicios utilizados por esta.
- Atención de consultas técnicas.

VAL-SVSUM-1: Se valorará la idoneidad y calidad de la propuesta de monitorización en relación con el modelo de prestación del servicio (metodología, organización, coordinación y escalado). (SOBRE 2)

5.3.3.2. Condiciones de prestación

Este servicio se prestará en modalidad 24x7, con dedicación completa, mediante una combinación de prestación localizada y deslocalizada. La prestación localizada se realizará en modalidad 12x5 y el resto se realizará de forma deslocalizada.

El adjudicatario garantizará la asignación inicial a este servicio, conforme a la modalidad de prestación establecida, de, como mínimo, el siguiente número de personas:

- 2 personas en turno de mañana correspondientes a la prestación localizada en modalidad 12x5, y en horario de 7 a 15h.
- 2 personas en horario de tarde correspondiente a la prestación localizada en modalidad 12x5, y en horario de 11 a 19h.
- El equivalente a 2 personas, en prestación deslocalizada, en calendario y horario complementario al de la prestación localizada para completar el servicio 24x7.

Los requisitos mínimos que debe cumplir el perfil profesional asignado a este servicio serán los establecidos para el puesto “TN1 – Especialista Técnico” conforme se indica en el apartado "Requisitos de cualificación para el personal del equipo del proyecto".

La prestación deslocalizada se realizará en calendario y horario complementario al de la prestación localizada. Este modo de prestación no requerirá de la adscripción exclusiva de personas concretas a lo largo del contrato, sino que podrá realizarse mediante un SOC remoto.

5.3.3.3. Elementos y Dimensionado

ELEM-HORA-OPERACIÓN-LOC (TN1 MON): Hora de servicio del personal localizado en horario 12x5.

ELEM-HORA-OPERACIÓN-DESLOC (TN1 MON): Hora de servicio del personal deslocalizado en horario 24x7 (desbordamiento en horario complementario).

5.3.4. Servicio avanzado de la plataforma de monitorización

5.3.4.1. Descripción del servicio

Este servicio garantizará una configuración optimizada de la plataforma de monitorización mediante la aplicación de conocimiento experto relativo a ésta y a la detección y respuesta de incidentes de seguridad.

Las tareas principales asociadas a este servicio son:

- Ajuste fino continuo en la detección de incidentes de seguridad de la plataforma y corrección de posibles falsos positivos.
- Gestión de los IOC/IOA del fabricante y de terceros.
- Integración de nuevas fuentes de eventos.
- Monitorización de incidentes de seguridad cuando, por las características del incidente o de los indicadores esto requiera personal altamente especializado.
- Búsqueda proactiva de caza de amenazas (*threat hunting*).
- Definición y documentación, alineadas con los procedimientos de AndalucíaCERT, y transferencia de conocimiento sobre casos de uso en esta área, incluyendo runbooks/playbooks para la detección y respuesta.
- Identificación y diseño de automatizaciones y optimizaciones.
- Diseño de cuadros de mandos y reporte periódico de situación.
- Informe singular de actividad y hallazgos. Se solicitará a petición del Responsable de Servicio para una alerta específica y concreta, y contendrá detalle de las investigaciones realizadas, metodología empleada, inteligencia añadida o implementada sobre la herramienta.
- Identificación y propuesta de mejoras del servicio y de la funcionalidad de la plataforma.
- Asesoramiento en los procesos de nuevos despliegues de la plataforma de monitorización.

VAL-SVSUM-2: Se valorará la idoneidad y calidad de la propuesta para el servicio avanzado en la optimización de la plataforma de monitorización en relación con el modelo de prestación de soporte (metodología, organización, relación de runbooks/playbooks, así como los recursos y fuentes de inteligencia consultadas y utilizadas para la realización de búsquedas proactiva de amenazas). (SOBRE 2)

5.3.4.2. Condiciones de prestación

Este servicio será prestado de dos formas:

- Localizada, en modalidad 8x5.
- Guardia telefónica, con disponibilidad en modalidad 24x7 y atención en caso de solicitud.

El adjudicatario garantizará la asignación inicial a este servicio, conforme a la modalidad de prestación establecida, de, como mínimo, el siguiente número de personas:

- 2 personas en turno de mañana correspondiente a la prestación localizada en modalidad 8x5, y en horario de 7 a 15h.
- 1 persona de guardia, en prestación deslocalizada, en calendario y horario complementario al de la prestación localizada para completar el servicio 24x7.

Los requisitos mínimos que debe cumplir el perfil profesional asignado a este servicio serán los establecidos para el puesto “TN2 – Especialista en ciberseguridad” conforme se indica en el apartado "Requisitos de cualificación para el personal del equipo del proyecto".

La guardia telefónica garantizará la disponibilidad de una persona para responder a incidentes críticos. Esta persona se desplazará a las instalaciones de AndalucíaCERT o de los organismos y entidades que forman parte de su Grupo Atendido cuando sea preciso. También podrá realizar las actuaciones necesarias de forma remota mediante un acceso seguro cuando las circunstancias lo permitan.

5.3.4.3. Elementos y Dimensionado

ELEM-HORA-SOPEXP-LOC (TN2 MON): Hora de servicio del personal localizado en horario 8x5.

ELEM-HORA-SOPEXP-GUARDIA (TN2 MON): Hora de servicio del personal de guardia en horario 24x7. (Guardia desbordamiento en horario complementario).

5.3.5. Respuesta a incidentes

Este servicio comprende las labores de respuesta a los incidentes de seguridad, incluyendo su resolución y cierre.

Dentro de este servicio se establecen los siguientes subservicios:

- Gestión de Incidentes de seguridad de Nivel 1 (TN1).
- Gestión de Incidentes de seguridad de Nivel 2 (TN2).
- Respuesta rápida in-situ a incidentes.

VAL-SVSUM-3: Se valorará la idoneidad y calidad de la propuesta de respuesta a incidentes en relación con el modelo de prestación de soporte (metodología, organización, herramientas, recursos y fuentes de inteligencia, documentación y capacidades de contextualización del incidente y equipo de coordinación de respuesta a incidentes), la propuesta de informes de respuesta (informe preliminar, informe técnico, informe ejecutivo) y transferencia de conocimiento. (SOBRE 2)

5.3.5.1. Subservicio de gestión de incidentes de seguridad de Nivel 1 (TN1)

5.3.5.1.1. Descripción

Este subservicio comprende las actividades destinadas a la recepción de notificaciones y el tratamiento de los incidentes de seguridad gestionados por AndalucíaCERT, incluyendo su resolución y cierre cuando estos sean susceptibles de ser atendidos por este primer nivel de atención.

Las actividades a desarrollar incluirán:

- Atención a los canales de recepción de solicitudes de servicio y notificaciones, entre los que se contarán:
  - Buzón de correo electrónico
  - Línea telefónica.
  - Sistema de gestión de tiques LUCIA (herramienta del CCN-CERT).
  - Cualquier otra vía de entrada que sea habilitada o solicitada por la persona responsable de la jefatura del proyecto.
- Atención de los incidentes de seguridad recibidos o detectados, incluyendo:
  - Análisis del incidente.
  - Tratamiento del incidente.
  - Seguimiento del incidente.
  - Resolución del incidente.
  - Interlocución con terceros: grupo atendido y otros equipos de respuesta.
- Atención de las consultas, peticiones e incidencias que lleguen a AndalucíaCERT.
- Escalado de incidentes de seguridad al nivel 2 cuando su complejidad o criticidad lo haga necesario.
- Tareas de apoyo a la gestión interna y a los sistemas de calidad.
- Generación de informes de servicio.
- Identificación y propuesta de mejoras del servicio y de la funcionalidad de la plataforma.

5.3.5.1.2. Condiciones de prestación

Este subservicio se prestará en modalidad 24x7, con dedicación completa, mediante una combinación de prestación localizada y deslocalizada. La prestación localizada se realizará en modalidad 12x5 y el resto se realizará de forma deslocalizada.

El adjudicatario garantizará la asignación inicial a este subservicio, conforme a la modalidad de prestación establecida, de, como mínimo, el siguiente número de personas:

- 2 personas en turno de mañana correspondientes a la prestación localizada en modalidad 12x5, y en horario de 7 a 15h.
- 2 personas en horario de tarde correspondiente a la prestación localizada en modalidad 12x5, y en horario de 11 a 19h.
- El equivalente a 2 personas, en prestación deslocalizada, en calendario y horario complementario al anterior hasta completar el servicio 24x7.

Los requisitos mínimos que debe cumplir el perfil profesional asignado a este servicio serán los establecidos para el puesto “TN1 – Especialista Técnico” conforme se indica en el apartado "Requisitos de cualificación para el personal del equipo del proyecto".

La prestación deslocalizada se realizará en calendario y horario complementario al de la prestación localizada. Este modo de prestación no requerirá de la adscripción exclusiva de personas concretas a la largo del contrato, sino que podrá realizarse mediante un SOC remoto.

5.3.5.1.3. Elementos y Dimensionado

ELEM-HORA-RESPUESTA-LOC (TN1 RES): Hora de servicio del personal localizado en horario 12x5.

ELEM-HORA-RESPUESTA-DESLOC (TN1 RES): Hora de servicio del personal deslocalizado en horario 24x7 (desbordamiento en horario complementario).

5.3.5.2. Subservicio de gestión de incidentes de seguridad de Nivel 2 (TN2)

5.3.5.2.1. Descripción

Este subservicio incluirá las mismas tareas que el Servicio de gestión de incidentes de seguridad de Nivel 1 (TN1) con respecto a aquellos incidentes que, por carga de trabajo o por razones de complejidad o requisitos de especialización o de otra índole, no puedan ser resueltos en el primer nivel de atención, así como la detección de amenazas avanzadas y la búsqueda proactiva de incidentes de seguridad.

La activación de este subservicio se podrá realizar de cualquiera de las siguientes formas:

- Por escalado de incidentes de seguridad desde el primer nivel de gestión (TN1)
- Por asignación directa desde el servicio de operación de la plataforma de monitorización de tipos de incidentes que deban ser asignados directamente al nivel 2 de gestión de incidentes (TN2).

También realizará tareas de soporte y mejora continua de los procedimientos.

5.3.5.2.2. Condiciones de prestación

Este subservicio se prestará en dos formas:

- Localizado, en modalidad 12x5.

- Guardia telefónica, con disponibilidad en modalidad 24x7 y atención en caso de solicitud.

El adjudicatario garantizará la asignación inicial a este subservicio, conforme a la modalidad de prestación establecida, de, como mínimo, el siguiente número de personas:

- 2 personas en turno de mañana correspondiente a la prestación localizada en modalidad 12x5, y en horario de 7 a 15h.
- 1 persona en horario de tarde correspondiente a la prestación localizada en modalidad 12x5, y en horario de 11 a 19h.
- 1 persona de guardia, en prestación deslocalizada, en calendario y horario complementario al de la prestación localizada para completar el servicio 24x7.

Los requisitos mínimos que debe cumplir el perfil profesional asignado a este servicio serán los establecidos para el puesto “TN2 – Especialista en ciberseguridad” conforme se indica en el apartado "Requisitos de cualificación para el personal del equipo del proyecto".

La guardia telefónica garantizará la disponibilidad de una persona para responder a incidentes críticos. Esta persona se desplazará a las instalaciones de AndalucíaCERT o de los organismos y entidades que forman parte de su Grupo Atendido cuando sea preciso. También podrá realizar las actuaciones necesarias de forma remota mediante un acceso seguro cuando las circunstancias lo permitan.

5.3.5.2.3. Elementos y Dimensionado

ELEM-HORA-RESPUESTA-LOC (TN2 RES): Hora de servicio del personal localizado en horario 8x5.

ELEM-HORA-RESPUESTA-GUARDIA (TN2 RES): Hora de servicio del personal localizado en horario 24x7 (Guardia desbordamiento en horario complementario).

5.3.5.3. Subservicio de respuesta rápida in-situ para soporte a la recuperación

5.3.5.3.1. Descripción

Este servicio consistirá en la prestación de apoyo técnico y organizativo en las instalaciones y sedes de AndalucíaCERT y de los organismos que forman parte de su grupo atendido para atender incidentes de seguridad de especial gravedad o complejidad. Los trabajos a realizar podrán incluir el asesoramiento, la asistencia tanto en materia de ciberseguridad como legal, la coordinación en la gestión del incidente, el despliegue de medidas de contingencia, etc.

Cada solicitud de este subservicio se gestionará como un proyecto, de acuerdo con lo indicado en el apartado “Entregables asociados a cada proyecto de respuesta rápida in-situ para la recuperación” con las salvedades indicadas en este epígrafe.

La activación de este servicio se iniciará por una de las dos siguientes circunstancias:

- Que el segundo nivel de gestión de incidentes (TN2) determine que es necesaria la participación de un equipo de respuesta rápida in-situ.
- Que la persona responsable del servicio lo solicite en relación con un incidente de seguridad.

En ambos casos, el adjudicatario remitirá a la persona responsable del servicio una propuesta de Plan de Trabajo conforme a lo establecido en el apartado “Entregables asociados a cada proyecto de respuesta rápida in-situ para la recuperación”.

La persona responsable del servicio podrá:

- Requerir del adjudicatario las correcciones y modificaciones que estime oportuno realizar sobre el plan de trabajo propuesto.
- Rechazar las actuaciones de respuesta rápida in-situ para la recuperación propuestas por el adjudicatario.
- Cancelar las peticiones realizadas por la persona responsable del servicio.
- Aprobar las actuaciones incluidas en el plan de trabajo propuesto.

Si en el plazo de 24 horas no se produjera ninguna de las actuaciones anteriores, se tendrá por aprobado el plan de trabajo presentado.

La persona responsable del servicio podrá requerir el cese de las actividades de respuesta rápida in-situ en cualquier momento durante la realización de las mismas, debiendo ser atendido este requerimiento de forma inmediata y no procediendo facturación alguna por las actuaciones que pudieran producirse a partir de ese momento.

El servicio se prestará mediante dos perfiles profesionales:

- Personal de respuesta in situ. Realizará funciones de apoyo a la resolución in-situ del incidente.
- Personal de respuesta in situ especialista en tecnología. Realizará funciones de consultoría y asesoramiento experto en áreas concretas de la tecnología y la ciberseguridad.

5.3.5.3.2. Condiciones de prestación

El servicio se ofrecerá de forma localizada en las sedes indicadas en la solicitud y el plan de trabajo aprobado.

El servicio podrá ser solicitado y deberá ser atendido en horario 24x7.

El personal que preste este servicio no podrá ser el mismo personal que esté asignado a los servicios con prestación localizada de este lote (Monitorización, Servicio avanzado de la plataforma, Gestión de incidentes nivel 1 y Gestión de incidentes nivel 2).

La persona responsable del servicio podrá requerir el desplazamiento a las ubicaciones que sea preciso de personal del adjudicatario cuando sea necesario para realizar tareas urgentes o necesarias para la elaboración del Plan Técnico de Despliegue o la adecuada prestación del servicio.

5.3.5.3.3. Elementos y Dimensionado

ELEM-JORNADA-INSITU-1: Hora de personal de respuesta in-situ.

ELEM-JORNADA-INSITU-2: Hora de personal de respuesta in-situ especialista en tecnología.

5.3.6. Nuevos despliegues

5.3.6.1. Descripción del servicio

En previsión de que posibles cambios futuros del ámbito de actuación de AndalucíaCERT, este servicio incluye los trabajos de apoyo a la ampliación de la plataforma de monitorización y los necesarios para la integración de las fuentes de información y recogida de eventos de nuevos organismos o nuevas entidades.

También se incluye en este servicio el redespliegue de equipamiento y despliegue de equipamiento nuevo como consecuencia de solicitud de nuevos suministros o de cambios sustanciales en las infraestructuras tecnológicas de la Junta de Andalucía como, por ejemplo, los cambios en los nodos de interconexión de la Red Corporativa de Comunicaciones de la Junta de Andalucía que podrían producirse como consecuencia de la evolución de esta.

Incluye el despliegue de nuevas sondas SAT, en caso de ser necesario.

Para cada uno de estos casos, y a petición de la dirección del proyecto, se deberá desarrollar un proyecto de implantación acompañado de estimación de esfuerzos (horas de trabajo), que podrá requerir, entre otras tareas:

- Elaboración del diseño del Plan Técnico de Despliegue, conforme a lo establecido en el apartado “Entregables asociados a cada proyecto de despliegue”.
- Recepción, en su caso, del equipamiento necesario para el despliegue de la solución propuesta.
- Despliegue de la solución propuesta.
- Pasado un periodo que permita la recolección de información y el análisis del funcionamiento de la solución propuesta, corrección de los errores detectados y optimización del sistema.

En el diseño y desarrollo de estas actividades se tomará como referencia lo establecido en el apartado “Plan de Ejecución del Proyecto Principal”.

Para ello, se contará con dos perfiles profesionales:

- Personal experto en ciberseguridad (TN2), que definirá los procedimientos a seguir y configuraciones a realizar y establecerá las actuaciones necesarias para el despliegue de los sistemas y equipos contemplados en este servicio y, si es necesario, prestará soporte al personal técnico de implantación de la solución.
- Personal técnico de implantación de la solución (TN1), que, siguiendo las instrucciones y las guías elaboradas por el personal experto en ciberseguridad, llevará a cabo las actuaciones necesarias para realizar el despliegue.

Los requisitos mínimos que deben cumplir los perfiles profesionales asignados a este servicio serán los establecidos para los puestos “TN1 – Especialista Técnico” y “TN2 – Especialista en ciberseguridad” conforme se indica en el apartado "Requisitos de cualificación para el personal del equipo del proyecto".

VAL-SVSUM-4: *Se valorará la idoneidad y calidad de la propuesta de procedimientos para el servicio de nuevos despliegues en relación con el modelo de prestación (metodología, organización y coordinación).* (SOBRE 2).

5.3.6.2. Condiciones de prestación

Este servicio se realizará a petición de la dirección del proyecto, que previamente al inicio aprobará el presupuesto de horas de trabajo contenido en el proyecto de implantación indicado más arriba.

Las tareas derivadas del proyecto de implantación se realizarán, como mínimo, en modalidad 8x5 con dedicación completa.

5.3.6.3. Elementos y Dimensionado

ELEM-HORA-NUEVOS-DESPL-TN1: Hora de nuevos despliegues TN1.

ELEM-HORA-NUEVOS-DESPL-TN2: Hora de nuevos despliegues TN2.

5.3.7. Formación y capacitación

5.3.7.1. Descripción del servicio

El suministro de la plataforma de monitorización y sus componentes se acompañarán de la correspondiente capacitación en el uso de la plataforma suministrada, destinada a empleados TIC de la

Administración de la Junta de Andalucía y sus entidades instrumentales dedicados a tareas de ciberseguridad.

Esta capacitación tendrá las siguientes características:

- Capacitación inicial: sobre la plataforma desplegada, sus características y gestión incluyendo, al menos:
    - Configuración y operación de los sensores de red y, si se incluyen en la solución, recolectores de logs suministrados.
    - Configuración y operación del SIEM suministrado.

  La acción tendrá dos convocatorias, en fechas a determinar con el responsable del contrato, para un aforo mínimo de 15 asistentes cada una y con una duración mínima de 20 horas lectivas.
- Capacitación adicional/de refuerzo: a lo largo de la duración del contrato se podrá requerir al contratista la convocatoria de capacitación adicional o refuerzo sobre aspectos de protección y respuesta a incidentes en equipo final propuestos por la adjudicataria, a solicitud del responsable del contrato. Cada acción tendrá una convocatoria, en fecha a determinar con el responsable del contrato, para un aforo mínimo de 15 asistentes cada una y con una duración mínima de 5 horas lectivas. Tres de las sesiones serán obligatorias, una por anualidad mientras que las otras tres serán bajo demanda del responsable del contrato.

Será responsabilidad del contratista la certificación de la capacitación realizada sobre el personal que asista a las sesiones descritas.

El adjudicatario remitirá a la persona responsable del servicio una propuesta de posibles actividades formativas a realizar durante cada año al inicio de este, sin perjuicio de la competencia de la persona responsable del servicio para aceptar o denegar la propuesta o de introducir modificaciones en la misma.

Se generará un entregable para cada acción formativa incluyendo la información pertinente sobre las mismas, conforme a lo indicado en el apartado “Entregables asociados al servicio de formación y capacitación”.

VAL-SVSUM-5: Se valorará la idoneidad y calidad de la propuesta en relación con los medios técnicos y materiales propuestos, como plataformas de formación, plataforma de entrenamiento, documentación y manuales, salas de capacitación; el personal propuesto por licitador para impartir la capacitación y la organización de los programas de capacitación inicial y adicional/refuerzo, en cuanto a número de sesiones, modalidad virtual o presencial, número recomendado de asistentes, contenido, horas y certificaciones. (SOBRE 2).

5.3.7.2. Condiciones de prestación

Las sesiones de capacitación serán impartidas en castellano y tendrán lugar en las instalaciones de la Junta de Andalucía en las provincias de Málaga o Sevilla o bien de manera virtual.

5.3.7.3. Elementos y Dimensionado

ELEM-FORM-INICIAL: Formación inicial.

ELEM-FORM-ADICIONAL: Formación adicional y de refuerzo.

5.3.8. Transición del servicio a la finalización del contrato

5.3.8.1. Descripción del servicio

En los últimos tres meses del contrato (o de sus posibles prórrogas), se iniciará un periodo de transición del servicio.

El alcance de la transferencia del servicio puede abarcar al contratista o al contratista y al fabricante.

Se identifican al menos las siguientes condiciones para su devolución:

- Al menos durante los **tres últimos meses** de duración del contrato, el adjudicatario del presente contrato deberá facilitar acceso en modo lectura a las plataformas de servicio para el conocimiento y aprendizaje de reglas creadas, configuraciones y políticas, indicadores de servicio, etc. garantizando con ello una transición efectiva del servicio con el inicio del siguiente contrato.
- El adjudicatario deberá realizar la entrega de un informe de transferencia del servicio con la documentación técnica y administrativa necesaria para el traspaso. Este informe se entregará con fecha tope dos meses antes de su finalización.
- El adjudicatario deberá garantizar el borrado de información sensible en los sistemas propios del adjudicatario que no pasen a ser explotados por la Junta de Andalucía con la transferencia del servicio, certificando mediante documento escrito la ejecución de dichos trabajos.
- Si aplica, el adjudicatario deberá realizar la devolución de toda la información de telemetría, eventos, alertas y otros metadatos.
- Si aplica, el adjudicatario deberá realizar el borrado seguro de toda la información de telemetría, eventos, alertas y otros metadatos, certificando mediante documento escrito la ejecución de dichos trabajos.
- Si aplica, el adjudicatario realizará la retirada de sistemas preexistentes que hayan dejado de ser necesarios.

VAL-SVSUM-6: Se valorará la propuesta para la transferencia de conocimiento en cuanto a documentación a transferir relativa a configuración y gestión, valorándose fases de transferencia, organización y contenido de sesiones de transferencia, documentación a entregar sobre configuración, reglas y automatismos implementados y procedimientos de borrado / devolución de información generada y manipulada durante el contrato. (SOBRE 2)

5.3.8.2. Condiciones de prestación

Este servicio será prestado de forma localizada en modalidad 8x5.

El adjudicatario deberá garantizar la asignación a este servicio de, como mínimo, una persona en modalidad 8x5 y dedicación completa durante 5 días hábiles.

5.3.8.3. Elementos y Dimensionado

ELEM-TRANSIC-SERVICIO: Transición del servicio.

5.3.9. Requisitos de cualificación para el personal del equipo del proyecto

Según corresponda en cada servicio, la ejecución deberá realizarse por personal con los perfiles profesionales establecidos en el apartado 4.C “solvencia técnica o profesional” del Anexo I del Pliego de Cláusulas Administrativas Particulares.

5.4. Elementos unitarios, consumo y facturación

5.4.1. Elementos unitarios

El Catálogo de elementos unitarios (en adelante, “catálogo”) es un documento que recoge todos los elementos unitarios que pueden ser solicitados por la Agencia Digital de Andalucía en la ejecución del contrato. Tendrán asignado precio unitarios y serán los únicos conceptos que puedan figurar en las facturas que emita el adjudicatario.

Tipo	Identificador	Componente	Escala de medida	Elementos comprometidos	Elementos bajo demanda
Suministro	**ELEM-IDS-PPAL**	**Sensores de red**	**Unidad**	**1**	
Suministro	**ELEM-IDS-1**	**Sensores de red**	**Unidad**		**2**
Suministro	**ELEM-IDS-5**	**Sensores de red**	**Unidad**		**2**
Suministro	**ELEM-IDS-10**	**Sensores de red**	**Unidad**		**1**
Suministro	**ELEM-RECOL-LOG-ADICIONAL**	**Recolectores de logs adicionales**	**Unidad**		**5**

Suministro	**ELEM-SIEM-BASE**	**Componentes de consolidación y gestión (trimestre)**	**Trimestre**	**11**	
Suministro	**ELEM-SIEM-AMPL1**	**Componentes de consolidación y gestión (trimestre)**	**Trimestre**		**10**
Suministro	**ELEM-SIEM-AMPL2**	**Componentes de consolidación y gestión (trimestre)**	**Trimestre**		**8**
Suministro	**ELEM-SIEM-AMPL3**	**Componentes de consolidación y gestión (trimestre)**	**Trimestre**		**5**
Suministro	**ELEM-SIEM-AMPL4**	**Componentes de consolidación y gestión (trimestre)**	**Trimestre**		**4**
Suministro	**ELEM-SAT-SONDA**	**Sondas SAT**	**Unidad**	**2**	**2**
Servicio	**ELEM-DESPLIEGUE**	**Despliegue**	**Unidad**	**1**	
Servicio	**ELEM-TRIMES-SYM**	**Trimestre de Servicio de mantenimiento**	**Trimestre**	**12**	
Servicio	**ELEM-FORM-INICIAL**	**Formación y capacitación**	**Unidad**	**2**	
Servicio	**ELEM-FORM-ADICIONAL**	**Formación y capacitación**	**Unidad**	**3**	**3**
Servicio	**ELEM-TRANSIC-SERV**	**Transición del servicio**	**Unidad**	**1**	
Servicio	**ELEM-JF-PROYECTO**	**Jefatura de proyecto**	**Hora (8x5)**	**1.350**	
Servicio	**ELEM-HORA-OPERACIÓN-LOC (TN1 MON)**	**Operación plataforma monitorización por hora (TN1)**	**Hora (12x5)**	**21.600**	
Servicio	**ELEM-HORA-OPERACIÓN-DESLOC (TN1 MON)**	**Operación plataforma monitorización por hora (TN1)**	**Hora (24x7: desbordamiento en horario complementario)**	**36.360**	
Servicio	**ELEM-HORA-SOPEXP-LOC (TN2 MON)**	**Servicio avanzado plataforma monitorización (TN2)**	**Hora (8x5)**	**10.800**	
Servicio	**ELEM-HORA-SOPEXP-GUARDIA (TN2 MON)**	**Servicio avanzado plataforma monitorización (TN2)**	**Hora (24x7: guardia desbordamiento en horario complementario)**	**18.180**	

Servicio	**ELEM-HORA-RESPUESTA-LOC (TN1 RES)**	**Respuesta a incidentes (TN1)**	**Hora (12x5)**	**21.600**	
Servicio	**ELEM-HORA-RESPUESTA-DESLOC (TN1 RES)**	**Respuesta a incidentes (TN1)**	**Hora (24x7: desbordamiento en horario complementario)**	**36.360**	
Servicio	**ELEM-HORA-RESPUESTA-LOC (TN2 RES)**	**Respuesta a incidentes (TN2)**	**Hora (12x5)**	**16.200**	
Servicio	**ELEM-HORA-RESPUESTA-GUARDIA (TN2 RES)**	**Respuesta a incidentes (TN2)**	**Hora (24x7: guardia desbordamiento en horario complementario)**	**18.180**	
Servicio	**ELEM-JORNADA-INSITU-1**	**Respuesta in situ**	**Jornada**		**9**
Servicio	**ELEM-JORNADA-INSITU-2**	**Respuesta in situ**	**Jornada**		**9**
Servicio	**ELEM-HORA-NUEVOS-DESPL-TN1**	**Nuevos despliegues (TN1)**	**Hora**		**270**
Servicio	**ELEM-HORA-NUEVOS-DESPL-TN2**	**Nuevos despliegues (TN2)**	**Hora**		**180**

5.4.2. Modelo de consumo

Al inicio del contrato se consumirán los elementos unitarios necesarios para el despliegue inicial (entre ellos, ELEM-DESPLIEGUE y ELEM-FORM-INICIAL). Tras dicho despliegue (fases I a VII de la ejecución del proyecto), se consumirán los elementos unitarios necesarios

- Los elementos unitarios asociados al componente de consolidación y gestión (ELEM-SIEM-BASE y ELEM-SIEM-AMPL1, ELEM-SIEM-AMPL2, ELEM-SIEM-AMPL3 y ELEM-SIEM-AMPL4) se consumirán al solicitarlos, al tratarse de licencias. Trimestralmente se planificará el consumo para el periodo siguiente, indicándose por el responsable del servicio el dimensionamiento (BASE o BASE + ampliaciones) que se requerirá. Si no se comunica, se mantendrá el dimensionamiento del periodo anterior.
- Los restantes elementos unitarios de tipo “suministro” se consumirán al finalizar la provisión e instalación de los mismos, tras su solicitud por el responsable del servicio.

- Los elementos unitarios de tipo “servicio” se consumirán de forma planificada: mensualmente se coordinará entre el responsable del servicio y el jefe de proyecto la previsión de consumo de elementos unitarios.
- Los elementos unitarios ELEM-FORM-ADICIONAL, ELEM-JORNADA-INSITU-1, ELEM-JORNADA-INSITU-2, ELEM-HORA-NUEVOS-DESPL-TN1, ELEM-HORA-NUEVOS-DESPL-TN2 se consumirán bajo demanda, a petición del responsable del servicio y previa estimación (si procede) del esfuerzo necesario. Se considerarán consumidos tras su ejecución.
- El resto de los elementos unitarios de tipo “servicio” se consumirán de forma planificada: mensualmente se coordinará entre el responsable del servicio y el jefe de proyecto la previsión de consumo, en base a las necesidades. Se considerarán consumidos, tras su ejecución, los elementos (horas, por ejemplo) realmente ejecutados.

5.4.3. Modelo de facturación

Mensualmente se recopilarán y certificarán los elementos unitarios consumidos, y trimestralmente se emitirán por el adjudicatario las facturas correspondientes a los consumos del trimestre anterior.

5.5. Ejecución del proyecto

Las actividades correspondientes al lote 1 se organizarán en proyectos.

Para su dirección, se considera una dedicación del Jefe de Proyecto (elemento de catálogo ELEM-JF-PROYECTO) al 25% en promedio durante todo el contrato.

El proyecto principal consistirá en el despliegue, gestión y operación de la plataforma de monitorización.

Se podrán definir proyectos auxiliares, derivados de cambios en las infraestructuras tecnológicas de la Junta de Andalucía o de cambios organizativos como, por ejemplo:

- Consultoría para la incorporación a la plataforma de monitorización de nuevos organismos o nuevas entidades por ampliación del grupo atendido de AndalucíaCERT.
- Redespliegue o nuevo despliegue de sondas y equipamiento debido a cambios en la Red Corporativa de Comunicaciones de la Junta de Andalucía (RCJA) o a cambios en las necesidades de la plataforma de monitorización.
- Consolidación de equipos físicos y lógicos de la plataforma de monitorización y/o reducción del número de estos.
- Reubicación de equipos físicos y lógicos de la plataforma de monitorización.

Otras actuaciones, como puede ser la integración de una nueva fuente, se gestionarán como una petición de cambio dentro del servicio que en cada caso corresponda.

5.5.1. Plan de ejecución del proyecto principal

El proyecto de implantación de la plataforma de monitorización y sus servicios asociados deberá realizarse conforme al siguiente esquema:

FASE	DURACIÓN ASIGNADA
Fase I. Definición del despliegue	10 días hábiles
Fase II. Suministro	15 días hábiles
Fase III. Instalación y configuración básica	15 días hábiles
Fase IV. Transición e integración de sistemas preexistentes	15 días hábiles
Fase V. Optimización	5 días hábiles
Fase VI. Formación	2 jornadas en paralelo a las fases II a V
Fase VII. Aceptación	5 días hábiles

Las tareas de configuración podrán realizarse de forma remota, previa aprobación de la persona responsable del servicio, siempre que sea posible hacerlo sin comprometer la seguridad del proceso ni de los sistemas.

VAL-PLAN-1: Se valorará el nivel de cumplimiento respecto de los requisitos del PPT, la calidad, idoneidad, detalle y explicaciones sobre la propuesta de Plan de ejecución del proyecto según el contenido indicado en el ANEXO X. SOBRE ELECTRÓNICO N.º 2.- DOCUMENTACIÓN RELATIVA A LOS CRITERIOS DE ADJUDICACIÓN VALORADOS MEDIANTE UN JUICIO DE VALOR." (SOBRE 2).

5.5.2. Fase I: Definición del despliegue

Con carácter previo a la instalación física del equipamiento y su configuración y el inicio de la prestación de los servicios, la empresa comunicará al responsable del contrato los datos de contacto señalados en el apartado "Organización del trabajo".

En esta fase se mantendrán reuniones donde el adjudicatario deberá proporcionar todos los detalles de la instalación y puesta en marcha, incluyendo su configuración y arquitectura. En las reuniones se abordarán todos aquellos aspectos que la Junta de Andalucía considere oportunos y que afecten a la instalación, configuración y puesta en marcha del equipamiento y la puesta en marcha y funcionamiento de los servicios.

La empresa realizará un análisis y un diseño detallado en un Plan Técnico de Despliegue que deberá incluir como mínimo, y a modo de referencia, el plan de instalación física y lógica para las distintas sedes implicadas.

El plazo máximo estimado para la entrega del Plan Técnico de Despliegue será de **diez (10) días hábiles**, a contar desde la fecha de formalización del contrato.

El Plan técnico de Instalación entregado por el adjudicatario deberá ser aprobado por la persona responsable del contrato. En caso de no aprobarlo, la persona responsable del contrato enviará comunicación a la persona responsable del proyecto en el plazo de dos días laborables, indicándole las causas y requiriéndole su corrección o modificación.

En caso de no producirse requerimiento de correcciones en el tiempo mencionado en el párrafo anterior, el Plan técnico de Instalación se tendrá por aprobado.

Con la aprobación del Plan técnico de Instalación, la persona responsable del contrato autorizará el comienzo de la Fase II.

Toda modificación del Plan técnico de Instalación que sea necesario introducir con posterioridad a su aprobación deberá ser sometida nuevamente a la aprobación de la persona responsable del contrato.

Durante la fase I se determinará el equipamiento que será utilizado por el personal del adjudicatario.

5.5.3. Fase II: Suministro

En esta fase se llevará a cabo la entrega del equipamiento y el material en las ubicaciones definidas a tal efecto.

El término “equipamiento” debe entenderse aquí en su significado más amplio, incluyendo tanto el equipamiento físico incluido en el contrato como el equipamiento lógico necesario para su funcionamiento, incluyendo el correspondiente a:

- La plataforma de monitorización de eventos con todos los elementos descritos en el apartado “Plataforma de monitorización”.
- Los servidores para las sondas SAT según se describe en el apartado “Sondas SAT”.

La empresa suministradora deberá realizar los procesos de identificación, etiquetado, grabado e inventariado del material conforme a lo establecido en el apartado “Etiquetado e inventariado de los bienes suministrados” del apartado “Condiciones generales”.

El plazo máximo estimado para el suministro será de **quince (15) días hábiles,** a contar desde la finalización de la fase I. Se entenderá que el equipamiento ha sido suministrado cuando se cumplan todas las siguientes condiciones:

- Que el equipamiento haya sido entregado en las sedes en las que deban ser instalados.
- Que el equipamiento entregado sea conforme a las especificaciones establecidas en este documento y el resto de la documentación de esta licitación, a la oferta presentada por el adjudicatario y al Plan Técnico de Instalación.
- Que el equipamiento no presente averías ni daños visibles o detectables.
- Que la persona responsable del contrato valide los puntos anteriores, con lo que autorizará el inicio de la siguiente fase.

5.5.4. Fase III: Instalación y configuración básica

En esta fase se realizará la instalación del equipamiento y la configuración inicial de la plataforma, de modo que esta quede preparada para su integración con otros sistemas y fuentes de información y eventos, incluyendo las siguientes actividades:

1. Instalación y configuración del equipamiento de red suministrado.
2. Instalación y configuración inicial del SIEM.
3. Instalación, configuración e integración de los sensores de red y recolectores de log necesarios, comprendidos en el ámbito de la presente licitación, incluyendo su integración con el SIEM.
4. Desarrollo de reglas de correlación y cuadros de mando específicos.
5. Comprobación del correcto funcionamiento de los sensores de red, el SIEM y el equipamiento de red.
6. Instalación configuración de las sondas SAT.

El adjudicatario realizará la instalación de todo el equipamiento e incluirá todos los elementos necesarios (cables de comunicaciones de cobre y fibra, cableado de alimentación, etc.) para asegurar que tanto la plataforma de monitorización y las sondas SAT quedan en un estado completamente funcional.

El adjudicatario se hará cargo, en caso de que la sede donde se alojará el equipamiento objeto de suministro no lo haga, de la retirada de todo el material de empaquetado y residuos que se haya generado durante el desembalado e instalación del equipamiento objeto de suministro, debiéndolos llevar a un punto limpio.

El plazo máximo estimado para la finalización de esta fase será de **quince (15) días hábiles** a contar desde la finalización de la fase II. Se entenderá que se han completado estas tareas cuando todos los sistemas suministrados estén plenamente funcionales de forma independiente de los sistemas preexistentes y pueda comenzar su integración con estos y estos extremos sean validados por la persona responsable del contrato, con lo que autorizará el inicio de la siguiente fase.

5.5.5. Fase IV: Transición e integración de sistemas preexistentes

En esta fase se realizarán las siguientes actividades:

1. Transición desde los sistemas preexistentes a la nueva plataforma de monitorización.
2. Retirada de sistemas preexistentes que hayan dejado de ser necesarios.
3. Integración de la nueva plataforma con las fuentes y sistemas preexistentes.

Para ello se contará con, cuando corresponda, la participación del adjudicatario de la licitación anterior, el de la presente y de AndalucíaCERT.

Asimismo, durante esta fase comenzará la prestación o la disponibilidad, según el caso, de los siguientes servicios:

- Soporte y mantenimiento de la plataforma de monitorización
- Servicio avanzado de la plataforma de monitorización
- Operación de la plataforma de monitorización
- Nuevos despliegues de la plataforma de monitorización
- Soporte y mantenimiento de las sondas SAT
- Respuesta a incidentes
- Formación y capacitación

La duración máxima estimada de esta fase será de **quince (15) días hábiles**, a contar desde la finalización de la fase III). Se entenderá que se han completado estas tareas cuando todos los sistemas preexistentes hayan sido integrados con la nueva plataforma de monitorización de eventos o hayan sido retirados, según proceda, la nueva plataforma se encuentre plenamente operativa y estos extremos sean validados por la persona responsable del contrato, con lo que autorizará el inicio de la siguiente fase.

Finalmente, la plataforma debe quedar configurada al menos con los siguientes casos de uso:

- Detección de tráfico de red de código malicioso.
- Detección de ataques por denegación de servicio.
- Detección de ataques por explotación de vulnerabilidades.
- Detección de sistemas pertenecientes a botnets.
- Detección de acceso sospechoso a dispositivos, sistemas y aplicaciones.

En esta fase también debe quedar completada la integración con las fuentes de ciberamenazas propuestas por el licitador.

5.5.6. Fase V: Optimización del sistema

Esta fase, de una duración estimada de **cinco (5) días hábiles**, incluirá un periodo de seguimiento tras la integración de los sistemas y las fuentes y, cuando se disponga de suficiente información de datos recogidos, una identificación de errores a corregir y de posibles mejoras y optimizaciones en el sistema, incluyendo los ajustes a realizar sobre los parámetros y métodos de detección para solucionar las situaciones de falsos positivos detectadas.

5.5.7. Fase VI: Formación

El licitador deberá incluir en su propuesta como mínimo las especificaciones incluidas en el apartado "Formación y capacitación".

La capacitación inicial se prestará en paralelo, a lo largo de las fases II, III, IV y V de la instalación, salvo modificaciones aprobadas por el responsable del contrato.

Se generará un entregable para cada acción formativa incluyendo la información pertinente sobre las mismas, conforme a lo indicado en el apartado "Entregables asociados al servicio de formación y capacitación".

5.5.8. Fase VII: Aceptación del sistema

En esta fase se verificará la correcta implementación del sistema y todos sus entregables mediante la realización de las correspondientes pruebas de aceptación, que en todo caso incluirán un análisis de vulnerabilidades y una prueba de penetración. Se estima una duración de **cinco (5) días hábiles**.

Para que se produzca la aceptación del sistema, será necesaria la entrega de la documentación contemplada a tal efecto en el apartado "Entregables para la aceptación del sistema".

Tras la verificación de los requisitos anteriores se confirmará por parte del responsable del contrato la finalización del proyecto de implantación.

5.5.9. Fase VIII. Operación

Durante esta fase se realizará la gestión de la plataforma de monitorización y de los incidentes de seguridad conforme a lo establecido para los distintos servicios aplicables.

5.5.10. Fase IX. Transición del servicio

Esta fase se realizará conforme a lo establecido en el apartado “Transición del servicio a la finalización del contrato”.

5.6. Entregables

La persona responsable del servicio establecerá los canales, los medios y el procedimiento que deberá utilizar el adjudicatario para realizar la entrega de cada uno de los elementos entregables. El adjudicatario no utilizará ningún otro canal o medio para ello ni realizará ninguna comunicación de estos entregables a otras personas o entidades ajenas a la Agencia Digital de Andalucía y a AndalucíaCERT sin un consentimiento expreso y por escrito del responsable del contrato.

El procedimiento establecido podrá incluir, además de la propia entrega, actividades adicionales como la emisión de notificaciones o el registro de la información en otros sistemas.

Previo informe favorable de la persona responsable del servicio y autorización de la persona responsable del contrato, la entrega de todos o algunos de los entregables incluidos en este apartado podrá ser sustituida, siempre que lo permita su contenido y forma de elaboración y se garantice el nivel de seguridad adecuado, por:

- La inclusión del entregable en un repositorio u otro tipo de sistema desde el que pueda ser obtenido por AndalucíaCERT, con notificación a las personas responsables del contrato y del servicio.
- La puesta a disposición de AndalucíaCERT de una funcionalidad automatizada que permita realizar su generación y obtención en tiempo real.

Todos los entregables deberán estar elaborados en idioma castellano, salvo que se dé alguna de las siguientes circunstancias:

- Que el entregable sea traducción de otro que ya obre en poder de la persona responsable del servicio o del contrato, según corresponda.
- Que el entregable sea traducción de otro y ambos sean remitidos o puestos a disposición de la persona responsable del contrato o del servicio, según corresponda, de forma conjunta o simultánea.
- Que así lo solicite o autorice expresamente la persona responsable del servicio.

Los elementos entregables que consistan en uno o varios documentos ofimáticos serán ofrecidos, siempre que su naturaleza lo permita, en uno de los siguientes formatos:

- OpenDocument.
- Office Open XML.

Los elementos entregables que consistan en uno o varios documentos de video o de video y audio serán ofrecidos, siempre que su naturaleza lo permita, en formato Mp4.

El responsable del servicio podrá establecer modelos y criterios para los entregables o requisitos en lo referente a su apariencia, disposición, índice de contenidos, marcado TLP, limpieza de metadatos, uso de logos y otros elementos de la imagen corporativa, etc.

Los entregables podrán ser revisados por el responsable del servicio/contrato y podrán ser rechazados parcial o totalmente si, a su juicio, no reúnen la calidad mínima exigible.

A modo de recopilación y resumen, se enumeran a continuación los entregables derivados de las actividades anteriores, ligadas tanto al suministro como a los servicios, así como su contenido mínimo.

5.6.1. Entregables de carácter general

- **Informe mensual de seguimiento**
    - Descripción general de los trabajos realizados y de los resultados obtenidos, justificando (donde proceda) los tiempos consumidos en cada una de las actividades y detallando los elementos unitarios facturables en el periodo.
    - Listado de los elementos unitarios consumidos a lo largo del mes.
    - Incidencias tanto técnicas como del equipo de trabajo.
    - Riesgos detectados y propuestas de mitigación.
    - Propuestas de mejora que se puedan aplicar para el cumplimiento de los objetivos de los servicios del lote.
    - Actas de las reuniones que hayan tenido lugar en ese periodo. Compete al licitador tomar notas y elaborar y difundir la correspondiente acta por cada reunión mantenida. Dicho documento deberá recoger, al menos: Lugar y fecha de reunión, horas de inicio y finalización, número de asistentes, orden del día, acuerdos y compromisos alcanzados por ambas partes, así como si procede, revisión de los acuerdos y compromisos alcanzados en reuniones previas.
- **Informe mensual de cumplimiento de ANS** que incluya, para cada servicio y ANS asociado:
    - Modo de cálculo de la penalización, cuando proceda, que podrá tomar uno de los siguientes valores conforme lo establecido en la documentación de la presente licitación:
        - Por exceso de tiempo con respecto al plazo establecido.
        - Por porcentaje de solicitudes o intervenciones que incumplan el ANS.
    - Cuando la penalización se calcule por tiempo superando el plazo establecido:
        - Tiempo asignado para el ANS.

- Tiempo, en las unidades establecidas para el ANS, que se ha superado el plazo. Si no se ha superado, se indicará cero (0).

- Cuando la penalización se calcule respecto del porcentaje de solicitudes o intervenciones que cumplan el ANS:
  - Porcentaje de solicitudes o peticiones para las que se ha incumplido en ANS con respecto al número total.

- El informe contendrá también un anexo en el que se mostrará la información anterior únicamente para aquellos servicios en los que se haya producido algún incumplimiento del ANS.

- **Informe anual del plan de formación del equipo de trabajo**
  - Plan de formación actualizado del personal del proveedor
  - Acciones formativas que se han llevado a cabo.
  - Evidencias de la realización.

- **Memoria final del proyecto**
  - Listado de entregables producidos.
  - Recursos consumidos.
  - Indicadores.
  - Lecciones aprendidas.
  - Propuesta de recomendaciones de actividades y objetivos a desarrollar y alcanzar en los siguientes meses en el ámbito de los servicios descritos en el presente pliego.
  - Actas de las reuniones mantenidas: Compete al licitador tomar notas y elaborar y difundir la correspondiente acta por cada reunión mantenida. Dicho documento deberá recoger, al menos: Lugar y fecha de reunión, horas de inicio y finalización, número de asistentes, orden del día, acuerdos y compromisos alcanzados por ambas partes, así como si procede, revisión de los acuerdos y compromisos alcanzados en reuniones previas.

5.6.2. Entregables asociados a la plataforma de monitorización

- Documentación técnica de la plataforma implementada:
  - Descripción de la arquitectura de la plataforma, tanto física como lógica, incluyendo el detalle de sus fuentes de eventos.
  - Configuración aplicada a los sensores de red.
  - Configuración aplicada al SIEM.

- Documentación de las APIs y otros mecanismos ofrecidos por la plataforma para la integración de nuevos elementos.
- Guías y manuales usados para las integraciones de elementos en la plataforma realizadas.
- Casos de uso implementados.

- Documentación administrativa de la plataforma implementada:
  - Datos de contacto, conforme a lo establecido en el apartado “Organización del trabajo”.
  - Copias de las licencias o autorizaciones de aquellos servicios y productos que lo requieran para su uso.
- Otra información necesaria para la operación de la plataforma:
  - Justificantes de entrega de credenciales necesarias para la gestión y uso de los sensores recolectores de tráfico de red.
  - Justificantes de entrega de credenciales necesarias para la gestión y uso del SIEM.
  - Justificantes de entrega de otras credenciales.
  - Cualquier otra documentación necesaria para la gestión, administración o el uso de la plataforma.

5.6.3. Entregables asociados a cada proyecto de despliegue

- Plan Técnico de Despliegue
  - Arquitectura del sistema y/o equipamiento desplegado, reflejando la relación con el preexistente. Diagramas físicos y lógicos.
  - Planificación de los roles, perfiles y divisiones necesarias en la plataforma para la clasificación de los equipos y la gestión de la misma para una estructura multiorganismo.
  - Análisis y selección de las fuentes a integrar en la solución, la confección de guías de configuración de las fuentes y asesoramiento en las labores de configuración de los equipos monitorizados.
  - Listado de necesidades de desarrollo para la integración de las fuentes no soportadas nativamente (out-of-the-box) por la plataforma.
  - Listado de sistemas y fuentes con los que se integrará la plataforma, cuando sea aplicable.
  - Identificación de dependencias del despliegue y partes involucradas: instalación en rack, conectividad de red, direccionamiento IP necesario, etc.

- Identificación de posibles situaciones de pérdida de continuidad del servicio como consecuencia del despliegue de la plataforma y la integración en ella de componentes tanto nuevas como preexistentes.
- Medidas a adoptar para evitar o reducir el efecto de las situaciones de pérdida de continuidad del servicio.
- Plan detallado de puesta en marcha y configuración, incluyendo estimación de tiempos para cada una de las tareas. Proceso de instalación, que incluya todos los elementos que son necesarios para disponer del equipamiento y las herramientas de gestión totalmente operativas.
- Plan de optimización, incluyendo una estimación del tiempo necesario para la recopilación de datos previa al inicio del proceso.
- Plan de pruebas de aceptación. Deberá cubrir al menos el cumplimiento de los requisitos técnicos y funcionales del pliego, otras características ofertadas por el licitante, así como un informe de seguridad de la plataforma. El informe de seguridad de la plataforma se basará en el Procedimiento de empleo seguro del producto según la respectiva guía CCN-STIC del CCN o en las buenas prácticas de seguridad del propio fabricante.
- Plan de formación, cuando sea aplicable.
- Plan de explotación y mantenimiento de la plataforma.
- Documentación técnica: Casos de uso y manuales de uso y administración.
- Acreditaciones de seguridad de los ordenadores del equipo de trabajo, para el personal localizado y deslocalizado, acorde a los controles de seguridad del ENS categoría Media.
- Identificación del responsable de seguridad y delegado de protección de datos del proveedor. Procedimiento de gestión de incidentes de seguridad en el proveedor.

5.6.4. Entregables asociados al lote como conjunto

- Documentación técnica de las componentes utilizadas. Para cada componente se entregará, siempre que sea aplicable, la siguiente documentación:
  - Fichas técnicas, incluyendo expresamente las capacidades de los elementos conforme a las configuraciones entregadas por el adjudicatario, así como sus posibles ampliaciones.
  - Manuales de instalación, configuración, administración y operación de los sensores de tráfico de red y recolectores de log.

- Manuales de instalación, configuración, administración y operación del SIEM. En caso de tratarse de una solución implantada en la nube, solo se aportará los documentos aplicables.

5.6.5. Entregables para la aceptación del sistema

Incluye el despliegue inicial y lo que aplique en los proyectos de ampliaciones:

- Documentación actualizada del Plan Técnico de Despliegue.
- Guías, manuales y cualquier otra documentación necesaria para el despliegue, configuración, administración y uso de la plataforma.
- Entregables de los cursos de formación. Para cada actividad se hará constar:
  a. Nombre de la actividad.
  b. Índice de contenidos.
  c. Número de horas de duración.
  d. Medios técnicos y audiovisuales utilizados
  e. Número de sesiones.
  f. Número de personas asistentes a cada sesión.
  g. Número de diplomas/certificados de aprovechamiento emitidos.

  Asimismo, se entregará copias de los materiales entregados o puestos a disposición de las personas asistentes, así como el utilizado por el personal docente para la impartición de la actividad.
- Inventario de los activos suministrados.
- Descripción de la base de datos de configuración de los activos suministrados (CMDB).
- Acuerdos de soporte, mantenimiento, suscripciones y garantía.
- Procedimiento de gestión de incidencias y peticiones, con protocolos de escalado bien definidos.
- Documentación de las pruebas de aceptación, incluyendo los resultados de:
  - Las pruebas de cumplimiento de requisitos técnicos y funcionales.
  - Las pruebas de rendimiento.

- Resultado del análisis de seguridad de la plataforma (análisis de vulnerabilidades y pruebas de penetración), emitido por una o varias empresas independientes, ajenas al adjudicatario.

5.6.6. Entregables asociados a los servicios de Soporte y mantenimiento de la Plataforma de Monitorización, Soporte, mantenimiento de las sondas SAT

- Informe mensual de soporte y mantenimiento:
  - Estadística de incidencias producidas durante el periodo en el marco de cada uno de los servicios indicados, así como de cada componente de la plataforma, clasificándolas según nivel de impacto y elementos afectados y haciendo indicación de cuántas de ellas afectaron a la disponibilidad de esta.
  - Para cada incidencia que haya supuesto o esté suponiendo la falta de disponibilidad total o parcial de algún elemento o de alguna funcionalidad:
    - Servicio al que corresponde la incidencia.
    - Número o código identificador de la incidencia.
    - URL, dirección u otro medio que permita consultar el estado de la incidencia en tiempo real.
    - Descripción de la incidencia.
    - Estado de la incidencia en el momento de la redacción del informe.
    - Indicación de las componentes afectadas y del alcance de la falta de disponibilidad.
    - Duración y fechas y horas de inicio y finalización de la falta de disponibilidad.
    - Análisis de las causas de la incidencia.
    - Medidas adoptadas para resolver la incidencia.
    - Medidas adoptadas para evitar que se vuelva a producir la misma incidencia u otra de naturaleza similar.
    - Propuesta de medidas adicionales, cuando sean necesarias.
  - Para cada problema detectado en el marco de cada uno de los servicios, entendiendo problema como la causa, o posible causa, de una o varias incidencias:
    - Servicio al que corresponde la incidencia.

- Número o código Identificador del problema.
- URL, dirección u otro medio que permita consultar el estado de la incidencia en tiempo real.
- Descripción a alto nivel del problema.
- Indicación de los efectos y consecuencias del problema, incluyendo estadísticas sobre las incidencias ocasionadas y las que podría ocasionar en el futuro.
- Estado del problema en el momento de la redacción del informe.
- Medidas adoptadas para resolver el problema.
- Medidas adoptadas para evitar que se reproduzca el problema u otro de naturaleza similar.
- Propuesta de medidas adicionales, cuando sean necesarias.

- Propuesta de mejoras en la plataforma o las sondas SAT, cuando existan.

5.6.7. Entregables asociados al servicio de operación de la plataforma de monitorización

- Informe mensual de incidencias que hayan afectado a cada componente de la plataforma de monitorización, clasificándolas según tipo y componente afectada y haciendo indicación de cuántas de ellas afectaron a la disponibilidad de esta.
- Nuevos casos de uso creados y mejorados.

5.6.8. Entregables asociados al servicio de respuesta a incidentes

- Informe mensual de incidentes que incluirá:
  - Estadística con, como mínimo, los siguientes datos, expresados tanto en total como desglosados por organismo o entidad:
    - Número de incidentes de seguridad gestionados.
    - Número de incidentes de seguridad por tipo de incidente.
    - Número de incidentes de seguridad por organismo o entidad.
    - Número de incidentes de seguridad por nivel potencial de severidad.
    - Número de incidentes de seguridad según el impacto o daño causado.

- Número de incidentes de seguridad según el nivel de soporte (TN1, TN2, experto) requerido para su atención.

  - Propuestas para una mejor gestión de incidentes de seguridad, cuando existan.

- Informe anual, a entregar en la primera quincena de cada año natural, que contendrá:
  - Estadística de incidentes de seguridad producidos, con el mismo contenido mínimo que el establecido para el informe mensual de resultados de la plataforma de monitorización.
  - Contexto y tendencias en materia de incidentes de seguridad.
- Informes de estadísticas acumuladas, emitidos a petición del responsable del servicio o del contrato, con el mismo contenido indicado para el informe anual.
- Informe final de estadísticas, a entregar a la finalización del contrato y sus posibles prórrogas, con el mismo contenido indicado para el informe anual.
- Informe de incidente de especial relevancia. Cuando se detecte un incidente de especial riesgo o impacto, además de realizar a la mayor brevedad posible una notificación a la persona responsable del servicio, se le hará entrega en el plazo máximo de 7 días a contar desde el momento de la detección de un informe con el siguiente contenido mínimo:
  - Código o número identificador del incidente.
  - URL, dirección u otro medio que permita consultar el estado del incidente en tiempo real.
  - Teléfono de contacto de las personas o unidades encargadas de la gestión del incidente.
  - Estado del incidente en el momento de la redacción del informe.
  - Explicación a alto nivel del incidente, sus consecuencias potenciales y el impacto producido.
  - Causas u origen del incidente.
  - Medidas adoptadas para hacer frente al incidente.
  - Medidas adoptadas para evitar que el incidente, u otros de similar naturaleza se repita en el futuro.
  - Propuesta de medidas adicionales, cuando sean necesarias.

Los apartados de datos estadísticos incluidos en el informe anual, el informe de estadísticas acumuladas y el informe final de estadísticas podrán ser sustituidos por el acceso a un sistema que permita obtener,

extraer y almacenar en todo momento dicho informe de forma actualizada y que cuente con la posibilidad de parametrizar los contenidos sin necesidad de componer consultas ni realizar configuraciones.

En la documentación de las configuraciones aplicadas a los sensores de red y el SIEM se incluirán las reglas de detección desarrolladas en el marco del contrato o sus posibles prórrogas, indicando para cada una su finalidad, una descripción a alto nivel de su funcionamiento y el código asociado.

Toda la documentación mencionada en este apartado deberá mantenerse siempre actualizada, haciendo entrega de una nueva versión de los documentos afectados, o poniéndolos a disposición de la persona responsable del contrato, cada vez que se produzca una modificación relevante.

El contratista y subcontratistas estarán obligados al cumplimiento de los compromisos en materia de comunicación, encabezamientos y logos que se contienen en el artículo 9 de la Orden HFP/1030/2021, de 29 de septiembre, así como, en su caso, a utilizar los modelos de documentos y formatos que establezca la persona responsable del contrato.

5.6.9. Entregables asociados a cada proyecto de respuesta rápida in-situ para la recuperación

- **Propuesta de plan de trabajo (anterior a la intervención)**
    - Identificación y descripción de la incidencia que justifica la necesidad de la respuesta rápida in-situ.
    - Fundamento de la necesidad de la respuesta rápida in-situ.
    - Número de personas que se propone para la intervención rápida in-situ, indicando para cada una de ellas:
        - Nombre y apellidos, cuando sea posible proporcionarlo en el momento de la propuesta.
        - Titulación, experiencia y certificaciones.
        - Perfil profesional, conforme a lo establecido en el apartado “Modelo de consumo”.
        - Actividades que llevará a cabo.
    - Compromiso de plazo máximo para la presencia in-situ del personal mencionado en el punto anterior.
- Informe de intervención programada (posterior a la intervención)
    - Índice.

- Resumen ejecutivo.
- Descripción de la intervención con indicación, para cada actuación realizada de:
  - Fecha y hora de realización.
  - Personas que llevaron a cabo la actuación.
  - Descripción de la actuación realizada.
  - Resultados obtenidos con la actuación.
- Conclusiones y propuestas de mejora
- Recursos consumidos en la intervención:
  - Número de personas por tipo de perfil profesional, conforme a lo establecido en el apartado de elementos unitarios.
  - Coste por hora del elemento unitario correspondiente a cada perfil profesional. conforme a lo establecido en el contrato.
  - Número de horas consumidas de cada perfil profesional.
  - Coste total correspondiente a cada perfil profesional.
  - Número total de horas correspondiente a todos los perfiles profesionales implicados en la prestación del servicio.
  - Coste total correspondiente a todos los perfiles profesionales implicados en la prestación del servicio.
- Referencias

5.6.10. Entregables asociados al servicio de formación y capacitación

- Documentación descriptiva de la sesión o actividad:
  - Nombre de la actividad.
  - Índice de contenidos.
  - Número de horas de duración.
  - Medios técnicos y audiovisuales utilizados
  - Número de sesiones.
  - Número de personas asistentes a cada sesión.

- Número de diplomas/certificados de aprovechamiento emitidos.

- Copias de los materiales entregados o puestos a disposición de las personas asistentes.
- Copia del material utilizado por el personal docente para la impartición de la actividad.

5.7. Acuerdo de nivel de servicio (ANS)

El adjudicatario se compromete a cumplir con unos niveles de calidad en la plataforma gestionada y en los servicios técnicos de asistencia atendiendo a los conceptos descritos en el presente pliego y en las condiciones mínimas que se detallan a continuación:

- Despliegue de proyectos.
- Disponibilidad de la plataforma.
- Atención y resolución de incidencias asociadas al suministro.
- Atención y resolución de consultas y peticiones.
- Gestión de incidentes de ciberseguridad.
- Servicio de guardia.
- Entrega de informes periódicos y singulares.

Se analizarán los ANS por trimestre de cierre de las actuaciones (provisiones, incidencias, consultas, etc.). El Responsable de Servicio informará con el detalle del grado de cumplimiento de los distintos ANS al adjudicatario.

Para los ANS directos, se exigirá el compromiso a cumplir para la realización de la actuación de la que se trate. En el caso de los ANS indirectos, se establecerán límites sobre las ratios obtenido, por trimestre de cierre. Se trata por tanto de un indicador de la calidad y del desempeño del adjudicatario según las condiciones asumidas al firmar el contrato.

En el caso que el Responsable de Servicio así lo determine podrá modificar la periodicidad con la que se realicen las mediciones de los ANS, pudiendo pasar a mensual o a cualquier otra periodicidad.

5.7.1. ANS Despliegue de proyectos

En este apartado se definen los parámetros de nivel de servicio relativos a los plazos para la ejecución de las actuaciones asociadas a cada proyecto, así como la entrega y puesta a disposición de los correspondientes elementos entregables.

El valor de compromiso será el establecido en el correspondiente Plan Técnico de Despliegue, aprobado conforme a lo establecido en el apartado “Plan de ejecución del proyecto principal”.

5.7.1.1. Compromisos

Se considerará que existe incumplimiento cuando se supere el límite del valor de compromiso de cada una de las fases.

VAL-ANS-1: Se valorará una mejora en el tiempo de despliegue de la solución. (SOBRE 3, NO INCLUIR EN SOBRE 2).

5.7.2. ANS Disponibilidad de la plataforma

En este apartado se definen los parámetros de nivel de servicio relativos a la **disponibilidad de la plataforma en la nube** que soporta la prestación los servicios del contrato, entendidas estas como interrupciones o degradaciones en el acceso a la consola, así como la operatividad básica de la consola.

La disponibilidad del servicio será entendida como el porcentaje de tiempo trimestral en que se encontrará operativa la plataforma una vez se encuentre esta en explotación.

El adjudicatario proporcionará servicio Web y/o API/REST para monitorizar la disponibilidad del servicio y los parámetros necesarios para su monitorización. Este servicio deberá ser tal, que la respuesta positiva al sondeo de este sea garantía de que el servicio global esté disponible con unos tiempos de respuesta adecuados. La no respuesta positiva al mismo tendrá consideración de indisponibilidad de la plataforma, con la única excepción que se encuentren caídas infraestructuras de responsabilidad única de la Agencia Digital de Andalucía que no hagan posible el sondeo. Para cada uno de los posibles métodos se deberá proporcionar:

- WEB: Acceso a una URL con login y verificar respuesta del servidor. Información necesaria: URL y usuario/pass para poder hacer login.
- API/REST: Consultar un método y esperar una respuesta que valide el servicio. Información necesaria: URL de la API (con autenticación) y respuesta esperada al método consultado.

El sondeo se realizará cada 5 minutos, siendo la no respuesta por dos veces consecutivas al sondeo o dos respuestas consecutivas con código de error comienzo de la medición de la indisponibilidad. Para el fin de la contabilización de la indisponibilidad será necesaria una única respuesta correcta.

5.7.2.1. Definición y cálculo de métricas

Definición y cálculo de métricas

La disponibilidad se calculará trimestralmente de acuerdo con la siguiente expresión:

$$PorcentajeDisponibilidadtrimestral = \frac{Ttot - TnoDisp}{Ttot} \times 100$$

Donde:

- Ttot: Tiempo total del periodo considerado
- TnoDisp: Tiempo de no disponibilidad de la plataforma

5.7.2.2. Condiciones de medida

El horario que aplica al cálculo de los tiempos será de 24x7, alineado con el horario de servicio del Soporte y mantenimiento para el correcto funcionamiento de la plataforma.

En el cálculo de los parámetros anteriormente definidos no se considerará el tiempo transcurrido en los siguientes casos, siempre y cuando sean debidamente justificados y recogidos en el sistema de gestión de incidencias y peticiones:

- Interrupciones de servicio que pudieran producirse por causas de fuerza mayor, acceso a Internet o problemas relacionados más allá del propio servicio o punto de demarcación del proveedor de infraestructura en la nube.

Al tratarse de una solución en nube no se consideran excluidas del cómputo las paradas programadas, es decir, las labores de mantenimiento que apliquen sobre la solución en nube no pueden traducirse en una indisponibilidad del servicio.

5.7.2.3. Compromisos

Se considerará que existe incumplimiento cuando la disponibilidad sea inferior al 99,60% trimestral, considerando un horario de servicio 24x7.

VAL-ANS-2: Se valorará una mejora de la disponibilidad sobre el mínimo requerido, hasta un máximo del 99,95%. (SOBRE 3, NO INCLUIR EN SOBRE 2).

5.7.3. ANS Atención y resolución de incidencias asociadas al suministro

En este apartado se definen los parámetros de nivel de servicio relativos a la atención y resolución de incidencias, entendidas estas como interrupciones o degradaciones del servicio asociadas al suministro prestado en explotación (el concepto también incluye fallas del propio suministro hardware). El suministro abarca todo lo descrito en el apartado "Suministro".

5.7.3.1. Definición y cálculo de métricas

En todos los casos, se medirá la atención con el tiempo de respuesta, y la resolución con el tiempo de resolución. Estos parámetros quedan definidos como sigue:

- **Tiempo de Respuesta:** Tiempo transcurrido desde la notificación realizada en sistemas (ya sea de manera reactiva por el Responsable de Servicio, o de forma proactiva por el adjudicatario) hasta el envío por parte del adjudicatario de la aceptación de la incidencia indicando el primer diagnóstico en el sistema de tickets en vigor.

$$Tiempoderespuesta = Horadeaceptación - Horadenotificacióndelaincidencia - ParadasdeReloj$$

- **Tiempo de Resolución:** Tiempo transcurrido desde que se acepta la incidencia hasta que la incidencia queda resuelta por parte del adjudicatario. Se calcula de la siguiente forma:

$$Tiempoderesolución = Horaderesolución - Horadeaceptación - ParadasdeReloj$$

- **Tiempo de Reparación:** es el tiempo suma del tiempo de respuesta y del tiempo de resolución:

$$TiempodeReparación = TiempodeRespuesta + TiempodeResolución$$

Una vez resuelta la incidencia por parte del operador y verificada por el Responsable de Servicio, existe la posibilidad de reapertura dentro de las 72 horas naturales si el incidente se reproduce. En este caso, el contador de tiempos para el cálculo de los ANS se reactivará desde el punto en el que se paró, contabilizando el tiempo desde la reapertura hasta la nueva resolución.

Los siguientes indicadores se emplearán para la evaluación del servicio y estarán sujetos a ANS:

- **Indicador de Reapertura de Incidencias (IRA)**: Cuenta el número de veces que se reabre una incidencia en las 72 horas naturales siguientes a la resolución por parte del contratista/adjudicatario; esto estará provocado, entre otras causas, por una reiteración de la incidencia, persistencia de la misma o no conformidad.
- **Tiempo de entrega de Informe de Resolución de incidencia (TE)**: Se define como el tiempo que transcurre desde que se **solicita el informe**, una vez resuelta la incidencia, hasta que el adjudicatario realiza la entrega del Informe de Resolución de Incidencia al Responsable del Servicio. En dicho informe se detallarán las causas de la incidencia, las acciones llevadas a cabo

para la resolución de la misma, medidas preventivas adoptadas, las conclusiones y las posibles acciones de mejora. Estos informes se solicitarán y se entregarán bajo demanda del Responsable de Servicio. Se establece un ANS para la entrega de informes en función de la criticidad de la misma.

Las medidas se realizan sobre el universo de incidencias que pasan por el adjudicatario (**NIIO**), es decir, por todas aquellas incidencias que se han asignado al adjudicatario en este contrato: aceptadas, no aceptadas, resueltas o no resueltas independientemente de la causa u origen de la incidencia. En este universo **NIIO**, se contabilizarán como incidencias incumplidas (**NIII**) aquellas en las que se ha sobrepasado bien el tiempo de respuesta, bien el tiempo de resolución, o ambos. En este universo **NIIO**, se contabilizarán como incidencias cerradas (**N**) aquellas en estado "cerrado" en el Sistema Integrado de Operación en vigor que determine el Responsable del Servicio.

Los tiempos de respuesta y/o resolución en caso de reapertura de incidencias serán acumulativos hasta que finalmente pasen a estado "cerrado" en el Sistema Integrado de Operación en vigor que determine el Responsable del Servicio. Esto será de aplicación para cualquier tiempo identificado como nivel de servicio.

5.7.3.2. Condiciones de medida

El horario que aplica al cálculo de los tiempos de respuesta, resolución de incidencias, reparación y entrega de informes será de **24x7**, alineado con el horario de prestación del servicio.

En el cálculo de los parámetros anteriormente definidos no se considerará el tiempo transcurrido en los siguientes casos, siempre y cuando sean debidamente justificados y recogidos en el sistema de gestión de incidencias y peticiones:

- Tiempos de no disponibilidad debidos a la imposibilidad de reposición del servicio por motivos no imputables a los adjudicatarios (p.ej. Inaccesibilidad de las instalaciones en caso de requerirse visita).
- Pérdidas de servicio debidas a causas de fuerza mayor (desastre natural) ajenas a la responsabilidad del adjudicatario.

Al tratarse de una solución en nube no se consideran excluidas del cómputo las paradas programadas, es decir, las labores de mantenimiento que apliquen sobre la solución en nube no pueden traducirse en una indisponibilidad del servicio.

Será responsabilidad del adjudicatario velar por la adecuada actualización de los estados en el sistema de tickets y reporte de incidencias.

Las incidencias se priorizarán de acuerdo a su criticidad, y se podrán recategorizar por el Responsable de Servicio.

La criticidad de una incidencia será:

- **ALTA:** si se produce pérdida total del servicio.
- **MEDIA**: degradación acusada del servicio prestado por la plataforma o afectación a la disponibilidad de un sistema singular de la Junta de Andalucía.
- **BAJA:** si se produce degradación leve permanente o degradación acusada esporádica del servicio prestado por la plataforma.

En el caso de incidencias masivas, se tomará la prioridad del servicio más exigente.

Si la degradación de los parámetros y/o microcortes no impiden operar los servicios soportados, aunque su funcionamiento no es el requerido, la incidencia se categorizará como de criticidad “baja”.

Las incidencias serán atendidas por orden de criticidad.

Existirán las siguientes particularidades:

- Serán siempre de criticidad alta aquellas en las que se produzca degradación total o acusada permanente del servicio prestado por la plataforma o impida la prestación de este servicio en las debidas condiciones de seguridad.
- No computarán para el cálculo del tiempo de resolución los tiempos de retardo debidos a la imposibilidad de resolución de las peticiones por motivos no imputables a los adjudicatarios, siempre y cuando sean debidamente justificados de acuerdo a los procedimientos en vigor establecidos por el Responsable de Servicio, debiendo estos estar claramente identificados en los sistemas de gestión. Será responsabilidad del adjudicatario velar por la adecuada actualización de los estados en sistema mediante los procedimientos en vigor.-
- En el cálculo de los parámetros anteriormente definidos no se considerará el tiempo transcurrido en los siguientes casos, siempre que estén debidamente recogidos en sistemas de gestión según se indiquen en los procedimientos de trabajo vigentes:
    - Tiempos de no disponibilidad debidos a la imposibilidad de reposición del servicio por motivos imputables al cliente (por ejemplo: inaccesibilidad de las instalaciones del cliente o gestión de incidencias con terceras partes involucradas en el servicio).-
    - Pérdidas de servicio debidas a causas de fuerza mayor (desastre natural) ajenas a la responsabilidad del adjudicatario.-

5.7.3.3. Compromisos

Se considerará que existe incumplimiento cuando se superen los valores de compromiso detallados en los siguientes apartados.

5.7.3.3.1. ANS DIRECTOS

Incidencias suministro: se considerará incumplido cuando se supere el límite del compromiso de Tiempo de Reparación.

ANS	Criticidad	Indicador		
		Tiempo de Respuesta	**Tiempo de Resolución**	**Tiempo de Reparación**
Incidencias	Alta	30 min	240 min	270 min
	Media	45 min	480 min	525 min
	Baja	60 min	600 min	660 min

Compromisos Incidencias

VAL-ANS-3: Se valorará el valor comprometido de este ANS por debajo del máximo aquí indicado. (SOBRE 3, NO INCLUIR EN SOBRE 2).

- **Informes de Incidencias suministro**: se considerará incumplido si la entrega supera el compromiso de tiempo establecido.

ANS	Criticidad	Indicador
		Tiempo de Entrega
Informe de Incidencias	Alta	480 min
	Media	1080 min
	Baja	1440 min

Compromisos Informes Incidencias

5.7.3.3.2. ANS INDIRECTOS

- **Cumplimiento en Tratamiento de Incidencias (CTII):** es el porcentaje total (100%) menos el porcentaje de incidencias incumplidas respecto del total de incidencias del contrato más 20. Se determina mediante la fórmula siguiente:

ANS	Fórmula	Compromiso

		CTII (CCTII)
Cumplimiento en Tratamiento de Incidencias (CTII)	$CTII = 100 - \left(\frac{NIII}{(NIIO + 20)} \right) * 100$	≥ 95%

- **Cumplimiento de Reapertura de Incidencias (CRA)**: es el porcentaje total (100%) menos el porcentaje del número de veces que se reabre una incidencia (IRA) respecto del total de incidencias cerradas del contrato (N) más 10. Se determina mediante la fórmula siguiente:

ANS	Fórmula	Compromiso CRA (CCRA)
Cumplimiento de Reapertura de Incidencias (CRA)	$CRA = 100 - \left(\frac{\sum IRA}{(N + 10)} \right) * 100$	≥ 90%

5.7.4. ANS Atención y resolución de consultas y peticiones

En este apartado se definen los parámetros de nivel de servicio relativos a la atención y resolución de consultas y peticiones relativas a la gestión y la administración del suministro, así como de la prestación del soporte asociado.

Este apartado trata de:

Consultas: Cualquier tipo de solicitud de información. El Responsable de Servicio, a lo largo del contrato, establecerá los tipos de consultas que estimen convenientes para la ejecución o seguimiento del proyecto. Entre otras, se encuentran las siguientes, que por norma general tendrán asignadas las prioridades indicadas. El Responsable de Servicio deberá categorizar (y podrá recategorizar posteriormente) cada petición en el momento inicial de la solicitud en función de su naturaleza y complejidad.

- Servicios: sobre funcionalidades del servicio, compatibilidad con otros servicios, recomendaciones de uso y/o instalación y otros. PRIORIDAD=1.
- Facturación: detalles de los servicios a facturar, actualización de importes y otros. PRIORIDAD=1. Aplicará PRIORIDAD=0 cuando la información demandada impida cerrar en tiempo un ciclo de facturación o la información sea requerida por razones legales.
- Otras. PRIORIDAD=1.

- **Peticiones**: se trata de solicitudes de nuevos despliegues o trabajos, cambios/aplicaciones de configuración sobre la plataforma (ej. altas/bajas de usuarios/grupos, solicitudes expresas de actualización software...).

  El Responsable de Servicio deberá categorizar (y podrá recategorizar posteriormente) cada petición en el momento inicial de la solicitud en función de su naturaleza y complejidad.

  PRIORIDAD=0 para solicitudes urgentes que sean necesarias para el correcto funcionamiento de la plataforma o los agentes desplegados, y/o cambios urgentes necesarios para no comprometer la seguridad de los organismos del Alcance del contrato. Aplicará PRIORIDAD=1 para resto de peticiones.

5.7.4.1. Definición y cálculo de métricas

Como parámetros de medida de la calidad de servicio se tomarán los siguientes:

- **Tiempo de Respuesta a Consultas:** Se define como el tiempo transcurrido entre la notificación de la consulta por parte del Responsable de Servicio hasta el envío por parte del adjudicatario de la aceptación de la consulta del servicio correspondiente.

Tiempo de respuesta = Hora de aceptación – Hora de notificación de la consulta - Paradas de Reloj

- **Tiempo de Resolución a Consultas:** Se define como el tiempo transcurrido entre la aceptación de la consulta por parte del adjudicatario del servicio y el envío al Responsable de Servicio de la consiguiente respuesta.

Tiempo de resolución = Hora de resolución – Hora de aceptación - Paradas de Reloj

- **Tiempo de Consultas**: Se define el tiempo de consultas como la suma del tiempo de respuesta y el tiempo de resolución a consultas; se utiliza para un compromiso de nivel de servicio directo.

T. Consulta = T. Respuesta + T. Resolución

- **Tiempo de Respuesta a Peticiones:** Se define como el tiempo transcurrido entre la notificación de la petición por parte del Responsable de Servicio hasta el envío por parte del adjudicatario de la aceptación de la petición del servicio correspondiente.

Tiempo de respuesta = Hora de aceptación – Hora de notificación de la petición - Paradas de Reloj

- **Tiempo de Resolución a Peticiones:** Se define como el tiempo transcurrido entre la aceptación de la petición por parte del adjudicatario del servicio y el envío al Responsable de Servicio de la consiguiente respuesta.

Tiempo de resolución = Hora de resolución – Hora de aceptación - Paradas de Reloj

- **Tiempo de Provisión a Peticiones:** Se define el tiempo de provisión de peticiones como la suma del tiempo de respuesta y el tiempo de resolución a peticiones; se utiliza para un compromiso de nivel de servicio directo.

T. Provisión = T. Respuesta + T. Resolución

- **Indicadores:**
  - **NCII,** es el Número de Consultas Incumplidas, es decir, las consultas en las que se ha sobrepasado bien el tiempo de respuesta, bien el tiempo de resolución o ambos.
  - **NCTT,** es el universo de medida, es el Total de Consultas que ha tramitado el adjudicatario en el mes objeto del estudio del contrato.
  - **NPII,** es el Número de Peticiones Incumplidas, es decir, las peticiones en las que se ha sobrepasado bien el tiempo de respuesta, bien el tiempo de resolución o ambos.
  - **NPTT,** es el universo de medida, es el Total de Peticiones que ha tramitado el adjudicatario en el mes objeto del estudio del contrato.

Con estos indicadores se establecen los ANS de consultas / peticiones indirectos:

- **ANS de Cumplimiento de Atención a Consultas (CC):** se define como el porcentaje total (100%) menos el porcentaje de las consultas incumplidas (**NCII**) en el contrato (en función de la prioridad) respecto del total de consultas tramitadas (**NCTT**) más 20 o 10 (en función de la prioridad) por el adjudicatario en el contrato.
  El periodo de cálculo es mensual (mes de cierre de las consultas). Se distinguen las de prioridad 0 de las de prioridad 1:

CC Prioridad 0 =100 - (Número de Consultas Incumplidas NCII Prioridad 0/(Total Consultas Tramitadas NCTT - Prioridad 0+20))*100
CC Prioridad 1 =100 - (Número de Consultas Incumplidas NCII Prioridad 1/(Total Consultas Tramitadas NCTT - Prioridad 1+10))*100

- **ANS de Cumplimiento de Atención a Peticiones (CP):** se define como el porcentaje total (100%) menos el porcentaje de las peticiones incumplidas (**NPII**) en el contrato (en función de la prioridad) respecto del total de peticiones tramitadas (**NPTT**) más 20 o 10 (en función de la prioridad) por el adjudicatario en el contrato.
  El periodo de cálculo es mensual (mes de cierre de las peticiones). Se distinguen las de prioridad 0 de las de prioridad 1:

CP Prioridad 0 =100 - (Número de Peticiones Incumplidas NPII - Prioridad 0/(Total Peticiones Tramitadas NPTT - Prioridad 0+20))*100
CP Prioridad 1 =100 - (Número de Peticiones Incumplidas NPII - Prioridad 1/(Total Peticiones Tramitadas NPTT - Prioridad 1+10))*100

Se considera como respuesta válida la respuesta a la consulta/petición por parte del adjudicatario con una justificación concreta y precisa de la misma en términos técnicos y operacionales, cubriendo todo el ámbito que se define en la consulta inicial.

Una vez resuelta la consulta/petición por parte del contratista, existe la posibilidad de reapertura dentro de las 72 horas naturales si la resolución no es correcta a criterio del Responsable de Servicio. En este caso, el contador de tiempos para el cálculo de los ANS se reactivará desde el punto en el que se paró, contabilizando el tiempo desde la reapertura hasta la nueva resolución.

5.7.4.2. Condiciones de medida

El horario que aplica al cálculo de los tiempos de respuesta y resolución de consultas y peticiones será de 12x5 en días laborables, orientativamente con inicio a las 7:00 AM sin perjuicio de reajuste por parte del Responsable de Servicio.

Se entiende por días laborables los comprendidos de lunes a viernes, quedando excluidos los festivos nacionales y autonómicos andaluces.

Para las consultas y peticiones definidas con prioridad 0, el horario a aplicar es de 24x7.

Se considera que han cumplido los acuerdos de entrega siempre que se cumplan por parte del adjudicatario los plazos comprometidos y se tramiten conforme a los procedimientos en vigor establecidos por el Responsable de Servicio. Estos estarán claramente recogidos en los sistemas de gestión que determine el Responsable de Servicio. Será responsabilidad del adjudicatario velar por la adecuada actualización de los estados en el sistema mediante los procedimientos en vigor.

5.7.4.3. Compromisos

5.7.4.3.1. ANS DIRECTOS

Consultas / Peticiones: se considerará incumplido cuando se supere el límite del compromiso de Tiempo de Consulta/Provisión.

El adjudicatario se comprometerá a cumplir determinados niveles de calidad para la respuesta ante consultas y peticiones.

La prioridad vendrá determinada por un factor de prioridad conforme a su naturaleza según la clasificación expuesta al inicio del presente apartado.

Se muestran a continuación los valores exigidos en la siguiente tabla de compromisos:

ANS	Prioridad	Indicador	

		Tiempo de Respuesta de Consultas /Peticiones (horas)	Tiempo de Resolución de Consultas /Peticiones (horas)	Tiempo de Consulta / Provisión (horas)	Horario
Peticiones	0	0,5	3,5	4	24x7
	1	1	7	8	12x5
Consultas	0	1	7	8	24x7
	1	1	11	12	12x5

Se considerará que existe incumplimiento cuando se supere el límite del compromiso de Tiempo de Consulta / Provisión según el horario de servicio indicado.

5.7.4.3.2. ANS INDIRECTOS

Cumplimiento Atención a Consultas (CC):

ANS	Prioridad	Compromiso CC (CCC)
Cumplimiento Atención a Consultas (CC)	0	>= 95%
	1	>= 90%

Cumplimiento Atención a Peticiones (CP):

ANS	Prioridad	Compromiso CP (CCP)
Cumplimiento Atención a Peticiones (CP)	0	>= 95%
	1	>= 90%

5.7.5. ANS Gestión de incidentes de ciberseguridad

En este apartado se definen los parámetros de nivel de servicio relativos a la atención y resolución de incidencias procedentes de alertas de seguridad, sea cual sea el modo de recepción de las mismas

(plataforma de monitorización centralizada, otras consolas de la Junta de Andalucía, herramientas del CCN, Red Nacional de SOCs u otras).

5.7.5.1. Definición y cálculo de métricas

En todos los casos, se medirá la atención con el tiempo de respuesta, y la resolución con el tiempo de resolución. Estos parámetros quedan definidos como sigue:

- **Tiempo de Respuesta:** Tiempo transcurrido desde la notificación realizada en sistemas (ya sea de manera reactiva por el Responsable de Servicio, o de forma proactiva por el adjudicatario) hasta el envío por parte del adjudicatario de la aceptación de la incidencia indicando el primer diagnóstico en el sistema de tickets en vigor.

$$Tiempoderespuesta = Horadeaceptación - Horadenotificacióndelaincidencia - ParadasdeReloj$$

- **Tiempo de Resolución:** Tiempo transcurrido desde que se acepta la incidencia hasta que la incidencia queda resuelta por parte del adjudicatario. Se calcula de la siguiente forma:

$$Tiempoderesolución = Horaderesolución - Horadeaceptación - ParadasdeReloj$$

- **Tiempo de Reparación:** es el tiempo suma del tiempo de respuesta y del tiempo de resolución:

$$TiempodeReparación = TiempodeRespuesta + TiempodeResolución$$

Una vez resuelta la incidencia por parte del operador y verificada por el Responsable de Servicio, existe la posibilidad de reapertura dentro de las 72 horas naturales si el incidente se reproduce. En este caso, el contador de tiempos para el cálculo de los ANS se reactivará desde el punto en el que se paró, contabilizando el tiempo desde la reapertura hasta la nueva resolución.

Los siguientes indicadores se emplearán para la evaluación del servicio y estarán sujetos a ANS:

- **Indicador de Reapertura de Incidencias (IRAA)**: Cuenta el número de veces que se reabre una incidencia en las 72 horas naturales siguientes a la resolución por parte del contratista/adjudicatario; esto estará provocado, entre otras causas, por una reiteración de la incidencia, persistencia de la misma o no conformidad.
- **Tiempo de entrega de Informe de Resolución de incidencia (TEA)**: Se define como el tiempo que transcurre desde que se **solicita el informe**, una vez resuelta la incidencia, hasta que el adjudicatario realiza la entrega del Informe de Resolución de Incidencia al Responsable del Servicio. En dicho informe se detallarán las causas de la incidencia, las acciones llevadas a cabo para la resolución de la misma, medidas preventivas adoptadas, las conclusiones y las posibles acciones de mejora. Estos informes se solicitarán y se entregarán bajo demanda del Responsable de Servicio. Se establece un ANS para la entrega de informes en función de la criticidad de la misma.

Las medidas se realizan sobre el universo de incidencias que pasan por el adjudicatario (**NIIOA**), es decir, por todas aquellas incidencias que se han asignado al adjudicatario en este contrato: aceptadas, no aceptadas, resueltas o no resueltas independientemente de la causa u origen de la incidencia. En este universo **NIIOA**, se contabilizarán como incidencias incumplidas (**NIIIA**) aquellas en las que se ha sobrepasado bien el tiempo de respuesta, bien el tiempo de resolución, o ambos. En este universo **NIIOA**, se contabilizarán como incidencias cerradas (**N**) aquellas en estado "cerrado" en el Sistema Integrado de Operación en vigor que determine el Responsable del Servicio.

Los tiempos de respuesta y/o resolución en caso de reapertura de incidencias serán acumulativos hasta que finalmente pasen a estado "cerrado" en el Sistema Integrado de Operación en vigor que determine el Responsable del Servicio. Esto será de aplicación para cualquier tiempo identificado como nivel de servicio.

5.7.5.2. Condiciones de medida

El horario que aplica al cálculo de los tiempos de respuesta, resolución de incidencias, reparación y entrega de informes será de **24x7**, alineado con el horario de prestación del servicio.

En el cálculo de los parámetros anteriormente definidos no se considerará el tiempo transcurrido en los siguientes casos, siempre y cuando sean debidamente justificados y recogidos en el sistema de gestión de incidencias y peticiones:

- Tiempos de no disponibilidad debidos a la imposibilidad de reposición del servicio por motivos no imputables a los adjudicatarios (p.ej. Inaccesibilidad de las instalaciones en caso de requerirse visita).
- Pérdidas de servicio debidas a causas de fuerza mayor (desastre natural) ajenas a la responsabilidad del adjudicatario.

Al tratarse de una solución en nube no se consideran excluidas del cómputo las paradas programadas, es decir, las labores de mantenimiento que apliquen sobre la solución en nube no pueden traducirse en una indisponibilidad del servicio.

Será responsabilidad del adjudicatario velar por la adecuada actualización de los estados en el sistema de tickets y reporte de incidencias.

Las incidencias se priorizarán de acuerdo a su peligrosidad, y se podrán recategorizar por el Responsable de Servicio. La peligrosidad estará determinada según la clasificación de la guía CCN-STIC 817 (Gestión de Ciberincidentes) del CCN-CERT.

A efectos de seguimiento de ANS, se establecen cuatro niveles de peligrosidad, de 0 a 3, siendo 0 el más exigente en cuanto a respuesta, resolución y reparación, y el 3 el menos exigente. Estos niveles se corresponden con los descritos en la guía CCN-STIC 817 de la siguiente forma:

- Peligrosidad “0”: niveles de peligrosidad 5 (CRÍTICO) o 4 (MUY ALTO) de CCN-STIC 817
- Peligrosidad “1”: nivel de peligrosidad 3 (ALTO) de CCN-STIC 817
- Peligrosidad “2”: nivel de peligrosidad 2 (MEDIO) de CCN-STIC 817
- Peligrosidad “3”: nivel de peligrosidad 1 (BAJO) de CCN-STIC 817

5.7.5.3. Compromisos

Se considerará que existe incumplimiento cuando se superen los valores de compromiso detallados en los siguientes apartados.

5.7.5.3.1. ANS DIRECTOS

Incidencias: se considerará incumplido cuando se supere el límite del compromiso de Tiempo de Reparación.

ANS	Peligrosidad	Indicador		
		Tiempo de Respuesta	**Tiempo de Resolución**	**Tiempo de Reparación**
Incidencias	0	30 min	180 min	210 min
	1	45 min	270 min	315 min
	2	90 min	540 min	630 min
	3	120 min	600 min	720 min

Compromisos Incidencias

VAL-ANS-4: Se valorará el valor comprometido de este ANS por encima del mínimo aquí indicado. (SOBRE 3, NO INCLUIR EN SOBRE 2).

- **Informes de Incidencias alertas**: se considerará incumplido si la entrega supera el compromiso de tiempo establecido.

ANS	Peligrosidad	Indicador
		Tiempo de Entrega

Informe de Incidencias	0	480 min
	1	1080 min
	2	1440 min
	3	2880 min

Compromisos Informes Incidencias

VAL-ANS-5: Se valorará el valor comprometido de este ANS por encima del mínimo aquí indicado. (SOBRE 3, NO INCLUIR EN SOBRE 2).

5.7.5.3.2. ANS INDIRECTOS

- **Cumplimiento en Tratamiento de Incidencias (CTIIA):** es el porcentaje total (100%) menos el porcentaje de incidencias incumplidas respecto del total de incidencias del contrato más 20. Se determina mediante la fórmula siguiente:

ANS	Fórmula	Compromiso CTIIA (CCTIIA)
Cumplimiento en Tratamiento de Incidencias (CTIIA)	$CTIIA = 100 - \left(\frac{NIIIA}{(NIIOA + 20)} \right) * 10$	≥ 95%

- **Cumplimiento de Reapertura de Incidencias (CRAA)**: es el porcentaje total (100%) menos el porcentaje del número de veces que se reabre una incidencia (IRA) respecto del total de incidencias cerradas del contrato (N) más 10. Se determina mediante la fórmula siguiente:

ANS	Fórmula	Compromiso CRAA (CCRAA)
Cumplimiento de Reapertura de Incidencias (CRAA)	$CRAA = 100 - \left(\frac{\sum IRAA}{(N + 10)} \right) * 100$	≥ 90%

5.7.6. ANS Servicio de guardia

En este apartado se definen los parámetros de nivel de servicio relativos al servicio de guardia contemplado en el presente lote.

Se establece el tiempo máximo de respuesta a incidencias en 30 minutos, así como el tiempo máximo de asistencia a instalaciones en 1 horas.

5.7.6.1. Compromisos

Se considerará que existe incumplimiento cuando se supere alguno de los límites de valores de compromiso.

5.7.7. ANS Entrega de informes periódicos y singulares

En este apartado se definen los parámetros de nivel de servicio relativos a la entrega de informes singulares y periódicos como los que se citan a continuación.

Quedan excluidos en este apartado los Informes de resolución de incidencias tratados en los apartados anteriores.

Este apartado trata de:

- **Informes singulares**: Informes especiales o a demanda, siendo en este caso solicitados por el Responsable de Servicio.
- **Informes periódicos**: Con objeto de que el Responsable de Servicio pueda llevar a cabo el oportuno seguimiento de los niveles de calidad, el adjudicatario del servicio suministrará los informes que determine el Responsable de Servicio en el ámbito de los Comités correspondientes; el formato y contenido de estos informes quedará fijado por el Responsable de Servicio.

5.7.7.1. Definición y cálculo de métricas

Como parámetros de medida de la calidad de servicio se tomarán los siguientes:

- **Tiempo de Entrega del Informe (TEI)**: Tiempo transcurrido desde la solicitud del informe has-ta la entrega validada de dicho informe por el adjudicatario.

TEI= Hora validación informe - Hora solicitud informe

5.7.7.2. Condiciones de medida

El horario que aplica al cálculo de los tiempos de respuesta y provisión de consultas y peticiones será de 12x5 en días laborables.

Se entiende por días laborables los comprendidos de lunes a viernes, quedando excluidos los festivos nacionales y autonómicos andaluces.

Para la entrega de los informes no computarán en la contabilización del Tiempo de Entrega del Informe (TEI) los tiempos de retardo debidos a la imposibilidad de la entrega en los sistemas habilitados por el Responsable de Servicio, por motivos no imputables al adjudicatario, siempre y cuando, sean debidamente justificados de acuerdo con los procedimientos en vigor establecidos por el Responsable de Servicio. Estos estarán claramente recogidos en los sistemas de gestión que determine el Responsable de Servicio. Será responsabilidad del adjudicatario informar de las incidencias objeto de dicho retraso para que puedan ser debidamente tenidas en cuenta.

Se considera que han cumplido los acuerdos de entrega siempre que se cumplan por parte del adjudicatario los plazos comprometidos y se tramiten conforme a los procedimientos en vigor establecidos por el Responsable de Servicio. Será responsabilidad del adjudicatario velar por la adecuada actualización de los estados en el sistema mediante los procedimientos en vigor.

5.7.7.3. Compromisos

Compromiso de entrega de informes:

INFORMES SINGULARES	COMPROMISO Tiempo de Entrega del (TEIC)
Plan Técnico de Despliegue referido en el apartado “Fase I: Definición del despliegue”.	2 semanas (10 días hábiles) a contar desde la fecha de formalización del contrato
Informe singular de actividad y hallazgos según apartado “Servicio avanzado de la plataforma de monitorización”	3 días a contar desde el momento en que el responsable de Servicio realiza la petición
Informe de incidente de especial relevancia según apartado “Entregables asociados al servicio de respuesta a incidentes”.	3 días a contar desde el momento de la detección de un incidente
Informe de estadísticas acumuladas según apartado “Entregables asociados al servicio de respuesta a incidentes”.	7 días a contar desde el momento en que el responsable de Servicio realiza la petición
Informe de transferencia del servicio referido en el apartado “Fase IX: Transición del servicio” y “Transición del servicio a la finalización del contrato”.	Este informe se entregará con fecha tope al inicio del penúltimo mes de la contratación, es decir, dos meses antes de su finalización.

INFORMES SINGULARES	COMPROMISO Tiempo de Entrega del (TEIC)
Informe final de estadísticas según apartado "Entregables asociados al servicio de respuesta a incidentes".	En el momento de finalizar el contrato y de sus posibles prórrogas

INFORMES PERIÓDICOS	COMPROMISO	PERIODICIDAD
Informe de actividad mensual donde se describan con detalle las actividades llevadas a cabo en cada uno de los servicios de soporte asociado según se indica en los apartados "Servicios asociados" y "Entregables".	Antes del 10º día natural del mes.	Mensual
Informe anual asociado al servicio de respuesta a incidentes según el apartado "Entregables asociados al servicio de respuesta a incidentes".	Primera quincena de cada año natural	Anual
Detalle de **Cumplimiento ANS**	Antes del 5º día laboral del mes.	Mensual

6. Lote 2: Servicios recurrentes y bajo demanda para apoyo al Centro de Operaciones de Seguridad de la Junta de Andalucía (AndalucíaCERT)

6.1. Objeto

El objeto de este lote es dotar a AndalucíaCERT de servicios recurrentes y bajo demanda que den soporte a su Catálogo de Servicios.

Las finalidades que se buscan con la contratación de estos servicios son las siguientes:

1. Permitir una evaluación y un diagnóstico global del estado técnico de la ciberseguridad en los organismos y entidades que forman parte del ámbito de actuación de AndalucíaCERT.
2. Permitir una actuación proactiva en materia de toma de medidas preventivas.
3. Permitir una detección temprana de las vulnerabilidades que pudieran presentar los sistemas y las aplicaciones.

4. Permitir una respuesta rápida ante incidentes de ciberseguridad.
5. Permitir una investigación eficaz de los incidentes de ciberseguridad.
6. Permitir el crecimiento del ámbito de actuación y de los servicios de AndalucíaCERT mediante un sistema escalable, adaptable y con alto grado de operatividad.

Si, durante la vigencia del contrato y sus posibles prórrogas, AndalucíaCERT cambiara de denominación o alguna de sus funciones relacionadas con el objeto del presente lote fueran asumidas por otro organismo o entidad, las menciones a AndalucíaCERT contenidas en este documento deberán considerarse como referidas a la nueva denominación o al organismo o entidad que asuma dichas funciones.

El presente lote estará compuesto por los siguientes elementos:

1. Servicio de alerta temprana y consultoría sobre vulnerabilidades.
2. Servicio de análisis de la superficie de exposición en Internet.
3. Servicio de análisis de vulnerabilidades.
4. Servicio de vigilancia digital e inteligencia de amenazas.
5. Servicio de análisis forense.
    - Subservicio de peritaje informático.
    - Subservicio de análisis DFIR.
6. Servicio de obtención, certificación y preservación de evidencias digitales.
7. Servicio de elaboración de informes técnicos.
8. Servicio de análisis de malware.
9. Servicio de realización de ciberejercicios.
10. Servicio de proyectos en protección, detección y respuesta.
11. Servicio de intervención especializada.

Salvo cuando se indique expresamente otra cosa en el presente documento, el ámbito de aplicación de los servicios incluidos en este lote será la Administración de la Junta de Andalucía y sus entidades instrumentales, así como los consorcios a los que se refiere el artículo 12.3 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía. Esto supone aproximadamente 85 organismos que forman el grupo atendido principal de AndalucíaCERT. Este ámbito podría ampliarse en base a convenios de colaboración con otras entidades.

Salvo cuando de indique expresamente otra cosa, toda mención a marcas y productos en el presente documento debe entenderse como realizada con carácter meramente orientativo o informativo.

Las mejoras y características adicionales no eximirán del cumplimiento de todos y cada uno de los requisitos establecidos en este Pliego de Prescripciones Técnicas.

La documentación mínima a entregar, de carácter general y específica de cada servicio, se encuentra descrita en el apartado “Entregables”.

Las ofertas deberán incluir, para cada servicio incluido en el presente lote:

- Enumeración de las herramientas principales y de apoyo que utilizará para ofrecer el servicio con indicación, cuando proceda, de sus versiones o modalidades de uso.
- Arquitectura software con la que se ofrecerá el servicio.
- Otros recursos que utilizará para prestar el servicio.
- Propuesta de procedimiento para la prestación del servicio. En todo caso, corresponderá a la persona responsable del contrato la aceptación o modificación, total o parcial, de la propuesta realizada.

Asimismo, las ofertas deberán incluir una descripción de las relaciones que se establecerán entre los distintos servicios del lote y detallar los mecanismos que se establecerán para consolidar de manera efectiva y aplicable la información obtenida de todos ellos.

Siempre que sea posible y adecuado para una prestación óptima de los servicios, el adjudicatario podrá utilizar una misma herramienta para ofrecer todos o varios de los servicios incluidos en el presente Lote.

6.2. Servicios recurrentes

VAL-SVREC-1: Se valorará con carácter general la idoneidad, calidad y flexibilidad de la arquitectura de los servicios recurrentes propuestos y cómo estos dan cumplimiento a los requisitos enumerados (SOBRE 2).

6.2.1. Servicio de Alerta temprana y asesoramiento sobre vulnerabilidades

6.2.1.1. Descripción

El objetivo de este servicio es:

- Identificar las vulnerabilidades a las que están expuestas las diferentes plataformas que sustentan los sistemas de información y la infraestructura TIC de los organismos y las entidades que forman parte del ámbito de actuación de AndalucíaCERT.
- Analizar la evolución de estas vulnerabilidades.
- Proporcionar información que permita minimizar los riesgos asociados a las vulnerabilidades encontradas.

Para ello se definen dos componentes:

- Plataforma de inventariado, contraste y alerta de vulnerabilidades.
- Consultoría y asesoramiento sobre vulnerabilidades.

6.2.1.1.1. Plataforma de inventariado, contraste y alerta de vulnerabilidades

REQ-ATV-1: Será un servicio prestado de manera no intrusiva que se basará en una herramienta puesta por el adjudicatario a disposición de la Junta de Andalucía y que se acompañará en su caso del equipamiento y servicios necesarios para constituir una plataforma de inventariado, contraste y alerta de vulnerabilidades que será denominada en este apartado "la Plataforma".

REQ-ATV-2: Dicha herramienta deberá ofrecer soporte para multitenant, permitiendo crear un entorno independiente para cada organismo del Grupo Atendido de AndalucíaCERT. El número inicial de tenants se estima en 85, debiendo garantizarse el correcto funcionamiento de esta Plataforma para al menos 120.

REQ-ATV-3: Deberá ser posible crear como mínimo los dos tipos de cuentas siguientes:

- Cuentas con acceso a solo uno de los entornos (tenant) definidos y la información contenida en este, para su uso por el correspondiente organismo. Para cada entorno deberá ser posible crear como mínimo 3 cuentas de este tipo.
- Cuentas con acceso a todos los entornos definidos, para permitir realizar una gestión global centralizada. Deberá ser posible crear como mínimo cinco cuentas de este tipo.

REQ-ATV-4: Cada tenant deberá disponer de mecanismos que le permitan la introducción y el almacenamiento de la información detallada de inventario de todos los productos TIC del correspondiente organismo, incluyendo empresa fabricante o desarrolladora, nombre de producto, modelos, versiones y otros datos relevantes, incluyendo identificación *Common Platform Enumeration* (CPE). Estos mecanismos deberán garantizar la posibilidad de introducir la mencionada información de todas las siguientes formas:

- Masiva, a partir de un fichero en formato normalizado (por ejemplo, CSV).
- Interactiva, para realizar altas, bajas y modificaciones.

En caso de que las herramientas utilizadas no proporcionaran alguna de estas funcionalidades, esta carencia deberá ser suplida por el adjudicatario, que deberá:

- Poner un sistema de realización de peticiones de servicio a disposición de AndalucíaCERT y de los organismos de su grupo atendido y mediante el cual se realizarán las peticiones de altas, bajas y modificaciones conforme a un modelo normalizado de petición, cuando esta afecte a un único activo, o a un formato normalizado de archivo, en otro caso.
- Atender las peticiones de servicio, llevando a cabo las operaciones solicitadas, conforme a los acuerdos de nivel de servicio y con sujeción a las posibles penalizaciones establecidas en la documentación de la presente licitación y en la oferta presentada.

REQ-ATV-5: Por otro lado, la herramienta recogerá de forma continuada información relevante de seguridad de diversas fuentes nacionales e internacionales, tanto gratuitas como de pago, integrándola en una base de datos completa y actualizada de vulnerabilidades.

REQ-ATV-6: La herramienta realizará de forma automática y desatendida la confrontación de la información de inventario de activos con la almacenada en la base de datos de vulnerabilidades, produciendo una relación de posibles vulnerabilidades aplicables al organismo. En esta relación deberá constar:

- La identificación y descripción de la vulnerabilidad.
- La relevancia de la vulnerabilidad según las plataformas, fabricantes y, en su caso, contexto particular de los Organismos de la Junta de Andalucía, con objeto de permitir establecer prioridades en el proceso de remediación.

REQ-ATV-7: La plataforma se limitará a identificar de manera pasiva las vulnerabilidades que pudieran mostrar los activos/productos en función de los datos e información que los caracterizan (fabricante, modelo, versión, etc) que consten en el inventario. Debe observarse que estas características, si bien pudieran guardar algún parecido, no son las propias de un escáner de vulnerabilidades, puesto que no se realizarán análisis sustentados en escaneos de las vulnerabilidades sobre los activos TI concretos. Por idénticos motivos, también queda alejada de gestores de vulnerabilidades para activos TI concretos. No se admitirán este tipo de productos si carecen de las capacidades descritas para la identificación automática y pasiva de vulnerabilidades según la información del inventario.

REQ-ATV-8: Para cada cuenta, la herramienta deberá permitir definir alertas automáticas que notifiquen de forma automática las posibles vulnerabilidades detectadas en los activos pertenecientes a su tenant a los que se haya suscrito o haya sido asignado. Estas alertas contendrán como mínimo la siguiente información:

- La identificación y descripción de la vulnerabilidad
- La relevancia de la vulnerabilidad y sus indicadores de riesgo asociado.
- Si se ha desarrollado una prueba de concepto que explote la vulnerabilidad. En este caso, se deberá ofrecer, de forma directa o indirecta, una referencia al menos a una de estas pruebas de concepto que tenga carácter representativo.
- Si se ha detectado que la vulnerabilidad está siendo explotada de forma activa.
- Información para eliminar la vulnerabilidad o reducir su impacto.

REQ-ATV-9: La información sobre posibles vulnerabilidades existentes en los activos de cada tenant, así como la de todos los tenant para las cuentas con acceso a todo el conjunto, deberá ofrecerse a través de un servicio de publicación web en el que apliquen las medidas necesarias para garantizar la seguridad del propio servicio y de los datos almacenados.

Correrán por cuenta del adjudicatario todos los gastos derivados de los servicios y productos software, así como del hardware y otro equipamiento incluido en la oferta, que sean necesarios para el funcionamiento de la Plataforma.

Las ofertas deberán indicar una relación del hardware que AndalucíaCERT y su grupo atendido debe proveer, si es necesario éste, para el funcionamiento de la Plataforma, con indicación pormenorizada de los requisitos que cada elemento debe cumplir. Todo hardware que no sea incluido expresamente en esta relación o que no se atenga a los requisitos indicados deberá ser proporcionado por el adjudicatario sin que pueda imputar coste alguno por él.

6.2.1.1.2. Consultoría y asesoramiento sobre vulnerabilidades

REQ-ATV-10: Este componente del servicio se integrará con la plataforma del punto anterior, y el adjudicatario planteará un dimensionamiento (FTE) que dedicará al mismo en cada momento.

REQ-ATV-11: El equipo de trabajo asociado a este componente deberá acumular conocimiento sobre AndalucíaCERT y su grupo atendido durante la prestación del servicio y aplicar este conocimiento para adecuar la información proporcionada por la plataforma de inventariado, contraste y análisis de vulnerabilidades a las necesidades de este organismo y su grupo atendido, así como complementarla con conocimiento experto.

REQ-ATV-12: La consultoría y asesoramiento sobre vulnerabilidades incluirá:

- Análisis del impacto de las vulnerabilidades de acuerdo con las características de los sistemas y del entorno de cada organismo y de la Junta de Andalucía.
- En su caso, actualización de la información contenida en la Plataforma de inventariado, contraste y análisis de vulnerabilidades. En particular, se realizará esta actualización de acuerdo con el análisis de impacto a que hace referencia el punto anterior.
- Identificación de vulnerabilidades recientes de impacto potencial alto.
- Propuesta de prioridades en las actuaciones necesarias para la eliminación o minimización del riesgo asociado a las vulnerabilidades.
- Entrega de información, documentos y URLs de referencia relativos a los cambios sobre los activos que sea necesario realizar para eliminar o minimizar el riesgo asociado a las vulnerabilidades.

REQ-ATV-13: Con carácter general, el adjudicatario ofrecerá estos servicios de consultoría y asesoramiento de forma proactiva, prestando especial atención a las circunstancias en que su personal determine que una o varias vulnerabilidades pudieran tener un impacto significativo sobre los activos monitorizados en el ámbito de este contrato. La persona responsable del servicio podrá establecer condiciones concretas en las que se deberá aplicar este punto, sin perjuicio de las situaciones en que el adjudicatario lo considere oportuno a iniciativa propia.

REQ-ATV-14: Cuando el responsable del servicio lo estime necesario, podrá remitir una consulta a la persona de contacto para este servicio con objeto de requerir el tratamiento de vulnerabilidades o circunstancias concretas.

Tanto las consultas relacionadas con este servicio como el soporte ofrecido a los organismos se realizarán a través de AndalucíaCERT, que actuará en todo caso de intermediario entre su grupo atendido y el adjudicatario.

REQ-ATV-15: El adjudicatario remitirá cada mes un informe de potenciales vulnerabilidades detectadas a cada uno de los organismos o tenants, así como un informe global a AndalucíaCERT. Se le proporcionará al adjudicatario la información de contacto necesaria para la remisión a cada tenant u organismo.

En caso de que la información de contacto proporcionada no fuera suficiente para hacer llegar el informe a algún organismo o tenant, el adjudicatario lo hará llegar a AndalucíaCERT, indicando las causas que hicieron imposible la entrega a su destinatario.

6.2.1.2. Condiciones de prestación

El adjudicatario deberá realizar las siguientes tareas en relación con las herramientas, productos y servicios en que se base la prestación de este servicio:

- Cuando sea necesario, instalación y/o despliegue, configuración y puesta en marcha.
- Cuando sea necesario, reinstalación y/o redespliegue y reconfiguración para garantizar la continuidad del servicio.
- Actualización continua de fuentes de información sobre vulnerabilidades.
- Monitorización, comprobando en todo momento su correcto funcionamiento.
- Mantenimiento, asegurando en todo momento su correcto funcionamiento y que se cuenta con versiones actualizadas.
- Soporte, resolviendo las incidencias que pudieran producirse en su uso o en su funcionamiento, incluyendo aquellas que pudieran requerir un nuevo despliegue total o parcial.

El adjudicatario deberá garantizar la disponibilidad de la plataforma en régimen de 24x7.

La consultoría y asesoramiento sobre vulnerabilidades será ofrecida de forma deslocalizada en modalidad 8x5.

Se considerará un número base de tecnologías a monitorizar de 150 como mínimo.

VAL-ATV-1: Se valorará el incremento de este dimensionamiento base (SOBRE 3, no incluir en sobre 2).

6.2.1.3. Elementos y Dimensionado

ELEM-ATV-BASE: Mensualidad del servicio.

ELEM-ATV-AMPLIACION: Incremento de un 10% del elemento base, con el correspondiente incremento de capacidad (activos/tecnologías a monitorizar, esfuerzo dedicado al servicio...). Bajo demanda, acumulable (se pueden requerir dos, para ampliar un 20% la capacidad, por ejemplo).

6.2.2. Servicio de Análisis de la Superficie de Exposición en Internet

6.2.2.1. Descripción

REQ-ASE-1: El servicio consistirá en la identificación de los servicios pertenecientes a AndalucíaCERT y los organismos que forman su grupo atendido que se encuentren expuestos a Internet, así como en el asesoramiento para la reducción de la superficie de exposición que permita mitigar el riesgo de posibles ataques durante todo el tiempo de vigencia del contrato y sus posibles prórrogas.

El servicio deberá ser prestado por el adjudicatario de forma deslocalizada utilizando sus propias infraestructuras o las que tenga contratadas o subscritas, así como las herramientas y los servicios gratuitos de que disponga.

REQ-ASE-2: Como requisito mínimo, el adjudicatario utilizará escáneres con los que realizará sondeos periódicos de los activos publicados en Internet. Durante estos sondeos, basados en el direccionamiento IP, se realizará el descubrimiento, la enumeración, la identificación y la caracterización de servicios publicados.

REQ-ASE-3: Los medios por los que se realice la identificación y caracterización de servicios incluirán como mínimo el análisis de la información proporcionada por las cabeceras (banners) de los diferentes servicios.

REQ-ASE-4: Los accesos a Internet y los servicios y escáneres utilizados deberán estar adecuadamente dimensionados tanto a nivel de hardware como de licenciamiento de uso para cubrir las necesidades derivadas del espacio de direcciones a monitorizar.

REQ-ASE-5: El adjudicatario designará una persona de referencia para este subservicio y proporcionará sus datos de contacto a la persona responsable del servicio conforme a lo indicado en el apartado “7. Organización del trabajo”. Esta persona y, en su caso, el resto del equipo de trabajo asociado a este servicio deberá acumular conocimiento sobre AndalucíaCERT y su grupo atendido durante la prestación del servicio y aplicar este conocimiento para:

- Proporcionar una interpretación de los datos obtenidos conforme a las necesidades y características de AndalucíaCERT y de los organismos que forman su grupo atendido.
- Complementar y contrastar la información obtenida con la producida por el servicio de Alerta Temprana de Vulnerabilidades.
- Realizar o proponer actualizaciones de la información obtenida en la Plataforma de Inventariado, Contraste y Análisis de Vulnerabilidades en razón de lo identificado mediante este servicio de Análisis de la Superficie de Exposición.

- Proponer la realización de análisis de activos más completos y profundos, en el marco del servicio de Análisis de Vulnerabilidades, según lo identificado a través de este servicio de Análisis de la Superficie de Exposición.
- Realizar recomendaciones para la reducción de la superficie de exposición y para la eliminación o mitigación de los riesgos que esta pueda suponer.

REQ-ASE-6: Los resultados de los análisis, enriquecidos con la información proporcionada por el personal asignado al servicio, serán presentados mediante informes periódicos, conforme a lo establecido en el apartado “Entregables del Servicio de Análisis de la Superficie de Exposición en Internet”.

REQ-ASE-7: Adicionalmente, se pondrá a disposición de AndalucíaCERT el hospedaje de dos máquinas virtuales en la nube para labores de verificaciones y pruebas de la superficie de exposición. Para evitar suspensiones del servicio, el adjudicatario gestionará con el proveedor de alojamiento de dichas máquinas virtuales las autorizaciones para la realización de pruebas contra el rango de direccionamiento objeto del servicio. Cada una de estas máquinas virtuales en la nube deberá satisfacer los siguientes requisitos mínimos:

Número de CPUs virtuales	2
Memoria RAM	4 GB
Capacidad de almacenamiento en discos virtuales	64 GB
Compatibilidad con sistemas	Linux y Windows

El adjudicatario deberá desplegar en estas máquinas virtuales el sistema operativo y el software necesario para su funcionamiento y para realizar las operaciones de análisis.

Las máquinas dispondrán de dirección IP pública estática asignada y todos los puertos de entrada y salida abiertos (sin restricciones en ese sentido). Contarán con conexión a red mínimo 100 Mbps y tráfico entrada/salida ilimitado.

6.2.2.2. Condiciones de prestación

El servicio será prestado de forma deslocalizada.

A título informativo y a efectos de estimar las necesidades iniciales del servicio indicamos que el direccionamiento está compuesto por 4.096 direcciones IP públicas. Actualmente, de ellas hay activas unas 1.000. Se estima, en general, un número de activos a monitorizar por el servicio base de 1500 como mínimo.

VAL-ASE-1: Se valorará el incremento de este dimensionamiento base (SOBRE 3, no incluir en sobre 2).

Toda ampliación del número de direcciones IP públicas deberá ser comunicada al adjudicatario por la persona responsable del contrato con al menos 5 días laborables de antelación.

6.2.2.3. Elementos y Dimensionado

ELEM-ASE-BASE: Mensualidad del servicio.

ELEM-ASE-AMPLIACION: Incremento de un 10% del elemento base, con el correspondiente incremento de capacidad (activos a monitorizar, esfuerzo dedicado al servicio...). Bajo demanda, acumulable (se pueden requerir dos, para ampliar un 20% la capacidad, por ejemplo).

6.2.3. Servicio de Análisis de vulnerabilidades

6.2.3.1. Descripción

Este servicio proporcionará las capacidades técnicas necesarias para el descubrimiento y análisis de vulnerabilidades en las infraestructuras TIC, aplicaciones y servicios de la Junta de Andalucía. Para ello se definen los siguientes subservicios:

- Desatendido de análisis de vulnerabilidades web
- Atendido de análisis de vulnerabilidades
    - Periódico
    - A demanda

6.2.3.2. Subservicio desatendido de análisis de vulnerabilidades web

6.2.3.2.1. Descripción

REQ-AVDESAT-1: El adjudicatario pondrá a disposición de AndalucíaCERT y de los organismos integrantes de su grupo atendido una plataforma de análisis de vulnerabilidades web, con objeto de que puedan analizar sus aplicaciones y servicios web de manera autónoma.

REQ-AVDESAT-2: La plataforma de análisis desatendido de vulnerabilidades web será implementada sobre la infraestructura de virtualización de la que dispone AndalucíaCERT y estará basada en herramientas de seguridad de tipo proxy, opensource (como, por ejemplo, OWASP Zed Attack Proxy o Burp Suite CE) y/o comerciales (por ejemplo, Burp Suite Enterprise) así como en otros tipos de software.

Las ofertas deberán indicar una relación del hardware que AndalucíaCERT y su grupo atendido debe proveer para el funcionamiento de este subservicio, con indicación pormenorizada de los requisitos que cada elemento debe cumplir. Todo hardware que fuera necesario durante la prestación del servicio que no

sea incluido expresamente en esta relación o que no se atenga a los requisitos indicados deberá ser proporcionado por el adjudicatario sin que pueda imputar coste alguno por él.

REQ-AVDESAT-3: Correrá por cuenta del adjudicatario el despliegue, mantenimiento y gestión de dicha plataforma como recurso compartido de los Organismos integrantes del Grupo Atendido, de acuerdo con las directrices e instrucciones recibidas desde AndalucíaCERT, con especial atención al mecanismo de arbitraje/reserva del mismo.

6.2.3.2.2. Condiciones de prestación

El adjudicatario deberá realizar las siguientes tareas en relación con la plataforma de análisis desatendido de vulnerabilidades web:

- Cuando sea necesario, instalación y/o despliegue, configuración y puesta en marcha.
- Cuando sea necesario, reinstalación y/o redespliegue y reconfiguración para garantizar la continuidad del servicio.
- Mantenimiento, asegurando en todo momento su correcto funcionamiento y actualización.
- Soporte, resolviendo las incidencias que pudieran producirse en su uso o en su funcionamiento, incluyendo aquellas que pudieran requerir un nuevo despliegue total o parcial.
- Gestión del arbitraje y de las reservas de uso de la plataforma de análisis desatendido de vulnerabilidades web para garantizar una adecuada asignación del recurso conforme a las solicitudes de uso de este.

El adjudicatario deberá garantizar la disponibilidad de la plataforma de análisis desatendido de vulnerabilidades web en régimen de 8x5.

La gestión de la plataforma de análisis de vulnerabilidades web se realizará en modalidad 8x5.

Se instalará un mínimo de 1 plataforma de análisis de vulnerabilidades web.

VAL-AVDESAT-1: Se valorará el incremento de este dimensionamiento base (SOBRE 3, no incluir en sobre 2).

6.2.3.2.3. Elementos y Dimensionado

ELEM-AVDESAT-BASE: Mensualidad del servicio.

ELEM-AVDESAT-AMPLIACION: Incremento de un 10% del elemento base, con el correspondiente incremento de capacidad (plataformas, esfuerzo dedicado al servicio...). Bajo demanda, acumulable (se pueden requerir dos, para ampliar un 20% la capacidad, por ejemplo).

6.2.3.3. Subservicio atendido de análisis de vulnerabilidades

6.2.3.3.1. Descripción

REQ-AVULN-1: Este subservicio consistirá en la ejecución de análisis de vulnerabilidades desde plataformas de escaneo y análisis desplegadas por el adjudicatario, en dos posibles modalidades:

- Periódica - Automatizada (programada)
- Puntual - Manual (bajo demanda)

Se podrán configurar distintos procesos de análisis de vulnerabilidades, de acuerdo con sus respectivos objetivos y con las características y circunstancias de los activos involucrados. El ámbito de los análisis de vulnerabilidades incluirá, de acuerdo con la configuración que en cada caso se establezca, tanto las infraestructuras, redes y sistemas como las aplicaciones y servicios web.

De forma independiente a su modalidad, programada o bajo demanda, los análisis de vulnerabilidades pertenecerán a una de las siguientes categorías:

- Análisis de vulnerabilidades sobre un subconjunto de activos de especial interés designados por la Dirección del Proyecto entre los diversos activos revelados por el servicio de Análisis de la Superficie de Exposición a Internet, ejecutado desde la red pública utilizando las infraestructuras propiedad del adjudicatario o las que tenga contratadas o subscritas, así como las herramientas y los servicios gratuitos de que disponga.
- Análisis de vulnerabilidades en sistemas y redes ubicadas en la Red Corporativa de la Junta de Andalucía. Para ello, el licitador deberá implementar un entorno de escaneo, que será desplegado sobre la infraestructura existente en AndalucíaCERT y/o puntos y sedes de interés estratégico en la Red Corporativa de la Junta de Andalucía. La Junta de Andalucía proporcionará el hardware necesario, corriendo en todo caso por cuenta del adjudicatario el despliegue, mantenimiento, operación y explotación de las distintas herramientas.

Las ofertas deberán indicar, en su caso, una relación del hardware que AndalucíaCERT y su grupo atendido debe proveer para el funcionamiento de este subservicio, con indicación pormenorizada de los requisitos que cada elemento debe cumplir. Todo hardware que fuera necesario durante la prestación del servicio que no sea incluido expresamente en esta relación o que no se atenga a los requisitos indicados deberá ser proporcionado por el adjudicatario sin que pueda imputar coste alguno por él.

El adjudicatario proporcionará los informes obtenidos como resultado de los análisis de vulnerabilidades.

VAL-AVULN-1: Se valorará que el ofertante podrá incorporar como mejora la puesta a disposición de una plataforma de gestión de vulnerabilidades vía web (SOBRE 2). Dicha herramienta sería puesta a disposición de los organismos del grupo atendido por AndalucíaCERT siendo su función la coordinación y seguimiento del ciclo de vida de las vulnerabilidades de activos que estos decidan ahí cargar, y caso de contemplarse en la oferta:

- Podrá desplegarse sobre la infraestructura hardware propia de la Junta de Andalucía (onprem) o en nube.

- Soportará multi-tenant, con un entorno por cada Organismo del Grupo Atendido de AndalucíaCERT y, posibilidad de disponer de varios usuarios con distintos roles por cada uno. Se estima un máximo de 85 entornos/tenants.
- Permitirá la importación de ficheros de auditoría de las principales herramientas de auditoría/análisis de vulnerabilidades del mercado.
- Se encontrará disponible 24x7.

Caso de ofertarse, el adjudicatario deberá exponer sus principales características y funcionalidades, modelo de prestación del servicio, soporte asociado, y requerimientos técnicos (conectividad, recursos, …) en caso de que proponga la instalación on-premise sobre infraestructura de virtualización de AndalucíaCERT.

6.2.3.3.2. Condiciones de prestación

El servicio se prestará, atendiendo a las características de los activos objeto de análisis y de la Red Corporativa de Comunicaciones de la Junta de Andalucía, tanto de forma localizada como deslocalizada.

Modalidad "Periódica-Automatizada"

AndalucíaCERT establecerá los días y las franjas horarias en que se realizará cada análisis automático, conforme a una modalidad de prestación 24x7.

El resultado de estos análisis periódicos automatizados de vulnerabilidades sobre los activos deberán ser almacenados de manera automática tras su generación durante un plazo de retención no inferior a 1 año, ya sea en la propia plataforma de escaneo y análisis, o bien en otro repositorio en red que el ofertante ponga a disposición para tal fin.

Modalidad "Puntual-Manual"

AndalucíaCERT establecerá los días y las franjas horarias en que se realizará cada análisis puntual solicitado.

Como resultado del análisis, en esta modalidad el servicio prestado por el adjudicatario no se limitará al mero traslado a AndalucíaCERT del resultado de las herramientas automatizadas utilizadas, siendo requisito que adicionalmente genere un informe de resultados que:

- Evalúe y valide manualmente los resultados obtenidos conforme a los activos y servicios analizados y las vulnerabilidades detectadas, contextualizando en el entorno desde y hacia el que se publican los servicios en el marco de la Red Corporativa de la Junta de Andalucía.
- Incluya información sobre el impacto de las vulnerabilidades detectadas y una propuesta de priorización de las acciones de remediación a acometer.

Igualmente, el ofertante deberá prestar soporte técnico experto para la mejor comprensión del impacto de las vulnerabilidades detectadas, su priorización y la definición de plan de acción por parte de AndalucíaCERT.

6.2.3.3.3. Elementos y Dimensionado

En función de la solución a ofertar, se deberán contemplar los elementos necesarios que permitan la ejecución de las dos categorías de análisis de vulnerabilidades expuestas anteriormente, esto es, desde Internet, y desde el interior de la Red Corporativa de la Junta de Andalucía.

A título informativo, se estima una demanda en torno a 15 análisis/mes en modalidad "Puntual-Manual".

El proveedor deberá incluir en su oferta un precio básico para este subservicio que contemple, como mínimo, 6.000 direcciones IP y 70 aplicaciones web, así como el de las posibles ampliaciones que pudieran ser necesarias conforme al Catálogo de Elementos Unitarios.

VAL-AVULN -2: Se valorará el incremento de este dimensionamiento base (SOBRE 3, no incluir en sobre 2).

ELEM-AVULN-BASE: Mensualidad del servicio.

ELEM-AVULN-AMPLIACION: Incremento de un 10% del elemento base, con el correspondiente incremento de capacidad (activos a monitorizar, esfuerzo dedicado al servicio...). Bajo demanda, acumulable (se pueden requerir dos, para ampliar un 20% la capacidad, por ejemplo).

6.2.4. Servicio de vigilancia digital e inteligencia de amenazas

6.2.4.1. Subservicio de vigilancia digital

El servicio de vigilancia digital constituye una solución integral para la detección temprana de amenazas mediante la monitorización e investigación de la información disponible sobre activos de la Junta de Andalucía y los organismos integrados en el grupo atendido de AndalucíaCERT, así como sobre posibles actividades que pudieran afectar a su seguridad.

REQ-VDIG-INTEL-1: La vigilancia digital se realizará sobre activos de distintos tipos: nombres de organismo o marcas., dominios, direccionamientos IP, términos específicos (palabras claves), aplicaciones para dispositivos móviles, aplicaciones y servicios web, cuentas de acceso…

REQ-VDIG-INTEL-2: El número mínimo estimado de objetivos a incluir inicialmente en esta lista es de 200.

VAL-VDIG-INTEL-1: Se valorará el incremento de este dimensionamiento base (SOBRE 3, no incluir en sobre 2).

Se le proporcionará al adjudicatario una propuesta inicial de objetivos a vigilar durante la fase de Definición del Despliegue del Plan de Ejecución del Proyecto Principal. Asimismo, se podrá completar y/o

actualizar la lista de objetivos a monitorizar en cualquier momento durante la duración del contrato y sus posibles prórrogas.

El adjudicatario, en base a su experiencia y conocimiento y de acuerdo con los casos de uso establecidos, podrá proponer en cualquier momento cambios en la lista de objetivos a monitorizar. Estas propuestas no tendrán carácter vinculante, debiendo contar con la aprobación de la persona responsable del servicio, que deberá producirse en el plazo máximo de 5 días hábiles a contar desde la recepción de la propuesta.

De no producirse respuesta en el plazo establecido en el párrafo anterior, la propuesta se considerará aceptada cuando suponga una adición de nuevos activos que no conlleve coste económico para AndalucíaCERT, su grupo atendido y la Agencia Digital de Andalucía. En cualquier otro caso, se considerará no aceptada.

REQ-VDIG-INTEL-3: El personal asignado por adjudicatario a este servicio utilizará un conjunto de fuentes de información que serán monitorizadas en tiempo real con el alcance necesario para la prestación del servicio. Las fuentes cubrirán las siguientes tipologías:

- Fuentes abiertas.
- Fuentes de acceso restringido.
- Fuentes que requieren inteligencia humana, como canales de Telegram, participación en foros, webs en la Dark Web (Tor, Freenet, I2P, …), etc.
- Redes sociales, foros, blogs y comunidades
- Sitios de pastes, de defacement y reinvindicación de acciones de hacking.
- Repositorios públicos de código fuente (Github…).
- Feeds de transparencia de certificados, sitios web que monitorizan suplantaciones de typosquatting.
- Sitios relativos a fugas de información.

El listado de fuentes deberá mantenerse actualizado durante el periodo de vigencia del contrato y sus posibles prórrogas.

REQ-VDIG-INTEL-4: Las fuentes usadas deberán permitir la detección, identificación y recopilación de información relativa a:

- Ataques potenciales o en preparación: Hacktivismo, campañas de malware, amenazas directas, etc.
- Intrusiones y vulneraciones de la seguridad.
- Vulnerabilidades detectadas por terceros.

- Filtraciones de datos: Fugas de información, publicación de credenciales robadas, etc.
- Posibles fraudes online.
- Presencia de aplicaciones maliciosas o fraudulentas.
- Suplantaciones de identidad.
- Dominios y webs fraudulentas
- Noticias falsas con implicaciones tecnológicas referidas a la Junta de Andalucía y sus organismos o al grupo atendido de AndalucíaCERT, que tengan especial repercusión y puedan afectar a la seguridad de los sistemas. No se incluirán en este punto aquellas noticias falsas cuyas repercusiones sean meramente políticas o de imagen corporativa salvo cuando pudieran tener un impacto negativo sobre los activos TIC de la Junta de Andalucía o al grupo atendido de AndalucíaCERT.
- Etc.

REQ-VDIG-INTEL-5: Ante la detección de una posible amenaza, se deberá enviar de forma inmediata una alerta a AndalucíaCERT, ya sea de forma automática a través de las herramientas usadas por el adjudicatario o de forma manual por parte del equipo de trabajo asignado al servicio. El contenido mínimo de dicha alerta será:

- Resumen y análisis de la información encontrada.
- Justificación de la alerta.
- Contexto de la alerta con enlaces, referencias a casos precedentes y cualquier otra información relevante.
- Análisis del impacto y posibles consecuencias.

REQ-VDIG-INTEL-6: El adjudicatario remitirá con periodicidad mensual un informe con el contenido mínimo establecido en el apartado “Entregables”.

REQ-VDIG-INTEL-7: El adjudicatario deberá también proporcionar, durante todo el período de vigencia del contrato y sus posibles prórrogas, al menos una cuenta con acceso completo y, cuando exista la opción, sin publicidad a cada una de las siguientes plataformas, así como a cualesquiera otras que se indique en su oferta para una mejor prestación del servicio:

- Shodan.io (Small Bussiness)
- Censys.io
- Pastebin

VAL-VDIG-INTEL-2: Se valorará que, además de los entregables definidos, se disponga por AndalucíaCERT de acceso a la herramienta subyacente al Subservicio de vigilancia digital (SOBRE 2).

VAL-VDIG-INTEL-3: Se valorará la disponibilidad de APIs para la explotación e integración del Subservicio de vigilancia digital (SOBRE 2).

6.2.4.2. Subservicio de inteligencia de amenazas

REQ-VDIG-INTEL-8: Este servicio proporcionará información actualizada acerca del contexto y las tendencias en materia de ciberseguridad, contemplando las amenazas, los actores, las campañas de ciberataque y cualquier otro aspecto que contribuya a establecer mecanismos de Prevención, Detección y Respuesta realistas y efectivos.

REQ-VDIG-INTEL-9: El adjudicatario utilizará una serie de herramientas y servicios de consulta y recopilación de indicadores de compromiso y amenazas de seguridad, consolidando la información procedente de diferentes fuentes para componer una imagen clara y consistente del estado y las tendencias de la ciberseguridad en los ámbitos nacional e internacional, así como en el de las administraciones públicas, las infraestructuras críticas y los servicios públicos a nivel nacional.

REQ-VDIG-INTEL-10: Las fuentes de las que se extraerá la información incluirán:

- Fuentes internas de que disponga el adjudicatario.
- Fuentes formales externas, como:
    - Informes y servicios de fabricantes de tecnología TIC y proveedores de servicios.
    - Servicios de alertas tempranas de seguridad.
    - Información procedente de otros CERTS y SOCs.
    - Sistemas y herramientas de reputación de dominios, direcciones IP y URLs.
    - Etc.
- Fuentes no formales externas, que en algunos casos podrán requerir actividades de inteligencia humana (HUMINT)
    - Uso de técnicas de OSINT.
    - Monitorización de foros y otros entornos y herramientas de intercambio de mensajes.
    - Monitorización de sitios y servicios de intercambio de información (Pastebin y similares).
    - Monitorización de sitios y servicios en la Web, la Deep Web y la Dark Web.
    - Etc.

Cabe destacar que ya se tiene acceso a la herramienta REYES del CCN-CERT, por tanto, las propuestas técnicas deberán tener en cuenta las fuentes de inteligencia integradas en esta herramienta para no ofrecerlas de forma redundante.

REQ-VDIG-INTEL-11: El personal asignado a este servicio por el adjudicatario analizará la información procedente de las distintas fuentes y generará los informes contemplados en el apartado “Entregables del Servicio de Inteligencias de Amenazas”.

REQ-VDIG-INTEL-12: Asimismo, cuando como resultado de este trabajo se detecten o determinen circunstancias que incrementen el nivel de riesgo para AndalucíaCERT o los organismos de su grupo atendido, se realizará de forma inmediata la correspondiente notificación a través de los medios de contacto proporcionados a tal efecto.

VAL-VDIG-INTEL-4: Se valorará que, además de los entregables definidos, se disponga por AndalucíaCERT de acceso a la herramienta subyacente al Subservicio de inteligencia de amenazas (SOBRE 2).

VAL-VDIG-INTEL-5: Se valorará la disponibilidad de APIs para la explotación e integración del subservicio de inteligencia de amenazas (SOBRE 2).

6.2.4.3. Condiciones de prestación

El servicio se ofrecerá de forma deslocalizada.

La adquisición y consolidación de información deberá ser realizada en modalidad 24x7, conforme a la naturaleza de las distintas fuentes.

Las consultas, incidencias, reclamaciones y otras comunicaciones relacionadas con la prestación del servicio deberán ser atendidas en horario 8x5.

6.2.4.4. Elementos y Dimensionado

ELEM-VDIG-INTEL-BASE: Mensualidad del servicio. Comprometida. Facturación trimestral.

ELEM-VDIG-INTEL-AMPLIACION: Incremento de un 10% del elemento base, con el correspondiente incremento de capacidad (activos a monitorizar, esfuerzo dedicado al servicio...). Bajo demanda, acumulable (se pueden requerir dos, para ampliar un 20% la capacidad, por ejemplo).

6.3. Servicios bajo demanda

Estos servicios se prestarán a petición del responsable del servicio, según lo indicado en los apartados “Modelo de consumo” y “Fase VII: Operación de los servicios”.

VAL-SVDEM-1: Se valorará con carácter general la idoneidad, calidad y flexibilidad de la arquitectura de los servicios propuestos y cómo estos dan cumplimiento a los requisitos enumerados (SOBRE 2).

6.3.1. Servicio de análisis forense

6.3.1.1. Descripción

Este servicio consistirá en la realización de actividades que permitan determinar los hechos sucedidos en los sistemas objeto de análisis y las circunstancias en que se han producido. El ámbito de estas investigaciones alcanzará tanto a los incidentes relacionados con amenazas externas como a aquellos derivados de causas internas.

Ejemplos de elementos típicos a esclarecer durante el análisis forense son:

- Determinar qué hechos han sucedido.
- Determinar cuándo sucedieron los hechos.
- Determinar quién ha realizado un ataque o una operación.
- Determinar su alcance e impacto.
- Determinar desde dónde (qué ubicaciones y qué equipos) se ha realizado.
- Determinar los medios utilizados.
- Determinar cómo ha sido llevado a cabo y la cadena temporal de acontecimientos.

Además, se deberá proporcionar las recomendaciones que corresponda según los resultados alcanzados.

Dentro del servicio de análisis forense se definen dos subservicios:

- Peritaje informático.
- Análisis DFIR

6.3.1.2. Subservicio de peritaje informático

El peritaje informático engloba todas aquellas tareas destinadas a la adquisición, conservación, documentación, análisis y presentación, mediante el uso de procedimientos estandarizados, de evidencias digitales con validez legal, relacionadas con un incidente o un delito que presente, pueda o pudiera presentar un impacto sobre la seguridad de los sistemas, la información, los recursos y los servicios.j

Mediante análisis forense, se determinará el origen y las causas de un incidente de seguridad, plasmando todo el procedimiento en un informe pericial informático que podrá ser ratificado ante la autoridad judicial, en caso de ser necesario. Para ello se deberá cumplir con lo establecido en la última versión publicada de la norma ISO/IEC 27037 “Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence” en cuanto sea aplicable a cada caso particular.

La persona o las personas que realicen el peritaje informático deberán realizar las siguientes tareas:

- La adquisición de la evidencia digital en los distintos soportes en que esta pueda ser encontrada: memoria volátil, discos de distintas tecnologías (mecánicos, de estado sólido, etc.), dispositivos móviles (como smartphones y tabletas), elementos electrónica de red (routers, switches, puntos de acceso WiFi, etc.), sistemas empotrados (dispositivos electromédicos, sistemas IoT, etc.), sistemas en la nube, etc.
- El aseguramiento y preservación de la cadena de custodia, impidiendo la contaminación de la evidencia y garantizando su validez legal.
- La preservación a largo plazo de las evidencias obtenidas, con las debidas condiciones de seguridad, al menos hasta la finalización de los correspondientes procesos judiciales o administrativos con, en caso de ser aplicable, sentencia firme.
- El uso de procedimientos estándar y de herramientas de reconocida fiabilidad y validez aceptadas en los procedimientos judiciales.
- La interpretación de los resultados de los análisis realizados.
- La plasmación de todo el proceso en un documento que dé respuesta a las preguntas planteadas y describa, minuciosamente, los protocolos y procedimientos empleados.
- Cuando se solicite, la presentación de resultados al responsable del contrato y a aquellas personas que éste estime oportuno durante una o varias sesiones en las que se utilizará diapositivas a modo de hilo conductor y en las que la persona o personas que hayan realizado el peritaje deberá responder a las preguntas y dudas que se le planteen.
- La defensa de dicho informe pericial ante los tribunales u otros órganos administrativos o judiciales, cuando sea preciso.

El adjudicatario deberá garantizar, incluso una vez finalizada su relación laboral con la persona o las personas que realicen los informes periciales, la disponibilidad de estas para acudir a tribunales y a órganos administrativos o judiciales para realizar las actividades de prestación de testimonio y de defensa, presentación y ratificación de los informes.

6.3.1.3. Subservicio de análisis DFIR

El servicio de DFIR (Digital Forensics & Incident Response – Forense Digital y Respuesta a Incidentes) incluirá aquellas actividades de respuesta rápida a incidentes cuyo objetivo sea determinar el origen de estos y proponer las posibles respuestas.

Se trata de un proceso orientado principalmente a la respuesta ante incidentes, no tanto a la obtención de pruebas válidas en procedimientos judiciales, ya que las actividades a realizar incluirán el análisis, estudio

e investigación, generalmente mediante el despliegue de software que realice operaciones de triaje u obtención de información, de sistemas en funcionamiento en los que podrían dejar rastro.

El personal técnico encargado de realizar el análisis DFIR deberá llevar a cabo las siguientes tareas:

- La elaboración de guías e instrucciones técnicas para el despliegue de agentes y software de triaje y adquisición de datos. Estos documentos deberán ser fácilmente interpretables y rápidamente implementables por el personal técnico informático responsable de los sistemas a analizar cuando se considere oportuna esta actuación por motivos de urgencia o eficacia.
- El despliegue de agentes y software de triaje y la adquisición de la evidencia digital en los distintos soportes en que esta pueda ser encontrada: memoria volátil, discos de distintas tecnologías (mecánicos, de estado sólido, etc.), dispositivos móviles (como smartphones y tabletas), elementos electrónica de red (routers, switches, puntos de acceso WiFi, etc.), sistemas empotrados (dispositivos electromédicos, sistemas IoT, etc.), sistemas en la nube…
- El análisis de información procedente de otros servicios y sistemas que proporcione evidencias útiles relacionadas con el sistema objeto de estudio: registros de actividad de otras máquinas y de otros servicios, registros de tráfico de red, etc. A efectos de facturación, estas actividades formarán parte del mismo análisis DFIR que las relativas al sistema principal objeto de estudio.
- La preservación de las evidencias obtenidas, al menos, hasta que el informe de resultados haya sido presentado y los trabajos aceptados.
- El empleo de procedimientos estándar y herramientas cuya validez y prestigio sean ampliamente reconocidos para la adquisición, tratamiento y análisis de las evidencias.
- La interpretación de los resultados de los análisis realizados.
- La elaboración de un informe que dé respuesta a las preguntas planteadas y aporte soluciones para contener, mitigar y erradicar el incidente objeto de estudio.
- Cuando se solicite, la presentación de resultados al responsable del contrato y a aquellas personas que éste estime oportuno durante una o varias sesiones en las que se utilizará diapositivas a modo de hilo conductor y en las que la persona o personas que hayan realizado el análisis DFIR deberá responder a las preguntas y dudas que se le planteen.

6.3.1.4. *Condiciones de prestación*

El servicio se prestará de forma deslocalizada, con asistencia a sedes y ubicaciones cuando sea necesario para la captura de evidencias, la presentación de resultados, la presentación, defensa y ratificación de informes ante órganos administrativos o judiciales o cualquier otra actividad necesaria para una adecuada prestación del servicio.

El servicio podrá ser solicitado y deberá ser atendido en horario 24x7.

La obtención de evidencias deberá ser realizada en horario 24x7.

Las tareas de análisis de evidencias y elaboración de informes y documentos podrán ser realizada en horario 8x5.

La persona responsable del servicio podrá requerir el desplazamiento de personal del adjudicatario a las ubicaciones donde se deberá realizar las actuaciones con anterioridad a la aprobación del Plan de Acción cuando estas actuaciones sean necesarias para la elaboración de dicho Plan o deban ser realizadas de forma urgente.

Las tareas de presentación de resultados y defensa ante tribunales y otros órganos judiciales y administrativos deberán realizarse conforme al horario del órgano o los órganos ante los que se lleven a cabo.

Se considerarán para este servicio, como elementos unitarios, jornadas de trabajo estándar y otras de especial complejidad. La distribución de tipos de jornadas para una petición de servicio concreta se establecerá de mutuo acuerdo entre el responsable del servicio y el jefe de proyecto, previamente al inicio de los trabajos, mediante la propuesta de plan de trabajo.

6.3.1.5. Elementos y dimensionamiento

ELEM-JORNADA-PERIT: Jornada peritaje informático.

ELEM-JORNADA-PERIT-COMPLEJO: Jornada peritaje informático de especial complejidad.

ELEM-JORNADA-DFIR: Jornada de análisis DFIR (Forense Digital y Respuesta a Incidentes).

ELEM-JORNADA-DFIR-COMPLEJO: Jornada de análisis DFIR (Forense Digital y Respuesta a Incidentes) de especial complejidad.

6.3.2. Servicio de obtención, certificación y preservación de evidencias digitales

6.3.2.1. Descripción

Este servicio contempla las actividades necesarias para la obtención de evidencias digitales, así como para su certificación y preservación en unas condiciones que permitan asegurar y demostrar, incluso en procedimientos judiciales, su autenticidad y no alteración, cuando no sean resultado del servicio de peritaje informático.

Casos típicos de ámbito de aplicación de este servicio será la certificación de:

- Existencia de perfiles falsos en redes sociales y del contenido y actividad de estos en casos de suplantación de la imagen o la identidad de la Junta de Andalucía o de un organismo del grupo atendido de AndalucíaCERT.
- Contenido de una página web.
- Presencia de documentación y ficheros en sitios y servicios de compartición de contenidos y redes peer-to-peer.
- Contenido de mensajes de correo electrónico o servicios y aplicaciones de mensajería, SMS o MMS, enviados o recibidos por personal de la Junta de Andalucía o de organismos del grupo atendido de AndalucíaCERT o que tenga relación con estos, cuando se cuente con la colaboración de la persona que los envió o los recibió.

Para ello, siempre que sean aplicables y en la medida en que sean necesarios para garantizar la validez de la evidencia en un procedimiento judicial, el adjudicatario hará uso de todos los siguientes elementos:

- Mecanismos de sellado de tiempo.
- Servicios de notaría o herramientas alternativas de reconocido prestigio, solvencia y validez como eGarante y otras similares.

Debe señalarse que en ningún caso será objeto de la presente licitación el ofrecimiento directo de estos servicios o herramientas a AndalucíaCERT, debiendo ser contratados, gestionados y utilizados por el adjudicatario, que correrá con los correspondientes costes.

Se con

6.3.2.2. Condiciones de prestación

El servicio se ofrecerá de forma deslocalizada, con asistencia a sedes y ubicaciones cuando sea necesario para su adecuada prestación.

El servicio podrá ser solicitado y deberá ser atendido en horario 24x7.

La persona responsable del servicio podrá requerir el desplazamiento de personal del adjudicatario a las ubicaciones donde se deberá realizar las actuaciones con anterioridad a la aprobación del Plan de Acción cuando estas actuaciones sean necesarias para la elaboración de dicho Plan o deban ser realizadas de forma urgente.

Se considerarán para este servicio, como elementos unitarios, certificaciones de evidencias y certificaciones de especial complejidad. El licitador deberá incluir en su propuesta una propuesta de categorización (estándar/compleja) de trabajos, en base a los casos típicos enunciados en el apartado anterior y a otros que añada en base a su conocimiento. El tipo de certificación para una petición de

servicio concreta se establecerá de mutuo acuerdo entre el responsable del servicio y el jefe de proyecto, previamente al inicio de los trabajos, mediante la propuesta de plan de trabajo.

6.3.2.3. Elementos y dimensionamiento

ELEM-CERTIF-EVIDENCIA: Obtención, Certificación y Preservación de Evidencias Digitales.

ELEM-CERTIF-EVIDENCIA-COMPLEJA: Obtención, Certificación y Preservación de Evidencias Digitales de especial complejidad.

6.3.3. Servicio de elaboración de informes técnicos

6.3.3.1. Descripción

El servicio consistirá en la elaboración bajo demanda de informes, guías y estudios específicos dirigidos a perfiles técnicos en los que se tratarán aspectos como recomendaciones de seguridad, guías de uso, buenas prácticas o prospectiva.

Cada informe tendrá una extensión típica de entre 15 y 40 páginas, cada una de las cuales contendrá un encabezado o marca en el que se indique el nivel de confidencialidad del documento. Los detalles sobre el mismo serán determinados por AndalucíaCERT en el momento de solicitar el servicio.

Los informes deberán estar escritos en castellano y contar con un nivel mínimo de calidad tanto en la forma (maquetación, presentación, uso correcto del idioma y las expresiones, etc.) como en el contenido técnico. Asimismo, se cuidará especialmente el uso inclusivo del lenguaje y su adecuación al público objetivo de cada informe. A efectos de referencia, cabe esperar que la calidad sea similar a la de las guías BP o CCN-STIC elaboradas por el CCN-CERT.

Para hacer uso de este servicio, el responsable del servicio podrá solicitar cada año al adjudicatario la remisión de una propuesta de temas a tratar en los informes. Esta lista, que incluirá como mínimo doce temas, no será en ningún caso vinculante, compitiendo únicamente al responsable del servicio la elección de los temas a tratar en cada informe.

6.3.3.2. Condiciones de prestación

El servicio se ofrecerá de forma deslocalizada, con asistencia a sedes y ubicaciones cuando sea necesario para su adecuada prestación.

El servicio podrá ser solicitado y deberá ser atendido en horario 8x5.

El volumen estimado de informes anuales es de 12.

Se considerarán para este servicio, como elementos unitarios, informes estándares y otros de especial complejidad. El tipo de informe o informes para una petición de servicio concreta se establecerá de mutuo acuerdo entre el responsable del servicio y el jefe de proyecto, previamente al inicio de los trabajos, mediante la propuesta de plan de trabajo.

6.3.3.3. Elementos y dimensionamiento

ELEM-INFORME-TÉCNICO: Elaboración de informe técnico.

ELEM-INFORME-TÉCNICO-COMPLEJO: Elaboración de informe técnico de especial complejidad.

6.3.4. Servicio de análisis de malware

6.3.4.1. Descripción

Este servicio consistirá en la realización de análisis de malware bajo demanda, con el objetivo de identificar las muestras analizadas (familia de malware, autoría, etc.), listar sus características y capacidades (método de infección, vía de propagación, daño potencial sobre el sistema, etc.), obtener un conjunto de indicadores relacionados con el malware (servidores de comando y control con los que contacta, hashes de los ficheros involucrados, etc.), y cualquier otra característica relevante para la gestión de los incidentes de seguridad relacionados con él.

Para hacer uso de este servicio, el responsable del servicio remitirá a la empresa adjudicataria una o varias muestras de malware (en el caso de que sean varias, todas pertenecerán a la misma campaña y/o familia de malware), a través de mecanismos seguros.

El adjudicatario deberá guardar secreto sobre las muestras y no podrá hacerlas públicas ni divulgarlas ni comunicarlas a terceros, ni utilizar herramientas o servicios que pudieran hacerlo, salvo cuando cuente con el consentimiento expreso y por escrito de la persona responsable del servicio.

Para cada muestra se realizará análisis tanto estáticos (sin llegar a ejecutar el malware) como dinámicos (ejecutando el malware en entornos controlados). Para ello, el adjudicatario deberá contar con su propio laboratorio de análisis de malware con herramientas de referencia en el sector, como analizadores (PeStudio, PE Explorer, Exeinfo PE, etc.), desensambladores (IDA Pro de Hex-Rays, Ghidra, etc.), *debuggers* (OllyDbg, Immunity Debugger, etc.), sistemas de *sandbboxing* (Cuckoo, Joe Sandbox, Falcon Sandbox, etc.) y otras.

Para cada análisis se deberá elaborar como mínimo los entregables contemplados en el apartado “Entregables”.

6.3.4.2. Condiciones de prestación

El servicio se ofrecerá de forma deslocalizada, con asistencia a sedes y ubicaciones cuando sea necesario para su adecuada prestación.

El servicio podrá ser solicitado y deberá ser atendido en horario 24x7.

Se considerarán para este servicio, como elementos unitarios, análisis estándares y otros de especial complejidad. El tipo de análisis para una petición de servicio concreta se establecerá de mutuo acuerdo entre el responsable del servicio y el jefe de proyecto, previamente al inicio de los trabajos, mediante la propuesta de plan de trabajo.

6.3.4.3. Elementos y dimensionamiento

ELEM-AN-MALWARE: Análisis de malware.

ELEM- AN-MALWARE-COMPLEJO: Análisis de malware de especial complejidad.

6.3.5. Servicio de realización de ciberejercicios

6.3.5.1. Descripción

Este servicio consistirá en la realización de ejercicios de ciberseguridad en organismos del grupo atendido de AndalucíaCERT con el objetivo de evaluar su grado de madurez en materia de ciberseguridad, medir la capacidad de respuesta, determinar posibles carencias, identificar mejoras y tecnologías que podrían ser incorporadas, proponer actividades formativas, etc.

El responsable del servicio podrá solicitar la realización de los siguientes tipos de ciberejercicio, que el adjudicatario deberá preparar y ejecutar:

Table-top. Usados habitualmente para poner a prueba el funcionamiento de los comités de crisis, los protocolos internos de actuación, etc. A partir de un guion previamente elaborado por el adjudicatario, se realizará una simulación de acciones ante una audiencia que deberá tomar decisiones al respecto. Dependiendo de estas decisiones, así como de valores determinados de forma aleatoria, el ciberejercicio tomará un curso u otro, siguiendo el proceso hasta llegar a su finalización.

Escenario real. Se realizan acciones reales sobre una audiencia o un sistema o conjunto de sistemas, con objeto de evaluar su nivel de seguridad. El objetivo puede incluir tanto recursos tecnológicos como organizativos o humanos. Ejemplos típicos de este tipo de ejercicio son la realización de forma controlada de ataques de phishing, los ataques mediante reparto o abandono de pendrives con código malicioso o las suplantaciones de servicio técnico.

Los ciberejercicios deberán plantear escenarios reales o plausibles. En el caso de los table-top, los cursos de acción y las probabilidades asignadas a los eventos aleatorios serán razonables y adecuados a casos reales o razonablemente posibles.

Los ejercicios, así como la presentación de sus resultados, podrán requerir el desplazamiento de personal del adjudicatario a cualquier punto de la Comunidad Autónoma de Andalucía y deberán ser realizados por personal experto en la materia que asegure un nivel técnico adecuado en la realización de los trabajos, analice de forma manual los resultados obtenidos y realice una propuesta de actividades y medidas a tomar.

6.3.5.2. Condiciones de prestación

El servicio se ofrecerá de forma deslocalizada, con asistencia a sedes y ubicaciones cuando sea necesario para su adecuada prestación.

El servicio podrá ser solicitado y deberá ser atendido en horario 8x5.

La realización de las pruebas podrá ser realizada por el adjudicatario en horario 24x7, pudiendo elegir el más adecuado a su naturaleza y objetivos, dentro de las limitaciones contempladas en la propuesta de organización de los trabajos aprobada por la persona responsable del servicio.

Se considerarán para este servicio, como elementos unitarios, jornadas estándar y otras de especial complejidad. La distribución de tipos de jornadas para una petición de servicio concreta se establecerá de mutuo acuerdo entre el responsable del servicio y el jefe de proyecto, previamente al inicio de los trabajos, mediante la propuesta de plan de trabajo.

Para una petición de servicio concreta se establecerá de mutuo acuerdo entre el responsable del servicio y el jefe de proyecto, previamente al inicio de los trabajos, mediante la propuesta de plan de trabajo.

VAL-CIBEREJ-PLATAF: Se valorará si la oferta incluye la puesta a disposición, sin coste, de AndalucíaCERT y la Agencia Digital de Andalucía de una plataforma que les permita realizar ciberejercicios de escenario real (SOBRE 3, no incluir en sobre 2), siempre que se cumplan todas las siguientes condiciones:

- Que se ofrezca como mínimo una cuenta de acceso a AndalucíaCERT y otra a la Agencia Digital de Andalucía, permitiendo ambas el diseño, ejecución, seguimiento y análisis de ciberejercicios.
- Que se ofrezca a AndalucíaCERT y a la Agencia Digital de Andalucía una sesión formativa sobre el funcionamiento de la plataforma y se les entregue los correspondientes manuales de uso.
- Que la plataforma permita, como mínimo, la organización, diseño, ejecución, seguimiento y análisis de campañas de phishing controlado.
- Que AndalucíaCERT y la Agencia Digital de Andalucía puedan utilizar la plataforma en todo momento de la duración del contrato y sus posibles prórrogas.

De incluirse el acceso a esta plataforma en la oferta, se deberá indicar (SOBRE 3, no incluir en sobre 2) el hardware, el software y los servicios en los que se basa la plataforma con indicación, cuando sea aplicable, de las correspondientes versiones y modalidades de uso.

6.3.5.3. Elementos y dimensionamiento

ELEM-JORNADA-EJERCICIOS-SIMPLE: Jornada de ciberejercicios.

ELEM-JORNADA-EJERCICIOS-COMPLEJA: Jornada de ciberejercicios de especial complejidad.

6.3.6. Servicio de proyectos en protección, detección y respuesta

6.3.6.1. Descripción

Este servicio consistirá en la realización de proyectos de tecnológicos relacionados con la protección, detección y respuesta a incidentes de ciberseguridad en el ámbito de las competencias de AndalucíaCERT.

Estos proyectos, cuyos resultados serán utilizados única y exclusivamente por AndalucíaCERT, podrán tomar diferentes formas:

- Estudio, diseño, definición y puesta en marcha de nuevos servicios para AndalucíaCERT, o mejoras a los ya existentes.
- Optimización y redefinición de políticas, procesos y procedimientos de seguridad y evolución del modelo de prestación de los servicios.
- Revisión de instrucciones técnicas.
- Asistencia técnica en el despliegue de nuevos sistemas, herramientas y productos relacionados con la ciberseguridad o en la integración de la monitorización de estos en la plataforma de monitorización existente en AndalucíaCERT.
- Asistencia técnica para la integración de herramientas, desarrollo de interfaces y automatización de procedimientos.
- Revisión de documentación, protocolos y procedimientos de trabajo técnicos de departamentos de ciberseguridad de los organismos de la Junta de Andalucía o del propio AndalucíaCERT.
- Etc.

6.3.6.2. Condiciones de prestación

El servicio se ofrecerá de forma deslocalizada, con asistencia a sedes y ubicaciones cuando sea necesario para su adecuada prestación.

El servicio podrá ser solicitado y deberá ser atendido en horario 8x5. La ejecución de los proyectos se realizará en horario 8x5 salvo que se acuerde otro entre la persona responsable del servicio y el adjudicatario.

6.3.6.3. Elementos y dimensionamiento

ELEM-CONS-JUNIOR: Jornada de consultor senior.

ELEM-CONS-SENIOR: Jornada de consultor senior.

6.3.7. Servicio de intervención especializada

6.3.7.1. *Descripción*

Este servicio consistirá en la realización de actividades de consultoría y soporte a AndalucíaCERT, a realizar en ubicaciones determinadas por este organismo, para atender necesidades especiales derivadas de eventos, circunstancias o acontecimientos de especial relevancia o impacto o que requieran personal altamente especializado. Ejemplos de causas que pueden motivar la solicitud de este servicio son:

- Participación de AndalucíaCERT en ciberjercicios como el ENISA CyberEupre o el INCIBE International CyberEx.
- Participación de AndalucíaCERT, u organización por parte de este organismo, de congresos, ferias y otros eventos relacionados con la Ciberseguridad.
- Operativos de soporte específico en acontecimientos planificados de especial trascendencia, como procesos electorales, tomas de posesión de altos cargos, celebración de reuniones políticas de relevancia en Andalucía, etc.

La persona responsable del servicio realizará, con carácter general, la solicitud de este servicio con un mínimo de 15 días de antelación a la fecha de inicio de las actividades solicitadas.

La prestación de este servicio puede implicar el desplazamiento del personal del adjudicatario a cualquier punto de la Comunidad Autónoma de Andalucía con objeto de realizar las actuaciones in situ necesarias o las presentaciones y actividades requeridas.

6.3.7.2. *Condiciones de prestación*

El servicio se ofrecerá de forma localizada o deslocalizada, dependiendo de la naturaleza de la solicitud y lo indicado en ella. En todo caso, se deberán realizar los desplazamientos asistencia a sedes y ubicaciones que sean necesarios para una adecuada realización de los trabajos o se deriven de los requisitos establecidos.

En general, el servicio podrá ser solicitado y deberá ser atendido en horario 8x5.

En los casos en que se solicite soporte para la gestión de incidentes de ciberseguridad, el servicio podrá ser solicitado y deberá ser atendido en horario 24x7.

La ejecución de los proyectos se realizará en horario conforme a lo establecido en la solicitud y el plan de trabajo aprobado.

Se considerarán para este servicio, como elementos unitarios, jornadas de trabajo de personal técnico u de personal técnico especialista. La distribución de tipos de jornadas para una petición de servicio concreta se establecerá de mutuo acuerdo entre el responsable del servicio y el jefe de proyecto, previamente al inicio de los trabajos, mediante la propuesta de plan de trabajo.

6.3.7.3. Elementos y dimensionamiento

ELEM-TECNICO: Jornada de personal técnico.

ELEM-TECNICO -ESPECIALISTA: Jornada de personal técnico especialista.

6.4. Elementos unitarios, consumo y facturación

6.4.1. Elementos unitarios

El Catálogo de elementos unitarios (en adelante, "catálogo") es un documento que recoge todos los elementos unitarios solicitables por la Agencia Digital de Andalucía en la ejecución del contrato. Tendrán asignado precio unitarios y serán los únicos conceptos que puedan figurar en las facturas que emita el adjudicatario.

Servicio	Elemento	Unidad	Elementos compromentdos	Estimación de elementos bajo demanda
Jefatura de proyecto	ELEM-JF-PROYECTO	Hora	1.350	
Ejecución de proyectos – Fases I a VI (Incluyendo formación fase V)	ELEM-IMPLANTACION-SERVICIOS	Unidad	1	
Alerta temprana y asesoramiento	ELEM-ATV-BASE	Mensualidad	34	

sobre vulnerabilidades				
Alerta temprana y asesoramiento sobre vulnerabilidades	ELEM-ATV-AMPLIACION	Mensualidad		10
Analisis de la Superficie de Exposiclón en Internet	ELEM-ASE-BASE	Mensualidad	34	
Analisis de la Superficie de Exposiclón en Internet	ELEM-ASE-AMPLIACION	Mensualidad		10
Análisis de Vulnerabilidades Web – Servicio Desatendido	ELEM-AVDESAT	Mensualidad	34	
Análisis de Vulnerabilidades Web – Servicio Desatendido	ELEM-AVDESAT-AMPLIACION	Mensualidad		10
Análisis de Vulnerabilidades - Atendido	ELEM-AVULN-BASE	Mensualidad	34	
Análisis de Vulnerabilidades - Atendido	ELEM-AVULN-AMPLIACION	Mensualidad		10
Vigilancia digital e inteligencia de amenazas	ELEM-VDIG-INTEL-BASE	Mensualidad	34	
Vigilancia digital e inteligencia de amenazas	ELEM-VDIG-INTEL-AMPLIACION	Mensualidad		10

Análisis forense	ELEM-JORNADA-PERIT	Jornada		30
Análisis forense	ELEM-JORNADA-PERIT-COMPLEJO	Jornada		30
Análisis forense	ELEM-JORNADA-DFIR	Jornada		30
Análisis forense	ELEM-JORNADA-DFIR-COMPLEJO	Jornada		30
Obtención, certificación y preservación de evidencias digitales	ELEM-CERTIF-EVIDENCIA	Unidad		18
Obtención, certificación y preservación de evidencias digitales	ELEM-CERTIF-EVIDENCIA-COMPLEJA	Unidad		18
Elaboración de informes técnicos	ELEM-INFORME-TÉCNICO	Unidad		18
Elaboración de informes técnicos	ELEM-INFORME-TÉCNICO-COMPLEJO	Unidad		15
Análisis de malware	ELEM- AN-MALWARE	Unidad		33
Análisis de malware	ELEM- AN-MALWARE-COMPLEJO	Unidad		12
Realización de ciberejercicios	ELEM-JORNADA-EJERCICIOS	Jornada		18
Realización de ciberejercicios	ELEM-JORNADA-EJERCICIOS-COMPLEJA	Jornada		9
Proyectos en protección, detección y respuesta	ELEM-CONS-JUNIOR	Jornada		90
Proyectos en protección, detección y respuesta	ELEM-CONS-SENIOR	Jornada		90
Intervención especializada	ELEM-TECNICO	Jornada		15
Intervención especializada	ELEM-TECNICO-ESPECIALISTA	Jornada		15

6.4.2. Modelo de consumo

Al inicio del contrato se consumirán los elementos unitarios necesarios para el despliegue inicial. Tras dicho despliegue (fases I a VI de la ejecución del proyecto), los servicios descritos en este lote se ejecutarán en dos modalidades, según se describe en la fase VII de la ejecución del proyecto:

- Los servicios recurrentes (alerta temprana, análisis de la superficie de exposición, análisis de vulnerabilidades y vigilancia digital e inteligencia de amenazas), de forma continuada, en forma de procesos/proyectos.
  Las mensualidades del servicio (elementos unitarios ELEM-XXX) se consumirán, por lo tanto, de forma continua.
  En algunos de los servicios recurrentes, y en previsión de cambios en las infraestructuras, ampliación de capacidades y/o de ámbito de actuación de AndalucíaCERT, se consideran elementos unitarios ELEM-XXX-AMPLIACION que permitirán, previa solicitud por parte del responsable del contrato, la ampliación de capacidades de los servicios.
- Los servicios bajo demanda (análisis forense, certificación de evidencias, análisis de malware, ciberejercicios, proyectos e intervención especializada) se ejecutarán a petición del responsable del servicio, que motivará la presentación por el adjudicatario de una propuesta de plan de trabajo. Tras la aprobación de ésta se ejecutará el servicio. Se consumirán así (total o parcialmente) los elementos unitarios (ELEM-XXX) que hayan sido presupuestados en la propuesta de plan de trabajo.

6.4.3. Modelo de facturación

Mensualmente se recopilarán y certificarán los elementos unitarios consumidos, y trimestralmente se emitirán por el adjudicatario las facturas correspondientes a los consumos del trimestre anterior.

6.5. Ejecución del proyecto

La ejecución se organizará mediante proyectos específicos siguiendo el procedimiento establecido en este apartado.

Para su dirección, se considera una dedicación del Jefe de Proyecto (elemento de catálogo ELEM-JF-PROYECTO) al 25% en promedio durante todo el contrato.

El proyecto principal consistirá en la implantación de los servicios requeridos en el presente lote, lo cual requerirá, entre otras tareas, la caracterización y procedimentación de los mismos, el despliegue de las herramientas necesarias en la infraestructura de la Junta de Andalucía y/o en la nube, la capacitación del personal, la puesta en producción de cada servicio y su operación durante toda la duración del contrato.

El proyecto de implantación de los servicios se realizará conforme a las fases establecidas en este epígrafe, estimándose un tiempo máximo total de ejecución de las **fases I a VI de ocho semanas**.

FASE	DURACIÓN MÁXIMA ESTIMADA
Fase I: Definición del Plan Técnico de Implantación de los servicios	10 días hábiles
Fase II: Preparación de las infraestructuras necesarias para el funcionamiento de las herramientas de soporte a los servicios	10 días hábiles
Fase III: Despliegue de sistemas y herramientas en infraestructuras de AndalucíaCERT y nube	10 días hábiles
Fase IV: Puesta en funcionamiento de los servicios	5 días hábiles
Fase V: Formación	8 jornadas, en paralelo, coincidiendo en el tiempo con las fases I a III
Fase VI: Aceptación del sistema	5 días hábiles
Fase VII. Operación de los servicios	Resto de la duración del contrato

VAL-PLANL2: Se valorará el nivel de cumplimiento respecto de los requisitos del PPT, la calidad, idoneidad, detalle y explicaciones sobre la propuesta de Plan de ejecución del proyecto (SOBRE 2).

VAL-SVS-1: Se valorará positivamente la presentación conjunta y organizada de la información correspondiente a distintos servicios en una única plataforma que permita interrelacionar y poner en contexto los datos proporcionados por estos (SOBRE 2).

VAL-SVS-2: Por último, se valorará la propuesta de integraciones y sinergias entre los servicios de este lote y los del lote 1 (SOBRE 2).

6.5.1. Fase I: Definición del despliegue

Con carácter previo al despliegue de los servicios, la empresa comunicará a la Dirección del proyecto los datos de contacto señalados en el apartado “Organización del trabajo”.

En esta fase se mantendrán reuniones donde el adjudicatario deberá proporcionar todos los detalles relativos a la puesta en marcha de los servicios, incluyendo su configuración y arquitectura y cualquier otro aspecto de estos que la Junta de Andalucía considere oportuno.

La empresa realizará un análisis y un diseño detallado en un Plan Técnico de Implantación que deberá incluir como mínimo, y a modo de referencia, el plan de instalación física y lógica de las herramientas soporte de los servicios en las distintas sedes implicadas, incluyendo:

1. Arquitectura del conjunto de herramientas y sistemas desplegados. Diagramas físicos y lógicos.
2. Identificación de dependencias del despliegue y necesidades para el despliegue de plataformas y sistemas en las infraestructuras de AndalucíaCERT o de los organismos de su grupo atendido.
3. Plan detallado de puesta en marcha y configuración de los servicios, incluyendo estimación de tiempos para cada una de las tareas.
4. Documentación técnica: Casos de uso y manuales de uso y administración.

Asimismo, el citado Plan deberá contener la caracterización completa de los servicios que se pretenden poner en marcha incluyendo al menos para cada uno de ellos de manera individualizada:

- Definición y alcance del servicio
- Flujos, Procedimientos e instrucciones de trabajo relacionadas con la prestación del mismo.
- Roles y responsabilidades de cada integrante del equipo.
- Mecanismos de interlocución.
- Matriz de escalados

El plazo máximo estimado de entrega de este Plan será de **diez (10) días hábiles,** a contar desde la fecha de formalización del contrato.

El Plan técnico de Implantación entregado por el adjudicatario deberá ser aprobado por la persona responsable del contrato. En caso de no aprobarlo, la persona responsable del contrato enviará comunicación a la jefatura del proyecto en el plazo de dos días laborables, indicándole las causas y requiriéndole su corrección.

En caso de no producirse requerimiento de correcciones en el tiempo mencionado en el párrafo anterior, el Plan técnico de Implantación se tendrá por aprobado.

Con la aprobación del Plan Técnico de Implantación, el responsable del contrato autorizará el comienzo de la Fase II.

Toda modificación del Plan Técnico de Implantación que sea necesario introducir con posterioridad a su aprobación deberá ser sometida nuevamente a la aprobación del responsable del contrato.

Durante la fase I se determinará el equipamiento que será utilizado por el personal del adjudicatario.

6.5.2. Fase II: Preparación de las infraestructuras necesarias para el funcionamiento de los servicios

Durante esta fase, AndalucíaCERT realizará las configuraciones en sus infraestructuras y solicitará a la Red Corporativa de Comunicaciones de la Junta de Andalucía las operaciones necesarias para asegurar el correcto funcionamiento de las herramientas que el adjudicatario desplegará sobre equipamiento de la Junta de Andalucía.

El adjudicatario realizará también durante esta fase, o con anterioridad a ella, las adquisiciones de productos y servicios que sean precisos para la puesta en marcha de los servicios que componen el presente lote.

El plazo máximo estimado para la realización de esta fase será de **diez (10) días hábiles,** a contar desde la finalización de la fase I.

6.5.3. Fase III: Despliegue de sistemas y herramientas en infraestructuras de AndalucíaCERT y nube

Durante esta fase, el adjudicatario realizará el despliegue de sistemas y herramientas sobre infraestructuras de AndalucíaCERT o de los organismos de su grupo atendido conforme a los requisitos establecidos para cada servicio. De manera análoga a la modalidad onprem, el adjudicatario provisionará y configurará inicialmente las herramientas de soporte que deban utilizarse desde la nube.

El plazo máximo para la finalización de esta fase será de **siete (7) días hábiles** a contar desde la finalización de la fase II.

6.5.4. Fase IV: Puesta en funcionamiento de los servicios

Durante esta fase se pondrán en explotación los servicios incluidos en el presente lote. Entre las tareas efectuadas, se incluirá la capacitación del equipo de trabajo de este lote en las herramientas y procedimientos de trabajo definidos para que pueda realizarse una correcta prestación de los servicios.

El inicio de las actividades propia de cada servicio se producirá:

- En el plazo máximo de **cinco (5) días hábiles** a contar desde la finalización de la fase II para los servicios que no dependan del despliegue de sistemas y herramientas en las infraestructuras de AndalucíaCERT o su grupo atendido.
- En el plazo máximo de **cinco (5) días hábiles** a contar desde la finalización de la fase III para los servicios que dependan del despliegue de sistemas y herramientas en las infraestructuras de AndalucíaCERT o su grupo atendido.

6.5.5. Fase V: Formación

El licitador deberá incluir en su propuesta como mínimo tres actividades formativas, de un mínimo de 15 horas lectivas cada una, sobre la plataforma de análisis desatendido de vulnerabilidades. El número aproximado de asistentes a cada sesión será de 20 personas.

Además, incluirá también al menos dos sesiones más, de 6 horas de duración, con un número aproximado de 10 asistentes a cada una, sobre otras herramientas y productos que ponga a disposición de AndalucíaCERT o sobre otros aspectos relevantes para asegurar un adecuado aprovechamiento de los resultados proporcionados por los distintos servicios.

Las sesiones de capacitación serán impartidas en castellano y tendrán lugar en las instalaciones de la Junta de Andalucía en las provincias de Sevilla y Málaga, o bien de manera virtual a través de medios telemáticos. Esta formación se podrá impartir en paralelo con el desarrollo de las fases II, III y IV del plan principal de ejecución del proyecto.

6.5.6. Fase VI: Aceptación del sistema

En esta fase se verificará la correcta implementación de los servicios y todos sus entregables, principalmente del Informe de implantación de los servicios. Se estima una duración de **cinco (5) días hábiles**.

Tras la verificación de los requisitos anteriores se confirmará por parte del responsable del contrato la finalización del proyecto de implantación y comenzará la operación de los servicios.

6.5.7. Fase VII. Operación de los servicios

Durante esta fase se realizará la operación y ejecución de los trabajos de este lote conforme a lo establecido para los distintos servicios aplicables.

La prestación de los servicios incluidos en el lote 2 se realizará

- De forma continuada o recurrente para los servicios de Alerta temprana, Análisis de la superficie de exposición, análisis de vulnerabilidades y vigilancia digital e inteligencia de amenazas.
- Bajo demanda para los servicios de análisis forense, certificación de evidencias, análisis de malware, ciberejercicios, proyectos e intervención especializada.

6.5.7.1. Servicios continuados o recurrentes

Los servicios recurrentes se organizarán en proyectos, interrelacionados entre sí y con los servicios del lote 1 de la contratación. Se ejecutarán continuamente, en el horario que corresponda a cada uno, de forma

gestionada por el adjudicatario, atenderán las peticiones que se remitan, emitirán los avisos y comunicaciones necesarios y generarán los resultados y entregables correspondientes.

Se podrán definir proyectos auxiliares, derivados de cambios significativos en las infraestructuras tecnológicas de la Junta de Andalucía o de tipo organizativo como, por ejemplo, los cambios en la composición del grupo atendido de AndalucíaCERT.

Otras actuaciones menores, como la adición de software a contemplar en el servicio de alerta temprana de vulnerabilidades, se gestionarán como una petición de cambio.

6.5.7.2. Servicios bajo demanda

Los servicios bajo demanda se prestarán a petición del responsable del servicio, siguiendo este flujo:

Solicitud

Las solicitudes de prestación de servicio serán remitidas a la jefatura del proyecto por la persona responsable del servicio y en ellas se indicará:

- El servicio o subservicio solicitado.
- El alcance y los objetivos a cumplir.
- Si se requiere o no la realización de una presentación de resultados y conclusiones en los términos indicados más adelante en este apartado. En caso de que la solicitud no indique este extremo, se asumirá que se requiere la realización de la presentación.
- La forma en que se deberán entregar los resultados y los medios y canales a utilizar para ello, cuando sean distintos de los establecidos con carácter general.
- Cualquier restricción o condición aplicable para garantizar el menor impacto posible sobre los activos implicados o para garantizar la adecuada prestación del servicio.
- Los contenidos adicionales necesarios para definir adecuadamente el servicio o el subservicio, conforme a lo establecido en el apartado correspondiente a éste.
- Los contenidos adicionales adecuados a la naturaleza, contexto y características de la solicitud.

Propuesta de plan de trabajo

Para cada solicitud, la persona que ejerza la jefatura del proyecto remitirá a la persona responsable del servicio una propuesta de plan de trabajo que incluirá una propuesta de plazos de ejecución y entrega, así como la estimación máxima de recursos necesarios para la ejecución, en base a los elementos unitarios correspondientes y, cuando proceda, de modificación de alcance, objetivos, condiciones o restricciones. Si es posible y procede, se detallará el personal adscrito al trabajo en cuestión y su cualificación.

La persona responsable del servicio podrá requerir del adjudicatario la información o las correcciones y modificaciones que considere oportunas sobre el contenido de la propuesta de trabajo y la composición del equipo de personas asignado. Una vez alcanzado un acuerdo en cuanto al alcance del servicio, resultados a entregar y plazos aplicables, estos serán utilizados para determinar los correspondientes costes y acuerdos de nivel de servicio.

Aprobación

La propuesta deberá ser aprobada por el responsable del contrato. Tras dicha aprobación podrá comenzar la ejecución.

Ejecución

Una vez aprobada esta propuesta, el adjudicatario procederá a la prestación del servicio en los términos establecidos y a la remisión o puesta a disposición de la persona responsable del servicio de los correspondientes entregables, a medida que estos se encuentren disponibles.

El adjudicatario dedicará a las tareas propias de cada proyecto el personal experto en la materia necesario, de modo que garantice la adecuada prestación del servicio.

Cuando así se contemple en la descripción de los servicios, la persona responsable del servicio podrá requerir el desplazamiento de personal del adjudicatario a una determinada ubicación antes de la aprobación del plan de trabajo para la realización de acciones urgentes o que pudieran ser necesarias para la correcta elaboración del mismo, o para garantizar la adecuada prestación del servicio.

Entregables

La persona responsable del servicio podrá requerir al adjudicatario en la solicitud del servicio o tras la remisión o puesta a disposición de elementos entregables, la realización de una o varias presentaciones en las que se detallará los resultados y las conclusiones alcanzadas utilizando como hilo conductor diapositivas y otros medios audiovisuales. Estas presentaciones estarán dirigidas a la persona responsable del servicio y a aquellas otras que este considere oportuno y durante ella la persona o personas que hayan planificado, dirigido o ejecutado el servicio deberán responder a las preguntas y dudas que se le planteen.

La persona responsable del servicio podrá requerir la grabación de estas presentaciones. Tanto el documento con las diapositivas y los recursos utilizados como la grabación tendrán consideración de elemento entregable.

Planes de trabajo generales

Con objeto de simplificar los trámites, el adjudicatario podrá elaborar, por iniciativa propia o a solicitud de la persona responsable del servicio o responsable del contrato, propuestas de planes de trabajo generales para uno o varios servicios y establecer en qué condiciones podrán ser aplicados. La persona responsable del servicio podrá acogerse a estos planes de trabajo generales siempre que se cumplan dichas

condiciones. Los planes de trabajo generales no serán vinculantes para la persona responsable del servicio, que podrá requerir un plan de trabajo específico siempre que lo considere oportuno para una mejor prestación del servicio.

VAL-PLANES-TRAB-GEN: Las ofertas podrán incluir propuestas de planes de trabajo generales, prediseñados, que tendrán la misma consideración que los presentados durante la ejecución del contrato (SOBRE 2).

6.6. Entregables

A modo de recopilación y resumen, se enumeran a continuación los elementos que deberán ser entregados por el adjudicatario como resultado de la prestación de los servicios comprendidos en el presente lote, así como sus contenidos mínimos.

La persona responsable del servicio establecerá los canales, los medios y el procedimiento que deberá utilizar el adjudicatario para realizar la entrega de cada uno de los elementos entregables. El adjudicatario no utilizará ningún otro canal o medio para ello ni realizará ninguna comunicación de estos entregables a otras personas o entidades ajenas a la Agencia Digital de Andalucía y a AndalucíaCERT sin un consentimiento expreso y por escrito del responsable del contrato.

El procedimiento establecido podrá incluir, además de la propia entrega, actividades adicionales como la emisión de notificaciones o el registro de la información en otros sistemas.

Previo informe favorable de la persona responsable del servicio y autorización de la persona responsable del contrato, la entrega de todos o algunos de los entregables incluidos en este apartado podrá ser sustituida, siempre que lo permita su contenido y forma de elaboración y se garantice el nivel de seguridad adecuado, por:

- La inclusión del entregable en un repositorio u otro tipo de sistema desde el que pueda ser obtenido por AndalucíaCERT, con notificación a las personas responsables del contrato y del servicio.
- La puesta a disposición de AndalucíaCERT de una funcionalidad automatizada que permita realizar su generación y obtención en tiempo real.

Todos los entregables deberán estar elaborados en idioma castellano, salvo que se dé alguna de las siguientes circunstancias:

- Que así esté contemplado de forma expresa en el presente documento.
- Que el entregable sea traducción de otro que ya obre en poder de la persona responsable del servicio o del contrato, según corresponda.

- Que el entregable sea traducción de otro y ambos sean remitidos o puestos a disposición de la persona responsable del contrato o del servicio, según corresponda, de forma conjunta o simultánea.
- Que así lo solicite o autorice expresamente la persona responsable del servicio.

Los elementos entregables que consistan en uno o varios documentos ofimáticos serán ofrecidos, siempre que su naturaleza lo permita, en uno de los siguientes formatos:

- OpenDocument.
- Office Open XML.

Los elementos entregables que consistan en uno o varios documentos de video o de video y audio serán ofrecidos, siempre que su naturaleza lo permita, en formato Mp4.

El responsable del servicio podrá establecer modelos y criterios para los entregables o requisitos en lo referente a su apariencia, disposición, índice de contenidos, marcado TLP, limpieza de metadatos, uso de logos y otros elementos de la imagen corporativa, etc.

Los entregables podrán ser revisados por el responsable del servicio/contrato y podrán ser rechazados parcial o totalmente si, a su juicio, no reúnen la calidad mínima exigible.

A modo de recopilación y resumen, se enumeran a continuación los entregables del presente lote, así como su contenido mínimo.

6.6.1. Entregables de carácter general

- **Plan técnico de implantación de los servicios**
    - Arquitectura del conjunto de herramientas y sistemas desplegados. Diagramas físicos y lógicos.
    - Identificación de dependencias del despliegue y necesidades para el despliegue de plataformas y sistemas en las infraestructuras de AndalucíaCERT.
    - Plan detallado de puesta en marcha y configuración de los servicios, incluyendo estimación de tiempos para cada una de las tareas.
    - Documentación técnica de las herramientas: Casos de uso / manuales de uso y administración
    - Caracterización y documentación de los servicios a implantar
        - Definición y alcance del servicio

- Flujos, procedimientos e instrucciones de trabajo relacionadas con la prestación del mismo.
- Roles, responsabilidades y dedicación de cada integrante del equipo.
- Mecanismos de interlocución.
- Matriz de escalados.
- Integraciones previstas de los servicios con herramientas y procesos existentes.

- **Informe de implantación de los servicios**
  - Informe detallando el resultado de la ejecución del Plan Técnico de Implantación, y que servirá como base para la aceptación del sistema.
  - Se incluirán los apartados del Plan Técnico de Implantación (arquitectura, documentación técnica de las herramientas, caracterización y procedimientos de uso de los servicios…) tal como hayan quedado definidos tras el proceso de implantación.
- **Informe mensual de seguimiento**
  - Descripción general de los trabajos realizados en los servicios del lote y de los resultados obtenidos, justificando (donde proceda) los tiempos consumidos en cada una de las actividades y detallando los elementos unitarios facturables en el periodo.
  - Listado de los elementos unitarios consumidos a lo largo del mes.
  - Incidencias tanto técnicas como del equipo de trabajo.
  - Riesgos detectados y propuestas de mitigación.
  - Propuestas de mejora que se puedan aplicar para el cumplimiento de los objetivos de los servicios del lote.
  - Actas de las reuniones que hayan tenido lugar en ese periodo. Compete al licitador tomar notas y elaborar y difundir la correspondiente acta por cada reunión mantenida. Dicho documento deberá recoger, al menos: Lugar y fecha de reunión, horas de inicio y finalización, número de asistentes, orden del día, acuerdos y compromisos alcanzados por ambas partes, así como si procede, revisión de los acuerdos y compromisos alcanzados en reuniones previas.
- **Informe mensual de cumplimiento de ANS** que incluya, para cada servicio y ANS asociado:
  - Modo de cálculo de la penalización, cuando proceda, que podrá tomar uno de los siguientes valores conforme lo establecido en la documentación de la presente licitación:
    - Por exceso de tiempo con respecto al plazo establecido.

- Por porcentaje de solicitudes o intervenciones que incumplan el ANS.
  - Cuando la penalización se calcule por tiempo superando el plazo establecido:
    - Tiempo asignado para el ANS.
    - Tiempo, en las unidades establecidas para el ANS, que se ha superado el plazo. Si no se ha superado, se indicará cero (0).
  - Cuando la penalización se calcule respecto del porcentaje de solicitudes o intervenciones que cumplan el ANS:
    - Porcentaje de solicitudes o peticiones para las que se ha incumplido en ANS con respecto al número total.
  - El informe contendrá también un anexo en el que se mostrará la información anterior únicamente para aquellos servicios en los que se haya producido algún incumplimiento del ANS.

- **Informe anual del plan de formación del equipo de trabajo**
  - Plan de formación actualizado del personal del proveedor
  - Acciones formativas que se han llevado a cabo.
  - Evidencias de la realización.

- **Memoria final del proyecto**
  - Listado de entregables producidos.
  - Recursos consumidos.
  - Indicadores.
  - Lecciones aprendidas.
  - Propuesta de recomendaciones de actividades y objetivos a desarrollar y alcanzar en los siguientes meses en el ámbito de los servicios descritos en el presente pliego.
  - Actas de las reuniones que hayan tenido lugar durante el contrato. Compete al licitador tomar notas y elaborar y difundir la correspondiente acta por cada reunión mantenida. Dicho documento deberá recoger, al menos: Lugar y fecha de reunión, horas de inicio y finalización, número de asistentes, orden del día, acuerdos y compromisos alcanzados por ambas partes, así como si procede, revisión de los acuerdos y compromisos alcanzados en reuniones previas.

- **Declaración de requisitos de funcionamiento**.
  - Para cada herramienta, plataforma o servicio proporcionado o utilizado por el adjudicatario para la prestación de los servicios incluidos en el presente lote se hará constar la siguiente información:

- Lista de direcciones IP y puertos a los que realizan conexiones las herramientas y productos utilizados.
- Lista de software utilizado para el soporte y la prestación del servicio, con indicación de las versiones de productos.
- En su caso, proveedores de servicios en la nube utilizados.
    - Para cada proveedor de servicios en la nube, estados en los que se encuentran ubicados los servidores utilizados para la prestación de servicios en la nube.

6.6.2. Entregables del servicio de alerta temprana y asesoramiento sobre vulnerabilidades

- **Informe mensual de potenciales vulnerabilidades detectadas en el marco del subservicio de plataforma de inventariado, contraste y análisis de vulnerabilidades y amenazas**. El adjudicatario elaborará dos tipos de informe: uno destinado a cada organismo o tenant, que incluirá únicamente los datos referidos a este y otro dirigido a AndalucíaCERT, con los datos correspondientes a todos los organismos o tenants.
    - Resumen ejecutivo con información sobre el número de potenciales vulnerabilidades y la evolución temporal de los datos. Se incluirá al menos datos para cada uno de los siguientes criterios:
        - Nivel de criticidad.
        - En el caso del informe dirigido a AndalucíaCERT, nivel de criticidad y organismo.
        - Nivel de criticidad y principales productos afectados.
        - Análisis de la evolución temporal de las vulnerabilidades detectadas.
    - Detalle de las vulnerabilidades detectadas, incluyendo:
        - Identificación y descripción de la vulnerabilidad.
        - Contexto y condiciones relevantes para entender la vulnerabilidad en el contexto de la Junta de Andalucía y el grupo atendido de AndalucíaCERT y establecer la prioridad de su tratamiento.
        - Indicador del nivel de relevancia e impacto de la vulnerabilidad para la Junta de Andalucía y el grupo atendido de AndalucíaCERT, de acuerdo con las características de las redes y los sistemas y del entorno de cada organismo y de la Junta de Andalucía.

- Información sobre medidas a tomar para la mitigación o eliminación de la vulnerabilidad.
- Enlaces y referencias sobre la vulnerabilidad y su contexto.

- Información sobre vulnerabilidades que han tenido un impacto global significativo durante el periodo.
- Propuesta de priorización de las actuaciones a realizar para la mitigación o eliminación de las vulnerabilidades.
- Documentación y recursos de referencia.
- Junto con cada informe, tanto en los dirigidos a AndalucíaCERT como en los destinados a los organismos o tenant, se entregará la información contenida en los distintos apartados en un formato de datos estructurado (por ejemplo: CSV, XML o JSON) que será determinado en cada momento por AndalucíaCERT.

6.6.3. Entregables del servicio de análisis de la superficie de exposición en Internet

- **Informe mensual de análisis de la superficie de exposición en Internet**.
  - Resumen ejecutivo.
    - Número total de activos detectados.
    - Número de cambios detectados en la infraestructura:
      - Nuevos equipos.
      - Nuevos servicios.
      - Cambios en versiones de servicios
      - Equipos que hayan dejado de estar accesibles.
      - Servicios que hayan dejado de estar accesibles.
  - Equipos y/o servicios detectados con potencial impacto significativo sobre la seguridad. Sin perjuicio de que posteriormente se aborde un análisis de vulnerabilidades en profundidad mediante el servicio correspondiente, se expondrá aquí una primera aproximación sobre:
    - Vulnerabilidades que podrían afectarles.
    - Riesgo que podrían implicar.
    - Recomendaciones para la mitigación del riesgo.

- Documentación y recursos de referencia.
- Se acompañará a cada informe de la información contenida en sus distintos apartados, así como un inventario completo de activos, con indicación de los puertos y servicios detectados para cada uno de ellos, en formato de datos estructurado (por ejemplo: CSV, XML o JSON) que será determinado en cada momento por AndalucíaCERT.

6.6.4. Entregables del servicio de análisis de vulnerabilidades

6.6.4.1. Entregables del subservicio de análisis desatendido de vulnerabilidades

- **Documentación de la plataforma de análisis desatendido de vulnerabilidades.**
  - Guía de uso de la plataforma.
  - Manuales de uso de las aplicaciones.
  - Casos de uso de especial relevancia.
- **Informe mensual de uso de la plataforma de análisis desatendido de vulnerabilidades**
  - Resumen ejecutivo.
  - Estadísticas de uso de la plataforma de análisis desatendido de vulnerabilidades.
  - Cronograma de uso de la plataforma de análisis desatendido de vulnerabilidades por parte de AndalucíaCERT y cada uno de los organismos de su grupo atendido.
  - Incidencias producidas en la plataforma de análisis desatendido de vulnerabilidades y acciones realizadas como respuesta a las mismas.
  - Operaciones de mantenimiento, ampliaciones y actualizaciones realizadas sobre la plataforma de análisis desatendido de vulnerabilidades y acciones realizadas como respuesta a las mismas.

6.6.4.2. Entregables del subservicio de análisis atendido de vulnerabilidades

- **Informe de cada análisis de vulnerabilidades, modalidad "Periódico-Automatizada"**
  - Datos del análisis: fecha y hora, origen, objetivos, aspectos destacables…
  - Relación de vulnerabilidades, indicando para cada una de ellas:
    - Identificación.

- Determinación del nivel de riesgo y de impacto asociado.
- Cualquier otra información relevante proporcionada por el análisis.

- **Informe de cada análisis de vulnerabilidades, modalidad "Puntual-Manual" (a demanda)**
  - Datos del análisis: fecha y hora, solicitante, origen, objetivos, aspectos destacables…
  - Relación de vulnerabilidades, indicando para cada una de ellas:
    - Identificación.
    - Determinación del nivel de riesgo y de impacto asociado.
    - Cualquier otra información relevante proporcionada por el análisis.
  - Evaluación manual de los resultados obtenidos conforme a los activos y servicios analizados y las vulnerabilidades detectadas, contextualizando en el entorno desde y hacia el que se publican los servicios en el marco de la Red Corporativa de la Junta de Andalucía.
  - Información sobre el impacto de las vulnerabilidades detectadas y una propuesta de priorización de las acciones de remediación a acometer.

6.6.5. Entregables del servicio de vigilancia digital e inteligencia de amenazas

- **Informe mensual del servicio de vgilancia digital**.
  - Resumen ejecutivo.
  - Cambios significativos apreciados en los activos y las potenciales amenazas a que se encuentran expuestos.
  - Detalle de las amenazas detectadas durante el periodo que afecten o pudiesen afectar significativamente a la Junta de Andalucía y los organismos integrados en el grupo atendido de AndalucíaCERT.
    - Campañas detectadas.
    - Recursos utilizados en las campañas detectadas.
    - Fugas y publicaciones no autorizadas de información.
    - Aplicaciones maliciosas o fraudulentas.
    - Suplantaciones de identidad.
  - Recomendaciones.
  - Documentación y recursos de referencia.
- **Informe mensual del servicio de Inteligencia de Amenazas**.
  - Resumen ejecutivo.

- Contexto de ciberseguridad nacional y e internacional y tendencias.
- Contexto de ciberseguridad en el ámbito de las administraciones públicas a nivel nacional y de Andalucía.
- Contexto de ciberseguridad en el ámbito de las Infraestructuras Críticas.
- Informe de detalle de las amenazas detectadas durante el periodo que afecten o pudiesen afectar significativamente a la Junta de Andalucía y los organismos integrados en el grupo atendido de AndalucíaCERT.
  - Identificación de la amenaza.
  - Descripción.
  - Indicadores de Compromiso.
  - Reglas Yara y/o Snort para la detección.
  - Recomendaciones para prevenir la amenaza y/o reducir su posible impacto.
  - Etc.
- Listado de fuentes utilizadas para el servicio de Inteligencia de Amenazas. En caso de no haber variado con respecto a las incluidas en el informe anterior, o en su caso las indicadas en la oferta, será suficiente con indicar este extremo.
- Documentación y recursos de referencia.

6.6.6. **Entregables del servicio de análisis forense**

6.6.6.1. ***Entregables del subservicio de peritaje informático***

- **Informe pericial**. El informe pericial deberá cumplir en todo caso con lo indicado en la última versión publicada de la norma UNE 197001 “Criterios generales para la elaboración de informes periciales”.
- **Informe de actividad de presentación y/o defensa de informe pericial ante tribunales y otros órganos administrativos o judiciales**.
  - Identificación del informe pericial.
  - Fecha de las actuaciones.
  - Lugar de las actuaciones.
  - Tribunales u órganos ante las que se realizan las actuaciones.
  - Descripción de las actuaciones realizadas.
  - Documentación acreditativa de las actuaciones realizadas.

- Cuando proceda, resultado o retroalimentación obtenida a partir de las actuaciones realizadas.
- Cuando proceda, identificación y descripción de otras actuaciones necesarias.

6.6.6.2. *Entregables del subservicio de análisis DFIR*

- **Guía o Instrucción técnica para el despliegue de agentes y software de triaje y adquisición de información**.
  - Descripción del agente o del software a desplegar.
    - Identificación.
    - Funcionalidades y objetivos del producto.
  - Requisitos para el despliegue.
  - Instrucciones de despliegue con capturas de pantalla de los momentos en los que sea necesaria interacción humana con el producto o con su proceso de instalación.
  - Instrucciones de inicio de la ejecución del software, cuando sea preciso.
  - Datos de contacto para la resolución de dudas e incidencias.
- **Informe de análisis DFIR**.
  - Antecedentes
    - Descripción del incidente.
    - Objetivos del análisis.
  - Resumen ejecutivo
  - Análisis Técnico
    - Herramientas utilizadas.
    - Tareas realizadas para la recolección de datos y evidencias
    - Descripción de las evidencias obtenidas
    - Tareas de análisis realizadas sobre las evidencias.
    - Resultados de las tareas de análisis.
    - Línea temporal de los sucesos identificados.

- Conclusiones.
- Recomendaciones para evitar que el incidente vuelva a producirse y/o reducir su impacto
    - Buenas prácticas.
    - Mejoras.
- Referencias y documentación relacionada.

6.6.7. Entregables del servicio de obtención, certificación y preservación de evidencias digitales

- **Documentación acreditativa de la validez y de la forma de recuperación de las evidencias derivadas del servicio de obtención, certificación y preservación de evidencias digitales**.

6.6.8. Entregables del servicio de elaboración de informes técnicos

- **Propuesta anual de materias a tratar**.
    - Relación de materias. Deberán incluirse al menos 12 materias en la propuesta.
    - Para cada materia.
        - Breve Descripción.
        - Justificación de la conveniencia de elaboración de informe.
        - Destinatarios potenciales del informe.
        - Cuando proceda, propuesta de fechas aproximadas para la publicación del informe.
- **Informe técnico**, con una extensión típica de entre 15 y 40 páginas.
    - Índice.
    - Información corporativa sobre AndalucíaCERT (será proporcionada por AndalucíaCERT al adjudicatario).
    - Objeto y alcance del informe.
    - Introducción o resumen de los temas abordados.
    - Desarrollo del tema en cuestión.

- Conclusiones.
- Glosario de términos.
- Bibliografía.

6.6.9. Entregables del servicio de análisis de malware

- **Informe de malware analizado**, con una extensión típica de entre 15 y 20 páginas.
  - Índice.
  - Información corporativa sobre AndalucíaCERT (será proporcionada por AndalucíaCERT al adjudicatario).
  - Resumen ejecutivo.
  - Detalles generales y e identificativos del malware.
  - Características funcionales del malware.
  - Procedimiento de infección.
  - Características técnicas del malware.
  - Técnicas de cifrado y ofuscación.
  - Técnicas de persistencia.
  - Conexiones de red realizadas.
  - Ficheros relacionados.
  - Técnicas de detección.
  - Técnicas de vacunación.
  - Técnicas de mitigación de efectos y limpieza del malware.
  - Referencias
- **Listado de indicadores de compromiso relacionados con malware analizado**, elaborado y entregado en formato estándar (OpenIOC o similar).
  - Acceso a direcciones IP.
  - Dominios relacionados.
  - URLs utilizadas.

- Hashes de ficheros.
- Etc.

- **Reglas de detección de tipo SNORT para la detección de malware analizado**.
- **Reglas YARA para la detección de malware analizado**.

6.6.10. Entregables del servicio de realización de ciberejercicios

- **Informe de realización de ciberejercicio**.
  - Índice.
  - Resumen ejecutivo.
  - Tipo, Alcance y objetivos.
  - Organización y planificación de los trabajos.
  - Resultados obtenidos.
  - Interpretación y análisis de los resultados.
  - Recomendaciones.
  - Referencias.

6.6.11. Entregables del servicio de proyectos en protección, detección y respuesta

- **Informe de proyecto de en protección, detección y respuesta**
  - Índice.
  - Resumen ejecutivo.
  - Descripción del Proyecto.
  - Organización y planificación de los trabajos.
  - El contenido acordado entre la persona responsable del contrato y el adjudicatario para los resultados del proyecto.
  - Referencias

6.6.12. Entregables del servicio de intervención especializada

- **Informe de intervención especializada**
    - Índice.
    - Resumen ejecutivo.
    - Descripción de la intervención.
    - Organización y planificación de los trabajos.
    - El contenido acordado entre la persona responsable del contrato y el adjudicatario para los resultados a obtener.
    - Referencias

6.7. Acuerdo de nivel de servicio (ANS)

El licitador deberá asumir y cumplir los plazos y niveles de servicio establecidos en este documento

Definiciones

A efectos de la determinación del cumplimiento de los acuerdos de nivel de servicio, se establecen las siguientes definiciones.

- **Tiempo de respuesta**:
    - **Cuando AndalucíaCERT o los organismos o entidades de su ámbito de actuación notifiquen incidencias, incidentes o solicitudes de servicio:** Tiempo transcurrido desde la notificación de una incidencia, un incidente o una solicitud de servicio hasta el momento en que el adjudicatario se pone en contacto con la persona o entidad emisora de la notificación.
    - **Cuando se detecten incidencias o incidentes de forma automática o de forma proactiva por el adjudicatario**: Tiempo transcurrido desde la detección hasta el momento en que el adjudicatario haya iniciado las actuaciones para su tratamiento y lo haya comunicado a AndalucíaCERT (el mayor de estos dos tiempos).
- **Tiempo de entrega del plan de acción**: Tiempo transcurrido desde la realización de una solicitud de servicio hasta el momento en que el adjudicatario presente el correspondiente plan de acción, con el contenido y las características indicadas en el apartado de Entregables del lote correspondiente.
- **Tiempo de resolución**:

- **Para las solicitudes de servicio**: Tiempo transcurrido desde la notificación una solicitud de servicio hasta que se ha dado respuesta completa a la misma y, en su caso, se ha generado la documentación correspondiente a su cierre.
- **Para las incidencias y los incidentes**: Tiempo transcurrido desde la notificación o detección de la incidencia o el incidente hasta el momento en que se le ha dado respuesta completa y, en su caso, se ha generado la documentación correspondiente a su cierre.

- **Tiempo de asistencia a las instalaciones**:
  - **Para incidencias del equipamiento con asistencia in-situ**: Tiempo transcurrido entre la notificación de la incidencia y el momento en que el personal técnico del adjudicatario o del soporte del producto se persone en la sede donde se encuentre el equipamiento afectado.
  - **Para incidencias e incidentes de seguridad o que afecten a sistemas y redes**: Tiempo transcurrido desde la asignación de la notificación de la incidencia o el incidente que requiera de asistencia hasta que el personal técnico del adjudicatario se persone en la sede o las sedes donde sea necesario realizar las actuaciones.
- **Tiempo de reposición del equipamiento de reemplazo**:
  - **Cuando se haya realizado la sustitución de un equipo por otro de reemplazo**: Tiempo transcurrido desde la puesta en servicio del equipo o de los equipos de reemplazo y el momento en que se vuelva a disponer del número de equipos de reemplazo establecidos en este documento.
- **Tiempo de sustitución definitiva de equipamiento**: Tiempo transcurrido desde la determinación de la necesidad de realizar una sustitución de uno o varios equipos y el momento en que, habiendo realizado la sustitución, se vuelva a disponer del número de equipos de reemplazo establecidos en este documento.
- **Disponibilidad**: Porcentaje del tiempo total que un sistema se encuentra plenamente operativo, proporcionando todas sus funcionalidades. Salvo que se indique expresamente otra cosa, se entenderá que la referencia para la disponibilidad es una prestación 24x7.
- **Tiempo de desplazamiento**: Tiempo transcurrido hasta la personación del personal del adjudicatario en una ubicación determinada por AndalucíaCERT, a contar desde la aprobación del correspondiente Plan de Acción o, para aquellos servicios que así lo contemplen, desde la realización de la solicitud de actuación presencial.

- **Periodo de realización**: Para las actividades que deban repetirse de forma periódica, tiempo transcurrido desde el inicio de la ejecución anterior de la actividad (o, en su caso, del inicio de la prestación del servicio correspondiente) y la ejecución actual.t

Condiciones generales de medida

- En la determinación de plazos y tiempos, para cada servicio incluido en cada lote, se aplicará el calendario y horario correspondiente a su modo de prestación.
- Para los plazos correspondientes a la ejecución de los proyectos se aplicará el calendario y horario correspondiente al modo de prestación 8x5.
- Para los plazos correspondientes a la planificación y ejecución de los proyectos se aplicará el calendario y horario correspondiente al modo de prestación 8x5, salvo que se establezca otra cosa en el correspondiente Plan de Acción.
- En el cálculo de los parámetros anteriormente definidos no se considerará el tiempo transcurrido en los siguientes casos, siempre y cuando sean debidamente justificados y recogidos en el sistema de gestión de incidencias y peticiones.
    - Paradas del servicio programadas por las partes para labores de mantenimiento.
    - Tiempos de no disponibilidad debidos a la imposibilidad de reposición del servicio por motivos no imputables a los adjudicatarios (por ejemplo, imposibilidad de acceso a instalaciones en las que deben realizarse los trabajos).
    - Pérdidas de servicio debidas a causas de fuerza mayor (por ejemplo, un desastre natural) ajenas a la responsabilidad del adjudicatario.

Será responsabilidad del adjudicatario velar por la adecuada actualización de los estados en el sistema de ticketing y gestión de consultas.

Informe de cumplimiento

Para la valoración del cumplimiento de ANS se utilizará el **Informe mensual de cumplimiento de ANS** emitido por el adjudicatario y descrito anteriormente.

Este informe debe entenderse sin perjuicio de las actividades que las personas responsables del contrato y del servicio puedan realizar conforme a su obligación de verificación y control del cumplimiento de lo establecido en la documentación correspondiente a la presente licitación y las condiciones ofertadas, así como de las mediciones que estas personas realicen relativas al cumplimiento de los ANS. Los plazos máximos se especifican en el apartado ANS Entrega de informes periódicos y singulares.

6.7.1. Disponibilidad inicial de todos los servicios

CRITERIO	VALOR DE COMPROMISO
Plazo para el inicio de la prestación de los servicios	5 días hábiles, a contar desde: • La finalización de la fase II del plan de ejecución del proyecto para los servicios que no dependan del despliegue de sistemas y herramientas en las infraestructuras de AndalucíaCERT. • La finalización de la fase III del plan de ejecución del proyecto para los servicios que dependan del despliegue de sistemas y herramientas en las infraestructuras de AndalucíaCERT.

El adjudicatario deberá asegurar la disponibilidad y prestación de todos los servicios incluidos en el presente lote en el plazo indicado.

Se considerará que existe incumplimiento cuando se supere el límite del valor de compromiso.

6.7.2. Actualización de relaciones de activos

Para aquellos servicios en los que se realice una monitorización, análisis o escaneo de un conjunto de activos determinados por AndalucíaCERT, se establece el siguiente Acuerdo de Nivel de Servicio

CRITERIO	VALOR DE COMPROMISO
Plazo de aplicación de los cambios de activos comunicados por AndalucíaCERT en los procesos correspondientes al servicio a los que dichos activos son aplicables.	5 días hábiles, a contar desde la comunicación de los cambios, salvo que en la comunicación de los cambios en los activos se establezca otro plazo mayor. Si los activos son utilizados en procesos de ejecución periódica, deberán incluirse en la ejecución siguiente a la finalización del plazo establecido en el apartado anterior.

Se considerará que existe incumplimiento cuando se supere el límite del valor de compromiso.

6.7.3. Presentación de informes

CRITERIO	VALOR DE COMPROMISO

Plazo de presentación de los entregables contemplados como de carácter periódico en el listado de entregables.	El décimo día natural posterior al periodo al que haga referencia el informe
Plazo de presentación de los entregables que deban ser elaborados y proporcionados como resultado de cada ejecución de un proceso o de un análisis.	10 días naturales a contar desde la finalización del proceso o el análisis a que haga referencia el entregable
Plazo de presentación de los informes contemplados en el listado de entregables que sean generados de forma automática.	5 días hábiles, a contar desde la finalización del proceso que generó el informe.

Se considerará que existe incumplimiento cuando se supere el límite del valor de compromiso.

VAL-ANS-6: Se valorará el valor comprometido de este ANS por debajo del mínimo aquí indicado. (SOBRE 3, NO INCLUIR EN SOBRE 2).

6.7.4. Incidencias en el funcionamiento de las plataformas y herramientas puestas a disposición de AndalucíaCERT

CRITERIO (lote 2)	VALOR DE COMPROMISO
Tiempo de resolución de incidencias críticas	5 horas
Tiempo de resolución de incidencias no críticas	12 horas

Este acuerdo de nivel de servicio no será aplicable a las plataformas y herramientas de terceros que el proveedor ofrezca en virtud exclusivamente de lo establecido en el último párrafo del subapartado

"Descripción" del epígrafe "Vigilancia digital" (Shodan.io, Censys.io, Pastebin y aquellos que se incluya en la oferta dentro de este grupo y no se utilicen para la prestación de otros servicios ni como plataforma principal para este).

Se considerará incidencias críticas aquellas en las que se produzca una degradación significativa o permanente del servicio prestado por la herramienta o plataforma o impida la prestación de este servicio en las debidas condiciones de seguridad. El resto de las incidencias serán consideradas no críticas.

Tendrán en todo caso consideración incidencia no crítica aquellas que afecten a la plataforma de análisis desatendido de vulnerabilidades.

Se considerará que existe incumplimiento cuando se supere el valor de compromiso.

VAL-ANS-7: Se valorará el valor comprometido de este ANS por debajo del mínimo aquí indicado. (SOBRE 3, NO INCLUIR EN SOBRE 2).

6.7.5. Periodo de realización de análisis y escaneado

CRITERIO	VALOR DE COMPROMISO
Periodo de realización de escaneos de la superficie completa de exposición en Internet	1 mes
Periodo de realización del conjunto de análisis periódicos automatizado de vulnerabilidades	1 mes

Se considerará que existe incumplimiento cuando se supere el valor de compromiso.

VAL-ANS-8: Se valorará el valor comprometido de este ANS por debajo del mínimo aquí indicado. (SOBRE 3, NO INCLUIR EN SOBRE 2).

6.7.6. Plazo de ejecución de los proyectos

CRITERIO	VALOR DE COMPROMISO
Plazo para la ejecución de las actuaciones asociadas a cada proyecto y la entrega o puesta a	El establecido en el correspondiente Plan de Acción.

disposición de los correspondientes elementos entregables	

Se considerará que existe incumplimiento cuando se supere el límite del valor de compromiso.

6.7.7. Tiempos de entrega de plan de acción y de desplazamiento

Los tiempos de desplazamiento establecidos en la siguiente tabla corresponden a los casos en que se requiera el desplazamiento del personal del adjudicatario antes de la aprobación del Plan de Acción para realizar tareas urgentes o que sean necesarias para la correcta elaboración del Plan de Acción o la adecuada prestación del servicio.

En otro caso, los tiempos de desplazamiento serán, cuando corresponda, los establecidos en el Plan de Acción aprobado.

Servicio / Subservicio	Tiempo de entrega del plan de acción	Tiempo de desplazamiento
Servicio de análisis forense	3 días hábiles	16 horas
Obtención, certificación y preservación de evidencias digitales	3 días hábiles	16 horas
Elaboración de informes	5 días hábiles	No aplica
Análisis de malware	5 días hábiles	El establecido en el Plan de Acción
Realización de ciberejercicios	5 días hábiles	El establecido en el Plan de Acción
Proyectos en protección, detección y respuesta	5 días hábiles	No aplica
Servicio de intervención especializada	5 días hábiles	16 horas

Se considerará que existe incumplimiento cuando se supere el límite del valor de compromiso.

7. Organización del trabajo

La organización definida en este apartado es de aplicación individual a cada lote de la contratación, o a ambos en caso de oferta integradora.

7.1. Dirección y seguimiento de los trabajos

El adjudicatario aportará su propia dirección y gestión al contrato, siendo responsable de la organización del servicio, de la calidad técnica de los trabajos que desarrolle y de las prestaciones y servicios realizados, en los términos del artículo 311 Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

La empresa contratista dispondrá, para la ejecución del contrato, de una estructura jerarquizada, que se hará responsable de impartir a sus trabajadores las correspondientes órdenes, criterios de realización del trabajo y directrices de cómo distribuirlo.

Será responsabilidad del adjudicatario impartir todas las órdenes, criterios de realización del trabajo y directrices a sus trabajadores/as, siendo la Agencia Digital de Andalucía y AndalucíaCERT del todo ajenas a estas relaciones laborales y absteniéndose, en todo caso, de incidir en las mismas.

Corresponderá, asimismo, de forma exclusiva al adjudicatario la vigilancia del horario de trabajo de los trabajadores, las posibles licencias horarias o permisos o cualquiera otra manifestación de las facultades del empleador.

También será responsabilidad exclusiva del adjudicatario, en la forma establecida en este documento y el resto de documentación de la actual licitación, asegurar que el servicio quede convenientemente cubierto.

Independientemente de la naturaleza de la causa (períodos vacacionales, enfermedad, baja laboral, etc.), en caso de que alguna persona del equipo de trabajo propuesto no pueda desempeñar el servicio objeto de este pliego, el adjudicatario está obligado a sustituir a dicha persona por otra de idéntica preparación, así como, salvo en los casos de sustituciones no programadas cuyas circunstancias lo hagan imposible, a comunicar dicha sustitución con al menos 15 días de antelación.

Corresponderán a la Agencia Digital de Andalucía y a AndalucíaCERT los poderes de verificación y control de la contrata establecidos en el Ley 9/2017, de 8 de noviembre, absteniéndose para ello de ejercer función alguna de control, dirección u organización del personal de la empresa contratista.

El adjudicatario deberá especificar un interlocutor único que organizará la ejecución de los servicios profesionales objeto del contrato de acuerdo con este pliego de condiciones técnicas, pondrá en práctica las instrucciones de la persona responsable del contrato e impartirá las pertinentes instrucciones al personal del adjudicatario.

Este interlocutor y los diferentes miembros del equipo deberán asistir a las reuniones que se convoquen relacionadas con las actividades desarrolladas por el presente contrato.

7.2. Funciones y responsabilidades

Existirá una organización específica prevista para el desarrollo de los trabajos en la que cada función quede perfectamente identificada, y cada función tenga asignada una persona responsable de su cumplimiento. Se establecen las siguientes figuras:

1. Responsable del contrato
2. Responsable del servicio
3. Jefatura del proyecto
4. Equipo del proyecto

7.3. Responsable del contrato

La Agencia Digital de Andalucía es la responsable del contrato, y le corresponde la supervisión de su ejecución, la adopción de decisiones y el dictado de las instrucciones necesarias con el fin de asegurar la correcta realización de este.

Se designará una persona responsable del contrato, entre cuyas actividades se encuentran:

- Coordinación y dirección del proyecto.
- Interlocución con el adjudicatario para impartir cuantas instrucciones y requerimientos sean convenientes o necesarios para la mejor prestación de los servicios.
- Comprobación y seguimiento del correcto cumplimiento y ejecución del contrato.
- Gestión de la demanda de recursos.
- Seguimiento de los Acuerdos de Nivel de Servicio (ANS), cálculo y propuesta de penalizaciones en su caso.
- Propuesta de cambios en el equipo de trabajo del adjudicatario durante la duración del contrato y sus posibles prórrogas en caso ser necesario para adecuarlo a las necesidades del servicio prestado definido en el pliego de prescripciones técnicas o la oferta presentada.

La persona responsable del contrato podrá delegar funciones de operación. gestión y seguimiento en la persona que, en su caso, se designe como responsable del servicio en AndalucíaCERT. En estos casos, la persona responsable del contrato comunicará al adjudicatario las delegaciones realizadas a la mayor brevedad posible y sin dilación indebida.

7.4. Responsable del servicio

La persona responsable del servicio realizará, por sí misma o a través del personal a su cargo, el seguimiento de las actividades propias de la gestión del contrato y de los acuerdos de nivel de servicio establecidos, así como aquellas que le sean delegadas por la persona responsable del contrato.

Asimismo, estudiará las solicitudes de autorización remitidas por el adjudicatario en relación con los tratamientos de datos personales y de la información utilizada.

La persona responsable del contrato podrá asumir, con carácter puntual o general, todas o parte de las funciones de la persona responsable del servicio.

La persona responsable del servicio podrá delegar en otras, con carácter puntual o general, todas o parte de sus funciones. En estos casos, la persona responsable del servicio comunicará al adjudicatario las delegaciones realizadas a la mayor brevedad posible y sin dilación indebida.

7.5. Jefatura del proyecto

El adjudicatario designará la persona que ejercerá la jefatura del proyecto, cuyas funciones incluirán:

- Interlocución con las personas responsables del contrato y del servicio, así como con cualquier otro punto de contacto que establezca la Agencia Digital de Andalucía o AndalucíaCERT.
- Organización, coordinación y control de la prestación de los servicios y la entrega de los suministros.
- Seguimiento, control, gestión y garantía del cumplimiento de las planificaciones de trabajos.
- Dirección y gestión del equipo de proyecto.
- Seguimiento, control y gestión de los trabajos y del cumplimiento del contrato para una ejecución eficaz y eficiente de este.
- Supervisión del grado de cumplimiento de los objetivos y criterios establecidos.
- Control de calidad y auditoría interna.
- Propuesta de las modificaciones que considere necesarias para la correcta ejecución de los servicios.
- Entrega de la información requerida para el control del contrato y la prestación de los servicios.

Esta persona se encontrará asignada al proyecto de forma permanente con una modalidad de prestación 8x5 y dedicación mínima del 25% a las funciones propias de la jefatura del proyecto.

Para reflejar los trabajos de este perfil (horas) se considerará el elemento unitario ELEM-JF-PROYECTO.

El puesto debe contar en todo momento con una persona suplente que permita cubrir indisponibilidades temporales, vacaciones y cualquier otra circunstancia que impida su adecuado desempeño por parte de la persona que lo esté ejerciendo, ya sea como titular o en virtud de una suplencia.

Cuando se produzca una suplencia en la jefatura del proyecto, el adjudicatario deberá comunicarlo a las personas responsables del contrato y del servicio a la mayor brevedad posible y sin dilación indebida. En dicha comunicación se indicará también el nombre, los datos de contacto y la cualificación profesional de la persona que propone para asumir la nueva suplencia, que en todo caso deberá cumplir con los requisitos establecidos para ejercer la jefatura del proyecto. Esta propuesta deberá ser aprobada por la persona responsable del servicio. Si no la rechazara de forma expresa en el plazo de cinco (5) días hábiles, se entenderá que se otorga la aprobación. En otro caso, el adjudicatario deberá realizar una nueva propuesta.

El adjudicatario dedicará a estas funciones personal con el perfil profesional establecido en el apartado 4.C "solvencia técnica o profesional" del Anexo I del Pliego de Cláusulas Administrativas Particulares.

La persona que ejerza la jefatura del proyecto podrá formar parte del equipo del proyecto, en cuyo caso deberá poseer la cualificación y experiencia necesarias para realizar las tareas en las que participe.

7.6. Equipo del proyecto

El equipo de proyecto será el responsable de la realización de todos los trabajos descritos en el presente pliego, ya sea presencialmente desde las instalaciones de la Junta de Andalucía o bien de manera deslocalizada. El adjudicatario aportará un equipo de trabajo integrado por cuantos técnicos de adecuada cualificación y nivel de dedicación sean necesarios en cada momento para la adecuada prestación de los servicios.

La falsedad en el nivel de conocimientos técnicos del personal ofertado y su experiencia, deducida del contraste entre la información especificada en la oferta y los conocimientos reales demostrados en la ejecución de los trabajos podrá ser motivo de la rescisión del contrato de forma unilateral por parte de la Agencia Digital de Andalucía, sin que el adjudicatario pueda reclamar cantidad alguna en concepto de indemnización por daños y perjuicios.

7.7. Datos de contacto

Durante la fase I de la ejecución del proyecto "Definición del despliegue", el adjudicatario comunicará al responsable del contrato los siguientes datos de contacto:

- Persona responsable de la jefatura del proyecto.
- Atención de solicitudes, consultas, incidencias y reclamaciones relacionadas con los servicios y su estado.

- Atención durante las guardias previstas (en lote 1).

Asimismo, en los informes y en las guías e instrucciones técnicas que se contempla, en algunos casos, en el apartado de Entregables correspondientes al Lote 2 deberá incluirse los datos de contacto pertinentes a efectos de resolución de dudas y otras incidencias.

En cada caso, se proporcionará como mínimo, la siguiente información:

1. Nombre y apellidos o denominación.
2. Número de teléfono. Deberá tratarse de un número de teléfono móvil o geográfico. No se permitirá el uso de números “90x”, “80x” o de tarificación adicional o especial.
3. Dirección de correo electrónico.

Para la atención de solicitudes e incidencias de los servicios se ofrecerá, además, una URL para el acceso a un servicio de comunicación y gestión de incidencias y solicitudes de servicio. No obstante, si durante la ejecución del contrato se estimara más eficaz, podrá acordarse con el responsable del servicio el uso de alguna herramienta de seguimiento desplegada en el ámbito de la Junta de Andalucía.

Como norma general, el adjudicatario garantizará la atención a los datos de contacto ofrecidos en modalidad de horario 8x5. Esta garantía deberá extenderse a la modalidad de horario 24x7 cuando estos datos estén vinculados a servicios prestados en dicha modalidad.

Sin perjuicio de que el adjudicatario pueda ofrecer un teléfono de contacto para cada servicio o para cada conjunto de servicios, deberá en todo caso proporcionar uno mediante el que sea posible comunicar las solicitudes e incidencias correspondientes a todos los servicios contratados, correspondiendo al adjudicatario cualquier posible gestión posterior de las comunicaciones recibidas.

Los datos de contacto proporcionados deberán mantenerse continuamente actualizados. Para ello, el adjudicatario comunicará a la persona responsable del contrato cualquier cambio con una antelación mínima de 7 días naturales o, si esto no fuera posible, sin dilación indebida.

7.8. Condiciones específicas aplicables al personal asignado al proyecto por el adjudicatario

Todo el personal asignado al proyecto por el adjudicatario deberá firmar un acuerdo de confidencialidad, disponer de las acreditaciones y certificaciones necesarias para garantizar su adecuado desempeño y mantenerlas a lo largo de la vigencia del contrato, así como sus posibles prórrogas.

7.9. Modificaciones del equipo de trabajo

Lo indicado en este apartado será aplicable a aquellos servicios que cuenten con un equipo estable durante el periodo de vigencia del contrato y sus posibles prórrogas. Por consiguiente, no es de aplicación para el caso de los servicios clasificados como bajo demanda.

Salvo cuando esté contemplado en la aprobación de un plan de trabajo conforme a lo establecido en el presente documento, las modificaciones de la composición de los equipos de trabajo no derivadas de la carga de trabajo que sean propuestas por la empresa adjudicataria deberán ser notificadas por escrito a la persona responsable del servicio, exponiendo las razones que obligan a la propuesta, con una antelación mínima de 15 días naturales.

La sustitución de algún miembro del equipo de proyecto deberá realizarse por un perfil de cualificación técnica igual o superior a la de la persona que se pretende sustituir.

La autorización de cambios en la composición inicial requerirá de la siguiente documentación:

- Solicitud de cambio la persona responsable del servicio, que incluirá una justificación detallada y suficiente, explicando el motivo que suscita el cambio.
- Presentación de al menos 3 personas candidatas, con un perfil de cualificación técnica igual o superior al de la persona que se pretende sustituir.
- Aceptación expresa de alguno de los candidatos por parte de la persona responsable del servicio

En cualquier caso, no se admitirán cambios que de manera acumulada en un corto intervalo de tiempo pudieran conducir a un comportamiento defectuoso de los servicios, lo cual acarreará la correspondiente penalización. En casos severos, podrá ser causa de resolución del contrato.

Cuando la persona responsable del servicio o la persona responsable del contrato lo estime oportuno, podrá evaluar el perfil y la formación de las personas integrantes del equipo de proyecto pudiendo ser causa de sanción o resolución del contrato el hecho de que éste no cumpla los requisitos demandados.

La persona responsable del servicio o la responsable del contrato podrán solicitar el cambio de cualquiera de los componentes del equipo de trabajo si existiesen razones suficientemente justificadas que lo aconsejasen.

Los posibles inconvenientes de adaptación al entorno de trabajo y al proyecto debido a las sustituciones de personal, deberán ser subsanados mediante periodos de solapamiento de personal durante al menos 15 días laborables, sin que esto devengue coste alguno para la Agencia Digital de Andalucía. Si ello no fuera posible, las horas de trabajo equivalentes a las dos primeras semanas de trabajo del miembro sustituto no serán facturables.

La falsedad en el nivel de conocimientos técnicos del personal ofertado y su experiencia, deducida del contraste entre la información especificada en la oferta y los conocimientos reales demostrados en la

ejecución de los trabajos podrá ser motivo de la rescisión del contrato de forma unilateral por parte de la Agencia Digital de Andalucía, sin que el adjudicatario pueda reclamar cantidad alguna en concepto de indemnización por daños y perjuicios.

Los servicios deberán contar en todo momento con, al menos, una persona suplente que permita cubrir indisponibilidades temporales, vacaciones y cualquier otra circunstancia que impida su adecuado desempeño por parte de una persona que lo esté realizando, ya sea como titular o en virtud de una suplencia.

7.10. Formación continua del equipo de trabajo

El personal del adjudicatario que se integre en el equipo del proyecto o ejerza su jefatura deberá estar adecuadamente formado y actualizado en las nuevas tecnologías de la información y la comunicación, nuevas amenazas y técnicas de ataque.

La formación incluirá, aparte de los aspectos ligados al proyecto, los siguientes

a) Configuración de sistemas.
b) Detección y reacción ante incidentes.
c) Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción.

El adjudicatario deberá proveer a sus recursos técnicos de un plan de formación adecuado para renovar sus conocimientos incluyendo las nuevas tecnologías que vayan apareciendo en el sector de la seguridad informática relacionados con el servicio que se presta, incluida la formación en las herramientas utilizadas en AndalucíaCERT. Dicho plan deberá ser definido en la oferta y comunicado su avance de ejecución al responsable del servicio de forma semestral.

Los periodos de formación deberán ser planificados y consensuados entre la persona responsable del servicio y el adjudicatario, de manera que no afecten a la calidad del servicio prestado, ni tengan impacto sobre los horarios de trabajo de los técnicos.

7.11. Seguimiento de los trabajos

La persona que ejerza la jefatura del proyecto y la persona responsable del servicio colaborarán para realizar un seguimiento continuo de la evolución del proyecto

El adjudicatario elaborará y remitirá o pondrá a disposición de la persona responsable del servicio todos los meses un Informe de seguimiento.

Además, el adjudicatario deberá elaborar toda la documentación necesaria en base a las distintas actuaciones objeto del contrato de modo que toda actividad quede perfectamente documentada y registrada.

Se realizarán reuniones de seguimiento, de periodicidad mensual, en las que participarán la persona que ejerza la jefatura del proyecto y la persona responsable del servicio, o en quien ésta delegue, en las que se revisará el grado de cumplimiento de los objetivos, las reasignaciones y variaciones de efectivos de personal dedicado al proyecto, las especificaciones funcionales de cada uno de los objetivos y la validación de las programaciones de actividades realizadas. La persona responsable del servicio podrá modificar la periodicidad de las reuniones de seguimiento si fuera necesario, así como establecer sistemas de celebración no presencial como, por ejemplo, videoconferencias.

Tras cada reunión de seguimiento, de las que se levantará acta, la persona responsable del servicio podrá rechazar en todo o en parte los trabajos realizados, en la medida que no respondan a lo especificado en las reuniones de planificación o no superasen los controles de calidad acordados.

Independientemente de las Reuniones de Seguimiento, en cualquier momento a lo largo de la duración del proyecto, podrán tener lugar Revisiones Técnicas, para tratar temas puntuales.

El adjudicatario se responsabilizará de que los recursos necesarios para la correcta prestación del servicio estén siempre disponibles. Para ello, deberá disponer en reserva materiales, recursos técnicos y humanos formados para poder mantener el servicio ante problemas de sistemas, vacaciones, bajas o cursos de formación. En todo momento habrá una persona responsable del adjudicatario que coordine los recursos que soportan los servicios licitados.

Si la Agencia Digital de Andalucía o AndalucíaCERT detectara, de forma planificada, la necesidad de recursos adicionales por nuevas tareas o picos esperados en las tareas anteriormente descritas, el adjudicatario deberá ser capaz de redimensionar sus medios humanos y materiales y sus recursos en el plazo de una semana. En caso de que, a la vista de las circunstancias, este plazo fuera manifiestamente insuficiente, la persona responsable del servicio podrá establecer otro mayor.

7.12. Transición del servicio a la finalización del proyecto

El personal asignado por el adjudicatario al proyecto participará si es preciso en la transición del servicio que se producirá conforme a lo indicado en el epígrafe del lote correspondiente, dentro de los tres meses previos al vencimiento del contrato y sus posibles prórrogas, y habiendo sido adjudicada una o varias nuevas licitaciones que den respuesta a las necesidades presentadas en este documento.

7.13. Memoria final del proyecto

Cuando finalice el contrato y sus posibles prórrogas, tras la transición del servicio a que hace referencia el apartado anterior, el adjudicatario deberá presentar una Memoria Final, como informe justificativo del alcance efectivo de los trabajos realizados, conforme a lo establecido en el apartado ‘Entregables’

8. Condiciones generales

8.1. Carácter de los requisitos

Los requisitos establecidos en el presente Pliego de Prescripciones Técnicas tienen la consideración de mínimos exigibles a cumplir en todo momento por el adjudicatario que, además, podrá incluir en su oferta mejoras y características adicionales.

Las mejoras y características adicionales no eximirán del cumplimiento de todos y cada uno de los requisitos establecidos en este Pliego de Prescripciones Técnicas y el resto de la documentación de la presente licitación.

8.2. Ubicación

A lo largo del presente Pliego se utilizarán los términos siguientes relativos a la ubicación con el sentido indicado en este epígrafe:

- **Grupo Atendido de AndalucíaCERT**: Conjunto de organismos a los que AndalucíaCERT presta servicios. Está constituido formalmente por los aproximadamente 85 organismos en el ámbito de aplicación del Decreto 1/2011 (modificado por el Decreto 70/2017) por el que se establece la Política de Seguridad TIC de la Administración de la Junta de Andalucía. Sin embargo, en base a convenios de colaboración u otras consideraciones, el Grupo Atendido Extendido puede incluir a entidades y organismos de la Administración Local o de la Universidades andaluzas, entre otros.
- **Servicio prestado de forma localizada**: Servicio que es prestado a través de la presencia en las sedes de AndalucíaCERT o de los organismos de su grupo atendido u otras ubicaciones determinadas por AndalucíaCERT. Esta presencia será física o bien, si así es acordado posteriormente entre ambas partes, en modalidad de teletrabajo. Por parte de la persona responsable del contrato o de la responsable del servicio se establecerán las limitaciones aplicables a los servicios prestados en modalidad de teletrabajo. El personal que en cada momento se encuentre teletrabajando estará sujeto a las mismas condiciones de horario y de dedicación que el que trabaje de forma presencial.
- **Servicio prestado de forma deslocalizada**: Servicio que es prestado, con carácter general, sin necesidad de presencia en las sedes de AndalucíaCERT o de los organismos de su grupo atendido u otras ubicaciones determinadas por AndalucíaCERT, sin perjuicio de los desplazamientos puntuales que pudieran ser necesarios para garantizar una adecuada prestación del servicio.

8.3. Horarios

En el presente Pliego se hará referencia a los siguientes términos con el sentido indicado en este epígrafe:

- **24x7**: Modalidad de prestación del servicio o de acceso al mismo en el que este deberá estar operativo y disponible durante todas las horas del día, todos los días de la semana, incluyendo festivos y cualquier otro día considerado como no laborable.
- **8x5**. Modalidad de prestación del servicio en el que este deberá estar operativo y disponible durante los días hábiles de la semana (de lunes a viernes, excluyendo festivos), durante 8 horas diarias que, salvo indicación en otro sentido, serán las comprendidas entre las 7:00 y las 15:00 horas. Esta franja horaria podrá ser modificada o dividida en varias, para uno o varios servicios y de forma permanente o temporal, por la persona responsable del contrato sin que, en ningún caso, incluya periodos comprendidos entre las 0:00 y las 6:00 horas ni entre las 20:00 y las 24:00 horas.
- **12x5**. Modalidad de prestación del servicio en el que este deberá estar operativo y disponible durante los días laborables de la semana (de lunes a viernes, excluyendo festivos), durante 12 horas diarias que, salvo indicación en otro sentido, serán las comprendidas entre las 7:00 y las 19:00 horas.
    - Dentro de la cobertura 12x5 se podrá establecer diferentes niveles de servicio para distintas franjas horarias que, salvo indicación en sentido contrario, serán:
        - **Turno de mañana**: Comprendido entre las 7:00 y las 15:00 horas.
        - **Turno de tarde**: Comprendido entre las 11:00 y las 19:00 horas.
    - El horario de prestación y su división en franjas horarias podrá ser modificada, para uno o varios servicios o para parte de un servicio, de forma permanente o temporal, por la persona responsable del contrato, con la obligación de comunicarlo al adjudicatario con al menos 5 días de antelación, sin que en ningún caso incluya periodos comprendidos entre las 0:00 y las 6:00 horas ni entre las 21:00 y las 24:00 horas.

Todas las referencias a horarios deberán entenderse como realizadas conforme al horario oficial vigente en cada momento en la Comunidad Autónoma de Andalucía.

El horario de trabajo se regirá, en cada caso, por lo indicado en los apartados correspondientes a la descripción de los servicios prestados.

8.4. Equipamiento y materiales de trabajo

La palabra “equipamiento” debe entenderse en este documento en su sentido más amplio, incluyendo tanto los elementos físicos (hardware) como los lógicos (software) y tanto el equipamiento informático y de comunicaciones como el que no tenga dicha calificación.

Para la realización de las tareas que se presten en modo localizado y deslocalizado, el adjudicatario dotará al equipo de trabajo del equipamiento hardware y software necesario para el adecuado desarrollo de estas, incluyendo los equipos y las licencias que precisen.

Si para la prestación de los servicios incluidos en este documento fuera preciso el acceso remoto a las redes o a los sistemas de AndalucíaCERT, el aseguramiento del acceso se realizará mediante los métodos establecidos por la Red Corporativa de la Junta de Andalucía (RCJA). Los costes derivados de la conexión subyacente al canal seguro correrán por cuenta de la empresa adjudicataria.

Al finalizar los servicios se comprometerá el adjudicatario a realizar una cancelación de toda la información y datos sensibles que hayan podido quedar en sus equipos informáticos con motivo de la gestión, poniendo posteriormente dichos equipos a disposición de la persona responsable del servicio para realizar un chequeo de dicha cancelación.

AndalucíaCERT pondrá a disposición del adjudicatario líneas de teléfono, con un número de cabecera, debiendo el adjudicatario identificar a las personas que usarán dichas líneas afectas al servicio, así como responsabilizarse de su uso exclusivamente profesional de las mismas, pudiendo la Agencia Digital de Andalucía y AndalucíaCERT exigir al adjudicatario las responsabilidades que proceda en caso de uso no adecuado de las mismas.

AndalucíaCERT pondrá a disposición del adjudicatario cuentas de correo electrónico pertenecientes al dominio de la Junta de Andalucía a efectos de la prestación del servicio, debiendo el adjudicatario identificar a las personas que usarán dichas direcciones afectas al servicio, así como responsabilizarse de su uso exclusivamente profesional de las mismas, pudiendo la Agencia Digital de Andalucía y AndalucíaCERT exigir responsabilidad al adjudicatario en caso de uso no adecuado de las mismas.

La definición exacta del equipamiento se acordará al inicio de los trabajos.

8.5. Aceptación y garantía de los suministros y servicios

La recepción y aceptación del equipamiento suministrado y de los servicios objeto de contratación será realizada por la persona responsable del servicio. Para ello, el adjudicatario deberá prestar satisfactoriamente los servicios de asistencia técnica descritos y asegurar su correcto funcionamiento, cumpliendo los requerimientos establecidos en este pliego.

Cuando existan disconformidades con la prestación de servicios, el responsable del servicio emitirá los informes pertinentes, que serán remitidos al contratista para que cumpla sus obligaciones, según lo anteriormente expuesto. No se procederá a dar por recibido y aceptado el objeto del contrato mientras no estén subsanadas satisfactoriamente todas las disconformidades manifestadas.

La reiteración continuada de disconformidades, o la falta de corrección de estas, así como el incumplimiento continuado de los niveles de servicio, a juicio del responsable del contrato, podrá ser motivo de la rescisión del contrato de forma unilateral por parte de la Agencia Digital de Andalucía, sin que el adjudicatario pueda reclamar cantidad alguna en concepto de indemnización por daños y perjuicios.

Todos los trabajos realizados en el marco de la duración del contrato tendrán una garantía de 12 meses a partir de la aceptación de estos por parte de la persona responsable del servicio. Durante dicho período se garantizará el mantenimiento correctivo de los trabajos realizados. Asimismo, durante el periodo de garantía se ofrecerá soporte telefónico y, de ser necesario, asistencia en las instalaciones de AndalucíaCERT, para la resolución de los problemas que se planteen y tengan su origen en los trabajos realizados que sean objeto del presente pliego.

8.6. Ausencia de costes adicionales

Cuando sea necesario para cumplir con los requisitos establecidos en el presente Pliego de Prescripciones Técnicas, la oferta realizada, el correspondiente Pliego de Cláusulas Administrativas Particulares y cualquier otro documento que forme parte de la presente licitación, poner a disposición de AndalucíaCERT y/o la ADA de los entregables indicados en ellos, o para prestar y asegurar el correcto funcionamiento de los servicios, serán por cuenta de la empresa adjudicataria todos los costes necesarios para la adecuada prestación de los servicios. Esto incluye, pero no se limita a:

- La confección y remisión o puesta a disposición de los elementos entregables.
- Los costes derivados de la formación que sea preciso impartir al personal del adjudicatario.
- La formación a personal designado por la persona responsable del servicio o del contrato, cuando así esté contemplado en el presente Pliego de Prescripciones Técnicas, la oferta realizada, el correspondiente Pliego de Cláusulas Administrativas Particulares y cualquier otro documento que forme parte de la presente licitación.
- Los desplazamientos, así como los gastos de peaje, aparcamiento, alojamiento, manutención y cualquier otro que pudieran producirse como consecuencia de ellos, el equipamiento, los materiales y las actuaciones necesarias para el diseño, la puesta en marcha, la configuración, la operación, la actualización y el mantenimiento de la solución, así como para los procesos de transferencia del servicio que pudieran producirse al inicio y a la finalización del contrato y sus posibles prórrogas.
- Los desplazamientos, así como los gastos de peaje, aparcamiento, alojamiento, manutención y cualquier otro que pudieran producirse como consecuencia de ellos, y las actuaciones que realice para prestar los servicios o realizar la puesta a disposición de los elementos entregables.
- El equipamiento, salvo cuando esté previsto en este documento que deberá ser proporcionado por AndalucíaCERT.
- El transporte y entrega de materiales y equipamiento.
- El mantenimiento y actualización del equipamiento.

- El suministro, uso y gestión de las licencias del software utilizado para la prestación de los servicios.
- El equipamiento y los soportes de información utilizados para la adquisición y conservación de las evidencias digitales, así como los gastos necesarios para mantenerlos con las debidas condiciones de seguridad.
- La conservación de las evidencias digitales en las debidas condiciones de seguridad jurídica y tecnológica.
- Los soportes de información o sistemas de publicación o generación utilizados para entrega o puesta a disposición de los elementos entregables, incluyendo los casos en que tengan como destino una entidad o un órgano judicial o administrativo distinto del responsable del contrato y del responsable del servicio.
- El desarrollo de software, la adaptación de productos o el desarrollo de interfaces con otros sistemas.
- La activación y uso de las capacidades y funcionalidades requeridas.
- La adquisición de, o suscripción a, reglas no gratuitas para el funcionamiento de los sistemas y los servicios, así como su actualización y uso.
- La adquisición de, o suscripción a, fuentes de inteligencia no gratuitas, así como su actualización y uso.
- La adquisición de, o suscripción a, cualquier otra fuente de información o servicio, así como su actualización y uso.
- Los servicios profesionales que necesite contratar el adjudicatario, así como su gestión y uso.
- Los suministros y el material fungible necesario para el funcionamiento de los sistemas y los servicios.
- Las sustituciones de equipamiento, reparaciones y transporte de equipamiento derivados de averías o funcionamiento de este no acorde a las especificaciones o los requerimientos, salvo cuando esté previsto en este documento que dicho equipamiento deberá ser proporcionado por AndalucíaCERT.
- Los cambios de horario para la prestación de aquellos servicios que tengan una modalidad distinta de 24x7, cuando sean conformes a lo establecido en el presente Pliego de Prescripciones Técnicas, el correspondiente Pliego de Cláusulas Administrativas Particulares y cualquier otro documento que forme parte de la presente licitación.

- Los gastos necesarios para realizar y securizar la conexión remota por parte del personal del adjudicatario a los sistemas y redes de AndalucíaCERT o de las entidades y organismos que formen parte de su ámbito de actuación.
- Cualquier otro elemento que sea necesario para la adecuada prestación del servicio, para garantizar la calidad y seguridad de este, para la puesta a disposición de AndalucíaCERT y/o la ADA de los elementos entregables y para el cumplimiento de los requisitos establecidos.

En ningún caso serán imputables estos tipos de gastos a la Agencia Digital de Andalucía o a AndalucíaCERT.

En la relación anterior se entenderá la palabra "equipamiento" en su sentido más amplio, incluyendo tanto los elementos físicos (hardware) como los lógicos (hardware) y tanto el equipamiento informático y de comunicaciones como el que no tenga dicha calificación.

8.7. Declaración de requisitos de funcionamiento

Con anterioridad o de forma conjunta a la firma del contrato, el adjudicatario deberá entregar a la persona responsable del contrato una declaración de requisitos de funcionamiento de la solución ofrecida que incluirá como mínimo la siguiente información:

1. En caso de que sea necesario desplegar equipamiento en las instalaciones o redes de los organismos que forman parte del grupo atendido de AndalucíaCERT:
    a. Identificación de los productos hardware y/o software a desplegar con indicación, cuando proceda, de sus versiones.
    b. Lista de direcciones IP y puertos a los que realizan conexiones dicho equipamiento.
    c. Otros requisitos para el funcionamiento del equipamiento.
2. En caso de que el adjudicatario utilice servicios alojados en Internet mediante los que se determine, trate o almacene información referida a los organismos que forman parte del grupo atendido de AndalucíaCERT:
    a. Lista de proveedores de servicios utilizados.
    b. Para cada proveedor, Estados en los que se encuentran ubicados los servidores utilizados para la prestación del servicio.

Cualquier cambio en la información recogida en este apartado deberá ser comunicada por el licitador a la persona responsable del contrato a la mayor brevedad posible y sin dilación indebida.

8.8. Requisitos de seguridad

Las propuestas deberán garantizar el cumplimiento de los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información que constituye el Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 311/2022, de 3 de mayo. En concreto, se deberá asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que son objeto de la presente contratación.

Para lograr esto, se aplicarán las medidas de seguridad indicadas en el anexo II del ENS, considerando que el sistema de información recae en la categoría de seguridad MEDIA conforme a los criterios establecidos en el anexo I del ENS, y que los sistemas que se desplieguen y los servicios que se presten como resultado de esta licitación entrarán en el alcance de certificación ENS (actualmente vigente) de AndalucíaCERT.

https://www.ccn-cert.cni.es/amparo/API/public/certificaciones/855/download/387

En concreto, y en cumplimiento de la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, el adjudicatario deberá estar en condiciones de exhibir la correspondiente Certificación de Conformidad con el Esquema Nacional de Seguridad, en categorías MEDIA como mínimo, en el alcance de prestación de los servicios que se presten.

Adicionalmente el adjudicatario colaborará, en su ámbito, en el mantenimiento del nivel de seguridad establecido para los sistemas de información de AndalucíaCERT, con los procesos de gestión del riesgo y cumplimiento, y con las auditorías de certificación que se lleven a cabo.

El adjudicatario deberá garantizar la seguridad de los medios que utilice para la prestación de los servicios, realizando los análisis de vulnerabilidades y pruebas de penetración pertinentes.

Se deberá prestar especial atención a los siguientes aspectos en la configuración y parametrización de la plataforma de monitorización:

- Mecanismos de identificación y autenticación.
  - Será deseable que realice la autenticación de usuarios de contra directorio LDAP.
- Mecanismos de protección de la información tratada
  - Será deseable que el sistema de ficheros se encuentre cifrado.
  - Borrado seguro de los ficheros.
  - Disponibilidad de mecanismos que aseguren la integridad de los datos.
  - Las transmisiones de información y eventos de seguridad deberán realizarse de forma cifrada.
- Generación y tratamiento de pistas de auditoría.

- Se debe disponer de mecanismos de auditoría que permitan conocer la actividad desarrollada por los técnicos operadores y administradores.

El adjudicatario tomará las medidas necesarias para garantizar la seguridad de las comunicaciones que establezca con AndalucíaCERT y con los organismos que forman su grupo atendido. En particular, establecerá mecanismos de cifrado robustos en los casos en que el canal utilizado sea un sistema de correo electrónico o de mensajería. AndalucíaCERT podrá establecer los tipos, mecanismos y herramientas de cifrado a utilizar.

Previamente a la aceptación de la plataforma el adjudicatario deberá abordar un análisis interno de seguridad de la plataforma, que deberá incluir un análisis de vulnerabilidades y pruebas de penetración, reflejando los resultados en el informe correspondiente.

La Dirección del Proyecto podrá requerir al adjudicatario, en cualquier momento de la ejecución del contrato, la entrega de un informe de cumplimiento de las medidas descritas en este apartado. Dicho informe, que no supondrá ningún coste para la Junta de Andalucía, será elaborado por una empresa independiente y de reconocida experiencia en el campo de la seguridad. Además, se deberá atender a las mejores prácticas sobre seguridad recogidas en las series de documentos CCN-STIC (Centro Criptológico Nacional-Seguridad de las Tecnologías de Información y Comunicaciones), disponibles en la web del CERT del Centro Criptológico Nacional (http://www.ccn-cert.cni.es/), así como a las recomendaciones de AndalucíaCERT, como centro especializado en la materia en el ámbito andaluz.

8.9. Vulnerabilidades e incidentes de seguridad

El adjudicatario deberá mantener constantemente actualizados el equipamiento, los sistemas y los servicios utilizados, aplicando los parches de seguridad oficiales, y deberá asegurar y monitorizar su correcta configuración.

El adjudicatario deberá comunicar a la persona responsable del contrato cualquier vulnerabilidad o incidente de seguridad que afecte o pudiera afectar a:

- Cualquier equipamiento, producto o servicio utilizado o proporcionado por el adjudicatario para el cumplimiento del contrato.
- La información obtenida o generada por el adjudicatario sobre los sistemas y las redes de la Junta de Andalucía y los organismos del grupo atendido de AndalucíaCERT, así como del personal que les preste servicio.

Esta comunicación se deberá realizar a la mayor brevedad posible y sin dilación indebida toda vez que se haga pública la vulnerabilidad o el incidente o que el adjudicatario tenga conocimiento de ello.

El adjudicatario deberá comunicar a la persona responsable del contrato las actuaciones realizadas para solucionar las vulnerabilidades y responder a los incidentes, así como para paliar sus efectos.

La persona responsable del contrato podrá dar instrucciones al adjudicatario acerca de actuaciones a realizar para la solución de vulnerabilidades y la respuesta a incidentes de seguridad. Dichas instrucciones deberán ser atendidas por el adjudicatario a la mayor brevedad posible y sin dilación indebida.

La palabra “equipamiento” debe entenderse en este apartado en su sentido más amplio, incluyendo tanto los elementos físicos (hardware) como los lógicos (hardware) y tanto el equipamiento informático y de comunicaciones como el que no tenga dicha calificación.

8.10. Confidencialidad de la información

El adjudicatario deberá garantizar la confidencialidad de toda información y documentación relativa, total o parcialmente a la Agencia Digital de Andalucía o a cualquier entidad u organismo incluido en el ámbito de la presente licitación a la que pudiera tener acceso en virtud de la ejecución del contrato.

Esta información no podrá ser transferida a terceros sin el consentimiento previo, expreso y por escrito, de la persona responsable del servicio.

La obligación de confidencialidad y reserva alcanzará al propio adjudicatario y el personal a su cargo, así como a cualquier persona, empresa u organización a la que pudiera recurrir el adjudicatario para la ejecución del contrato o el soporte al mismo. La responsabilidad de su cumplimiento recaerá, en todo caso, sobre el adjudicatario.

A la finalización del contrato y sus posibles prórrogas, el adjudicatario devolverá a la persona responsable del servicio todas las información y documentación que le hayan sido suministradas en sus soportes originales. En todo caso, el adjudicatario será responsable de los daños y perjuicios que se deriven del incumplimiento de esta obligación.

Quedará totalmente prohibida la realización de copias de archivos en soportes físicos que abandonen las instalaciones de AndalucíaCERT o su grupo atendido, salvo cuando estén autorizadas por la persona responsable del servicio.

El adjudicatario deberá establecer e implantar procedimientos y mecanismos internos adecuados para mantener ficheros, locales, programas y equipos en las debidas condiciones de seguridad, con objeto de garantizar la confidencialidad de la información y definir el personal responsable de la misma.

El adjudicatario, sin perjuicio de lo dispuesto en el Reglamento General de Protección de Datos (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, únicamente tratará los datos conforme a las instrucciones de la persona responsable del servicio y no los aplicará o utilizará con fin distinto al del presente contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el caso de que el adjudicatario, o cualquiera de sus miembros, destinen los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será responsable de las infracciones cometidas.

Con carácter previo al inicio de la ejecución del contrato, el adjudicatario deberá suscribir con la Agencia Digital de Andalucía un "Acuerdo de confidencialidad y no revelación", conforme al modelo establecido por esta.

También estará obligado a firmar un "Acuerdo de confidencialidad y no revelación" el personal del adjudicatario que tenga acceso a información y documentación electrónica de uso exclusivo por personal de la Agencia Digital de Andalucía o AndalucíaCERT.

Cualquier incumplimiento de estos supuestos supondrá la resolución inmediata del contrato y la toma, por parte de la Agencia Digital de Andalucía, de las medidas legales oportunas.

En cualquier caso, el adjudicatario queda obligado al cumplimiento íntegro de la Ley Orgánica 3/2018, de 05 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, así como de las directrices que se fijen en relación con la gestión de riesgos digitales del Proyecto.

8.11. Propiedad

Todos los estudios y documentos, así como los productos y subproductos elaborados por el contratista como consecuencia de la ejecución del presente contrato serán propiedad de la Junta de Andalucía, que podrá reproducirlos, comunicarlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el adjudicatario autor material de los trabajos.

El adjudicatario renunciará expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del presente contrato pudiera corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados en base a este pliego de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa de la persona responsable del servicio.

Específicamente, todos los derechos de explotación y titularidad de las aplicaciones informáticas y programas de ordenador desarrollados al amparo de esta contratación corresponderán únicamente a la Junta de Andalucía.

Si el adjudicatario recurriera a materiales, suministros, procedimientos y equipos para la ejecución del objeto del contrato, deberá obtener las cesiones, autorizaciones y permisos necesarios de los titulares de las patentes, modelos y marcas de fabricación correspondiente, corriendo de su cuenta el pago de los derechos e indemnizaciones por tales conceptos.

El adjudicatario deberá tomar las medidas necesarias para evitar que se produzcan plagios o violaciones de derechos de autor en los documentos que elabore. Todo texto utilizado como referencia deberá ser convenientemente citado en la bibliografía. Cuando incluya recursos audiovisuales o de cualquier otro tipo que no sean de uso libre (por ejemplo, *Creative Commons* que permita obras derivadas y uso comercial), el adjudicatario deberá contar con los derechos, licencias o autorizaciones correspondientes. El adjudicatario

será responsable de toda reclamación relativa a la propiedad intelectual, industrial y comercial, y deberá indemnizar a la Agencia Digital de Andalucía y a AndalucíaCERT por todos los daños y perjuicios que para la misma puedan derivarse de la interposición de reclamaciones de terceros.

Si, una vez finalizado el contrato y sus posibles prórrogas, el uso de los productos que componen la plataforma de análisis desatendido de vulnerabilidades no supusiera coste para AndalucíaCERT, y si es posible la transferencia de las licencias de uso implicadas, el responsable del contrato podrá decidir que dicha plataforma pase a ser propiedad de la Agencia Digital de Andalucía.

El equipamiento a suministrar conforme al apartado 5.2 Suministro pasará en todo caso a ser propiedad de la Agencia Digital de Andalucía. El adjudicatario no podrá utilizarlo durante la ejecución del contrato y sus posibles prórrogas para otra finalidad que las contempladas en el contrato, salvo que la persona responsable del contrato emita instrucción en este sentido o lo autorice de forma expresa. Tampoco podrá reclamar su devolución ni durante la ejecución del contrato y sus posibles prórrogas ni con posterioridad a su conclusión, salvo cuando hayan sido objeto de sustitución por otro equipamiento que haya pasado a ser propiedad de la Agencia Digital de Andalucía (reemplazo permanente).

Si sobre algún equipo a suministrar se hubiera establecido obligación de mantener un equipo de reemplazo rápido (excluyéndose de este concepto los equipos en alta disponibilidad, que no se considerarán de reemplazo sino en servicio), o la oferta presentada así lo ofreciera, dicho equipamiento de sustitución será propiedad del adjudicatario.

En los casos de reemplazo permanente, el equipamiento de sustitución pasará a ser propiedad de la Agencia Digital de Andalucía y el reemplazado pasará a ser propiedad del adjudicatario.

8.12. Etiquetado e inventariado de los bienes suministrados

Todos los bienes suministrados mediante el presente expediente que tengan carácter inventariable, como por ejemplo servidores, deberán ser etiquetados por la entidad adjudicataria para su inventariado por parte de la Junta de Andalucía, de cara a cumplir con lo dispuesto en la Ley 4/86, de 5 de mayo, del Patrimonio de la Comunidad Autónoma de Andalucía en su artículo 14, así como la Orden de 23 de octubre de 2012, por la que se desarrollan determinados aspectos de la política informática de la Junta de Andalucía.

Lo anterior será también de aplicación a los equipos de reemplazo utilizados en los casos de sustitución permanente.

El etiquetado físico se realizará mediante etiquetas que proporcionará la Junta de Andalucía. El proceso completo de etiquetado debe realizarlo la empresa adjudicataria, y los costes asociados a este proceso estarán incluidos dentro de los trabajos a realizar dentro de esta contratación. La empresa adjudicataria deberá realizar todos los pasos indicados en el procedimiento de inventariado de los bienes incluidos en la presente contratación y tomar todas las medidas necesarias para garantizar que los bienes son entregados

con la correspondiente entrada en el Censo de Recursos Informáticos de la Junta de Andalucía (CRIJA) y con la correspondiente etiqueta adherida al equipo en los términos que describe el procedimiento de inventariado. Se proporcionará el procedimiento de inventariado al adjudicatario durante la ejecución del contrato.

Para aquellos bienes que permitan un etiquetado lógico, será obligatorio seguir una nomenclatura unificada para la Junta de Andalucía. Será responsabilidad del Organismo cumplir con la normativa de nomenclatura según se indique en el procedimiento de inventariado de bienes.

8.13. Obligaciones de información y documentación

Durante la ejecución de los trabajos objeto del contrato, el contratista se compromete, en todo momento, a facilitar a las personas designadas por la persona responsable del servicio la información y documentación que éstas soliciten para disponer de un pleno conocimiento 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.

Asimismo, el adjudicatario estará obligado a asistir y colaborar, a través del personal que designe a este propósito, en las reuniones de seguimiento del proyecto definidas por la persona responsable del servicio, quien se compromete a citar con la debida antelación al personal del contratista.

Como parte de las tareas objeto del contrato, el contratista se compromete a generar la documentación de los trabajos realizados, de acuerdo con los criterios que establezca en cada caso la persona responsable del servicio.

En este sentido, el contratista deberá informar a la persona responsable del servicio sobre distintos aspectos relacionados con el funcionamiento y la calidad de los servicios prestados.

Salvo indicación expresa en contrario, las especificaciones, informes, diagramas, planos, dibujos y cualquier otro documento relativo al objeto del contrato, serán aportados en castellano, cualquiera que sea el soporte y/o formato utilizado para la transmisión de información.

El contratista proporcionará, sin coste adicional, una copia en soporte informático portátil (llave USB, disco duro, etc.) con toda la documentación generada durante la prestación de los servicios objeto del contrato.

8.14. Aclaración de ofertas

La Agencia Digital de Andalucía podrá requerir a los oferentes para que formulen por escrito las aclaraciones necesarias para la comprensión de algún aspecto de las ofertas presentadas. Para ello en las ofertas, deberán aparecer los datos de contacto de la o las personas habilitadas para realizar las aclaraciones. En ningún caso se admitirá que en proceso de aclaraciones el licitador varíe los términos expresados en su oferta. Sólo se tomará en consideración la información que facilite el análisis de la solución propuesta inicialmente.

Si tras la solicitud de aclaraciones quedasen aspectos indefinidos, tales como la duración y extensión de los trabajos, proyectos, experiencia o formación presentados como méritos personales o de la empresa, la valoración de los mismos podrá ser nula.

Así mismo, si la Agencia Digital de Andalucía lo considerase oportuno, podrá requerir a todos o a algunos de los ofertantes seleccionados que realicen ante ella una presentación general de su oferta. En este caso, los ofertantes recibirán la citación a través de la persona habilitada con un plazo no inferior a tres días naturales a la realización de esta, que se llevará a cabo en el lugar y condiciones recogidas en la citación. El contenido de la presentación será en todo caso aclaratorio y en ella no podrán introducirse variaciones de los contenidos ofertados.

8.15. Cláusula de Género

Las empresas licitantes, en la elaboración y presentación de sus propuestas creativas, deberán tener en cuenta lo establecido en la Ley 12/2007, de 26 de noviembre, para la promoción de la igualdad de género en Andalucía, con respecto al uso no sexista del lenguaje y la transmisión de una imagen de igualdad entre hombres y mujeres y libre de estereotipos sexistas.

8.16. Calidad de los trabajos

Sin perjuicio de las obligaciones asumidas en su oferta, el adjudicatario deberá seguir los procedimientos de aseguramiento de la calidad existentes en la ejecución del contrato.

El contratista reconoce el derecho de la Agencia Digital de Andalucía a examinar por medio de auditores, externos o propios, el fiel cumplimiento de los trabajos por él realizados y su adecuación a lo establecido en el presente Pliego.

La realización de auditorías será comunicada al adjudicatario con dos semanas de antelación a su inicio. Las inspecciones serán comunicadas con un día de antelación.

Todo el material e información requerida para dichas inspecciones y auditorías por el equipo auditor estará disponible sin restricciones para la Agencia Digital de Andalucía.

El adjudicatario tendrá la obligación de:

- Facilitar el acceso al material solicitado por el grupo auditor.
- Designar personas responsables que acompañen al personal auditor.
- Facilitar un entorno de trabajo adecuado en el mismo lugar en que tiene lugar la auditoría.
- Cooperar con la persona que conduzca la auditoría.
- Participar en las reuniones que convoque la persona que conduzca la auditoría.

- Analizar los datos encontrados para garantizar la veracidad del informe.
- Emprender a la mayor brevedad posible y sin dilación indebida las acciones correctoras y/o preventivas necesarias.
- Emitir una respuesta oficial a los defectos de los que informe el grupo de auditores.

En Sevilla, a fecha de firma electrónica

EL JEFE DEL SERVICIO DE CIBERSEGURIDAD

Eloy Rafael Sanz Tapia

Cofinanciado por la Unión Europea

9. Anexo I

9.1. Infraestructura actual y dimensionamiento

A título informativo, la plataforma de monitorización desplegada, que será sustituida mediante el Lote 1 del presente contrato, se basa en el producto Alienvault USM Appliance. Está desplegada en 4 sedes con los siguientes dispositivos (appliances):

- Nodo central (CPD Zoco): 1 Federation Server.
- Nodo servicios horizontales (CPD Zoco): 1 Standard Server, 1 Standard Sensor.
- Nodo de interconexión (CPD Zoco): 1 Enterprise Server, 1 Enterprise Logger, 2 Enterprise Sensor, 1 Standard Sensor.
- Nodo de interconexión (CPD Cica): 1 Enterprise Server, 1 Enterprise Logger, 2 Enterprise Sensor, 1 Standard Sensor.
- Capacidad extra: 1 All-in-one, 5 Standard Server.

Adicionalmente, se dispone de conmutadores de paquetes (network packet broker) Netscout PFS 5010

9.2. Fuentes de eventos

A continuación, se muestran los tipos de fuentes (en negrita) con los que se debe integrar la solución ofertada, ya sea de forma nativa o mediante desarrollo a medida.

9.2.1. Nodos de interconexión

Los nodos de interconexión responden a los siguientes fabricantes / tecnologías:

- FW L2 **Forcepont Firewall**
- FW L1 **Fortinet Fortigate**
- Proxy web **Symantec, Bluecoat**
- Proxy reverse **Symantec**
- Balanceadores **Boll**
- Balanceadores **F5**
- DNS **Infoblox**
- **Radius** VPN/APN
- **FortiVPN**

- Sinhole **Apache httpd**
- FW L2 **Checkpoint**
- FW L1 **Paloalto**

9.2.2. Servicios horizontales

Se incluyen servicios horizontales como el correo electrónico corporativo, servicios de ofimática en la nube, servicios de compartición de inteligencia y otros:

En cuanto a los servicios horizontales habría que tener en cuenta los siguientes servicios / tecnologías:

- Correo electrónico: Sistema basado en software libre (**Exim, Dovecot, Apache httpd**). Pasarela de seguridad Kaspersky (**KLMS, KATA**).
- Sistemas de colaboración: Consigna, Ficheros Junta (**OwnCloud**), escritorio remoto (**ISL**).
- **Microsoft Defender for Cloud Apps**: Aplicaciones **Office 365**.
- **Microsoft Exchange**.
- **Checkpoint Harmony Mobile**.
- EDR (**en proceso de implantación**)
- WIFI corporativa
- Recolector de amenazas reportadas por terceros: **IntelMQ**.
- Sensores Snort/Suricata

9.2.3. Otros

- **DNS Microsoft Windows**.
- **IIS Microsoft Windows**.
- **Apache Tomcat**.
- DB **Oracle**.
- Auditoría linux (RedHat).
- FW **Fortigate**.
- Antivirus **TrendMicro ApexOne Central**.
- **Switch HP**.

- McAfee: 1 **McAfee ESM.**
- Ossec/Wazuh.
- Integración de alarmas de seguridad de los principales fabricantes: Microsoft CASB, …
- Integración de eventos de seguridad de los principales proveedores de servicios en nube
- Integración con alarmas de la herramienta del CCN-CERT (microclaudia, REYES, LUCIA, sensores SAT)