PLIEGO DE PRESCRIPCIONES TÉCNICAS

Mixto de suministro de licencias y soporte asociado de una solución para la detección y respuesta a ciberincidentes en equipo final (EDR)

EXPTE. CONTR. 2022/816345

1. Antecedentes

En la Administración de la Junta de Andalucía, las competencias en materia de ciberseguridad están atribuidas a la Agencia Digital de Andalucía por el Decreto 128/2021, de 30 de marzo, por el que se aprueban los Estatutos de la Agencia Digital de Andalucía (en adelante ADA).

Los fines de la ADA, expresados en el artículo 6.2 de sus Estatutos, incluyen

> "*a) La definición y ejecución de los instrumentos de tecnologías de la información, telecomunicaciones, ciberseguridad y gobierno abierto y su estrategia digital, en el ámbito de la Administración de la Junta de Andalucía, sus agencias administrativas y sus agencias de régimen especial.*
>
> *b) La definición y coordinación de las políticas estratégicas de aplicación y de seguridad de las tecnologías de la información y de las comunicaciones en el ámbito del sector público andaluz no incluido en el párrafo anterior, incluyéndose los consorcios referidos en el artículo 12.3 de la Ley 9/2007, de 22 de octubre, así como la ejecución de los instrumentos comunes que las desarrollen y la definición y contratación de bienes y servicios de carácter general aplicables.*"

En concreto, el artículo 6.3 de los citados Estatutos le atribuye las competencias en

> "*ñ) El desarrollo y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones de la Administración de la Junta de Andalucía y del sector público andaluz.*
>
> *o) La gestión de los recursos comunes para la prevención, detección y respuesta a incidentes y amenazas de ciberseguridad en el ámbito de la Administración de la Junta de Andalucía y del sector público andaluz.*"

Estas competencias, en virtud del artículo 15.3.c de los Estatutos, serán desarrolladas por la Dirección General de Estrategia Digital.

El CSIRT[1] autonómico, **AndalucíaCERT**, es la capacidad de respuesta a incidentes de seguridad de la Administración de la Junta de Andalucía. Su misión, encomendada por la Política de Seguridad TIC de la Junta de Andalucía[2], es el desarrollo de acciones centralizadas de prevención, detección y respuesta a incidentes en el ámbito de la Administración de la

[1] *Computer Security Incident Response Team* (Equipo de Respuesta ante Incidentes de Seguridad Informática)

Junta de Andalucía. El servicio, bajo la dirección de la Unidad de Seguridad TIC Corporativa de la Junta de Andalucía, se presta desde la localidad sevillana de Tomares por parte de la Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A. (SANDETEL) y se ha anunciado ya su extensión a la localidad de Málaga.

AndalucíaCERT presta actualmente a su grupo atendido una serie de servicios. Entre ellos se encuentran los de detección de incidentes, apoyados en infraestructuras de monitorización desplegadas principalmente en el perímetro de la Red Corporativa de Telecomunicaciones de la Administración de la Junta de Andalucía (RCJA).

AndalucíaCERT es uno de los pocos CSIRT autonómicos de España que ya forma parte de la Red Nacional de SOC, impulsada por el CCN-CERT y es un referente en el uso de la herramienta Lucía, para la comunicación de incidentes de seguridad.

[2] Artículo 12.1 del 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 (modificado por el Decreto 70/2017, de 6 de junio).

2. Objeto del contrato

La situación actual de crecimiento de los incidentes de ciberseguridad recomienda ampliar las medidas de seguridad de la forma más completa posible, así como disponer de capacidades de respuesta rápida que unidas a las de detección permitan contener los incidentes de forma rápida y centralizada.

Uno de los principales puntos de inicio de los ciberincidentes son los **equipos finales** (equipos de usuario o servidores) y su protección, habitualmente encomendada a los antivirus y sistemas de protección de punto final (EPP) debería ser complementada con sistemas de detección y respuesta en punto final (EDR).

Las soluciones EDR permiten detectar ataques que los EPP pasan por alto. Se basa en tecnologías que monitoriza y evalúa todas las actividades de los equipos finales, como eventos de usuario, acciones sobre archivos, procesos, modificaciones en registros, actividad de memoria y red. Las tecnologías referidas son el Machine learning, la analítica de datos, sandboxing y la inteligencia de ciberamenazas, entre otras. Las soluciones EDR están especialmente indicadas para ataques de ransomware (secuestro de datos), recientemente sufridos en campañas contra ministerios y administraciones públicas en general.

La madurez de AndalucíaCERT en la monitorización y gestión de incidentes unida a la capacidad de contratación centralizada de la ADA recomiendan la adquisición una solución EDR para la detección y respuesta a ciberincidentes en los equipos finales del Sector Público Andaluz.

El **objeto** de este contrato es, por consiguiente, el suministro de licencias de una solución para la detección y respuesta a ciberincidentes en equipo final (EDR) desde AndalucíaCERT, para todos los equipos finales de los organismos referidos en el apartado Alcance del contrato y con los Requisitos del suministro de la licencia indicados en los apartados subsiguientes. El suministro llevará implícito la instalación y puesta en marcha de la solución, y la integración con otros elementros y servicios de seguridad.

También es objeto de este contrato contar con un soporte inherente al suministro, para la capacitación inicial y de refuerzo, y el soporte funcional y técnico en el uso de la plataforma, en los términos descritos en el apartado Soporte asociado.

Se consideran potenciales equipos finales los dispositivos de usuario (PCs, thin clients, terminales móviles y tablets) y los servidores.

Puesto que no es posible conocer en el momento de la preparación de este expediente el número de licencias necesarias, por estar subordinadas a las necesidades de la Junta de

Andalucía, estas se irán suministrando conforme se vaya realizando el despliegue en los organismos previstos en el alcance de esta contratación (véase Fase 3: Despliegue) sin que exista un compromiso mínimo de consumo.

Se estima que durante la vida de esta contratación se podrán alcanzar **hasta 135.000 equipos finales**, sin perjuicio de que se alcancen más equipos, siempre que no se alcance el presupuesto máximo del contrato y según la distribución de anualidades, y sobre la base de que **no existe compromiso por parte de la Agencia Digital de Andalucía para alcanzar esta estimación**.

Mismas circunstancias concurren para el caso del soporte asociado, pues el volumen de esfuerzo depende directamente del número de licencias a desplegar y, para determinados servicios de soporte de forma acumulativa, para todas las licencias desplegadas. Así pues el soporte se irá propocionando conforme se vaya realizando el despliegue en los organismos previstos en el alcance de esta contratación, sin que exista un compromiso mínimo de consumo.

Así, se trata pues de un contrato "**en función de las necesidades**", con un presupuesto máximo, de acuerdo a lo regulado en la disposición adicional trigésima tercera de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP).

Se puede concluir que se trata de un contrato mixto con prestaciones propias tanto del contrato de suministro como de servicios. A tenor de lo dispuesto en el artículo 18 de la LCSP, se tramita a efectos de su adjudicación como de suministro en función de las necesidades, por ser ésta la prestación de mayor importancia económica, formulándose los precios en términos unitarios referidos a los distintos componentes de la prestación o a las unidades de la misma que se entreguen o ejecuten.

El objeto del contrato está alineado con la Estrategia Nacional de Ciberseguridad recogida en la Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional[3], en particular, con el Objetivo 1 "*Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales*" y sus líneas de acción I y II.

3 https://www.boe.es/eli/es/o/2019/04/26/pci487

3. Alcance del contrato

La RCJA constituye la red privada más grande y extensa del territorio nacional. Es una red que interconecta los organismos que componen la Administración de la Junta y sus entes instrumentales. La interconexión de las redes de todos los organismos supone grandes ventajas para la utilización de sistemas de información horizontales y corporativos, pero a su vez constituye un reto para la securización frente a ciberamenazas.

En este sentido es necesario contar con capacidades de detección de amenazas, especialmente amenazas avanzadas (APT) y respuesta frente a las mismas mediante soluciones tipo "EDR" para todo tipo de endpoint (ordenadores, servidores, etc). Este tipo de soluciones permitirán detectar de forma temprana comportamientos sospechosos relacionados con ciberataques que no pueden ser detectados por los antivirus tradicionales.

Dada la permeabilidad existente entre los organismos que componen la RCJA, estas capacidades tienen que estar **unificadas** en todo el ámbito de **la Administración de la Junta de Andalucía, de sus entidades instrumentales y de los consorcios** referidos en el artículo 12.3 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía. También podrán formar parte **otras instituciones de la Junta de Andalucía previa suscripción de un convenio**.

Por esta razón, se prevé que esta contratación sea realizada por la ADA, según se dispone en la *Resolución de 9 de marzo de 2022 de la Dirección Gerencia de la Agencia Digital de Andalucía, por la que se declaran en determinados ámbitos bienes y servicios de carácter general como instrumentos comunes de desarrollo de las políticas estratégicas de aplicación y de seguridad en las tecnologías de la información y de las comunicaciones*. (BOJA nº 56 de 23 de marzo de 2022)[4]

De este modo, el alcance del contrato lo constituyen todos los organismos de la Administración de la Junta de Andalucía, sus entidades instrumentales, los consorcios referidos en el artículo 12.3 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía y otras instituciones de la Junta de Andalucía previa suscripción de un convenio. Se refleja el listado, a fecha de redacción de este documento, en el ANEXO III: Entes en el ámbito.

[4] https://juntadeandalucia.es/boja/2022/56/38

4. Requisitos del suministro de la licencia

REQ-1 Se requiere el suministro de una solución EDR, de protección, detección y respuesta, basada en agentes de equipo final de usuario y servidor, de última generación, no basada en firmas[5], consola de operación en cloud (nube) pública y caza de amenazas (*threat hunting*) en la nube. A efectos de verificación de este requisito se consideran plataformas basadas en firmas a aquellas que se basan en la capacidad de identificar una muestra de malware o virus mediante la correlación de la información contenida en una base de datos específica del fabricante de seguridad (base de datos o archivo de firmas) y una cadena de caracteres específica resultado de aplicar funciones matemáticas concretas sobre la muestra.

REQ-2 Los agentes recibirán las configuraciones, políticas e indicadores de la consola, ejecutarán las actividades de detección y las respuestas preaprobadas y trasladarán a la consola tanto alertas como telemetría.

REQ-3 Desde la consola se realizará el seguimiento del despliegue en distintos ámbitos u organismos, se establecerán centralizadamente configuraciones y políticas, se difundirán indicadores, se recibirán alertas y telemetría y se realizarán acciones de contención y de caza de amenazas.

Las licencias EDR (en adelante, licencias) responderán por todos los requisitos establecidos en este apartado.

Las licencias suministradas tendrán <u>un periodo de garantía de 48 meses incluido</u> en el precio unitario de la misma, contado desde el hito de certificación según se describe en el Fase 3: Despliegue.

4.1. Arquitectura de la solución

Considerando el importante tamaño de los entornos a cubrir así como la diversidad de servicios, horarios y criticidades prestados por los organismos referidos en el Alcance del contrato, es fundamental disponer de una solución tecnológica que agregue la información generada por los miles de puestos de usuario y servidor y muestre, preferentemente, desde un punto de entrada único e integrado, toda la información de relevancia que permita prevenir, detectar y remediar de forma ágil y rápida cualquier incidente de seguridad.

Adicionalmente, la plataforma tecnológica sobre la que se apoye el servicio debe facilitar, en el caso de que se produzca un incidente, toda la información forense de relevancia que permita al equipo de la ADA investigar las causas, vías de entrada, vulnerabilidades

5 Veáse https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3034-ccn-stic-834-proteccion-ante-codigo-danino-en-el-ens/file.html para la definición de “firma”.

explotadas, atribución, etc, vinculadas al ataque de forma que pueda aplicar medidas a futuro para evitar nuevas ocurrencias.

REQ-4 Por estos motivos, todos los requisitos de seguridad demandados en el presente pliego deben ser cubiertos **por un único fabricante de seguridad**, una **única tecnología** y, preferentemente, **una única interfaz o consola**. Es decir, la solución propuesta debe facilitar el acceso a todas las funcionalidades demandadas, preferentemente desde una única interfaz o consola, entendiéndose ésta como un único portal web en el que se recojan todas las capacidades.

Se valorarán aquellas soluciones que propongan una sola consola sobre aquellas que requieran más de una. A efectos de valoración de la interfaz o consola única, no se considerarán valorables aquellas soluciones que requieran vincular, enlazar o integrar distintas plataformas o aplicaciones web, dominios o consolas para cubrir las funcionalidades requeridas o aquellas que integren estas consolas en un portal de aplicaciones. **(SOBRE 2)**

REQ-5 Será necesario que la solución propuesta por el licitador, **a nivel de producto**, 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 “MEDIA” o superior, para la familia EDR (ENDPOINT DETECTION AND RESPONSE). Los licitadores deberán indicar con precisión el producto y versión ofertada.

En el PCAP se incluye una penalidad por el incumplimiento de este requisito.

REQ-6 La **solución ofertada debe encontrarse dentro de ciclo de vida de soporte del fabricante** de seguridad, no debiendo encontrarse en estado fin de vida (end of life) o fin de soporte (end of support) por parte del fabricante. Las condiciones de soporte anunciadas por el fabricante en su documentación pública (datasheets de producto y de soporte, página web oficial del fabricante, etc.) deben permitir verificar este requisito.

REQ-7 Debe tratarse de una solución **100% nativa en cloud (nube) pública** del fabricante de seguridad 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 un único agente software en cada elemento de puesto de usuario o servidor.

REQ-8 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-9 Los servicios en cloud pública del fabricante (su proveedor de infraestructura en nube) deben estar alojados en datacenters de la Unión Europea y disponer de la certificación de **ENS nivel ALTO**.

REQ-10 La solución propuesta debe garantizar la continuidad de servicio y su **disponibilidad en horario 24x7x365**. La solución debe ser **autoescalable** y no debe requerir el mantenimiento de ninguna infraestructura garantizando la misma calidad de servicio independientemente de la demanda.

> **NOTA**: En el apartado 9.1.1. ANS Disponibilidad de la plataforma centralizada se expresa la disponibilidad mínima requerida y se indica que será objeto de valoración la mejora de esta disponibilidad. **ESTA MEJORA SE INDICARÁ EN EL SOBRE 3, NO INCLUIR EN SOBRE 2. ES DECIR, BAJO NINGÚN CONCEPTO DEBE INDICARSE EN EL SOBRE 2 EL VALOR OFRECIDO PARA LA DISPONIBLIDAD DE LA PLATAFORMA.**

REQ-11 La solución debe disponer de control de acceso con **doble factor de autenticación**, soportar SSO (**SAML 2.0**), **múltiples usuarios y diferentes roles** para permitir el acceso a diferentes ámbitos o funcionalidades.

REQ-12 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.

> **NOTA**: En el apartado 9.1.1. ANS Disponibilidad de la plataforma centralizada se expresa la disponibilidad mínima requerida y se indica que será objeto de valoración la mejora de esta disponibilidad. **ESTA MEJORA SE INDICARÁ EN EL SOBRE 3, NO INCLUIR EN SOBRE 2. ES DECIR, BAJO NINGÚN CONCEPTO DEBE INDICARSE EN EL SOBRE 2 EL VALOR OFRECIDO PARA LA DISPONIBLIDAD DE LA PLATAFORMA.**

REQ-13 Las comunicaciones entre la consola y los agentes tendrán que ser **cifradas**. Los licitadores indicarán los mecanismos de cifrado empleados.

REQ-14 La solución debe proporcionar la **capacidad de agrupar hosts** basados en identificadores de host, OU de Active Directory o etiquetas para la aplicación de políticas.

REQ-15 La solución **debe proporcionar una API rica y robusta** para integración con herramientas de terceros. Se valorarán las **integraciones y casos de uso con las herramientas del CCN-CERT. (SOBRE 2)**

Aunque el Nodo de Interconexión de la RCJA provee de políticas y mecanismos de gestión centralizada de seguridad y visibilidad de red entre la RCJA e Internet, es necesario tener en cuenta la gran diversidad de soluciones y configuraciones de red específicas (firewalls, proxies, etc.) en los datacenters de los distintos Organismos que se encuentran en el Alcance del contrato.

Adicionalmente a las políticas globales de la Junta de Andalucía, estas infraestructuras de red específicas son gestionadas con políticas locales de los distintos Organismos. En situaciones de respuesta a incidentes, en las que puede ser necesario bloquear el acceso a Internet de un conjunto de equipos significativo, será necesario garantizar la conectividad con los dominios en cloud y direcciones IP vinculadas a la gestión de la seguridad de los endpoints así como a los dominios indicados por el CERT del Centro Criptológico Nacional (CCN-CERT).

De esta forma, es necesario que los requisitos de conectividad entre los agentes y la plataforma cloud sean lo más estáticos y simples posibles, siendo esta una condición esencial para garantizar la visibilidad, el control y la capacidad de respuesta ante incidentes, en la medida que un cambio en los requisitos de conectividad debe replicarse, además de en el Nodo de Interconexión de la RCJA, en multitud de plataformas de comunicaciones de los distintos Organismos.

REQ-16 Por este motivo, los agentes instalados en cada uno de los puestos de usuario o servidor deben requerir, para cumplir con todas las funcionalidades requeridas en el presente pliego, **únicamente la conexión a un máximo de 2 (dos) dominios de Internet que corresponderán hasta un máximo de 10 (diez) direcciones IP correspondientes** a la infraestructura cloud del fabricante de seguridad. No serán válidas soluciones que requieran la conexión a un mayor número de dominios o mayores necesidades de visibilidad de entre redes para garantizar las funcionalidades de seguridad demandadas.

4.2. Agente de equipo final

Considerando el amplio ecosistema tecnológico de los organismos que forman parte del Alcance del contrato, en el que existe una gran variedad de equipos de puesto de usuario y servidor, alto grado de obsolescencia, multitud de configuraciones hardware, de sistemas operativos, de aplicaciones y niveles de actualización, para garantizar el éxito del proyecto y su despliegue y difusión, es necesario que se disponga de una solución EDR de

- Fácil despliegue de la solución,
- que minimice el impacto en rendimiento en el puesto de trabajo o servidor final
- y cuya implantación no suponga una interrupción en los servicios productivos.

Por este motivo se deberán cumplir con los siguientes requisitos:

- **REQ-17** Para el cumplimiento de todas las funcionalidades requeridas en el presente pliego debe disponerse de **un único agente instalado** en los puestos de usuario o servidores no siendo válidas soluciones que requieran distintos agentes para proporcionar todas las funcionalidades solicitadas.

- **REQ-18** El agente a desplegar en los puestos de usuario o servidor debe poder **convivir con los sistemas de protección de puestos (Antivirus/EPP) existentes** en los activos de la Junta de Andalucía (entre los que se encuentran soluciones de fabricantes como Broadcom-Symantec, Kaspersky Labs, McAfee o Sophos) manteniendo todas sus funcionalidades, no debiendo producirse incompatibilidades o requerimientos de desconexión de capacidades de la solución propuesta o de la solución de protección de puesto existente en el endpoint.

- **REQ-19** El agente a desplegar en los puestos de usuario o servidor debe poder **convivir con las soluciones microCLAUDIA y CLAUDIA del CCN**, manteniendo todas sus funcionalidades, no debiendo producirse incompatibilidades o requerimientos de desconexión de capacidades de la solución propuesta o de la solución de protección de puesto de microCLAUDIA y CLAUDIA del CCN.

- **REQ-20** Considerando que las soluciones de Antivirus/EPP desplegadas en la Junta de Andalucía hacen uso de motores de detección basados en firmas, **no se admitirán** soluciones que requieran el uso de **motores de detección basados en firmas** independientemente de los formatos y extensión de los ficheros de firmas. A efectos de verificación de este requisito se consideran “motores de detección basados en firmas” a aquellos que se basan en la capacidad de identificar una muestra de malware o virus mediante la correlación de la información contenida en una base de datos específica del fabricante de seguridad (base de datos o archivo de firmas) y una cadena de caracteres específica resultado de aplicar funciones matemáticas concretas sobre la muestra.

- **REQ-21** Para simplificar, agilizar y minimizar los tiempos de despliegue de la solución así como para evitar problemas de incompatibilidades durante el despliegue y fallos durante la instalación, el **agente software a desplegar y su instalador** debe ser el **mismo para cada familia** de Sistemas Operativos entendiéndose esto como:

- Un único agente para sistemas Windows (incluyéndose en esta familia los sistemas Windows Server en sus versiones 2008R2 y superiores, Windows 10 y superiores y Windows 7SP2 y superiores).
- Un único agente para cada distribución en sistemas Linux (en todas las versiones/distribuciones soportadas).
- Un único agente para sistemas iOS disponible y descargable desde market público (Apple AppStore).
- Un único agente para sistemas Android disponible y descargable desde market público (Google Play).

- **REQ-22** El agente a instalar en los endpoints debe ser **compatible**, estar soportado y ofrecer todas las funcionalidades demandas en, al menos, los sistemas operativos referidos en el ANEXO I: Sistemas Operativos a soportar.
- **REQ-23** Para garantizar que el despliegue de la solución no produce afección a la disponibilidad y continuidad de los servicios productivos, la instalación completa del agente en cada uno de los puestos de trabajo o servidores debe poder hacerse **sin reinicio y sin intervención del usuario**.

  Se entiende por instalación completa sin reinicio al despliegue del agente en cada uno de los endpoints quedando enrolado en la plataforma cloud y completamente funcional para todas y cada una de las funcionalidades requeridas en el presente pliego **sin necesidad de reinicio del sistema o intervención manual del usuario**. Esta **misma condición** aplica **también a las actualizaciones periódicas** del agente.
- **REQ-24** Considerando de especial importancia en el proyecto el despliegue de la solución en servidores críticos y teniendo en cuenta los requisitos de disponibilidad y continuidad de los servicios críticos alojados en éstos, se valorarán **soluciones que minimicen las dependencias con el software y middleware del servidor**, esto es, soluciones que para su instalación completa con todas las funcionalidades requeridas activas, necesiten los mínimos requisitos del host en cuanto a parches, drivers, service packs, bibliotecas del sistema y otros elementos software y no hagan uso de librerías del sistema para aplicar funcionalidades de protección. Los licitadores tendrán que indicar la lista de requisitos necesarios y ésta estar contrastada con información oficial del fabricante. **(SOBRE 2)**

Considerando que la solución tecnológica que se oferte debe desplegarse en la totalidad de los puestos de usuario y servidores de los organismos del Alcance del contrato, con una gran diversidad tecnológica (a nivel hardware y software) e importante nivel de obsolescencia, es fundamental disponer de un agente que minimice el impacto en los sistemas productivos debiendo requerir los mínimos recursos hardware del host

Para todos los sistemas operativos soportados, los requisitos hardware mínimos de instalación del agente demandados o recomendados, publicados en fuentes de información públicas contrastadas (datasheets oficiales de producto publicados, páginas web del fabricante de seguridad, documentación oficial publicada por el CCN-CERT, etc.) deben ser inferiores a los que se detallan a continuación:

- **REQ-25** Consumo máximo de CPU en servidores y PCs de usuario: el consumo total de los procesos vinculados al agente de la solución debe ser **inferior al 3% de la/las CPUs físicas o virtuales**. Este consumo máximo de CPU debe ser garantizado no admitiéndose soluciones que, durante la ejecución de procesos y operaciones relacionados con el funcionamiento de la solución con todas las funcionalidades demandadas activas, superen el consumo máximo indicado. Se valorarán soluciones que reduzcan los requisitos establecidos. **(SOBRE 2)**
- **REQ-26** Requisito mínimo de Memoria RAM en servidores y PCs de usuario: el requisito mínimo de instalación demandado o recomendado para la instalación del producto en cuanto a **memoria RAM debe ser inferior a 100MB** (Mega Bytes). No se admitirán soluciones cuyo requisito mínimo de instalación demandado o recomendado de memoria RAM sea superior a 100MB o que, durante la ejecución de procesos y operaciones relacionados con el funcionamiento de la solución con todas las funcionalidades demandadas activas, superen esta capacidad. Se valorarán soluciones que reduzcan los requisitos mínimos establecidos. **(SOBRE 2)**
- **REQ-27** Requisito mínimo de espacio de disco en servidores y PCs de usuario: el requisito mínimo de instalación demandado o recomendado para la instalación del producto en cuanto a **espacio en disco debe ser inferior a 150MB** (Mega Bytes). No se admitirán soluciones cuyo requisito mínimo de instalación demandado o recomendado de espacio en disco sea superior a 150MB o que, durante la ejecución de procesos y operaciones relacionados con el funcionamiento de la solución con todas las funcionalidades demandadas activas,

superen esta capacidad. Se valorarán soluciones que reduzcan los requisitos mínimos establecidos. **(SOBRE 2)**

- **REQ-28** El tamaño en disco del instalador del **agente descomprimido no debe ser superior a 70MB**.
- **REQ-29** El agente a instalar en los puestos de usuarios o servidores debe ser **compatible** con **infraestructuras físicas y virtuales**.
- **REQ-30** La tecnología de endpoint debe poder **desplegarse mediante herramientas de despliegue comunes** (políticas de grupo de directorio activo, herramientas de despliegue software, etc.).

  Se valorará que la solución EDR **disponga de capacidades de securización basadas en tokens** para controlar, permitir o bloquear la instalación y desinstalación del agente en los endpoints. De esta forma, en los casos que se consideren necesarios, aunque se disponga del paquete de instalación o de permisos para el lanzamiento de scripts de despliegue, deberá disponerse de un token específico para poder enrolar un endpoint a la plataforma. Igualmente, debe disponerse de un token específico para poder realizar la desinstalación del agente. **(SOBRE 2)**
- **REQ-31** El agente de endpoint debe admitir **actualizaciones de software controladas por políticas** desde la plataforma en la nube. Las actualizaciones del agente serán controladas mediante políticas y grupos pudiendo ser priorizadas. Estas políticas deben permitir realizar controles de cambio N-1, N-2 para cumplir con los requisitos de versionado.
- **REQ-32** El agente de punto final debe estar habilitado para permitir que se realicen **acciones de alerta y respuesta a incidentes en tiempo real** cuando los usuarios están **en itinerancia**.
- **REQ-33** El agente debe disponer de **capacidades de integración con terceros** para disponer de **capacidades de detección en elementos IoT/OT**.
- **REQ-34** La tecnología de punto final debe ser **compatible con plataformas en la nube** como Amazon Web Services EC2, Google Cloud Platform y Azure. Es decir, la plataforma propuesta debe permitir la aplicación de las funcionalidades requeridas en entornos de despliegue en nube pública en modo **IaaS** (Infrastructure as a Service) y en modo **PaaS** (Platform as a Service).

- **REQ-35** La solución propuesta debe tener **soporte de contenedores (OCI)** mediante la captura de la actividad y los metadatos de los contenedores. La solución debe proporcionar una visibilidad completa de los contenedores y añadir seguridad en tiempo de ejecución.
- **REQ-36** La **telemetría** extraída de los endpoints así como los **detalles forenses**, deben poder **enviarse** a la plataforma cloud **en tiempo real**. En caso de que no exista conectividad entre la consola cloud y el endpoint para el envío de telemetría, el agente instalado se encargará de guardar y custodiar esta información hasta que se retome esta conectividad y pueda realizarse el envío a la plataforma cloud.
- **REQ-37** La instalación del agente debe **permitir** incluir la **parametrización** para arquitecturas de **red y seguridad** basadas **en proxy**.
- **REQ-38** La instalación del agente debe ofrecer la posibilidad de incluir **parametrización** para asignación de **Tags informativas** a los endpoints en los que se realiza el despliegue.
- **REQ-39** Considerando la diversidad de sistemas operativos a cubrir y niveles de parcheo, todas las funcionalidades de seguridad requeridas deben proveerse independientemente de la versión de sistema operativo y nivel de parches sobre el que se encuentre instalado el agente. Es decir, **la solución propuesta debe cumplir con todas las funcionalidades de seguridad** requeridas siempre que el agente se encuentre desplegado en un endpoint que disponga de un sistema operativo soportado, **siendo independiente de su versión o estado de parcheo**.
- **REQ-40** El **agente de punto final operará** tanto en el espacio del **usuario** como en el del núcleo (**Kernel**).

4.3. Funcionalidades requeridas

4.3.1. Funcionalidades de seguridad

REQ-41 La plataforma debe facilitar la **comunicación de alertas de detección en tiempo real**, por ejemplo, por correo electrónico, y proporcionar **informes y cuadros de mando** en tiempo real.

REQ-42 Debe **mostrarse en la consola una puntuación de riesgo de las amenazas en tiempo real**. Esta puntuación de riesgo debe ser dinámica y evolucionar en tiempo real en función de las distintas métricas que se utilicen para su cálculo, permitiendo a los administradores conocer en todo momento el estado y severidad de amenazas y ataques.

REQ-43 La plataforma debe **proporcionar un registro de auditoría de la actividad** de los usuarios incluidas las tareas de gestión y respuesta a incidentes. Esta información de auditoría debe ser accesible desde la propia interfaz o a través de API.

REQ-44 La información contenida en este **registro de auditoría** debe contener al menos la siguiente información: creación de administradores, cambios de permisos, login a la plataforma, actividad durante la sesión, conexiones a host, comandos ejecutados, inicio y duración de la sesión.

REQ-45 La plataforma debe ser **accesible desde un navegador web**.

Consideraciones de retención de información en la plataforma cloud:

- Al menos debe ofrecerse la siguiente retención para las siguientes tipologías de información almacenada:
  - **REQ-46** Acceso a los **metadatos** relacionados con todas las amenazas generadas desde la plataforma: 365 días.
  - **REQ-47** Acceso bajo demanda a los **detalles forenses** completos de todas las amenazas detectados por la plataforma: 90 días.
  - **REQ-48** Acceso bajo demanda a toda la **telemetría** almacenada de eventos de los endpoints para la realización de investigaciones para detección retrospectiva y búsqueda de amenazas/threat hunting: 7 días.
  - **REQ-49** Debe ser posible facilitar la posibilidad de obtener una **réplica offline** de los datos enriquecidos de los sensores para su uso y posible tratamiento en plataformas de data lake.
- **REQ-50** Debe proporcionar mecanismos que permitan el **acceso a la plataforma desde múltiples organismos** o departamentos.

4.3.2. Funcionalidades de orquestación y automatización

Considerando las capacidades de penetración, la velocidad de propagación y daño en organizaciones que están causando los últimos ciberataques registrados en ámbitos público y privado, y la escasez de profesionales cualificados en el mercado, es necesario disponer de soluciones que permitan automatizar y orquestar acciones de respuesta y minimizar los tiempos de respuesta ante incidentes.

REQ-51 Se requiere, por tanto, que **la solución propuesta permita realizar automatizaciones y orquestaciones de tareas y respuestas automáticas en base a criterios de telemetría y/o detección**. Los licitadores expondrán en su propuesta cómo se implementan estas funcionalidades y sus capacidades, referidas a casos de uso.

REQ-52 La solución propuesta propondrá la **inclusión de las capacidades de automatización y orquestación preferentemente en la misma consola o interfaz de acuerdo con el apartado Arquitectura de la solución (REQ-4**), 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)**

A efectos de valoración de la interfaz o consola única, no se considerarán válidas soluciones que requieran vincular, enlazar o integrar distintas plataformas o aplicaciones web, dominios o consolas para cubrir las funcionalidades requeridas o aquellas que integren estas consolas en un portal de aplicaciones.

Igualmente se valorará que la solución propuesta para cubrir esta funcionalidad **no requiera el despliegue de soluciones adicionales que requieran la instalación de servicios, servidores o entornos adicionales (on-premise) o en entornos de nube pública de la Junta de Andalucía. (SOBRE 2)**

REQ-53 Las capacidades de automatización de la plataforma deben incluir, al menos, las siguientes enumeradas:

- Capacidad de creación de flujos de trabajo y playbooks de automatización mediante interfaz visual en la propia plataforma. Los usuarios administradores de la plataforma deben disponer de permisos para la creación/edición de estos playbooks.
- Contar con disparadores de acciones.
- Capacidad de establecer condiciones de forma secuencial como paralela.
- Capacidad de establecer acciones de respuesta
- Debe poder disponerse de un versionado de los playbooks o flujos de trabajo creados.
- Debe proporcionar un log de ejecución del flujo de trabajo creado.
- Todos los eventos de telemetría del endpoint podrán usarse como elementos de una condición.

Se valorarán las capacidades y funcionalidades de automatización, así como la simplificación de los mecanismos de generación de éstas y la inclusión de estas funcionalidades en la plataforma única. **(SOBRE 2)**

4.3.3. Funcionalidades preventivas y de detección

Como ya se ha expuesto en el apartado Arquitectura de la solución, todas las capacidades preventivas y de detección deben estar cubiertas por un único fabricante de seguridad, una única tecnología y, preferentemente, una única plataforma.

La plataforma propuesta debe cumplir con al menos las siguientes características:

- **REQ-54** La solución propuesta debe ser una plataforma de seguridad de última generación que utilice **técnicas de aprendizaje automático/machine learning** para la prevención previa a la ejecución de malware conocido y desconocido.

  Se valorará que entre las capacidades de detección y prevención se incluya la detección de técnicas, tácticas y procedimientos y los indicadores de ataque (IoAs) susceptibles de ser utilizados por agentes maliciosos. **(SOBRE 2)**

- **REQ-55** Las capacidades preventivas deben estar disponibles **tanto en línea como fuera de línea**, es decir, deben poder aplicarse las políticas definidas independientemente de si el puesto de trabajo o servidor se encuentra o no conectado a la red.

- **REQ-56** Debe permitir la puesta en **cuarentena** de malware detectado y ofrecer la posibilidad de restaurar o poner en lista blanca los archivos de cuarentena directamente desde la plataforma de gestión.

- **REQ-57** Debe disponer de capacidad de **enviar los archivos en cuarentena a un entorno de detonación (sandbox)** para su análisis automático mediante el uso de análisis estáticos y dinámicos avanzados.

- **REQ-58** Debe disponer de la capacidad para la **generación de listas blancas y negras de hashes de archivo personalizables**.

- **REQ-59** La plataforma debe proporcionar capacidades de detección basadas en el **análisis de comportamiento** posterior a la ejecución de un malware, permitiendo la protección contra las actividades habituales del ransomware (cifrado de archivos, eliminación de archivos sombra, etc.)

- **REQ-60** Proporcionará una detección y prevención basada en el comportamiento posterior a la ejecución, basada en el Indicador de Ataque (IoA) mapeado según el marco MITRE ATT&CK. Este tipo de reglas de detección debe soportar reglas relacionadas con procesos (hasta 3 niveles de procesos y líneas de comando asociadas), ficheros y comunicaciones. En todos los casos debe ofrecerse la posibilidad de ofrecer detección y bloqueo.

- **REQ-61** Tendrá capacidad de **convertir las detecciones en una prevención, incluidas las detecciones basadas en el comportamiento**. Las prevenciones deben detener los ataques antes de que se produzcan daños en el sistema operativo. Por ejemplo, evitar la inyección de procesos antes de que se produzca, de modo que el proceso objetivo no se vea interrumpido o comprometido.
- **REQ-62** La solución debe ofrecer protección de la memoria, por ejemplo, ASLR, protección contra la sobreescritura de la gestión de excepciones estructuradas, protección de páginas nulas, preasignación de la pila, etc.
- **REQ-63** La solución debe ser capaz de prevenir el uso malicioso de Powershell y los ataques con scripts.
- **REQ-64** La solución debe ser capaz de **restringir el uso de USB mientras se está fuera de línea,** incluyendo, pero sin limitarse a, el tipo de dispositivo y la función.
- **REQ-65** La solución debe ser capaz de realizar **controles preventivos contra ataques sin archivos, mientras se está desconectado**.
- **REQ-66** La solución debe proporcionar la capacidad de escribir detecciones y bloqueos de comportamiento personalizadas basadas en artefactos relacionados con la creación de procesos, la creación de archivos, las conexiones de red y las búsquedas de dominios.
- **REQ-67** La solución debe detectar las técnicas habituales de robo de credenciales.
- **REQ-68** La solución debe facilitar acciones de respuesta que incluyan el aislamiento del endpoint de la red o la conexión remota interactiva con el endpoint. Durante esta conexión, los administradores deben poder realizar **acciones de análisis, contención, respuesta y remediación**, debiendo estar soportada por la solución la ejecución de scripts por parte de los administradores en lenguaje Powershell para entornos de endpoints Windows durante esta conexión remota.
- **REQ-69** El agente de punto final debe capturar continuamente los eventos en bruto, incluso cuando no están asociados a alertas y detecciones.

- **REQ-70** La solución debe **correlacionar y presentar automáticamente la telemetría y los metadatos (IoC) relacionados con el ataque en una línea de tiempo**. Por ejemplo, argumentos de línea de comandos, escrituras de archivos, solicitudes DNS, conexiones IP, etc.
- **REQ-71** La solución debe **soportar la ingestión de IoC** (hashes, ip , dominios y url) vía API, que se mantendrán en la plataforma por un periodo determinado de tiempo y que serán utilizados durante todo el ciclo de prevención/detección de la plataforma. Se debe permitir hasta 100.000 IoC. Adicionalmente se requiere que sea posible indicar un comentario con información adicional relativa al IoC cargado en la plataforma y su periodo de expiración. Debe poder realizarse bloqueo de los IoC de tipo hashes y detección de los IoC de tipo dominio y hash.
- **REQ-72** La solución debe permitir **adaptarse a los diferentes niveles de riesgo**, para lo cual, deberá ser posible modificar en la consola y de forma independiente para la parte preventiva y parte de detección, al menos, 5 estados o severidades de aplicación de políticas de seguridad.
- **REQ-73** La solución debe correlacionar el vector de infección y la intención de los atacantes de la amenaza en relación con la cadena de ataque, **correlacionando con la telemetría, el árbol de procesos y la inteligencia de la amenaza**.
- **REQ-74** La solución debe **correlacionar las detecciones con los principales actores de la amenaza (estado-nación y crimen electrónico)** cuando sea aplicable, indicando la atribución de la detección con los agentes principales agentes maliciosos.
- **REQ-75** La solución debe ser **capaz de contener a nivel de red** remotamente un punto final utilizando mecanismos no relacionados con el cortafuegos del sistema operativo. La contención a nivel de red debe persistir después de un reinicio.
- **REQ-76** La solución debe proporcionar la **capacidad de conectarse remotamente a los sistemas de destino** con el fin de recopilar pruebas forenses adicionales (volcados de memoria completos, registro, archivos, etc.) y realizar tareas de remediación tales como cierre de procesos, modificación del registro de Windows, etc.
- **REQ-77** La solución debe proporcionar **capacidades** para enviar archivos **a sistemas remotos**, ejecutar archivos, ejecutar scripts, matar procesos, ajustar claves de registro y otras tareas necesarias durante la respuesta a incidentes.
- **REQ-78** La solución debe proporcionar una **API para integrarse con herramientas comunes de orquestación y automatización,** así como con sistemas de gestión de

casos. Los licitadores proporcionarán una descripción de las funcionalidades integrables vía API.

- **REQ-79** La solución debe transmitir la telemetría EDR en tiempo real para la consulta en vivo y **los resultados deben ser completos incluso cuando los puntos finales están fuera de línea.**
- **REQ-80** La solución debe proporcionar una **grabación continua de los eventos clave** para el análisis retrospectivo de todos los eventos recogidos. Se valorará la diversidad de eventos capturados, así como su idoneidad para la detección de amenazas. **(SOBRE 2)**
- **REQ-81** La solución debe proporcionar una **amplia cobertura de eventos**, manteniendo reducido ancho de banda para los datos transmitidos por punto final o carga de trabajo cada 24 horas. Se valorará que la solución haga un uso reducido del ancho de banda para el envío de datos de telemetría desde el agente. **(SOBRE 2)**
- **REQ-82** La solución debe recoger a través de **múltiples métodos de recopilación de eventos** en el punto final (llamadas api, ETW, controlador de filtro del núcleo, etc.). Se valorará la diversidad de métodos de recopilación de eventos. **(SOBRE 2)**
- **REQ-83** La solución debe **asociar el contexto del usuario** (local o de dominio) con los eventos relevantes en todos los sistemas operativos de Microsoft.
- **REQ-84** El agente debe **ofrecer opciones de filtrado para las detecciones** realizadas que permitan visualizarlas en función de, al menos: Severidad, Táctica, Técnica, Periodo de tiempo de la detección, estado de gestión de la vulnerabilidad, Fichero afectado y analista asignado.
- **REQ-85** La solución debe ofrecer la posibilidad de **asignar a un analista el trabajo** de respuesta sobre una detección.
- **REQ-86** La solución debe **ofrecer información de terceros** relativa a una detección (Ej: detecciones en VirusTotal, información en Google).
- **REQ-87** La **solución debe ofrecer en cada detección** la **información** relativa al usuario, al Host, a las vulnerabilidades presentes en el host, procesos, registro de sistema, actividades de red y resoluciones DNS.
- **REQ-88** La solución debe **ofrecer una vista gráfica** que permita observar el árbol de procesos relacionado con una detección.

- **REQ-89** La solución debe ofrecer a un analista **capacidades de inclusión de comentarios** relativos a las tareas realizadas en respuesta a una detección.
- **REQ-90** La solución debe **ofrecer información relativa a las configuraciones de seguridad** realizadas en entornos de **cloud pública** (al menos AWS, Azure y Google Cloud) y poder programar análisis de forma periódica relativos a esta funcionalidad.
- **REQ-91** La solución debe mostrar **información** relativa a **controles de cumplimiento** CIS, NIST y PCI en entornos AWS y Google Cloud.
- **REQ-92** La solución debe ofrecer **detección de amenazas basada en comportamiento** e inteligencia de amenazas que permita alertar y bloquear amenazas y que adicionalmente ofrezca información relativa a:
    - Vector de entrada utilizado por el atacante.
    - Compresión de las tácticas y técnicas utilizadas por el atacante.
    - Periodo temporal en el que se enmarca la amenaza.
    - Activos comprometidos.
    - Contextualización de los procesos seguidos por el atacante a lo largo de la cadena de ataque.

4.3.4. Funcionalidades de protección contra ataques basados en identidad

En el escenario actual de incidentes de seguridad en entidades públicas y privadas ha quedado de manifiesto que, debido al uso de credenciales de usuario o servicio obtenidas de forma ilícita, las capacidades de ataque de los ciberdelincuentes se han visto potenciadas de forma exponencial, al poder realizar propagación y desplazamiento lateral en las redes de la organización.

Las credenciales de usuario y servicio en el escenario actual de la Junta de Andalucía, en el que existen múltiples instancias de Directorio Activo asociadas a los distintos Organismos con diferentes políticas de gestión, se han convertido en elementos críticos a proteger para garantizar la seguridad de los distintos entornos.

REQ-93 Considerando la especial relevancia de los mecanismos de gestión de identidades en el control, detección, contención y prevención de incidentes de seguridad se requieren **funcionalidades de seguridad específicas orientadas a la protección de estos activos**. Específicamente se requieren capacidades de seguridad vinculadas a la protección de entornos de Directorio Activo, así como detección de ataques basados en vulnerabilidades de protocolos de autenticación. Adicionalmente, se requieren funcionalidades que permitan detectar y bloquear el uso ilícito de credenciales, intentos de suplantación de identidad, propagación lateral, acceso a recursos y activos críticos.

Se valorará que las **capacidades de detección y prevención** puedan aplicarse en arquitecturas **de Directorio Activo en formato on-premise** (infraestructura, servicios de directorio activo y controladores de dominio en entornos propios de la Junta de Andalucía), **cloud** (servicios e infraestructura de Directorio Activo ubicados en entorno de nube pública) o **híbridos** (convivencia de las dos modalidades anteriores). **(SOBRE 2)**

REQ-94 Las **capacidades de protección contra ataques basados en identidad deben proveerse utilizando el mismo agente único** que en el resto de las funcionalidades solicitadas. No serán válidas soluciones que requieran un agente adicional para cubrir las funcionalidades demandadas en este apartado o el despliegue de soluciones adicionales que requieran la instalación de servicios, servidores o entornos adicionales en el ámbito de la Junta de Andalucía o en entornos de nube pública.

REQ-95 La solución propuesta debe **permitir la definición e implantación políticas de detección, bloqueo o acceso condicional** (mediante la integración con herramientas de autenticación de doble factor) basadas en desviación de comportamiento respecto a la línea base de comportamiento de usuario. La solución debe posibilitar el análisis de comportamiento del usuario para detectar amenazas con una respuesta contextual automatizada que redirija el comportamiento de riesgo del usuario y detenga proactivamente las amenazas.

Se valorará que la solución disponga de funciones de aprendizaje automático del entorno, permita hacer seguimiento de los comportamientos a lo largo del tiempo y aplicar políticas flexibles que puedan adaptarse automáticamente a medida que cambien las circunstancias del entorno. **(SOBRE 2)**

REQ-96 La solución propuesta debe incorporar **capacidades de descubrimiento de objetos de directorio activo** mostrando información acerca de cuentas de usuario, de servicio, cuentas privilegiadas, etc. facilitando la aplicación de políticas y buenas prácticas de administración del Directorio Activo.

Se valorarán las **capacidades de descubrimiento** y la riqueza de la información recopilada por la solución. Asimismo, se valorará **que la solución facilite una puntuación de riesgo procesable para cada objeto/entidad** del directorio (usuario, cuenta, dispositivo) que permita representar la probabilidad de exposición a una brecha o un incidente, así como información sobre la **postura de seguridad** del entorno. **(SOBRE 2)**

REQ-97 La solución propuesta debe poder enriquecer las capacidades de threat hunting **permitiendo realizar consultas en la información de telemetría** relacionadas con atributos y eventos del tráfico de autenticación, atributos de usuarios, dispositivo, métodos de acceso, cambios en la cuenta, etc. Se valorarán las capacidades añadidas por estas funcionalidades de enriquecimiento de las funcionalidades de threat hunting. **(SOBRE 2)**

REQ-98 Adicionalmente, considerando la relevancia y criticidad especial de las infraestructuras de sistemas que sustentan los sistemas de identidad de Directorio Activo (Controladores de Dominio), es necesario que estas funcionalidades específicas de seguridad orientadas a la protección de identidades puedan **convivir sin impacto en rendimiento de estos sistemas**.

REQ-99 Se valorará que las funcionalidades de seguridad vinculadas a protección contra ataques basados en identidad estén incluidas en la **misma plataforma tecnológica** evitando las soluciones que requieran vincular, enlazar o integrar distintas plataformas web, dominios o consolas para cubrir las funcionalidades requeridas. **(SOBRE 2)**

Asimismo, **se valorarán las capacidades de** la solución **propuesta en la definición y aplicación de políticas de detección, bloqueo o acceso condicional** en base a comportamiento respecto a línea base, protocolos de acceso, activos críticos, hosts utilizados en el acceso, entre otros. **(SOBRE 2)**

4.3.5. Funcionalidades de búsqueda activa de amenazas (threat hunting)

La plataforma propuesta debe proporcionar la capacidad de realizar búsquedas de amenazas (threat hunting) sobre la información de telemetría generada por los endpoints.

Al menos, debe disponer de las siguientes especificaciones y funcionalidades:

REQ-100 La solución propuesta debe **supervisar la actividad de procesos de los endpoints** enviando de forma continua y en tiempo real información de eventos y detalles forenses a la plataforma cloud. Debe permitirse la **exportación de la información de telemetría** recopilada a formatos comunes como CSV, XML y raw.

REQ-101 La solución debe **mostrar información detallada de cada endpoint** en lo relativo a procesos y servicios, comandos ejecutados por herramientas de administración, actividad de Scripts, actividades relativas a registro, tareas programadas y políticas de Firewall y actividades de red.

REQ-102 La solución debe **proporcionar la capacidad de realizar una búsqueda de eventos** sin procesar utilizando un lenguaje de consulta estructurado a través de toda la telemetría de eventos recopilada (apilamiento de datos). La solución debe proporcionar consultas predefinidas para todas las actividades relacionadas con el usuario y el punto final así como artefactos forenses. Las búsquedas deben poder realizarse utilizando la interfaz de usuario. Estas búsquedas deben poder incluir, al menos, hashes específicos, nombres de fichero, parámetros de líneas de comandos, direcciones IP, dominios, eventos sin procesar, claves de registro, etc.

REQ-103 Debe **permitir las búsquedas en la información generada por toda la base instalada** sin producir afectación a los endpoints o incrementar los consumos de recursos hardware del agente instalado.

REQ-104 La solución debe proporcionar **informes de búsqueda de amenazas y análisis de líneas de tiempo,** así como proporcionar un **informe para demostrar la línea de tiempo completa de los eventos que ocurren en un host**. La solución debe proporcionar un **informe** que demuestre la **cronología** completa de los eventos de un proceso.

Se valorarán las capacidades de la solución para la realización de **la búsqueda de amenazas**, en concreto se valorará la granularidad y variedad de los eventos de telemetría recopilados, las capacidades del motor de almacenamiento y búsqueda en la realización de consultas específicas, reglas o búsquedas predefinidas, integración con las capacidades de inteligencia de amenazas del fabricante. **(SOBRE 2)**

4.3.6. Funcionalidades relacionadas con la Gestión de TI y vulnerabilidades

REQ-105 Todas las **funcionalidades demandadas deben ser accesibles, preferentemente, desde la misma interfaz única indicada en Arquitectura de la solución** (**REQ-4**), desde la que se prestan todas las funcionalidades de seguridad, entendiéndose ésta como un único portal web en el que se recojan todas las capacidades. Es decir, Se valorarán aquellas soluciones que ofrezcan las funcionalidades demandadas relacionadas con la Gestión de TI y vulnerabilidades desde la misma interfaz única indicada en Arquitectura de la solución (REQ-4). **(SOBRE 2)**

A efectos de valoración de la interfaz o consola única, no se considerarán valorables aquellas soluciones que requieran vincular, enlazar o integrar distintas plataformas o aplicaciones web, dominios o consolas para cubrir las funcionalidades requeridas o aquellas que integren estas consolas en un portal de aplicaciones.

La base instalada de puestos de usuario y servidores a cubrir se caracteriza por una gran heterogeneidad y dispersión. A las dificultades de gestión propias de la multitud de sistemas operativos, niveles de parcheo y configuraciones hardware, se suma una gran dispersión de endpoints a lo largo de toda la geografía de Andalucía, lo que dificulta enormemente la gestión de activos y operación del puesto de usuario.

La superficie de exposición a riesgos de seguridad será mayor en la medida en que la plataforma tecnológica y el agente solicitados no se encuentren convenientemente desplegados en la mayoría de endpoints de la Junta de Andalucía.

REQ-106 De esta forma es necesario que la plataforma propuesta facilite **información de aquellos activos en los que no se encuentre desplegada la solución**, indicando sobre cuales de éstos sería posible desplegarla.

Adicionalmente, considerando la amplitud del entorno a cubrir y los posibles problemas de seguridad vinculados a las aplicaciones instaladas es necesario disponer de información acerca de las aplicaciones desplegadas en los equipos, su uso y sus vulnerabilidades declaradas.

Por estos motivos, la plataforma propuesta debe disponer de las siguientes funcionalidades:

- **REQ-107** La solución debe proporcionar un **inventario completo de activos**. Se valorará la granularidad de la información acerca del hardware y software de cada uno de los endpoints recopilada por la solución. **(SOBRE 2)**
- **REQ-108** La solución debe ser **capaz de identificar los activos no gestionados** (activos en los que no se encuentra desplegado el agente) **sin** realizar **escaneo** de red ni otros métodos invasivos.
- **REQ-109** La solución debe ser **capaz de identificar los activos en los que no es posible desplegar el agente de protección**, como por ejemplo las impresoras u otros elementos conectados a la red.
- **REQ-110** La solución debe proporcionar un **inventario de aplicaciones completo** y con capacidad de búsqueda. Adicionalmente debe ofrecer información sobre su uso.
- **REQ-111** La solución debe proporcionar una funcionalidad completa de **supervisión de cuentas privilegiadas**.
- **REQ-112** La solución debe ser capaz de **identificar las vulnerabilidades del sistema operativo en tiempo real** sin tener que hacer un escaneo interactivo y

debe realizarse con el mismo agente único de la solución instalado en cada uno de los endpoints.

- **REQ-113** La solución debe **mostrar los recursos del sistema** de la máquina.
- **REQ-114** La solución debe **proporcionar visibilidad en el firmware y la BIOS**.
- **REQ-115** La solución debe ofrecer la **capacidad de buscar endpoints** utilizando su **MAC**.
- **REQ-116** La solución debe mostrar información relativa a la presencia de cifrado del almacenamiento en entornos Windows.
- **REQ-117** La solución debe ser capaz de **identificar las vulnerabilidades de las aplicaciones** que suelen ser explotadas (por ejemplo, Java, Flash, Adobe), sin tener que hacer un escaneo interactivo y debe realizarse con el mismo agente único de la solución instalado en cada uno de los endpoints.
- **REQ-118** La solución debe **mostrar la configuración de seguridad** del sistema operativo **Windows** del parque de endpoint desplegado. Los aspectos mínimos a contemplar son:
    - Credential Guard
    - DMA Guard
    - IOMMU
    - Secure Boot
    - Secure MOR
    - System Guard
    - System Hvci
    - System secure boot
    - System VBSS
    - UEFI memory Protection
- **REQ-119** La solución debe mostrar información relativa al tiempo **de cambio de password en las cuentas** de usuario.
- **REQ-120** La solución debe mostrar información relativa a los **intentos de login fallidos** en los endpoints.

- **REQ-121** La solución debe ofrecer **información relativa a los parches desplegados del Sistema Operativo y/o aplicaciones**, y a los endpoints pendientes de reinicio tras la aplicación de un parche.

- **REQ-122** Debe incluir **capacidades de descubrimiento de sistemas Shadow IT** no protegidos de forma continua.

- **REQ-123** Posibilidad de **buscar Vulnerabilidades de CVE**. Mostrar los equipos con vulnerabilidades CVE concretas, con la información relativa de los mismos.

- **REQ-124** Utilizando la inteligencia integrada de explotación de vulnerabilidades y amenazas, se debe **poder identificar qué vulnerabilidades del entorno representan el mayor riesgo**, y **crear informes y cuadros de mando** para el seguimiento de estas vulnerabilidades. Se valorará que la solución propuesta, basándose en las capacidades y servicios de inteligencia de amenazas del fabricante de seguridad, muestre en la propia consola web información acerca de la vulnerabilidad detectada indicando si existe evidencia de actividad y uso a nivel mundial de la vulnerabilidad por parte de algún agente malicioso. **(SOBRE 2)**

- **REQ-125** Debe **facilitarse remediación recomendada**, indicando los parches de mayor impacto a desplegar. De forma que pueda utilizarse esta información para complementar la política de parcheo.

- **REQ-126** Deben **verse los parches instalados** para identificar qué parches están activos en el entorno, **o qué parches se han instalado**, pero están pendientes de reiniciar.

- **REQ-127** Posibilidad de **Integración con otros elementos como NDR, SIEM, TIP y SOAR**.

- **REQ-128** La solución debe **mitigar los riesgos asociados a los dispositivos USB**. Debe ofrecerse visibilidad de los dispositivos USB en lo relativo a:

    - Tipo de dispositivo
    - Marca del dispositivo y fabricante
    - Uso de los dispositivos USB
    - Supervisión de los archivos escritos en el almacenamiento USB

  Debe posibilitarse el control del uso de los dispositivos USB e implantar políticas específicas.

- **REQ-129** La solución debe ofrecer la **capacidad de crear políticas y reglas de firewall del host Windows**. Debe ofrecer la posibilidad de crear políticas de firewall basadas en plantillas o desde cero en estos hosts.
- **REQ-130** Debe ofrecerse la posibilidad de **validación de reglas de firewall de host** para evitar que los administradores creen reglas defectuosas, pudiendo desplegar las políticas en modo de monitorización antes de su paso a producción.
- **REQ-131** Las **funcionalidades de gestión de firewall** del endpoint deben ofrecerse utilizando el mismo agente que ofrece el resto de las funcionalidades requeridas.

4.3.7. Funcionalidades relacionadas con la inteligencia de ciberamenazas

La Junta de Andalucía, siendo administración pública, está sujeta a un conjunto de regulaciones y legislación en materia de seguridad y protección de datos. Entre otras obligaciones, se encuentra la obligación específica de notificación de incidentes de seguridad al CERT del Centro Criptológico Nacional (CCN-CERT).

Adicionalmente, existe intercambio de información de seguridad entre la red de SOCs nacional de las distintas administraciones públicas. Por este motivo, para que el intercambio de información sea adecuado y completo es necesario proporcionar información acerca del contexto del incidente o detección permitiendo, en ocasiones, que esta información pueda aprovecharse por otro organismo, pudiendo aplicar políticas proacticas (por ejemplo, la carga en sus sistemas de los de indicadores de compromiso vinculados a un agente malicioso detectado, parcheo de vulnerabilidades explotadas activamente por este agente, identificación de campañas, etc.).

Asímismo, la información de inteligencia de ciberamenazas en el marco de una respuesta a un incidente de seguridad, es determinante a la hora de aplicar mecanismos de contención (para evitar su propagación) o agilizar las acciones de respuesta y remediación, minimizando el impacto en los servicios.

REQ-132 Por estos motivos la plataforma propuesta **debe incluir en la misma en la misma consola un módulo de inteligencia** que contextualice de forma automática las alertas y realice la atribución automática de actores maliciosos relacionados con la alerta, facilitando:

- Ofrecer inteligencia de técnica, táctica, operacional y estratégica.
- Proveer un API para aportar análisis, enriquecimiento y contexto a los Indicadores de Compromiso (IoCs) y artefactos facilitados por los usuarios.

Se valorará la metodología de recolección de inteligencia, los informes de inteligencia, diversidad de agentes maliciosos investigados, las capacidades de reconocimiento de riesgo digital según la información de la Junta de Andalucía en Internet, Dark Web / Deep Internet / Dark Network, perfiles de actores, indicadores de solución y datos. **(SOBRE 2)**

Asimismo, se valorarán las funcionalidades de integración de las capacidades y paquetes de inteligencia del fabricante de seguridad con la solución tecnológica propuesta, la capacidad de generar atribuciones de detecciones y ataques a agentes maliciosos y las capacidades de contextualización de los incidentes. **(SOBRE 2)**

4.4. Implantación y puesta en marcha

El suministro de las licencias vendrá acompañado de su correspondiente instalación y puesta en marcha, de forma que serán responsabilidad del contratista las tareas de planificación de la ejecución del proyecto y de aprovisionamiento y configuración inicial del sistema.

Las actividades de este servicio se reflejan en el apartado Fase 1: Definición del despliegue de este documento.

Estas actividades se consideran incluidas en el coste de las licencias del EDR y no darán lugar a facturación diferenciada.

4.5. Soporte y mantenimiento del fabricante

REQ-133 Asociado a la licencia de equipo final, durante la duración del contrato, se prestará un **soporte y mantenimiento del fabricante** 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 las mismas.
- Soporte del fabricante al despliegue y la puesta en marcha.
- 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 reporte de incidencias se realizará mediante el Sistema integrado de operaciones (SIO). Los tiempos de respuesta vinculados a la atención a incidencias deben ser al menos los siguientes:

  - Incidencias de máxima prioridad: tiempo de respuesta igual o inferior a 2 horas.

  - Resto de incidencias: tiempo de respuesta igual o inferior a 6 horas.

  Se valorará la mejora de los tiempos de respuesta indicados. **(SOBRE 3, NO INCLUIR EN SOBRE 2. CRITERIO 2.5).**

- 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. CRITERIO 2.6).**

Para la prestación de este soporte, será requisito que el fabricante de la solución EDR 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.

4.6. Garantía del suministro

El suministro de las licencias tendrá asociada una garantía de 48 meses, contada desde el hito de certificación correspondiente, según se describe en el apartado 6.3. (Fase 3: Despliegue).

> "Los hitos de certificación consistirán en la contabilización y posterior certificación de las licencias desplegadas el último día del mes de certificación (meses 3, 9, 15, 21, 27, 33, 39 y 45 del contrato)."

Esa certificación se considerará la fecha del acto formal y positivo de recepción o conformidad, y comienzo de la garantía de 48 meses sobre cada elemento del suministro.

La garantía del suministro responderá por el correcto funcionamiento de la solución EDR así como por las funcionalidades ofertadas por el licitador a los requerimientos establecidos en el apartado 4.3. (Funcionalidades requeridas) durante todo el plazo de garantía. Durante dicho plazo de garantía se tendrá 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 las mismas.

5. Soporte asociado

Asociados al suministro de licencias será necesario prestar un soporte para

- la capacitación en el uso de la plataforma,
- el soporte funcional y técnico en el uso de la plataforma, para el correcto funcionamiento de la misma, la caza de amenazas y la respuesta a incidentes.

en los términos descritos en los siguientes apartados.

Hay que tener en cuenta que la instalación, puesta en marcha de la solución y la integración con otros elementos y servicios de seguridad, ya ha sido descrita en el apartado Implantación y puesta en marcha.

Considerando la criticidad del soporte y las necesidades de especialización necesarias para ofrecer este soporte con garantías, se valorará que los licitadores pertenezcan (sean miembros) de **CSIRT.es** y/o de **TRUSTED INTRODUCER** y/o de **FIRST**. **(SOBRE 2)**

Para la verificación de esta propuesta se acudirá a los listados de membresía de:

- https://csirt.es/index.php/es/miembros
- https://www.trusted-introducer.org/directory/teams.html
- https://www.first.org/members/teams/

Para la organización, coordinación y control que garantice una ejecución eficaz y eficiente del objeto del contrato, así como para la interlocución y del reporte a la ADA será necesaria la figura de una persona que desempeñe la **Jefatura de Proyecto**. Sus responsabilidades están definidas en el apartado Jefatura de proyecto.

Este servicio estará prestado en horario 12x5, de forma deslocalizada y los requisitos mínimos del perfil son los siguientes:

Requisitos mínimos – Jefatura de Proyecto
TITULACIÓN
Grado en Ingeniería o equivalente en la especialidad de informática y/o telecomunicaciones.
FORMACIÓN TÉCNICA
- Conocimientos acreditados en gestión y soporte de productos de seguridad del fabricante (EDR).

- Conocimientos en administración de Microsoft Windows y Linux. - Conocimientos en Gestión de incidentes de seguridad.
ACTIVIDAD PROFESIONAL
- Al menos 60 meses de experiencia en gestión de proyectos. - Al menos 36 meses de experiencia en la organización y gestión de equipos técnicos especialistas en la detección y remediación de incidencias de seguridad. - Al menos 24 meses de experiencia en proyectos de despliegue y gestión de soluciones de seguridad EDR.

Se valorará el cumplimiento por encima de los mínimos requeridos, con interés en se proponga un perfil que cuente con **CISM** (Certified Information Security Manager) en el momento de presentar la oferta. **(SOBRE 3, NO INCLUIR EN SOBRE 2. CRITERIO 2.4)**

5.1. Capacitación en el uso de la plataforma

De igual modo, el suministro se acompañará 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. La acción tendrá tres convocatorias (Fase 4: Capacitación inicial del Plan de ejecución), en fechas a determinar con el responsable del contrato, para un mínimo de 20 asistentes cada una y con una duración mínima de 20 horas lectivas.
- **Capacitación adicional/de refuerzo**: a lo largo de la duración del contrato (Fase 6: Explotación del servicio del Plan de Ejecución), 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 mínimo de 25 asistentes cada una y con una duración mínima de 4 horas lectivas.

Las sesiones serán realizadas en las instalaciones de la Junta de Andalucía o bien de manera virtual. Será responsabilidad del contratista la certificación de la capacitación realizada sobre el personal que asista a las sesiones descritas.

Tanto para la capacitación inicial como la adicional / refuerzo se proporcionará una descripción de:

i. Los medios técnicos y materiales propuestos, como plataformas de formación, plataforma de entrenamiento, documentación y manuales, salas de capacitación.

ii. El personal propuesto por licitador para impartir la capacitación.

iii. La organización de los programas de capacitación inicial y adicional/refuerzo, en cuanto a número de sesiones, modalidad virtual o presencial, nº recomendado de asistentes, contenido, horas y certificaciones.

5.2. Soporte funcional y técnico en el uso de la plataforma EDR

La licencia de uso tendrá asociada, además del Soporte y mantenimiento del fabricante, un soporte funcional y técnico para el correcto funcionamiento de la plataforma, caza de amenazas y, de forma excepcional, respuesta a incidentes.

Este soporte deberá sustentarse sobre los servicios de un SOC/CSIRT preexistente del ofertante.

Este soporte en función de su naturaleza podrá ser prestado de forma localizada, deslocalizada e in-situ:

- **Soporte localizado** en las instalaciones de AndalucíaCERT: servicios que el adjudicatario deberá prestar a través de un equipo de trabajo adscrito y ubicado físicamente en la sede de AndalucíaCERT de Sevilla y/o Málaga.
- **Soporte deslocalizado**: soporte que el adjudicatario (contratista y/o fabricante) deberá prestar de manera deslocalizada desde su SOC/CSIRT propio y/o con recursos diferenciados de los adscritos a los servicios prestados en las instalaciones de AndalucíaCERT.
- **Soporte in-situ**: servicios que el adjudicatario (contratista y/o fabricante) deberá prestar in situ en sedes de la Junta de Andalucía en situaciones excepcionales para la resolución de incidentes.

Todos los trabajos se realizarán de acuerdo con los procedimientos, formatos, sistemas y aplicaciones implantados en AndalucíaCERT.

Los servicios de soporte estarán sujetos a Acuerdos de Nivel de Servicio (ANS) y se prestarán por parte del contratista o del fabricante, pero en todo caso por personal técnico cualificado en la solución.

Se valorarán mejoras para la reducción de determinados tiempos asociados a dichos ANS (**SOBRE 3, NO INCLUIR EN SOBRE 2. CRITERIOS 2.3, 2.8, 2.9 y 2.10**).

5.2.1. Soporte para el correcto funcionamiento de la plataforma

Este soporte estará prestado en horario **12x5** en días laborables, de **forma localizada**, por personal técnico ubicado en AndalucíaCERT, cuya sede actualmente está localizada en Tomares (Sevilla) y/o en el futuro también en Málaga capital.

El equipo de trabajo se organizará en dos niveles funcionales que ejecutarán distintas tareas según su conocimiento y capacidad:

- Grupo de Técnicos de Primer Nivel (TN1), integrado por técnicos especialistas de respuesta a incidentes.
- Grupo de Técnicos de Segundo Nivel (TN2), integrado por técnicos especialistas de respuesta a incidentes expertos.

Este servicio engloba las labores propias de gestión de la plataforma, así como de la monitorización de incidentes de seguridad basados en los eventos generados por la solución.

Las tareas propias a desarrollar serán las siguientes:

- Una vez finalizada la fase de despliegue, podrán realizar entre otras actividades, el alta de nuevos organismos, asesoramiento a los mismos en la instalación de nuevos agentes, elaboración de paquetes de software, por incrementos o modificaciones en la base instalada de equipos. El despliegue de estos agentes se realizará por parte del Área de Puesto de Trabajo y de los organismos, con sus propias herramientas y personal.
- Elaboración de los procedimientos manuales de instalación y configuración del agente para aquellos equipos que no se pueda automatizar su instalación.
- Coordinación, asesoramiento y resolución de incidencias al Área de Puesto de Trabajo y a los organismos.
- Asesoramiento y resolución de incidencias para migraciones (por ejemplo, a infraestructura VDI).
- Gestión y ajuste de la plataforma: gestión del inventario, gestión de usuarios y permisos, y ajuste fino, entre otras.
- Ejecución de todo tipo peticiones de solicitud, entre las que se incluyen aquellas tipificadas "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.

- Desarrollo e implantación de integraciones con otros sistemas de AndalucíaCERT: LUCIA, REYES, MISP, etc.
- Configuración y despliegue de políticas de detección y respuesta automática.
- Gestión de los IOC/IOA del fabricante y de terceros.
- Atención a las detecciones y monitorización de alertas de seguridad, recepción de alertas procedentes del soporte a la caza de amenazas o de otras fuentes, ejecución de acciones de respuesta, gestión de los incidentes en la plataforma LUCÍA de AndalucíaCERT y coordinación con los puntos de contacto (PoC) para la contención y erradicación. Notificación y escalado de las alertas según los procedimientos que se establezcan.
- Atención y resolución de incidencias según ANS Atención y resolución de incidencias.
- Monitorización de la disponibilidad del servicio.
- Coordinación, asesoramiento y resolución de incidencias al Área de Puesto de Trabajo y a los organismos, con motivo de mal funcionamiento o denegación del servicio del agente o consola.
- Mantenimiento de la plataforma y los agentes: actualizaciones, aseguramiento de la disponibilidad, solución de incidencias.
- Interlocución con el servicio de soporte y mantenimiento del fabricante.
- Seguimiento y corrección de los posibles falsos positivos que se produzcan, mediante generación de excepciones.
- Documentación de las respuestas automáticas configuradas, comunicación de las mismas al Área de Puesto de Trabajo y a los organismos.
- Diseño de cuadros de mandos y reporte periódico de situación.
- Definición y documentación, alineadas con los procedimientos de AndalucíaCERT, y transferencia de conocimiento sobre casos de uso en este área, incluyendo runbooks/playbooks para la detección y respuesta.
- Identificación y propuesta de mejoras del servicio y de la funcionalidad de la plataforma.

- En general, atención de consultas técnicas.

Los técnicos TN1 y TN2 deberán disponer de formación especializada del fabricante en el producto EDR ofertado, si éste cuenta con un programa de este tipo.

Requisitos mínimos – Técnicos TN1
TITULACIÓN
Formación Profesional de Grado Medio o Técnico en FP, Bachiller superior, FP2 o equivalente en la especialidad de informática y/o telecomunicaciones.
FORMACIÓN TÉCNICA
- Conocimientos acreditados en gestión y soporte de productos de seguridad del fabricante (EDR). - Conocimientos en administración de Microsoft Windows y Linux. - Gestión de incidentes de seguridad.
ACTIVIDAD PROFESIONAL
- Al menos 6 meses realizando labores de administración, implantación, mantenimiento y soporte de sistemas Windows y Linux. - Al menos 6 meses de experiencia en gestión de redes de más de 1.000 PC's distribuidos en varias sedes. - Al menos 6 meses de experiencia trabajando en un equipo de ciberseguridad, preferiblemente en un SOC o un CERT.

Requisitos mínimos – Técnicos TN2
TITULACIÓN
Formación Profesional de Grado Superior o Técnico Superior en FP o equivalente en la especialidad de informática y/o telecomunicaciones.
FORMACIÓN TÉCNICA
- Conocimientos acreditados en gestión y administración de productos de seguridad del fabricante (EDR). - Conocimientos en administración de Microsoft Windows y Linux. - Gestión de incidentes de seguridad complejos.

ACTIVIDAD PROFESIONAL
- Al menos 12 meses realizando labores de administración, implantación, mantenimiento y soporte de sistemas Windows y Linux. - Al menos 12 meses de experiencia en gestión de redes de más de 1.000 PC's distribuidos en varias sedes. - Al menos 12 meses de experiencia trabajando en un equipo de ciberseguridad, preferiblemente en un SOC o un CERT.

Para ambos perfiles, TN1 y TN2, se valorará el cumplimiento por encima de los mínimos requeridos, con interés en que cuenten con certificaciones **CompTIA Security +** en el momento de presentar la oferta o el compromiso de que dispondrán de ella en un plazo máximo de 3 meses desde su incorporación como TN1 o TN2. **(SOBRE 3, NO INCLUIR EN SOBRE 2. CRITERIO 2.4)**

Complementariamente, se ofrecerá un **soporte deslocalizado**, desde el SOC del adjudicatario o/y en el del fabricante, en el horario complementario, para garantizar una cobertura **24x7** del servicio, y también que actúe como desbordamiento en caso de incidentes de especial relevancia durante el horario del soporte localizado antes descrito. Este soporte deslocalizado realizará, al menos, las siguientes tareas:

- Atención a las detecciones y monitorización de alertas de seguridad, recepción de alertas procedentes del soporte a la caza de amenazas o de otras fuentes, ejecución de acciones de respuesta, gestión de los incidentes en la plataforma LUCÍA de AndalucíaCERT y coordinación con los puntos de contacto (PoC) para la contención y erradicación. Notificación y escalado de las alertas según los procedimientos que se establezcan.
- Atención y resolución de incidencias según ANS Atención y resolución de incidencias.
- Monitorización de la disponibilidad del servicio.
- Coordinación, asesoramiento y resolución de incidencias al Área de Puesto de Trabajo y a los organismos, con motivo de mal funcionamiento o denegación del servicio del agente o consola.
- Ejecución de peticiones de solicitud 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.

- Interlocución con el servicio de soporte y mantenimiento del fabricante.

Con **periodicidad mensual** se entregará por parte del contratista un **informe de actividad del Soporte para el correcto funcionamiento de la plataforma** donde se pormenoricen con detalle las actividades llevadas a cabo por el soporte localizado y deslocalizado respecto del listado de tareas antes enumerado para ambos tipos de soporte. En el apartado ANS de entrega de informes periódicos y singulares se concreta el compromiso máximo de entrega de este informe.

Se valorará la integración entre los niveles de soporte localizado y deslocalizado, la idoneidad de las tareas a realizar por uno y otro, y el balanceo de la carga de trabajo entre ambos niveles. **(SOBRE 2)**.

En el apartado ANS Soporte para el correcto funcionamiento de la plataforma se establecen los umbrales mínimos requeridos para considerar que el soporte se presta a satisfacción. El incumplimiento de los mismos dará lugar a la imposición de penalidades por cumplimiento defectuoso.

5.2.2. Soporte para la caza de amenazas

La solución propuesta debe proporcionar un soporte de búsqueda proactiva de amenazas (threat hunting). Este soporte de threat hunting gestionado debe apoyarse en los programas internos de inteligencia del fabricante de seguridad propuesto y debe notificar las detecciones o incidentes de relevancia detectados en los que se considere que debe existir respuesta o actuación por parte de la Junta de Andalucía para responder y/o minimizar el impacto ante un posible ataque.

Este servicio estará prestado, indistintamente, de forma **deslocalizada** en el SOC del adjudicatario o/y en el del fabricante, en **horario 24x7**.

El objetivo es detectar actividades que no se pueden descubrir mediante técnicas tradicionales, y que permita detectar ataques en fase temprana, detectar equipos comprometidos por amenazas persistentes avanzadas, anomalías de comportamiento o compromisos por personal interno, entre otros.

Las actividades a desarrollan serán las siguientes:

- Actividades de caza de amenazas, en base a campañas activas y a informes de ciberinteligencia, así como a peticiones expresas desde el responsable del contrato.

- Notificación y escalado, al soporte para el correcto funcionamiento de la plataforma, de las amenazas detectadas según los procedimientos que se establezcan. Propuesta de acciones de contención y erradicación. Colaboración con el soporte anteriormente descrito para su puesta en marcha.
- **Informe periódico de actividad y hallazgos**. Al menos, informe mensual con alertas encontradas en el período, investigaciones trabajadas, metodología empleada, inteligencia añadida o implementada sobre la herramienta.
- **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.
- Definición y documentación, alineadas con los procedimientos de AndalucíaCERT, y transferencia de conocimiento sobre casos de uso en este área, incluyendo runbooks/playbooks para la detección y respuesta.
- Identificación y propuesta de mejoras del servicio.

En el apartado 9.2. ANS Soporte para la caza de amenazas se establecen los umbrales mínimos requeridos para considerar que el soporte se presta a satisfacción. El incumplimiento de los mismos dará lugar a la imposición de penalidades por cumplimiento defectuoso.

Se valorará el modelo de prestación de este soporte, considerando de valor propuestas que detallen la forma en la que se presta éste: metodología y herramientas utilizadas, fuentes de información e inteligencia consultadas y utilizadas para la realización de búsquedas, participación del fabricante de la plataforma de seguridad para complementar el soporte a la caza de amenazas añadiendo sus propias fuentes de inteligencia y capacidades de búsqueda y detección, integración con la solución tecnológica propuesta para la generación de detecciones específicas vinculadas la caza de amenazas, mecanismos y canales de comunicación y notificación, organización, entre otros aspectos. **(SOBRE 2)**

5.2.3. Soporte para la respuesta a incidentes

Este soporte será prestado de forma **deslocalizada** e **in situ**, a demanda del responsable del contrato, en horario **24x7**, ante situaciones que requieran un apoyo extraordinario y presencial para la contención y erradicación de un ciberincidente especialmente grave y complejo.

Las tareas a realizar serán las siguientes:

- Recopilación de la información pertinente, identificación de las causas del incidente, identificación de las labores a realizar y entrega de plan de acción.
- Apoyo en la contención de la amenaza y en la recuperación y restauración del servicio.
- A demanda del Responsable de Servicio, desplazamiento a la sede en la que se haya producido el incidente. Apoyo y colaboración, con las Áreas y/o organismos afectados, en la planificación de las medidas de respuesta. Las sedes podrán estar ubicadas en cualquier punto del territorio de Andalucía.
- Documentación de las actuaciones realizadas en un **informe final** y transferencia de conocimiento.

La solicitud de asistencia para el soporte a incidentes se realizará a través del Sistema integrado de operaciones (SIO).

La dinámica del soporte se describe en el apartado 9.3. ANS Soporte para la respuesta a incidentes.

Los gastos derivados por desplazamiento, alojamiento y manutención serán responsabilidad del contratista.

En el apartado 9.3. ANS Soporte para la respuesta a incidentes se establecen los umbrales mínimos requeridos para considerar que el soporte se presta a satisfacción. El incumplimiento de los mismos dará lugar a la imposición de penalidades por cumplimiento defectuoso.

Se valorará el modelo de prestación de este soporte, considerando de valor propuestas que detallen la forma en la que se presta éste: metodología de actuación en respuesta a incidentes, herramientas utilizadas, recursos y fuentes de inteligencia, documentación y capacidades de contextualización del incidente y equipo de coordinación de respuesta a incidentes, entre otros aspectos. **(SOBRE 2)**

Se valorará también la participación del fabricante de la solución EDR, a modo de **bolsa de horas sin coste adicional** (al menos, 150 horas para todo el periodo de duración de la contratación), para complementar el soporte a la respuesta a incidentes añadiendo sus propias capacidades. **(SOBRE 3, NO INCLUIR EN SOBRE 2. CRITERIO 2.7)**

6. Plan de ejecución del proyecto

El proyecto de ejecución de esta contratación con carácter general seguirá la siguiente planificación de referencia:

- Fase 1. Definición del despliegue. Tiempo estimado: 3 semanas, semanas a contar desde la fecha de formalización del contrato.
- Fase 2. Provisión y configuración inicial de la plataforma. Tiempo estimado: 4 semanas, a contar desde la finalización de la fase 1.
- Fase 3. Despliegue. Tiempo estimado: continuo a lo largo de vida de la contratación.
- Fase 4. Capacitación inicial. Tiempo estimado: Antes de finalizar el mes 3, contado desde la formalización.
- Fase 5. Optimización de la plataforma. Tiempo estimado: continuo a lo largo de vida de la contratación.
- Fase 6. Explotación del sistema y formación adicional/refuerzo. Tiempo estimado: continuo a lo largo de vida de la contratación.
- Fase 7. Transferencia del servicio. Tiempo estimado: 3 meses, antes de la finalización del contrato.

El contratista contará con un equipo de trabajo conformado por expertos en la tecnología ofertada con amplia experiencia en la solución.

6.1. Fase 1: Definición del despliegue

En esta primera fase se mantendrán reuniones para la elaboración de un Plan Técnico de Despliegue que incluirá, al menos:

1) Arquitectura del sistema. Diagramas físicos y lógicos. Identificación de proveedores involucrados y certificaciones de seguridad
    - Proveedores de la nube involucrados, incluyendo dependencias de proveedores terceros (IaaS/PaaS/SaaS).
    - Certificaciones y evaluaciones de seguridad (SOC 2 Type 2 reports, ISO/IEC 27001) de la plataforma EDR, incluyendo dependencias de proveedores terceros (IaaS/PaaS/SaaS).
2) Plan detallado de puesta en marcha y configuración inicial, incluyendo estimación de tiempos para cada una de las tareas. Procedimientos de aprovisionamiento e

instalación, que incluya detalle de los elementos que son necesarios para disponer del sistema totalmente operativo. Identificación de los interlocutores involucrados.

3) Planificación de los roles, perfiles y divisiones necesarias en la plataforma para la clasificación de los equipos finales y la gestión de la misma para una estructura multiorganismo.
4) Plan de pruebas de aceptación. Deberá cubrir al menos el cumplimiento de los requisitos técnicos y funcionales del apartado Requisitos del suministro, otras características ofertadas por el licitante, carga/huella de uso de recursos del agente, 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.
5) Plan de optimización. Se debe maximizar la detección de las amenazas y minimizar la indisponibilidad (especialmente los falsos positivos con afectación a la disponibilidad de servicios en el equipo final).
6) Procedimientos de detección y respuesta (manual/automática, reactiva/proactiva).
7) Procedimiento de gestión de incidencias, consultas y peticiones (identificación de herramientas empleadas).
8) Procedimiento de inventariado según se prevé en el apartado Inventariado de los Servicios en CMDB.
9) Planificación de necesidades para la integración con sistemas externos.

   (**SOBRE 2**, desde punto "*1) Arquitectura del sistema*" hasta punto "*9) Planificación de necesidades para la integración con sistemas externos*").

10) Documentación técnica. Manuales de usuario y administración.
11) Plan de explotación y mantenimiento de la plataforma.
12) 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.
13) Identificación del responsable de seguridad y delegado de protección de datos del proveedor. Procedimiento de gestión de incidentes de seguridad en el proveedor.

El plazo máximo de entrega del **Plan técnico de despliegue** se estipula en el apartado ANS de entrega de informes periódicos y singulares, que para este informe es de **tres semanas** a contar desde la fecha de formalización del contrato.

Una vez aprobado el Plan técnico de despliegue el responsable del contrato autorizará el comienzo de la Fase 2.

6.2. Fase 2: Provisión y configuración inicial de la plataforma

En esta fase se llevará a cabo la configuración inicial de la plataforma EDR para su despliegue y se hará una recopilación de necesidades del número de equipos finales necesario proteger por cada organismo de los incluidos en el Alcance del contrato.

El plazo máximo es de **cuatro semanas** a contar desde la finalización de la fase 1.

La siguiente tabla recoge, de forma orientativa, el número de equipos finales censados en los sistemas de la Junta de Andalucía de una parte de sus organismos. Del resto de organismos que figuran en el Alcance del contrato no se dispone de información, y tendrá que ser recabada en esta fase.

En esta fase preparatoria <u>se determinará por el Responsable del Contrato la idoneidad de que la totalidad o un subconjunto de estos equipos sea cubierto o no por la solución EDR</u>.

Etiquetas de fila	Cuenta de Organismo
AACID	111
AAE	341
AAIICC	635
ACREA	82
AEFPA	954
AGAPA	3126
AIDEA	408
AMAYA	1709
AndaluciaCERT	36
AOPJA	140
APAE	458
ASAG	756
ASBG	1941
ASCS	1090
ASSDA	1185
AVRA	672
CAA	94
CAAC	60

CAGPDS-CAPDER	3216
CAGPDS-CMAOT	3171
CCPH	1815
CECEU	1235
CED	4091
CEFTA	4364
Centinela	1
CFIOT	3425
CHIFE	5261
CIPSC	3656
CPAI	3861
CSF	2959
CTD	719
CTPDA	157
CTRJAL-SGJ	15359
CTRJAL-SGT	765
EPES	819
EPPA	299
EPSP	944
FPS	344
IAAP	386
IAJ	239
IAM	328
IAPH	196
IECA	640
IFAPA	874
PAG	269
RTVA	1124
SAE	6048
SAS	53508
Total general	**133872**

6.3. Fase 3: Despliegue

Se realizará el aprovisionamiento de los organismos con sus estructuras dependientes en la plataforma multi-organismo (contenedor, cuentas de administradores, perfiles…).

Incluirá el desarrollo de paquetes de software para distribuir el agente a través de las herramientas de despliegue de software del organismo, y la elaboración de los procedimientos manuales de instalación y configuración del agente para aquellos equipos que no se pueda automatizar su instalación.

El despliegue de los agentes se realizará por parte de los organismos, con sus propias herramientas y personal.

El elemento unitario de consumo será la “Licencia para equipo final desplegado con una garantía de 48 meses”. Para este elemento unitario se establecerá un precio unitario en el Catálogo de elementos unitarios y precios.

El inductor de consumo asociado a este elemento unitario es el “Nº de equipos final con la solución EDR desplegada / mes ".

Con esta fase comenzará el despliegue de las licencias adquiridas en los equipos finales, y se dará inicio a la fase 5 y la explotación de la fase 7 (la fase 4, de capacitación inicial, se ejecutará en paralelo a las fases 3 y 5).

Habida cuenta de que el despliegue en los equipos finales dependerá de los organismos del alcance de este contrato, se considera que durante toda la vida del contrato se podrán realizar despliegues de la solución EDR.

Una planificación orientativa en cuanto al número de “Licencia para equipo final desplegado con una duración de 48 meses” a suministrar y por hitos de certificación sería la siguiente:

Mes	Estimación de Nº de equipos finales con la solución EDR desplegada / mes	Nº de equipos finales con la solución EDR desplegada (**acumulado** por meses)	Certificación Licencias	Estimación de nº de licencias a certificar por hito
1	10.000	10.000	-	-
2	20.000	30.000	-	-
3	30.000	60.000	Sí	60.000
4	5.000	65.000	-	-
5	5.000	70.000	-	-
6	5.000	75.000	-	-
7	5.000	80.000	-	-
8	5.000	85.000	-	-
9	5.000	90.000	Sí	30.000
10	5.000	95.000	-	-
11	5.000	100.000	-	-
12	5.000	105.000	-	-
13	5.000	110.000	-	-

14	5.000	115.000	-	-
15	5.000	120.000	Sí	30.000
16	1.600	121.600	-	-
17	1.600	123.200	-	-
18	1.600	124.800	-	-
19	1.600	126.400	-	-
20	1.600	128.000	-	-
21	1.600	129.600	Sí	9.600
22	400	130.000	-	-
23	400	130.400	-	-
24	400	130.800	-	-
25	400	131.200	-	-
26	400	131.600	-	-
27	400	132.000	Sí	2.400
28	300	132.300	-	-
29	300	132.600	-	-
30	300	132.900	-	-
31	300	133.200	-	-
32	300	133.500	-	-
33	300	133.800	Sí	1.800
34	100	133.900	-	-
35	100	134.000	-	-
36	100	134.100	-	-
37	100	134.200	-	-
38	100	134.300	-	-
39	100	134.400	Sí	600
40	100	134.500	-	-
41	100	134.600	-	-
42	100	134.700	-	-
43	100	134.800	-	-
44	100	134.900	-	-
45	100	135.000	Sí	600
46	0	135.000	-	-
47	0	135.000	-	-
48	0	135.000	-	-
total uds	**135.000**	**5.566.300**		**135.000**

Es decir, que se estima que en el mes 3 se puedan certificar unas 60.000 licencias, en el mes 9 30.000 licencias y así hasta un total estimado de 135.000 licencias, según se describe en la siguiente tabla.

Mes	Estimación de "Licencias para equipo final desplegado" a suministrar (garantía 48 meses)
3	60.000
9	30.000
15	30.000
21	9.600
27	2.400
33	1.800
39	600
45	600
Total unidades	135.000

No obstante, como así se ha indicado en el Objeto del contrato, las licencias necesarias se irán suministrando conforme se vaya realizando el despliegue en los organismos previstos en el alcance de esta contratación (véase Fase 3: Despliegue) <u>sin que exista un compromiso mínimo de consumo ni total, ni parcial en los hitos de certificación</u> que se explican a continuación. De igual modo, será posible alcanzar mayor número de equipos de los establecidos por hito, siempre que no se alcance el presupuesto máximo del contrato y según la distribución económica de anualidades.

Como así se ha expuesto, en el mes 3 desde la formalización de la contratación y, posteriormente, cada 6 meses, se establecerán **hitos de certificación** de las licencias desplegadas en el periodo inmediatamente anterior.

Los hitos de certificación consistirán en la contabilización y posterior certificación de las licencias desplegadas el último día del mes de certificación (meses 3, 9, 15, 21, 27, 33, 39 y 45 del contrato). El plazo de garantía de 48 meses de las licencias, descrito en el apartado 4.6. Garantía del suministro, comenzará tras este hito de certificación.

Para la certificación de las licencias suministradas será necesario además entregar la siguiente documentación:

1. Documentación de la entrega: Documentación del despliegue realizado en el periodo, configuración por organismo, organismos cubiertos, tipología de equipos finales desplegados, fechas de despliegue, incidencias de despliegue, actas de reuniones de despliegue.
2. Documentación de las pruebas de aceptación.

Durante los periodos entre hitos de certificación se podrán hacer despliegues de la solución de EDR sin limitación en número, y de cuyo resultado se dará cuenta en el hito de certificación inmediatamente posterior. La facturación de las licencias certificadas se realizará en el mes posterior a la certificación (mes + 1).

Ejemplo:

Mes desde la formalización del contrato	Hito de Certificación	Licencias estimadas	Nº de equipos final con la solución EDR desplegada / mes	Nº de equipos final con la solución EDR desplegada (acumulado total por meses)
1	-	0	10.531	10.531
2	-	0	16.894	27.425
3	Sí	60.000	24.568	51.993
Licencias certificadas			**51.993**	
4	-	0	6.975	58.968
5	-	0	6.534	65.502
6	-	0	5.567	71.069
7	-	0	6.347	77.416
8	-	0	5.456	82.872
9	Sí	30.000	5.324	88.196
Licencias certificadas			**36.203**	

En el mes 3 se certificarán 51.993 licencias y en el mes 9, 36.203 licencias. Estas licencias se facturarán en el mes 4 y 10 respectivamente, según el precio unitario del Catálogo de elementos unitarios y precios.

A criterio y aprobación del responsable del contrato, esta planificación estimada y su duración podrán sufrir cambios, siempre que no sea por causas imputables al contratista y siempre que se ajuste a la distribución presupuestaria.

Sin perjuicio de lo anterior, cuando a lo largo de la vida del contrato se produzca la sustitución de equipos ya existentes se procederá al reciclado de las licencias ya existentes sobre los equipos sustituidos.

6.4. Fase 4: Capacitación inicial

En esta fase, que se desarrollará de forma paralela a las fases 3 y 5, se realizarán acciones de capacitación según los requisitos establecidos en el apartado Capacitación en el uso de la plataforma.

El elemento unitario de consumo será la "Acción de capacitación inicial", la cual se celebrará en fechas a determinar con el responsable del contrato, con tres ediciones, para un mínimo de 20 asistentes cada una y con una duración mínima de 20 horas lectivas cada una.

A efectos de estimaciones de consumo se prevé una única acción de capacitación inicial (con tres ediciones) que se realizará antes del mes 3 contado desde la firma del contrato.

La certificación de esta acción de formación se hará en el mes 3.

6.5. Fase 5: Optimización de la plataforma

Esta fase, con carácter continuo, incluirá el seguimiento de los despliegues, la configuración necesaria de la plataforma para ajustarse a los mismos, eliminando incompatibilidades y falsos positivos, y mejorando la eficiencia y la capacidad de detección y respuesta.

Cuando a lo largo de la vida del contrato se produzcan cambios en la plataforma de equipos finales, por actualizaciones de software (ej: sistemas operativos), o cambios de configuración que puedan colisionar con el actual funcionamiento de la solución EDR, se llevará a cabo una nueva optimización de la plataforma por el equipo de soporte.

6.6. Fase 6: Explotación del servicio

Durante esta fase transcurre la práctica totalidad del contrato y en ella se llevará a cabo el Soporte funcional y técnico en el uso de la plataforma EDR según lo previsto en su correspondiente apartado 5.2. Todas estas acciones responden a un servicio especializado y específico para la detección y respuesta a ciberincidentes en equipo final que llevará implícita la instalación y puesta en marcha de la solución y la integración con otros elementos y servicios de seguridad además del soporte inherente al suministro, para la capacitación inicial y de refuerzo, y el soporte funcional y técnico en el uso de la plataforma.

Esta fase transcurre en paralelo desde el comienzo del despliegue de los agentes en la Fase 3: Despliegue.

La explotación del servicio está directamente relacionada con el despliegue de la solución EDR en los equipos finales. Puesto que es posible que el despliegue se extienda durante todo el contrato la actividad de soporte no se conoce a priori, sino que será en función de las necesidades, sin que exista un compromiso mínimo de consumo.

Una estimación de los esfuerzos requeridos, por tipo de soporte, a lo largo del contrato sería la siguiente.

- **Jefatura de proyecto**, realizando las tareas y actividades descritas en el apartado Jefatura de proyecto.

  Para este soporte el esfuerzo a realizar vendrá determinado en todo momento por las horas de Jefatura de Proyecto empleadas al mes, es decir,

  - el elemento unitario de consumo es el "Hora de Jefatura de Proyecto". Para este elemento unitario se establecerá un precio unitario en el Catálogo de elementos unitarios y precios.
  - El inductor de consumo asociado a este elemento unitario es la "Nº Horas Soporte Jefatura de Proyecto certificadas / mes".

  Se estima un esfuerzo equivalente a una dedicación estimada mensual de 30 horas. El esfuerzo total estimado es de 1.440 horas en 48 meses.

  Se describe en esta fase la estimación prevista para la Jefatura de Proyecto por uniformidad con otros soportes, pero se prevé la participación de la jefatura de proyecto desde el inicio de la ejecución del contrato, en todas sus fases.

- Soporte para el correcto funcionamiento de la plataforma (**soporte localizado**)

  - Soporte Técnicos de Primer Nivel (TN1): Para este soporte el esfuerzo a realizar vendrá determinado en todo momento por las horas de soporte por técnico TN1 empleadas al mes, es decir,

    - el elemento unitario de consumo es el "Hora de Soporte para el correcto funcionamiento de la plataforma (soporte localizado TN1)". Para esta unidad de consumo se establecerá un precio unitario en el Catálogo de elementos unitarios y precios.
    - El inductor de consumo asociado a este elemento unitario es el "Nº Horas Soporte Localizado TN1 certificadas".

    Se estima un esfuerzo equivalente a 2 Técnicos de Primer Nivel (TN1), con posibilidad de incrementar a 1 técnico adicional a partir del mes 13 (inclusive) del contrato. El esfuerzo total estimado es de 19.800 horas en 48 meses.

  - Soporte Técnicos de Segundo Nivel (TN2): Para este soporte el esfuerzo a realizar vendrá determinado en todo momento por las horas de soporte por técnico TN2 empleadas al mes, es decir,

- el <u>elemento unitario</u> de consumo es el "Hora de Soporte para el correcto funcionamiento de la plataforma (soporte localizado TN2)". Para esta unidad de consumo se establecerá un precio unitario en el Catálogo de elementos unitarios y precios.
- El <u>inductor de consumo</u> asociado a este elemento unitario es el "Nº Horas Soporte Localizado TN2 certificadas".

Se estima un esfuerzo equivalente a 2 Técnicos de Segundo Nivel (TN2), con posibilidad de incrementar a 1 técnico adicional a partir del mes 25 (inclusive) del contrato. El esfuerzo total estimado es de 18.000 horas en 48 meses.

La siguiente tabla muestra la estimación de consumo a realizar por meses, durante la vida del contrato:

Mes	Soporte locali-zado– Perfil TN1 (horas)	Soporte localiza-do– Perfil TN2 (horas)	Jefatura de pro-yecto (horas)
1	300	300	30
2	300	300	30
3	300	300	30
4	300	300	30
5	300	300	30
6	300	300	30
7	300	300	30
8	300	300	30
9	300	300	30
10	300	300	30
11	300	300	30
12	300	300	30
13	450	300	30
14	450	300	30
15	450	300	30
16	450	300	30
17	450	300	30
18	450	300	30
19	450	300	30
20	450	300	30
21	450	300	30
22	450	300	30
23	450	300	30

24	450	300	30
25	450	450	30
26	450	450	30
27	450	450	30
28	450	450	30
29	450	450	30
30	450	450	30
31	450	450	30
32	450	450	30
33	450	450	30
34	450	450	30
35	450	450	30
36	450	450	30
37	450	450	30
38	450	450	30
39	450	450	30
40	450	450	30
41	450	450	30
42	450	450	30
43	450	450	30
44	450	450	30
45	450	450	30
46	450	450	30
47	450	450	30
48	450	450	30
	19.800	**18.000**	**1.440**

Tanto para la Jefatura de proyecto como para el Soporte para el correcto funcionamiento de la plataforma (soporte localizado) los esfuerzos a realizar se determinarán a demanda del Responsable del contrato, que fijará las necesidades previstas con carácter mensual y de forma anticipada.

A criterio y aprobación del responsable del contrato, esta planificación estimada y su duración podrán sufrir cambios, siempre que no sea por causas imputables al contratista y siempre que se ajuste a la distribución presupuestaria.

En el mes 3 desde la formalización de la contratación y, posteriormente, cada tres meses, se establecerán **hitos de certificación** del soporte prestado en el periodo inmediatamente anterior. Es decir, los hitos de certificación son **trimestrales**.

Los hitos de certificación consistirán en la contabilización y posterior certificación del Nº de horas empleadas en cada uno de los meses que median entre hitos de certificación. La facturación del soporte certificado se facturará en el mes posterior a la certificación (mes + 1).

Ejemplo:

Mes	Hito de Certificación	Soporte localizado– Perfil TN1 (horas)	Soporte localizado– Perfil TN2 (horas)	Jefatura de proyecto (horas)
1	-	256	256	28
2	-	320	300	30
3	Sí	280	280	29
Horas certificadas		**856**	**836**	**87**
4	-	295	295	32
5	-	280	295	30
6	Sí	295	295	28
Horas certificadas		**870**	**885**	**90**
7	-	300	285	30
8	-	300	285	30
9	Sí	280	285	30
Horas certificadas		**880**	**855**	**90**

Las horas certificadas en los hitos "mes 3", "mes 6" y "mes 9" se facturarán en los meses 4, 7 y 10 respectivamente, según el precio unitario del Catálogo de elementos unitarios y precios.

- Soporte para el correcto funcionamiento de la plataforma (**soporte deslocalizado**) en horario complementario al soporte localizado, para garantizar una cobertura 24x7 del servicio.

  Para este soporte el esfuerzo a realizar vendrá determinado en todo momento por el número de equipos finales sobre los que esté desplegada la solución de EDR, es decir,

  - el elemento unitario de consumo es el "Soporte deslocalizado para el correcto funcionamiento de la plataforma por equipo final con la solución EDR desplegada". Para esta unidad de consumo se establecerá un precio unitario en el Catálogo de elementos unitarios y precios.
  - El inductor de consumo asociado a este elemento unitario es el "Nº de equipos finales con la solución EDR desplegada / mes".

Para obtener un consumo estimado unidades sobre el "Soporte de equipo final con la solución EDR desplegada / mes", se puede acudir a la tabla incluida en el apartado Fase 3: Despliegue respecto del despliegue orientativo de la solución sobre los equipos finales mes a mes y su acumulado. No obstante, se recuerda que no existe un compromiso mínimo de consumo ni total, ni parcial en los hitos de certificación que se explican a continuación. De igual modo, será posible alcanzar mayor número de equipos de los establecidos por hito, siempre que no se alcance el presupuesto máximo del contrato y según la distribución económica de anualidades.

Puesto que el número de equipos finales irá aumentando según el despliegue de la solución EDR se establece que, a efectos de certificación y posterior facturación, será el día 15 de cada mes o día laborable más próximo (exceptuando festivos nacionales y regionales) cuando se contabilicen los equipos finales que aparezcan en la consola de la solución EDR. Esa cantidad será la tenida en cuenta a efectos de certificación y posteriormente facturación en concepto de soporte deslocalizado, según se expone a continuación.

En el mes 3 desde la formalización de la contratación y, posteriormente, cada tres meses, se establecerán hitos de certificación del soporte prestado en el periodo inmediatamente anterior. Es decir, los hitos de certificación son **trimestrales**.

Los hitos de certificación consistirán en la contabilización y posterior certificación del número de equipos finales con la solución EDR desplegada - según se ha expuesto - en cada uno de los meses que median entre hitos de certificación. La facturación del soporte certificado se facturará en el mes posterior a la certificación (mes + 1).

Ejemplo:

Mes	Hito de Certificación	Soporte deslocalizado para el correcto funcionamiento de la plataforma por equipo final con la solución EDR desplegada / mes (nº de equipos finales con la solución EDR desplegada) (día 15 de cada mes)
1	-	10.012
2	-	25.086
3	Sí	54.578
Nº de equipos finales con la solución EDR desplegada en el trimestre		**89.676**
4	-	61.890
5	-	74.368

6	Sí	82.560
Nº de equipos finales con la solución EDR desplegada en el trimestre		**218.818**
7	-	83.490
8	-	89.887
9	Sí	95.578
Nº de equipos finales con la solución EDR desplegada en el trimestre		**268.955**

El número de unidades de "Soporte deslocalizado para el correcto funcionamiento de la plataforma por equipo final con la solución EDR desplegada / mes (nº de equipos finales con la solución EDR desplegada)" en los hitos "mes 3", "mes 6" y "mes 9" se facturarán en los meses 4, 7 y 9 respectivamente según el precio unitario del Catálogo de elementos unitarios y precios.

- Soporte para la **caza de amenazas**, según se describe en el apartado Soporte para la caza de amenazas. Estará prestado, indistintamente, de forma localizada o deslocalizada en el SOC del adjudicatario o/y en el del fabricante, en horario 24x7.

  Para este soporte el esfuerzo a realizar vendrá determinado en todo momento por el número de equipos finales sobre los que esté desplegada la solución de EDR, es decir,

  - el elemento unitario de consumo es el "Soporte caza de amenazas por equipo final con la solución EDR desplegada / mes". Para esta unidad de consumo se establecerá un precio unitario en el Catálogo de elementos unitarios y precios.
  - El inductor de consumo asociado a este elemento unitario es el "Nº de equipos finales con la solución EDR desplegada / mes".

  Para obtener un consumo estimado unidades sobre el "Soporte caza de amenazas por equipo final con la solución EDR desplegada / mes", se puede acudir a la tabla incluida en el apartado Fase 3: Despliegue respecto del despliegue orientativo de la solución sobre los equipos finales mes a mes y su acumulado. No obstante, se recuerda que no existe un compromiso mínimo de consumo ni total, ni parcial en los hitos de certificación que se explican a continuación. De igual modo, será posible alcanzar mayor número de equipos de los establecidos por hito, siempre que no se alcance el presupuesto máximo del contrato y según la distribución económica de anualidades.

  Puesto que el número de equipos finales irá aumentando según el despliegue de la solución EDR se establece que, a efectos de certificación y posterior facturación, será el día 15 de cada mes o día laborable más próximo (exceptuando festivos nacionales y regionales) cuando se contabilicen los equipos finales que aparezcan en la consola de la solución EDR. Esa cantidad será la tenida en cuenta a efectos de certificación y posteriormente facturación en concepto de soporte para la caza de amenazas, según se expone a continuación.

En el mes 3 desde la formalización de la contratación y, posteriormente, cada tres meses, se establecerán hitos de certificación del soporte prestado en el periodo inmediatamente anterior. Es decir, los hitos de certificación son **trimestrales**.

Los hitos de certificación consistirán en la contabilización y posterior certificación del número de equipos finales con la solución EDR desplegada - según se ha expuesto - en cada uno de los meses que median entre hitos de certificación. La facturación del soporte certificado se facturará en el mes posterior a la certificación (mes + 1).

Ejemplo:

Mes	Hito de Certificación	Soporte caza de amenazas por equipo final con la solución EDR desplegada / mes (nº de equipos finales con la solución EDR desplegada) (día 15 de cada mes)
1	-	10.012
2	-	25.086
3	Sí	54.578
Nº de equipos finales con la solución EDR desplegada en el trimestre		**89.676**
4	-	61.890
5	-	74.368
6	Sí	82.560
Nº de equipos finales con la solución EDR desplegada en el trimestre		**218.818**
7	-	83.490
8	-	89.887
9	Sí	95.578
Nº de equipos finales con la solución EDR desplegada en el trimestre		**268.955**

El número de unidades de “Soporte caza de amenzas por equipo final con la solución EDR desplegada / mes (nº de equipos finales con la solución EDR desplegada)” en los hitos “mes 3”, “mes 6” y “mes 9” se facturarán en los meses 4, 7 y 9 respectivamente según el precio unitario del Catálogo de elementos unitarios y precios.

- Soporte para la **respuesta a incidentes**, según se describe en el apartado Soporte para la respuesta a incidentes.

  Será prestado de forma deslocalizada e in situ, a demanda del responsable del contrato, en horario 24x7, ante situaciones que requieran un apoyo extraordinario y presencial para la contención y erradicación de un ciberincidente especialmente grave y complejo.

  Para este soporte el esfuerzo a realizar vendrá determinado en todo momento por las horas de soporte para la respuesta a incidentes empleadas al mes, es decir:

  - El elemento unitario de consumo es el “Hora Soporte respuesta incidentes / mes”. Para esta unidad de consumo se establecerá un precio unitario en el Catálogo de elementos unitarios y precios.
  - El inductor de consumo asociado a este elemento unitario es el “Nº Horas Soporte respuesta incidentes certificada / mes”.

  Se estima un esfuerzo equivalente a 120 horas / año. El esfuerzo total estimado es de 480 horas en 48 meses, sin que exista un compromiso mínimo de consumo ni total, ni parcial en los hitos de certificación que se explican a continuación. De igual modo, será posible alcanzar mayor número de horas de las establecidas por hito, siempre que no se alcance el presupuesto máximo del contrato y según la distribución económica de anualidades.

  En el mes 3 desde la formalización de la contratación y, posteriormente, cada tres meses, se establecerán hitos de certificación del soporte prestado en el periodo inmediatamente anterior. Es decir, los hitos de certificación son **trimestrales**.

  Los hitos de certificación consistirán en la contabilización y posterior certificación del Nº de horas de soporte para respuesta a incidentes en cada uno de los meses que median entre hitos de certificación. La facturación del soporte certificado se facturará en el mes posterior a la certificación (mes + 1).

  Ejemplo:

Mes	Hito de Certificación	Nº Horas Soporte respuesta incidentes certificada / mes
1	-	0

2	-	4
3	Sí	0
Horas certificadas		**4**
4	-	6
5	-	0
6	Sí	2
Horas certificadas		**8**
7	-	0
8	-	0
9	Sí	4
Horas certificadas		**4**

Las horas certificadas en los hitos "mes 3", "mes 6" y "mes 9" se facturarán en los meses 4, 7 y 9 respectivamente, según el precio unitario del Catálogo de elementos unitarios y precios.

Durante esta fase de Explotación se realizarán también las actividades de **capacitación adicional o de refuerzo** descritas en el apartado Capacitación en el uso de la plataforma.

- El elemento unitario de consumo será la "Acción de capacitación adicional o refuerzo". Para esta unidad de consumo se establecerá un precio unitario en el Catálogo de elementos unitarios y precios. Cada acción tendrá una convocatoria, en fecha a determinar con el responsable del contrato, para un mínimo de 25 asistentes cada una y con una duración mínima de 4 horas lectivas.
- El inductor de consumo será el "Nº de acciones de capacitación adicional / mes" que se realicen.

A efectos de estimación de consumo, se prevé que se requieran 7 sesiones de refuerzo para un total de 48 meses.

En el mes 3 desde la formalización de la contratación y, posteriormente, cada tres meses, se establecerán hitos de certificación del soporte prestado en el periodo inmediatamente anterior. Es decir, los hitos de certificación son **trimestrales**.

Los hitos de certificación consistirán en la contabilización y posterior certificación del Nº de acciones de capacitación adicional en cada uno de los meses que median entre hitos de certificación. La facturación del soporte certificado se facturará en el mes posterior a la certificación (mes + 1).

Ejemplo:

Mes	Hito de Certificación	Nº de acciones de capacitación adicional / mes
1	-	0
2	-	0
3	Sí	0
Acciones de capacitación certificadas		**0**
4	-	0
5	-	0
6	Sí	1
Acciones de capacitación certificadas		**1**
7	-	0
8	-	0
9	Sí	1
Acciones de capacitación certificadas		**1**

Las acciones de capacitación certificadas en los hitos "mes 3", "mes 6" y "mes 9" se facturarán en los meses 4, 7 y 9 respectivamente, según el precio unitario del Catálogo de elementos unitarios y precios.

6.7. Fase 7: Transferencia/devolución del servicio

El adjudicatario deberá garantizar que la Junta de Andalucía pueda continuar con la explotación de los servicios, las tecnologías ofertadas y configuraciones adoptadas una vez finalizado el contrato sin que se produzca interrupción en el servicio como consecuencia del cambio.

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

Estas actividades serán coordinadas por el Jefe de proyecto y con la colaboración del equipo puesto a disposición por el contratista.

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 al adjudicatario entrante 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 según se estipula en el apartado ANS de entrega de informes periódicos y singulares se entregará con fecha tope al inicio del mes 47 de la contratación, es decir, 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 deberá prestar soporte para la desinstalación de los agentes EDR desplegados.

7. Resumen de Estimaciones para el suministro y el soporte asociado

La siguiente tabla muestra de forma orientativa los diferentes elementos unitarios del Catálogo de elementos unitarios y precios, la fase asociada del Plan, el inductor de consumo / Unidades de contratación, la estimación de contratación y los meses de certificación de las unidades de contratación, tanto para el suministro de licencias, como para el soporte asociado.

Elemento Unitario	Fase	Inductor de consumo / Uds de contratación	Uds estimadas a contratar en 48 meses	Observaciones sobre la estimación realizada	Certificación	Contabilización
SUMINISTRO						
Licencia para equipo final desplegado con la funcionalidad requerida en apartado 4 PPT (garantía de 48 meses)	Fase 3: Despliegue	Nº de equipos finales con la solución EDR desplegada / mes	135.000	135.000 en 48 meses.	Meses 3, 9, 15, 21, 27, 33, 39 y 45 del contrato	Mensual, a día 15 de cada mes o laborable más próximo
SOPORTE						
Acción de Capacitación inicial	Fase 4: Capacitación inicial	Acción de capacitación inicial	1	1	Mes 3 del contrato	Mensual, a cierre del último día del mes en que se hubiera impartido
Acción de Capacitación adicional o de refuerzo	Fase 6. Explotación del servicio	Nº Acciones de capacitación adicional contabilizadas / mes	7	7 en 48 meses.	Trimestral	Mensual, a cierre del último día del mes en que se hubiera impartido
Hora Jefatura de proyecto	Todas las Fases.	Nº Horas Jefatura de proyecto contabilizadas / mes	1.440	30 horas / mes. 1440 horas en 48 meses	Trimestral	Mensual, a cierre del último día del mes
Hora de Soporte para el correcto funcionamiento de la plataforma (soporte localizado TN1)	Fase 6. Explotación del servicio	Nº Horas Soporte Localizado TN1 contabilizadas / mes	19.800	Se estima un esfuerzo equivalente a 2 Técnicos de Primer Nivel (TN1), con posibilidad de incrementar a 1 técnico	Trimestral	Mensual, a cierre del último día del mes

				adicional a partir del mes 13 (inclusi- El esfuerzo total estimado es de 19.800 horas en 48 meses		
Hora de Soporte para el correcto funcionamiento de la plataforma (soporte localizado TN2)		Nº Horas Soporte Localizado TN2 contabilizadas / mes	18.000	Se estima un esfuerzo equivalente a 2 Técnicos de Segundo Nivel (TN2), con posibilidad de incrementar a 1 técnico adicional a partir del mes 25 (inclusive) del contrato El esfuerzo total estimado es de 18.000 horas en 48 meses	Trimestral	Mensual, a cierre del último día del mes
Soporte deslocalizado para el correcto funcionamiento de la plataforma por equipo final con la solución EDR desplegada / mes	Fase 6. Explotación del servicio	Nº de equipos finales con la solución EDR desplegada contabilizados / mes	5.566.300	Dependiente del Nº de equipos finales con la solución EDR desplegada en el mes correspondiente El esfuerzo total estimado es de 5.566.300 uds de soporte en 48 meses	Trimestral	Mensual, a día 15 de cada mes o laborable más próximo
Soporte caza de amenazas por equipo final con la solución EDR desplegada / mes	Fase 6. Explotación del servicio	Nº de equipos finales con la solución EDR desplegada contabilizados / mes	5.566.300	Dependiente del Nº de equipos finales con la solución EDR desplegada en el mes correspondiente El esfuerzo total estimado es de 5.566.300 uds de soporte en 48 meses	Trimestral	Mensual, a día 15 de cada mes o laborable más próximo
Hora de Soporte para la respuesta a incidentes	Fase 6. Explotación del servicio	Nº Horas Soporte respuesta incidentes contabilizadas / mes	480	120 horas/año	Trimestral	Mensual, a cierre del último día del mes

Junta de Andalucía

Financiado por la Unión Europea NextGenerationEU

La tabla que se incluye a continuación indica los hitos de certificación para el suministro y soporte asociado:

Mes desde la formalización del contrato	Certificación Licencias	Jefatura de proyecto	SOPORTE FUNCIONAL Y TÉCNICO EN EL USO DE LA PLATAFORMA EDR					Capacitación inicial (fase 4 del apartado 6 del PPT)	Capacitación adicional (a lo largo de la fase 6 del apartado 6).
			SOPORTE PARA EL CORRECTO FUNCIONAMIENTO DE LA PLATAFORMA			Soporte para la caza de amenazas	Soporte para la respuesta a incidentes		
			Soporte localizado-Perfil TN1	Soporte localizado-Perfil TN2	Soporte deslocalizado 24x7				
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	Sí	Sí	Sí	Sí	Sí	Sí	-	Sí
7	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-
9	Sí	Sí	Sí	Sí	Sí	Sí	Sí	-	Sí
10	-	-	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-
12	-	Sí	Sí	Sí	Sí	Sí	Sí	-	Sí
13	-	-	-	-	-	-	-	-	-
14	-	-	-	-	-	-	-	-	-
15	Sí	Sí	Sí	Sí	Sí	Sí	Sí	-	Sí
16	-	-	-	-	-	-	-	-	-
17	-	-	-	-	-	-	-	-	-
18	-	Sí	Sí	Sí	Sí	Sí	Sí	-	Sí
19	-	-	-	-	-	-	-	-	-
20	-	-	-	-	-	-	-	-	-
21	Sí	Sí	Sí	Sí	Sí	Sí	Sí	-	Sí
22	-	-	-	-	-	-	-	-	-
23	-	-	-	-	-	-	-	-	-
24	-	Sí	Sí	Sí	Sí	Sí	Sí	-	Sí

25	-	-	-	-	-	-	-	-	-
26	-	-	-	-	-	-	-	-	-
27	Sí	Sí	Sí	Sí	Sí	Sí	Sí	-	Sí
28	-	-	-	-	-	-	-	-	-
29	-	-	-	-	-	-	-	-	-
30	-	Sí	Sí	Sí	Sí	Sí	Sí	-	Sí
31	-	-	-	-	-	-	-	-	-
32	-	-	-	-	-	-	-	-	-
33	Sí	Sí	Sí	Sí	Sí	Sí	Sí	-	Sí
34	-	-	-	-	-	-	-	-	-
35	-	-	-	-	-	-	-	-	-
36	-	Sí	Sí	Sí	Sí	Sí	Sí	-	Sí
37	-	-	-	-	-	-	-	-	-
38	-	-	-	-	-	-	-	-	-
39	Sí	Sí	Sí	Sí	Sí	Sí	Sí	-	Sí
40	-	-	-	-	-	-	-	-	-
41	-	-	-	-	-	-	-	-	-
42	-	Sí	Sí	Sí	Sí	Sí	Sí	-	Sí
43	-	-	-	-	-	-	-	-	-
44	-	-	-	-	-	-	-	-	-
45	Sí	Sí	Sí	Sí	Sí	Sí	Sí	-	Sí
46	-	-	-	-	-	-	-	-	-
47	-	-	-	-	-	-	-	-	-
48	-	Sí	Sí	Sí	Sí	Sí	Sí	-	Sí

8. Catálogo de elementos unitarios y precios

El Catálogo de elementos unitarios y precios es un documento que recoge todos los elementos unitarios de suministro y soporte asociado solicitables por la Agencia Digital de Andalucía.

Los elementos unitarios del catálogo vendrán con indicación de su precio con y sin IVA y serán los únicos conceptos que puedan figurar en las facturas que emita el adjudicatario.

El Catálogo recogerá los siguientes ítems:

- Suministros:
    - Licencia para equipo final desplegado con la funcionalidad requerida en apartado 4 PPT (garantía de 48 meses)
- Soporte:
    - Acción de Capacitación inicial, según requisitos establecidos en los apartados Capacitación en el uso de la plataforma y Fase 4: Capacitación inicial del PPT.
    - Acción de Capacitación adicional o de refuerzo, según requisitos establecidos en los apartados Capacitación en el uso de la plataforma y Fase 6: Explotación del serviciodel PPT.
    - Hora Jefatura de proyecto, según los requisitos establecidos en los apartados Soporte asociado y Jefatura de proyecto del PPT.
    - Hora de Soporte para el correcto funcionamiento de la plataforma (soporte localizado TN1), según los requisitos establecidos en los apartados Soporte para el correcto funcionamiento de la plataforma y Fase 6: Explotación del servicio del PPT.
    - Hora de Soporte para el correcto funcionamiento de la plataforma (soporte localizado TN2), según los requisitos establecidos en los apartados Soporte para el correcto funcionamiento de la plataforma y Fase 6: Explotación del servicio del PPT.
    - Soporte deslocalizado para el correcto funcionamiento de la plataforma por equipo final con la solución EDR desplegada / mes, según los requisitos establecidos en los apartados Soporte para el correcto funcionamiento de la plataforma y Fase 6: Explotación del servicio del PPT.

- Soporte caza de amenzas por equipo final con la solución EDR desplegada / mes, según los requisitos establecidos en los apartados Soporte para la caza de amenazas y Fase 6: Explotación del servicio del PPT.
- Hora de Soporte para la respuesta a incidentes, según los requisitos establecidos en los apartados Soporte para la respuesta a incidentes y Fase 6: Explotación del servicio del PPT.

En el fichero de ProposicionEconomica_EDR.xlsx en la pestaña “Catálogo elementos unitarios” se recogerá el precio de los elementos unitarios enumerados.

Mensualmente se solicitará un **informe de planta** de elementos suministrados y contabilizados según se dispone en el apartado 6.6. Fase 6: Explotación del servicio y de acuerdo al ANS establecido en el apartado 9.4. ANS de entrega de informes periódicos y singulares.

9. Acuerdos 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:

- Disponibilidad de la plataforma centralizada.
- Atención y resolución de incidencias.
- Atención y resolución de consultas y peticiones.
- Monitorización de alertas de seguridad.
- Soporte para la caza de amenazas.
- Soporte para la Respuesta avanzada a incidentes.
- Entrega de informes periódicos y singulares.

Se utilizará el Sistema integrado de operaciones (SIO) para el seguimiento de incidencias, consultas y peticiones (actuaciones), y servirá como herramienta de seguimiento y medida del cumplimiento de los ANS.

Se analizarán los ANS por meses de cierre de las actuaciones (provisiones, incidencias, consultas, …). 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 mes 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 trimestral o a cualquier otra periodicidad.

9.1. ANS Soporte para el correcto funcionamiento de la plataforma

9.1.1. ANS Disponibilidad de la plataforma centralizada

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

La disponibilidad del servicio será entendida como el porcentaje de tiempo mensual en que se encontrará operativa la plataforma EDR una vez se encuentre ésta 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 del mismo sea garantía 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.

9.1.1.1. Definición y cálculo de métricas

La disponibilidad se calculará mensualmente de acuerdo a la siguiente expresión:

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

Donde:

T_{tot}: Tiempo total del periodo considerado

T_{noDisp}: Tiempo de no disponibilidad de la plataforma

9.1.1.2. Condiciones de medida

El horario que aplica al cálculo de los tiempos será de **24x7**, alineado con el horario de servicio del Soporte 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 EDR en nube no pueden traducirse en una indisponibilidad del servicio.

9.1.1.3. Compromisos

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

Se valorará una mejora de la disponibilidad sobre el mínimo requerido, hasta un máximo del 99,95%. **(SOBRE 3, NO INCLUIR EN SOBRE 2. CRITERIO 2.2)**.

9.1.2. ANS Atención y resolución de incidencias

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 prestado por la plataforma en explotación, ya sean estas motivadas por fallos software, de configuración, etc, así como la afectación en la disponibilidad de servicios legítimos en el equipo final. Se entiende como “servicio” la entidad sobre la que se abre la incidencia. En todo caso queda a criterio del Responsable de Servicio la determinación exacta del “servicio”.

Ejemplos de incidencias pueden ser indisponibilidad de algún servicio por bloqueo de un programa informático legítimo por parte del agente EDR, o degradación en el equipo final por uso excesivo de CPU por parte del agente EDR, entre otros.

No se consideran en este apartado las actividades de soporte a respuesta a incidentes, cuyo ANS se aborda en el apartado 9.3. ANS Soporte para la respuesta a incidentes ni así tampoco las acciones de mitigación y respuesta que se deriven de la monitorización de alertas de seguridad.

9.1.2.1. 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.
- **Indicador de Incidencias Reiteradas (IIR)**: se define como el número de incidencias consecutivas del mismo servicio por causas imputables al adjudicatario en el periodo de tiempo establecido para la medida. En el mes “M” se contabilizarán las reiteraciones de los 90 días anteriores.
- **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 a través de la herramientas de gestión Sistema Integral de Operaciones. Se establece un ANS para la entrega de informes en función de la criticidad de la misma en el apartado 9.1.2.3.1.

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 un mismo 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.

9.1.2.2. 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 servicio del Soporte 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:

- 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 EDR 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 severidad, y se categorizarán por el Responsable de Servicio.

La severidad 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:
    - Indisponibilidad de servicios en los puestos de trabajo y los servidores con afectación en más de 50 equipos.
    - Indisponibilidad de servicios en los puestos de trabajo y los servidores de sistemas singulares
- **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 severidad "baja".

Las incidencias se clasifican en cuatro tipos en función de la prioridad en su resolución. La prioridad que se calcula según la tabla siguiente:

PRIORIDAD		**SEVERIDAD INCIDENCIA**		
		ALTA	**MEDIA**	**BAJA**
CRITICIDAD	**Extrema**	0	0	1
	Alta	1	2	2
	Media	2	2	3

Existirán las siguientes particularidades:

- Serán siempre de criticidad extrema las que afecten a la disponibilidad de la plataforma centralizada y/o su conectividad con la red de la Junta de Andalucía.

Para el resto de incidencias, será el Responsable de Servicio el que determine la criticidad.

- Se entiende por días laborables los comprendidos de lunes a viernes, quedando excluidos los festivos nacionales y autonómicos andaluces.
- 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 (p.ej. inaccesibilidad de las instalaciones), 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.
    - La responsabilidad de la parada en sistemas por estos motivos recae en el adjudicatario; la activación en el Responsable de Servicio.

9.1.2.3. Compromisos

9.1.2.3.1. ANS DIRECTOS

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

ANS	Prioridad	Indicador		
		Tiempo de Respuesta (minutos)	Tiempo de Resolución (minutos)	Tiempo de Reparación (minutos)

Incidencias	0	30	240	270
	1	45	480	525
	2	60	600	660
	3	60	660	720

Compromisos Incidencias

Se valorará el valor comprometido de este ANS por encima del mínimo aquí indicado.

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

ANS	Prioridad	Indicador Tiempo de Entrega (minutos)
Informe de Incidencias	0	480
	1	1080
	2	1440
	3	2880

Compromisos Informes Incidencias

9.1.2.3.2. 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%

- **Cumplimiento en Reiteración de incidencias (CIIR):** es el porcentaje total (100%) menos el porcentaje del sumatorio del indicador de Reiteradas (IIR) para cada incidencia del servicio i respecto del total de incidencias cerradas en el mes "M" objeto del cálculo más 20. Se determina mediante la fórmula siguiente:

ANS	Fórmula	Compromiso CCIIR
Cumplimiento en Reiteración de incidencias (CIIR)	$CIIR = 100 - \left(\frac{\sum_{i=1}^{n} IIR_i}{N+20} \right) * 100$	≥ 95%

Donde:

IIRi = número de reiteraciones de incidencias del servicio i-ésimo, entendido esto como la entidad sobre la que se abre la incidencia, en los 90 días anteriores al día 1 del mes M.
n = número de servicios con reiteración de incidencias en el contrato.
N = número de incidencias del contrato cerradas en el mes.

9.1.3. 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 del Soporte para el correcto funcionamiento de la plataforma (localizado y deslocalizado), entendidas éstas como consultas técnicas de la solución y peticiones/provisiones en la gestión y administración de la solución.

El seguimiento de los niveles de servicio referidos se realizará en el Sistema integrado de operaciones (SIO).

Este apartado trata de:

- **Consultas**: Cualquier tipo de solicitud de información no contemplada en ninguno de los puntos anteriores. El Responsable de Servicio, a lo largo del contrato, establecerá los tipos de consultas que estimen convenientes para la ejecución del proyecto; entre otras, se encuentran las siguientes (indicando el nivel de prioridad de las mismas). La categorización de cada petición se realizará por el Responsable de Servicio 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: sobre 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 cambios/aplicaciones de configuración sobre la plataforma una vez que los agentes ya han sido desplegados, es decir, cuando ya están en fase explotación. (p.e. altas/bajas de usuarios/grupos, solicitudes expresas de actualización software…). 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. La categorización de cada petición se realizará por el Responsable de Servicio en el momento inicial de la solicitud, en función de su naturaleza y complejidad.

9.1.3.1. 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:

CC Prioridad 0 =100- (Número de Peticiones Incumplidas NPII - Prioridad 0/(Total Peticiones Tramitadas NPTT - Prioridad 0+20))*100
CC 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.

9.1.3.2. 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, para las actividades exclusivas del

Soporte para el correcto funcionamiento de la plataforma localizado y de 24x7 para deslocalizado.

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

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.

9.1.3.3. Compromisos

9.1.3.3.1. 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.

9.1.3.3.2. 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%

9.1.4. ANS Monitorización de alertas de seguridad

En este apartado se definen los parámetros de nivel de servicio relativos a la **monitorización de alertas de seguridad** del Soporte para el correcto funcionamiento de la plataforma, entendidas estas como la gestión de las alertas de seguridad generadas automáticamente por la plataforma, detectadas por el soporte para el correcto funcionamiento o notificadas por el equipo de caza de amenazas. Se entiende como "servicio" la entidad sobre la que se abre la incidencia. En todo caso queda a criterio del Responsable de Servicio la determinación exacta del "servicio".

No se consideran en este apartado las actividades de soporte a respuesta a incidentes, cuyo ANS se aborda en el apartado 9.3. ANS Soporte para la respuesta a incidentes ni así tampoco las acciones relacionadas con el soporte para la caza de amenazas cuyo ANS se aborda en el apartado 9.2. ANS Soporte para la caza de amenazas.

9.1.4.1. 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 equipo de caza de amenazas o por el soporte para el correcto funcionamiento, o de forma proactiva por la solución) hasta el envío por parte del adjudicatario de la aceptación de la incidencia:

$$Tiempoderespuesta = Horadeaceptaci\acute{o}n - Horadenotificaci\acute{o}ndelaincidencia - ParadasdeReloj$$

- **Tiempo de Resolución:** Tiempo transcurrido desde que se acepta la incidencia hasta que la incidencia queda resuelta o escalada por parte del adjudicatario. Este tiempo incluye el análisis de la incidencia, así como la determinación de si es un falso positivo o no. En caso de que no sea una falso positivo se debe aplicar la respuesta previamente autorizada o escalar el plan de respuesta recomendado al área u organismo; la gestión debe quedar registrada en LUCIA. Se calcula de la siguiente forma:

$$Tiempoderesoluci\acute{o}n = Horaderesoluci\acute{o}n - Horadeaceptaci\acute{o}n - ParadasdeReloj$$

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

$$TiempodeReparaci\acute{o}n = TiempodeRespuesta + TiempodeResoluci\acute{o}n$$

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.

Con el objetivo de mejorar la calidad y prevenir posibles incidencias de seguridad, se podrá requerir al adjudicatario una serie de informes de incidencias de monitorización de alertas de seguridad, con la determinación de la causa/origen de la incidencia, pasos seguidos hasta su resolución, medidas preventivas adoptadas, etc.

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

- **Indicador de Reapertura de Incidencias de Monitorización de Alertas de Seguridad (IRAM)**: Cuenta el número de veces que se reabre una incidencia de monitorización de alertas de seguridad en las 72 horas naturales siguientes a la resolución por parte del contratista; esto estará provocado, entre otras causas, por una reiteración de la incidencia, persistencia de la misma o no conformidad

- **Indicador de Incidencias Reiteradas de Monitorización de Alertas de Seguridad (IIRM)**: se define como el número de incidencias de monitorización de alertas de seguridad consecutivas del mismo servicio por causas imputables al adjudicatario en el periodo de tiempo establecido para la medida. En el mes "M" se contabilizarán las reiteraciones de los 90 días anteriores.
- **Tiempo de entrega de Informe de Resolución de incidencia de Monitorización de Alertas de Seguridad**: Se define como el tiempo que transcurre desde que se solicita el informe, una vez resuelta la incidencia de monitorización de alertas, hasta que el adjudicatario realiza la entrega del Informe de Resolución de Incidencia de Monitorización de Alertas de Seguridad 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 de la Gestión del Servicio a través de las herramientas de gestión habituales (Sistema Integral de Operaciones, email, etc.). Se establece un ANS para la entrega de informes en función de la criticidad de la misma en el apartado 9.1.4.3.1.
- Las medidas se realizan sobre el universo de incidencias de Monitorización de Alertas de Seguridad que pasan por el adjudicatario (NIIOM), es decir, por todas aquellas incidencias que se han asignado al adjudicatario en un mismo contrato: aceptadas, no aceptadas, resueltas o no resueltas independientemente de la causa u origen de la incidencia. En este universo NIIOM, se contabilizarán como incidencias incumplidas (NIIIM) aquellas en los que se ha sobrepasado bien el tiempo de respuesta, bien el tiempo de resolución, o ambos. En este universo NIIOM, se contabilizarán como incidencias cerradas (NM) 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 de monitorización de alertas de seguridad 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.

9.1.4.2. 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 servicio del Soporte 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:

- 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 EDR 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 categorizarán 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

9.1.4.3. Compromisos

9.1.4.3.1. ANS DIRECTOS

- **Incidencias de monitorización de alertas de seguridad:** 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**

		(minutos)	(minutos)	(minutos)
Incidencias	0	30	180	210
	1	45	270	315
	2	90	540	630
	3	120	600	720

Compromisos Incidencias de monitorización de alertas

Se valorará el valor comprometido de este ANS por encima del mínimo aquí indicado.

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

ANS	Peligrosidad	Indicador Tiempo de Entrega (minutos)
Informe de Incidencias	0	480
	1	1080
	2	1440
	3	2880

Compromisos Informes Incidencias de monitorización de alertas

9.1.4.3.2. ANS INDIRECTOS

- **Cumplimiento en Tratamiento de Incidencias de Monitorización de alertas de seguridad (CTIIM):** es el porcentaje total (100%) menos el porcentaje de incidencias de monitorización incumplidas (NIIIM) respecto del total de incidencias de monitorización (NIIOM) del contrato más 20. Se determina mediante la fórmula siguiente:

ANS	Fórmula	Compromiso CCTIIM
Cumplimiento en Tratamiento de Incidencias de monitorización de alertas (CTIIM)	$CTTIM = 100 - \left(\frac{NIIIM}{(NIIOM + 20)} \right) * 10($	≥ 95%

- **Cumplimiento de Reapertura de Incidencias de Monitorización de alertas de seguridad (CRAM):** es el porcentaje total (100%) menos el porcentaje entre el número de veces que se reabre una incidencia (sumatorio IRAM) respecto del total de incidencias cerradas (NM) del contrato más 10. Se determina mediante la fórmula siguiente :

ANS	Fórmula	Compromiso CCRAM
Cumplimiento de Reapertura de Incidencias de monitorización de alertas (CRAM)	$CRAM = 100 - \left(\frac{\sum IRAM}{(NM+10)} \right) * 100$	≥ 90%

- **Cumplimiento en Reiteración de incidencias de Monitorización de alertas de seguridad (CIIRM):** es el porcentaje total (100%) menos el porcentaje entre el sumatorio del indicador de Reiteradas (IIRM) para cada incidencia del servicio-i y el total de incidencias cerradas en el mes “M” objeto del cálculo más 20. Se determina mediante la fórmula siguiente:

ANS	Fórmula	Compromiso CCIIRM
Cumplimiento en Reiteración de incidencias de monitorización de alertas (CIIRM)	$CIIRM = 100 - \left(\frac{\sum_{i=1}^{n} IIRM_i}{N+20} \right) * 100$	≥ 95%

Donde:

IIRMi = número de reiteraciones de incidencias de monitorización de alertas del servicio i-ésimo, entendido esto como la entidad sobre la que se abre la incidencia, en los 90 días anteriores al día 1 del mes M.
n = número de servicios con reiteración de incidencias en el contrato.
NM = número de incidencias del contrato cerrados en el mes.

9.2. ANS Soporte para la caza de amenazas

En este apartado se definen los parámetros de nivel de servicio relativos al soporte de asistencia de caza de amenazas descrito en el apartado Soporte para la caza de amenazas.

El seguimiento de los niveles de servicio referidos se realizará en el Sistema integrado de operaciones (SIO).

9.2.1. Definición y cálculo de métricas

La correcta prestación del servicio se medirá en base dos parámetros de cumplimiento. Uno, referido al reporte de la actividad con carácter periódico mensual, y otro, referido al reporte singular respecto de amenazas concretas que se vayan identificando/detectando.

El reporte se materializará en forma de informes incluidos en las actividades previstas para el Soporte para la caza de amenazas :

- **Informes periódicos de actividad y hallazgos**, referidos en el apartado 5.2.2. Soporte para la caza de amenazas 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 un informe mensual; el formato y contenido de estos informes quedará fijado por el Responsable de Servicio. Dicho informe deberá contemplar, al menos:
  - Alertas de seguridad encontradas en el período.
  - Investigaciones trabajadas durante el período (ya sea abiertas en el mismo, o no cerradas desde períodos anteriores).
  - Metodología empleada (MITRE ATT&CK).
  - Inteligencia añadida o implementada en el período sobre la herramienta (búsquedas de amenazas, casos de uso desarrollados...).
- **Informes singulares de actividad y hallazgos**, referidos en el apartado 5.2.2. Soporte para la caza de amenazas Son informes cuya entrega es única. 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.

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 hasta la entrega validada de dicho informe por el adjudicatario.

TEI= Hora validación informe - Hora solicitud informe

9.2.2. Condiciones de medida

El horario que aplica al cálculo de entrega de informes será de **24x7** alineado con el horario de servicio del Soporte para la caza de amenazas .

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 a los procedimientos en vigor establecidos por el Responsable de Servicio. Estos estarán claramente recogidos en los sistemas de gestión que el Responsable de Servicio. Será responsabilidad del adjudicatario informar de las incidencias objeto de dicho retraso para que puedan ser debidamente tenidas en cuenta.

Los informes deberán ser puestos a disposición del Responsable de Servicio a través de canal seguro, o bien cifrando el documento a través de clave pública PGP.

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.

9.2.3. Compromisos

Compromiso de entrega de informes:

INFORMES SINGULARES	PERIODICIDAD	COMPROMISO (TEIC) Tiempo de Entrega
Informe singular de actividad y hallazgos	Singular no periódico. A demanda.	24 horas desde su solicitud en horario 24x7
Informes periódicos de actividad y hallazgos	Mensual	Antes del 10º día natural del mes.

9.3. ANS Soporte para la respuesta a incidentes

En este apartado se definen los parámetros de nivel de servicio relativos al servicio de respuesta avanzada a incidentes descrito en el apartado Soporte para la respuesta a incidentes, para la respuesta a brechas e incidentes de seguridad de especial gravedad y complejidad.

9.3.1. Definición y cálculo de métricas

En todos los casos, se medirá la atención con el tiempo de respuesta, el Tiempo de Preparación y entrega de Plan de Acción y el Tiempo de inicio de las actividades de remediación. Adicionalmente, cuando se requiera por el Responsable de Servicio, el Tiempo de Desplazamiento a sede.

La dinámica será la siguiente:

- El responsable de Servicio requerirá al adjudicatario soporte para respuesta a incidentes. En la solicitud se indicará si es necesario desplazamiento a sede, sin perjuicio de que se pueda solicitar en un momento posterior.
- Posteriormente el adjudicatario enviará aceptación de la solicitud de soporte.
- A partir de este momento, el adjudicatario deberá recopilar la información pertinente, identificar las labores a realizar y entregar un Plan de Acción.
- Presentado el plan de acción, el Responsable de Servicio requerirá al adjudicatario el inicio de las actividades de remediación si estuviera de acuerdo con el Plan de Acción propuesto. En caso contrario, se requerirá un nuevo Plan de Acción al adjudicatario. Esta iteración podrá repetirse cuantas veces sea necesario.
- Si fuera necesario, a demanda del Responsable de Servicio, se desplazarán el/los recursos a las instalaciones afectadas para comenzar las tareas orientadas a la recuperación del servicio afectado y al análisis de las causas del incidente.
- Documentación de las actuaciones realizadas a modo de informe final y transferencia de conocimiento. El informe final contendrá un resumen de, al menos, acciones realizadas, metodología empleada, activos analizados, hallazgos, tácticas y técnicas observadas, indicadores obtenidos, probables causas raíz, posibles atribuciones y recomendaciones a aplicar.

Estos parámetros quedan definidos como sigue:

- **Tiempo de Respuesta:** Tiempo transcurrido desde la solicitud realizada por el Responsable de Servicio hasta el envío por parte del adjudicatario de la aceptación de la solicitud de soporte:

$$Tiempoderespuesta = Horadeaceptación - HoradeNotificacióndelasolicitud - ParadasdeReloj$$

- **Tiempo de Preparación y entrega de Plan de Acción:** Tiempo transcurrido desde que se acepta la solicitud por parte del adjudicatario hasta que entrega un Plan de Acción (hora de resolución). Se calcula de la siguiente forma:

Junta de Andalucía

Financiado por la Unión Europea NextGenerationEU

$$\mathit{TiempodePreparacionyEntregadePlan}=\mathit{Horaderesolución}-\mathit{Horadeaceptaciónadjudicatario}-\mathit{ParadasdeR}$$

- **Tiempo de presentación de un nuevo Plan de Acción:** Tiempo transcurrido desde que se acepta la solicitud por parte del adjudicatario de un nuevo Plan de Acción hasta que se entrega (hora de resolución). Se calcula de la siguiente forma:

$$\mathit{TiempodePreparacionyEntregadeNuevoPlan}=\mathit{Horaderesolución}-\mathit{Horadeaceptaciónadjudicatario}-\mathit{Para}$$

- **Tiempo de inicio de las actividades de remediación:** es el tiempo que transcurre desde la notificación de aprobación del Plan de Acción por parte del Responsable de Servicio hasta el envío por parte del adjudicatario de la aceptación del inicio de las actividades, dando comienzo a la ejecución del Plan:

$$\mathit{TiempodeInicioActividades}=\mathit{Horadeaceptaciónadjudicatario}-\mathit{HoradenotificacióndeAprobaciónporRespo}$$

Adicionalmente, cuando se requiera por parte del Responsable de Servicio:

- **Tiempo de Desplazamiento a sede:** es el tiempo máximo para que el adjudicatario desplace el/los recursos a las instalaciones afectadas. Se medirá como el periodo que transcurre entre la notificación del adjudicatario de que ha llegado a la sede y la notificación por parte del adjudicatario de la aceptación de la solicitud de desplazamiento a sede:

$$\mathit{TiempodeDesplazamiento}=\mathit{Horadenotificacion}\ \mathrm{EstoyenSede}-\mathit{Horadeaceptaciónadjudicatario}-\mathit{Paradasde}$$

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

TEI= Hora validación informe - Hora solicitud informe

9.3.2. Condiciones de medida

El horario que aplica al cálculo de los tiempos de respuesta y resolución de incidencias será de **24x7** alineado con el horario de servicio del Soporte para la respuesta a incidentes.

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 EDR 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 casos.

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 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 informar de las incidencias objeto de dicho retraso para que puedan ser debidamente tenidas en cuenta.

Los informes deberán ser puestos a disposición del Responsable de Servicio a través de canal seguro, o bien cifrando el documento a través de clave pública PGP.

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.

9.3.3. Compromisos

Se considerará que existe incumplimiento cuando se supere el límite del compromiso del Tiempo definido en la siguiente tabla de tiempos máximos:

ANS	Indicador					
	Tiempo de Respuesta TRC (horas)	**Tiempo de Preparación y entrega de Plan de Acción TPPAC (horas)**	**Tiempo de Preparación y entrega de Nuevo Plan de Acción TPNPAC (horas)**	**Tiempo de inicio de las actividades de remediación TIARC (horas)**	**Tiempo para desplazamiento a la sede – cuando se requiera – TDSC (horas)**	**Tiempo de Entrega del Informe Final TEIC (horas)**
Respuesta a	0,5	3	1,5	0,5	7	12

incidentes						

9.4. ANS de entrega de informes periódicos y singulares

En este apartado se definen los parámetros de nivel de servicio relativos a la entrega de informes singulares solicitados a demanda del Responsable de Servicio, y periódicos como los que se citan a continuación.

Quedan excluidos en este apartado los Informes de resolución de incidencias tratados en el apartado anterior sobre ANS Atención y resolución de incidencias, los Informes singulares de actividad y hallazgos y los Informes periódicos de actividad y hallazgos del apartado ANS Soporte para la caza de amenazas y el Informe final de soporte a la respuesta de incidentes del ANS Soporte para la respuesta a incidentes.

El seguimiento de los niveles de servicio referidos se realizará en el Sistema integrado de operaciones (SIO).

Este apartado trata de:

- **Informes singulares**: Son informes cuya entrega es única. Estos informes deberán ser elaborados a demanda a petición del 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.

9.4.1. Definición y cálculo de métricas

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

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

TEI= Hora validación informe - Hora solicitud informe

9.4.2. 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 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 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.

9.4.3. Compromisos

Compromiso de entrega de informes:

INFORMES SINGULARES	COMPROMISO Tiempo de Entrega del (TEIC)
Plan Técnico de Despliegue referido en el apartado Fase 1: Definición del despliegue	3 semanas a contar desde la fecha de formalización del contrato
Informe de transferencia del servicio referido en el apartado Fase 7: Transferencia/devolución del servicio	Este informe se entregará con fecha tope al inicio del mes 47 de la contratación, es decir, dos meses antes de su finalización.

INFORMES PERIÓDICOS	COMPROMISO	PERIODICIDAD
Informe de actividad mensual del Soporte para el correcto funcionamiento de la plataforma descrito en el apartado 5.2.1.	Antes del 10º día natural del mes.	Mensual
Detalle de **Cumplimiento ANS**	Antes del 5º día laboral del mes.	Mensual
Informe de planta: de elementos suministrados y contabilizados según se	TEI<=5 días laborables desde la	Mensual

INFORMES PERIÓDICOS	COMPROMISO	PERIODICIDAD
indica en el apartado Catálogo de elementos unitarios y precios.	solicitud del informe en los sistemas provistos por la Gestión/el Responsable del Servicio.	

10. Sistemas de información para el seguimiento del contrato

10.1. Sistema integrado de operaciones (SIO)

El Sistema Integrado de Operaciones (en adelante, SIO) es la herramienta utilizada por la persona el Responsable del Contrato y el Responsable de Servicio (véase roles en Responsable del contrato y Responsable de servicio) para gestionar los procedimientos referentes a la operativa de provisión, incidencias y facturación, y se encuentra dividido, entre otros, en los siguientes módulos:

- Gestión de catálogo, organigrama e inventario de servicios. Este módulo centraliza las funcionalidades y entidades básicas en los que se apoyan el resto de módulos.
- Gestión de incidencias y provisiones. Soporta los procesos de Incidencias y Provisión de servicio.
- Verificación y control de facturación. Implementa el proceso de Facturación de servicios.
- Informes. Módulo usado para la generación de informes sobre los Servicios (seguimiento de servicios, medición de ANS, cálculo de penalizaciones, etc.).

Tanto las mediciones de cumplimiento de los ANS como las penalizaciones asociadas serán extraídas de SIO (o del sistema que la persona Responsable del Contrato determine) y de los informes generados por éste. El adjudicatario podrá comprobar su funcionamiento en coordinación con la persona Responsable del Contrato.

Una descripción más detallada de SIO se puede encontrar en el ANEXO II: Descripción del Sistema Integrado de Operaciones (SIO).

10.1.1. Interacción del adjudicatario con SIO

El adjudicatario del servicio podrá optar por una de estas dos alternativas:

A. Uso de licencias REMEDY para operar directamente en SIO. Estas licencias pueden ser solicitadas al Responsable de Servicio (SANDETEL), quien la facturara conforme a su tarifario.

B. Integración de sus sistemas con las interfaces de Remedy

A) La interacción sería manual desde conexión Web segura;

El Responsable de Servicio pondrá a disposición del adjudicatario una interfaz a la herramienta SIO, facilitando manual de uso de SIO y proporcionando la información necesaria para el acceso al sistema, así como la documentación asociada y las vías de soporte a usuarios del sistema.

El adjudicatario dispondrá de las licencias de software necesarias para dicha conexión Web segura a SIO, tal y como se especifica en ANEXO II: Descripción del Sistema Integrado de Operaciones (SIO), según el número de usuarios y la concurrencia de estos que haya estimado para el servicio, y manteniendo en cualquier caso un mínimo de unidades de contingencia.

El adjudicatario tendrá que abonar el coste de adquisición de las licencias de software necesarias según corresponda por el número de usuarios que utilice.

B) En el caso de que opte por la integración realizará las adaptaciones y desarrollos necesarios en sus sistemas, así como las pruebas y mantenimientos de los mismos para la integración de dichos sistemas con SIO. Esta integración se realizará mediante el bus de servicios empresariales de la Gestión del Servicio que expondrá una API Web basada en protocolos estándar (Web-services). Se proporcionará a los adjudicatarios la siguiente documentación técnica:

- Interfaz de los Servicios Web publicados por SIO.
- Interfaz de los Servicios Web a publicar por los sistemas de los adjudicatarios.
- Protocolos de comunicación entre los sistemas para cada proceso (Incidencias, Provisión, Facturación, Informes, Consultas, etc.).

El adjudicatario correrá con los gastos de adaptación y mantenimiento correctivo y evolutivo de sus sistemas. El adjudicatario proporcionara un punto de entrada único con atención 24x7 para el mantenimiento de la interfaz con SIO, definiendo un plan de contingencia para situaciones de no disponibilidad. Los tiempos de respuesta y resolución ante incidencias de la interfaz del adjudicatario con SIO, se medirán y penalizaran según el ANS de resolución de avería, tendrá criticidad extrema y severidad en función del impacto de la avería del sistema.

El plazo máximo de adaptación al Web Service, en caso de optar por esta opción es de seis meses.

Para facilitar el período de integración durante los seis meses siguientes a la formalización del contrato (plazo máximo de adaptación a Web Service) el Responsable de Servicio facilitará el acceso a SIO desde conexión Web segura; facilitará manual de Uso SIO y proporcionará la información necesaria para el acceso al sistema, así como la documentación asociada, y las vías de soporte a usuarios del sistema.

El adjudicatario tendrá que abonar el coste de adquisición de las licencias de software necesarias según corresponda por el número de usuarios que utilice.

10.1.2. Inventariado de los Servicios en CMDB

El adjudicatario confirmará en sus sistemas las licencias activadas y el tenant al que pertenecen. Estos datos serán remitidos, con la periodicidad determinada en el apartado 9.4.3. Compromisos para los **informes de planta**, a la Agencia Digital de Andalucía para su validación, y se generará por parte del adjudicatario - de acuerdo a las especificaciones del sistema de ticketing SIO y los datos que sea preciso almacenar para la explotación y mantenimiento (fecha, número de serie, organismo, perfil, MAC y otra información que sea relevante) - el archivo con los datos estructurados para la carga en CMDB. Este procedimiento deberá incluir también un apartado para las bajas y modificaciones.

11. Organización del trabajo

Para el equipo de trabajo que el contratista disponga en la ejecución de este contrato se estará a lo dispuesto en los siguientes apartados.

11.1. Funciones y responsabilidades

11.1.1. Responsabilidades

Es responsabilidad de la empresa contratista impartir todas las órdenes, criterios de realización del trabajo y directrices a sus trabajadores/as, siendo la ADA del todo ajena a estas relaciones laborales y absteniéndose, en todo caso, de incidir en las mismas. Corresponde asimismo a la empresa contratista, de forma exclusiva, la vigilancia del horario de trabajo de los trabajadores, las posibles licencias horarias o permisos o cualquiera otra manifestación de las facultades del empleador. No obstante, es responsabilidad exclusiva del contratista, en la forma establecida en los pliegos, asegurar que el servicio quede convenientemente cubierto.

De ahí que, independientemente de la naturaleza de la causa (períodos vacacionales, enfermedad, baja laboral, etc.), en caso de que el equipo de trabajo propuesto no pueda desempeñar el servicio objeto de este pliego, la empresa adjudicataria está obligada a sustituir a dicho equipo por uno de idéntica preparación, así como a comunicar dicha sustitución con al menos 15 días de antelación. Se establece un objetivo máximo de 21 días para la incorporación del nuevo recurso, contados desde el día inmediatamente posterior al último día de desempeño del recurso sustituido.

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:

11.1.2. Responsable del contrato y Responsable de servicio

La ADA 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 del mismo.

Se designará un responsable del contrato, entre cuyas actividades se encuentran:

- Coordinación y dirección del contrato.
- 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 ANS, cálculo y propuesta de penalizaciones en su caso.
- Propuesta y aceptación de cambios en el equipo de trabajo del adjudicatario durante la duración del contrato caso de no ajustarse a las necesidades del servicio prestado definido en el pliego de prescripciones técnicas.

Adicionalmente, se puede hacer uso de la figura de "**Responsable de servicio**" para el seguimiento de actividades propias de la gestión del contrato y de los ANS de los servicios. Esta figura será desempeñada por personal de la Sociedad Andaluza para el Desarrollo de las Telecomunicaciones (SANDETEL) en virtud del encargo de gestión vigente en materia de ciberseguridad.

11.1.3. Jefatura de proyecto

La persona será designada por el adjudicatario. Entre sus funciones principales se encontrarán las siguientes:

- Interlocución con el responsable del contrato.
- Seguimiento, control y gestión de los trabajos y del cumplimiento del contrato.
- Dirección y gestión del equipo de proyecto.
- Responsable del cumplimiento de la planificación.
- Proposición de las modificaciones que considere necesarias para la correcta ejecución de los servicios.
- Entrega de la información requerida para el control del contrato.
- Supervisión y reporte del cumplimiento de objetivos, criterios y niveles de calidad, asegurando los niveles de calidad del servicio.

11.1.4. Equipo de trabajo

El equipo de trabajo 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.

Todo el personal asignado al proyecto deberá firmar un acuerdo de confidencialidad, ofrecer garantías suficientes de sus acreditaciones de seguridad y mantenerlas a lo largo de la vigencia del contrato.

11.1.5. Constitución inicial del equipo de trabajo

El equipo de trabajo localizado que se incorporará tras la formalización del contrato para la ejecución de los trabajos deberá estar formado por los componentes relacionados en la oferta adjudicataria y consecuentemente valorados por la ADA.

Puesto que el trabajo a desarrollar requiere de un periodo de adaptación y de adquisición de conocimiento en las materias que son objeto de la presente contratación, la empresa adjudicataria velará por contar con un equipo de trabajo estable durante el plazo que dure la prestación.

11.1.6. Modificaciones del equipo de trabajo

La valoración final de la calidad de los servicios prestados por las personas adscritas a la ejecución del contrato corresponde al responsable del contrato designado por la ADA, siendo potestad suya solicitar el cambio de cualquiera de los componentes del equipo de trabajo, con un preaviso de quince días, por otro de igual perfil técnico-profesional, si existen razones justificadas que lo aconsejen.

Si es el adjudicatario el que propone el cambio de una de las personas del equipo de trabajo, deberá solicitarlo por escrito con quince días naturales de antelación, y se autorizará por la ADA en las mismas condiciones que se requieren para la autorización de cambios puntuales en la composición del equipo de trabajo.

La autorización de cambios puntuales en la composición del mismo requerirá de las siguientes condiciones:

- Solicitud de cambio al Responsable del Contrato. Incluirá una justificación escrita, detallada y suficiente, explicando el motivo que suscita el cambio. Se considera dentro de esta categoría las sustituciones de personal que tienen como origen una baja en la empresa adjudicataria.
- Presentación de, al menos, DOS personas candidatas con un perfil de cualificación técnica acorde con lo requerido en este pliego y con las mejoras de perfil ofertadas, en un plazo no superior a 21 días naturales, contados desde la fecha de solicitud antes referida.

- Aceptación expresa de alguna de las personas candidatas por parte del responsable del contrato.
- Incorporación de la persona candidata en un plazo no superior a 15 días naturales.

El Tiempo máximo de incorporación del reemplazo en las sustituciones de personal no superará los 36 días (21 + 15) naturales, contados desde la solicitud de cambio formulada al Responsable del Contrato.

Los posibles inconvenientes de adaptación al entorno de trabajo y al proyecto debidos a las sustituciones en los componentes del equipo de trabajo, deberán subsanarse mediante periodos de solapamiento sin coste adicional, durante el tiempo necesario.

Cuando se trate de modificaciones en el equipo adscrito a la ejecución del servicio, imputables al contratista, se establece un número máximo de sustituciones de DOS recurso durante la ejecución del contrato por tipo de perfil (TN1, TN2 o Jefe de Proyecto). A los efectos de su cómputo, no se tendrán en cuenta las modificaciones en el equipo que sean consecuencia de incapacidad temporal o permanente del recurso sustituido, o bien por cambio de provincia en la prestación del servicio a petición del responsable del contrato.

Asimismo, durante todo el plazo de ejecución del contrato, el adjudicatario deberá mantener los niveles de calidad del servicio objeto del mismo, por lo que deberá instrumentar los servicios de suplencia que estime oportunos, que serán cubiertos siempre con el mismo personal suplente, a los efectos de ocasionar el mínimo impacto en la prestación del servicio.

De igual modo, ante necesidad del servicio será posible la incorporación de nuevo personal para la ampliación del equipo de trabajo, según las siguientes pautas :

- Solicitud de incorporación de nuevo personal del Responsable del Contrato, que será notificada al contratista vía SIO.
- Presentación de, al menos, DOS personas candidatas con un perfil de cualificación técnica acorde con lo requerido en este pliego y con las mejoras de perfil ofertadas, en un plazo no superior a 21 días naturales, contados desde la fecha de solicitud antes referida.
- Aceptación expresa de alguna de las personas candidatas por parte del responsable del contrato.
- Incorporación de la persona candidata en un plazo no superior a 15 días naturales.

El Tiempo máximo de incorporación de nuevo de personal no superará los 36 días (21 + 15) naturales, contados desde la solicitud de cambio formulada al Responsable del Contrato.

La falsedad en el nivel de conocimientos técnicos del personal ofertado, así como la sustitución de alguno de los componentes del equipo adscrito a la ejecución de los trabajos, sin observar el procedimiento y requisitos exigidos en los apartados anteriores, facultará a la ADA para instar la resolución del contrato.

11.1.7. Formación continua del equipo de trabajo

Es esencial que el personal esté adecuadamente formado y actualizado en las nuevas tecnologías de la información y la comunicación, en especial en la solución EDR implementada, en las nuevas amenazas y técnicas de ataque, así como en las posibilidades de detección y repuesta frente a amenazas.

El adjudicatario deberá proveer a los recursos técnicos que presten el Soporte para el correcto funcionamiento de la plataforma de un plan de formación adecuado para renovar sus conocimientos incluyendo las nuevas tecnologías que vayan apareciendo en el sector de la ciberseguridad relacionadas con el servicio que se presta, especialmente en el uso de la solución EDR implementada.

Dicho plan deberá ser definido en la oferta, y contemplará un informe semestral al responsable del contrato sobre las actividades de formación realizadas en el periodo y las planificadas para el siguiente periodo.

Los periodos de formación deberán ser planificados y consensuados entre la ADA y el adjudicatario, de tal manera que no deben afectar a la calidad del servicio prestado, ni impactar sobre los horarios de trabajo de los técnicos.

11.2. Seguimiento y control de la ejecución del contrato

El seguimiento y control de la ejecución del contrato se efectuará sobre las siguientes bases:

- Seguimiento continuo de la evolución del servicio entre la Jefatura de proyecto, único interlocutor ante la ADA, el responsable del contrato que la ADA designe y/o el responsable del servicio.
- El seguimiento se articulará en Comités de seguimiento con participación de los roles citados y todo aquel personal necesario para su correcto funcionamiento.
- En los Comités de seguimiento se entregará y analizará un informe consolidado de las actividades desarrolladas en el último periodo.
- La ADA determinará los procedimientos y herramientas a utilizar para poder llevar a cabo el seguimiento y control del servicio.

- Los Comités de Seguimiento tendrán una periodicidad de entre un mes y tres meses. Independientemente de estos comités, 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, es obvio, que 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.

11.3. Material necesario para el equipo de trabajo en la prestación del servicio

Para la realización de las tareas que se presten en modo localizado y deslocalizado, el adjudicatario dotará al equipo de trabajo el equipamiento microinformático de hardware y licencias necesario para el adecuado desarrollo de las mismas.

El adjudicatario dotará de las conexiones necesarias para el acceso remoto seguro a las redes informáticas de la ADA, siendo por cuenta de la empresa adjudicataria los costes derivados de dicha conexión y el aseguramiento del acceso. El acceso está motivado por el uso de las herramientas de AndalucíaCERT (por ejemplo, LUCIA), así como para la resolución de incidencias del agente en el equipo final.

Al finalizar los servicios se comprometerá el adjudicatario a realizar una cancelación de toda la información y datos sensibles que hayan podido quedar en los equipos informáticos con motivo de la gestión, poniendo posteriormente dichos equipos a disposición de la ADA para realizar un chequeo de dicha cancelación.

La ADA 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 ADA exigir responsabilidad al adjudicatario en caso de cualquier uso no debido de las mismas.

La ADA 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 ADA exigir responsabilidad al adjudicatario en caso de cualquier uso no debido de las mismas.

12. Condiciones generales

12.1. Lugar de la prestación de los trabajos

Como se ha expuesto en el apartado Soporte asociado, los trabajos, según se traten, podrán realizarse de forma **localizada** en AndalucíaCERT, cuya sede actualmente está localizada en Tomares (Sevilla) y/o en el futuro también en Málaga capital, o **deslocalizada**, en la sede/s del SOC/CSIRT preexistente/s del contratista.

También, de forma excepcional, en cualquier **sede** los organismos que forman parte del Alcance del contrato, ante situaciones que requieran un apoyo extraordinario y presencial para la contención y erradicación de un ciberincidente especialmente grave y complejo.

El horario de servicio, según se trate, será 12x5 o 7x24, en los términos expuestos en el apartado Soporte asociado.

12.2. Requisitos de seguridad

Las proposiciones deberán garantizar el cumplimiento de los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información que constituyen 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, en función de los tipos de activos presentes en el sistema de información y las dimensiones de información relevantes, considerando las categorías de seguridad en las que recaen los sistemas de información objeto de la contratación según los criterios establecidos en el anexo I del ENS.

El responsable del contrato 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.

Deberá también tenerse en cuenta lo dispuesto en 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 (modificado por el Decreto 70/2017, de 6 de junio) y en su desarrollo a partir de la Orden de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía y normativa asociada. Se atenderá también a la normativa interna materia de Seguridad TIC.

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, así como a las guías y procedimientos aplicables elaborados por la Unidad de Seguridad TIC Corporativa de la Junta de Andalucía y por el SOC autonómico AndalucíaCERT.

12.3. Propiedad intelectual

Toda la documentación del proyecto junto con las implementaciones realizadas deberá entregarse en formato digital.

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 Agencia Digital de Andalucía, quien podrá reproducirlos, 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 Agencia Digital de Andalucía. Específicamente todos los derechos de explotación y titularidad de las aplicaciones informáticas y programas de ordenador desarrollados al amparo de esta contratación corresponden únicamente a la Agencia Digital de Andalucía.

12.4. Formato de los entregables

Los documentos serán entregados en soporte informático conforme a las directrices que en su momento determine la ADA y, en cualquier caso, de acuerdo al Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

De manera general, toda la documentación del proyecto tendrá que ser entregada en castellano, en los siguientes formatos electrónicos:

- Formato editable ISO/IEC 26300 (formato OpenDocument de OASIS).
- Formato no editable para su preservación a largo plazo ISO 19005-1:2005 (PDF/A-1).

También podrá requerirse, exclusivamente en los casos en que se considere conveniente, su entrega en papel (en carpeta o encuadernada).

13. Confidencialidad y Protección de Datos de Carácter Personal

El adjudicatario deberá garantizar la confidencialidad e integridad de los datos manejados y de la documentación facilitada.

En este sentido, deberá sujetarse a los preceptos legales en materia de protección de datos personales recogidos en la "Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales" y en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril "Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)".

Si alguna de las personas integrantes de la empresa adjudicataria destina los datos a otra finalidad, los comunica o los utiliza incumpliendo las instrucciones de la Agencia, la empresa contratada será responsable de las infracciones cometidas.

Además, deberán cumplir con las medidas de seguridad, normas y procedimientos que en cada caso establezca esta Agencia, dentro de este procedimiento se incluye la firma de un documento de confidencialidad y protección de datos entre la empresa y la Agencia y que alcance a todos los trabajadores.

Los licitadores deberán cumplir con los principios de protección de datos descritos en las disposiciones de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, así como otras disposiciones reglamentarias.

Así mismo durante la ejecución de los trabajos y en cualquier momento derivado de ello se estará a lo dispuesto en el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016.

14. ANEXO I: Sistemas Operativos a soportar

- Sistemas basados en WINDOWS
  - Servidores 64-bit
    - Windows Server 2019
    - Windows Server Core 2019
    - Windows Server 2016:
      - 1803 (equivalente a Windows 10 Redstone 4)
      - 1709 (equivalente a Windows 10 Redstone 3)
      - 1607 LTSC (equivalente a Windows 10 Redstone 1)
      - Windows Server Core 2016
    - Windows Server 2012 R2
    - Windows Storage Server 2012 R2
    - Windows Server 2012
    - Windows Server 2008 R2 SP1
  - Workstations 64-bit
    - Windows 10 October 2020 Update
    - Windows 10 May 2020 Update
    - Windows 10 November 2019 Update (v1909, 19H2)
    - Windows 10 October 2018 Update (v1809, Redstone 5)
    - Windows 10 April 2018 Update (v1803, Redstone 4)
    - Windows 10 Anniversary Update (v1607, Redstone 1)
    - Windows 10 v1507
    - Windows 10 IOT Enterprise 20H2
    - Windows 10 IOT Enterprise v2004 (20H1)
    - Windows 10 IOT Enterprise v1909 (19H2)
    - Windows 10 IOT Enterprise v1809 (Redstone 5)

        - Windows 8.1
        - Windows 7 SP1
        - Windows 7 Embedded POSReady
    - Workstation 32-bits
        - Windows 10 October 2020 Update (v20H2, build 19042)
        - Windows 10 May 2020 Update (v2004, 20H1)
        - Windows 10 November 2019 Update (v1909, 19H2)
        - Windows 10 October 2018 Update (v1809, Redstone 5)
        - Windows 7 SP1
        - Windows 7 Embedded POSReady
- Sistemas basados en LINUX
    - Servidores x86_64
        - Amazon Linux 2
        - Amazon Linux AMI
            - 2018.03
            - 2017.09
        - CentOS
            - 8.3: sensor version 6.14.11110 and later
            - 8.2: sensor version 5.34.9917 and later
            - 8.1: sensor version 5.27.9101 and later
            - 8.0
            - 7.9
            - 7.8
            - 7.4 - 7.7
            - 6.7 - 6.10
        - Debian

    - 10
    - 9.1-9.4
- Oracle Linux
    - Oracle Linux 8 - UEK 6
    - Oracle Linux 7 - UEK 6
    - Oracle Linux 7 - UEK 3, 4, 5
    - Oracle Linux 6 - UEK 3, 4
    - Red Hat Compatible Kernels (supported RHCK kernels are the same as for RHEL)
- Red Hat Enterprise Linux (RHEL)
    - 8.3
    - 8.2
    - 8.1
    - 8.0
    - 7.9
    - 7.8
    - 7.4 - 7.7
    - 6.7 - 6.10
- SUSE Linux Enterprise (SLES)
    - 15 - 15.2. SLES 15 SP2
    - 12.2 - 12.5. SLES 12 SP5
    - 11.4
- Ubuntu
    - 20.04 LTS
    - 18-AWS
    - 18.04 LTS

- 16-AWS
- 16.04 LTS and 16.04.5 LTS

- Sistemas basados en Apple/MAC
  - macOS Big Sur 11.0 y posteriores
  - macOS Big Sur 11.1 y posteriores
  - macOS Catalina 10.15 y posteriores
  - macOS Mojave 10.14 y posteriores
- DISPOSITIVOS MÓVILES
  - Todas las versiones de sistema operativo Android.
  - Todas las versiones de Sistema operativo iOS

15. ANEXO II: Descripción del Sistema Integrado de Operaciones (SIO)

En este apartado se describen las características funcionales básicas del Sistema Integrado de Operaciones.

SIO es la herramienta utilizada para gestionar los procedimientos referentes a la operativa de provisión, incidencias y facturación.

Este sistema se encuentra sometido a un proceso de mejora continua soportada en las norma ISO 20000 y las mejores prácticas ITIL; entre otras aplicaciones, se integra en la gestión del cambio de la base de datos de los servicios (CMDB), esto hace imprescindible su uso correcto y generalizado tanto por el adjudicatario como por el Responsable del Contrato y el Responsable de Servicio según las responsabilidades que a cada uno se le asigna en el presente PPT, en el desarrollo de los procedimientos también incluidos en el presente PPT y de las mejoras que en el curso del proyecto se determinen por el Responsable del Contrato, dentro de la mejora continua.

Para facilitar la integración de los sistemas propios de los adjudicatarios y SIO se utilizará un web service para el intercambio de información; la información requerida será determinada por el Responsable de Servicio tanto en la frecuencia de actualizaciones como en la calidad de éstas. Los campos vienen determinados por el formato de ticket empleado según el proceso operativo de que se trate.

15.1. Descripción General

El Sistema Integrado de Operaciones se encuentra dividido en los siguientes módulos:

- Gestión de catálogo, organigrama e inventario de servicios. Este módulo centraliza las funcionalidades y entidades básicas en los que se apoyan el resto de módulos.
- Gestión de incidencias y provisiones. Este módulo soporta los procesos de Incidencias y Provisión de Servicio.
- Verificación y control de facturación. Implementa el proceso de Facturación de servicios.
- Informes. Módulo usado para la generación de informes sobre los Servicios (seguimiento de servicios, medición de ANS, cálculo de penalizaciones, etc.).

15.2. Organización funcional

A continuación se describen los diferentes módulos funcionales que conforman SIO.

15.2.1. Módulo de Gestión de Catálogo, Organigrama e Inventario

Este módulo es el que permite gestionar de forma directa las entidades de información relativas a:

- Catálogo de elementos unitarios. Entre otras cosas, la información que se gestiona en este módulo es utilizada por el módulo de provisiones para presentar los posibles elementos que se pueden solicitar. El adjudicatario proveerá la información necesaria para configurar este Catálogo, en los formatos indicados por la persona Responsable de Servicio (codificación y tabulación según catálogo de JdA). Incluirá al menos la siguiente información:
    - Descripción de cada elemento de catálogo disponible.
    - Costes asociados a cada elemento, en general toda la información necesaria para permitir una verificación automática de la factura que emiten los adjudicatarios.
    - Dependencias e incompatibilidades entre los elementos de Catálogo.
    - ANS que aplica a cada tipo de operación posible sobre cada elemento de Catálogo. Se contemplarán todas las especificadas en el apartado de ANS.
    - Para cada una de las operaciones anteriores, se tendrá que especificar además la siguiente información:
        - Si requiere o no corte del servicio para su ejecución.
        - Atributos: información requerida al solicitante de la operación para su ejecución, e información que proporcionará el adjudicatario para el posterior mantenimiento del mismo. El Responsable de Servicio podrá extender esta lista de atributos según las necesidades que existan. El adjudicatario deberá introducir esta información durante la provisión, siendo necesario este proceso para la aceptación del servicio.
        - Penalización en caso de incumplimiento del ANS asociado a la operación.

- Organigrama de entidades organizativas de la Junta de Andalucía (Organismos, unidades organizativas, sedes, contactos, responsabilidades, centros de facturación y coste, etc.). Será el repositorio de referencia para el adjudicatario y para el el Responsable de Servicio en cuanto a la identificación de entidades (ej.: codificación, etc.). En Incidencias y Provisión de Servicios se hará referencia a este repositorio para ubicar la localización de los servicios asociados con la petición.
- Inventario de licencias desplegadas existentes y ligadas a las sedes de diferentes Organismos de la Junta de Andalucía. El Inventario será el repositorio de referencia para la validación de la facturación emitida por el adjudicatario.

15.2.2. Módulo de Gestión de Incidencias y Provisiones

Es el módulo en el que se registran y tramitan las incidencias y las peticiones de provisión de nuevos elementos del Catálogo de elementos unitarios y precios, o modificaciones sobre elementos ya en explotación.

SIO ofrecerá una interfaz de usuario específica al adjudicatario, en la que podrá consultar todos los datos necesarios para tramitar la petición (dirección de la sede, persona de contacto, categorización de incidencia, etc.).

SIO proporcionará información adicional sobre el ANS que aplica a cada petición, así como de la fecha objetivo para cumplir con dicho ANS. Asimismo, el adjudicatario tendrá que actualizar periódicamente, con la periodicidad y contenido mínimos que defina el Comité correspondiente, la información necesaria en estas peticiones para poder hacer seguimiento de las mismas, e informar debidamente.

En concreto, el adjudicatario tendrá que prestar especial atención en la información en el sistema de la Fecha del hito Listo Para Servicio (en adelante LPS).

En el caso de las provisiones de nuevos elementos el adjudicatario recibirá la petición en forma de tabla el detalle de los elementos solicitados, con referencia a la codificación proporcionada por cada adjudicatario para la configuración del Catálogo. El adjudicatario tendrá que usar esta información para configurar la facturación de los elementos provistos. Igualmente, esta información será utilizada para alimentar la base de datos de elementos en explotación.

En general, no se aceptará el hito Listo Para Facturación de elementos (en adelante LPF) a un pedido hasta que éste no esté en servicio, excepto incumplimiento grave por parte del Organismo solicitante por sus tareas de migración, y siempre validado por el Responsable de Servicio.

15.2.3. Módulo de Verificación y Control de Facturación

Este módulo permite las siguientes modalidades de facturación:

- Facturación realizada por el adjudicatario a según propuesta confeccionada por el Responsable de Servicio.
- Facturación por parte del adjudicatario tras remisión y comprobación por parte del el Responsable de Servicio de la propuesta de factura.
- Facturación confeccionada por el Gestor.

El módulo de verificación y control de facturación se utilizará para contrastar la facturación emitida por el adjudicatario, con el Inventario de elementos activos, como parte del proceso de facturación.

El adjudicatario especificará, con el detalle necesario para la configuración en el Módulo de Facturación, las reglas de facturación que apliquen a cada elemento, al realizarse cualquier operación que afecte a la facturación. Sólo se aplicarán reglas de facturación permitidas por SIO.

15.2.4. Módulo de Informes

El módulo de informes engloba la funcionalidad destinada al análisis y presentación de información originada y mantenida por el resto de módulos de SIO.

- Datos relativos al catálogo, organigrama e inventario.
- Datos relativos a las incidencias y provisiones (informes de ANS, penalizaciones, actividad servicios, etc.)
- Datos relativos a la facturación.
- Datos relativos al consumo de elementos unitarios, tales como licencias suministradas, horas de soporte consumidas, número de acciones de capacitación, etc.

El módulo de Informes será la herramienta mediante la cual se extraerán los datos oficiales de incumplimientos de ANS por parte del adjudicatario, y los cálculos de penalizaciones que apliquen a raíz de dichos incumplimientos. El adjudicatario podrán verificar el diseño y funcionamiento de estos informes.

La Agencia Digital de Andalucía decida que la solución a adoptar para la medición de algún ANS sea a través de otros sistemas de Supervisión y Monitorización bien de la Agencia Digital de Andalucía o bien del adjudicatario, este deberá facilitar dicha información de manera que sea integrable y gestionable en SIO.

16. ANEXO III: Entes en el ámbito

Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa

Consejería de Economía, Hacienda y Fondos Europeos

Consejería de Desarrollo Educativo y Formación Profesional

Consejería de Empleo, Empresa y Trabajo Autónomo

Consejería de Salud y Consumo

Consejería de Agricultura, Pesca, Agua y Desarrollo Rural

Consejería de Universidad, Investigación e Innovación

Consejería de Turismo, Cultura y Deporte

Consejería de Fomento, Articulación del Territorio y Vivienda

Consejería de Inclusión Social, Juventud, Familias e Igualdad

Consejería de Sostenibilidad, Medio Ambiente y Economía Azul

Consejería de Política Industrial y Energía

Consejería de Justicia, Administración Local y Función Pública

Agencia Andaluza de Cooperación Internacional para el Desarrollo

Agencia Andaluza de Instituciones Culturales

Agencia Andaluza de la Energía

Agencia Andaluza del Conocimiento

Agencia de Gestión Agraria y Pesquera de Andalucía

Agencia de Innovación y Desarrollo de Andalucía

Agencia de Medio Ambiente y Agua de Andalucía

Agencia de Obra Pública de la Junta de Andalucía

Agencia de Servicios Sociales y Dependencia de Andalucía

Agencia de Vivienda y Rehabilitación de Andalucía

Agencia Digital de Andalucía

Agencia Pública Andaluza de Educación

Agencia Pública de Puertos de Andalucía

Agencia Pública Empresarial de la Radio y Televisión de Andalucía

Agencia Pública Empresarial Sanitaria Bajo Guadalquivir

Agencia Pública Empresarial Sanitaria Costa del Sol

Agencia Pública Empresarial Sanitaria Hospital Alto Guadalquivir

Agencia Pública Empresarial Sanitaria Hospital de Poniente de Almería

Agencia Tributaria de Andalucía

Andalucía Emprende, Fundación Pública Andaluza

Apartahotel Trevenque, S.A.

Canal Sur Radio y Televisión, Sociedad Anónima

Centro Andaluz de Arte Contemporáneo

Cetursa Sierra Nevada, S.A.

Consorcio Centro Andaluz Formación Medioambiental Desarrollo Sostenible

Consorcio Centro de Formación en Comunicaciones y Tecnologías de la Información de Málaga

Consorcio de Transporte Metropolitano de la Costa de Huelva

Consorcio de Transporte Metropolitano del Área de Almería

Consorcio de Transporte Metropolitano del Área de Córdoba

Consorcio de Transporte Metropolitano del Área de Granada

Consorcio de Transporte Metropolitano del Área de Jaén

Consorcio de Transporte Metropolitano del Área de Málaga

Consorcio de Transporte Metropolitano del Área de Sevilla

Consorcio de Transporte Metropolitano del Campo de Gibraltar

Consorcio Metropolitano de Transportes de la Bahía de Cádiz

Consorcio Palacio de Congresos y Exposiciones de Granada

Consorcio Parque de las Ciencias de Granada

Consorcio Sanitario Público del Aljarafe

Empresa Andaluza Gestión Instalaciones y Turismo Juvenil S.A.

Empresa Pública de Emergencias Sanitarias

Empresa Pública de Gestión de Activos S.A.

Empresa Pública para la Gestión del Turismo y del Deporte de Andalucía, S. A.

Escuela Andaluza de Salud Pública, S.A.

Extenda-Empresa Pública Andaluza de Promoción Exterior, S.A.

Fundación Andalucía Olímpica, Fundación Pública Andaluza

Fundación para el Desarrollo Sostenible de Doñana y su Entorno-Doñana 21 Fundación Pública Andaluza

Fundación Pública Andaluza Agregación de Fundaciones de Sevilla

Fundación Pública Andaluza Banco Agrícola de don José Torrico y Lopéz Calero

Fundación Pública Andaluza Barenboim-Said

Fundación Pública Andaluza Centro de Estudios Andaluces

Fundación Pública Andaluza Centro de las Nuevas Tecnologías del Agua

Fundación Pública Andaluza El Legado Andalusí Medio Propio Personificado

Fundación Pública Andaluza Hospital San Rafael

Fundación Pública Andaluza Instituto de Estudios sobre la Hacienda Pública de Andalucía, Medio Propio

Fundación Pública Andaluza Juan Nepomuceno Rojas

Fundación Pública Andaluza para la Gestión de la Investigación en Salud de Sevilla

Fundación Pública Andaluza para la Integración Social de Personas con Enfermedad Mental

Fundación Pública Andaluza para la Investigación Biosanitaria de Andalucía Oriental-Alejandro Otero

Fundación Pública Andaluza para la Investigación Malagueña en Biomedicina y Salud

Fundación Pública Andaluza Parque Tecnológico de Ciencias de la Salud de Granada

Fundación Pública Andaluza Progreso y Salud

Fundación Pública Andaluza Rey Fahd Bin Abdulaziz

Fundación Pública Andaluza Rodríguez-Acosta

Fundación Pública Andaluza San Juan de Dios de Lucena y Fundaciones Fusionadas de Córdoba

Fundación Real Escuela Andaluza del Arte Ecuestre Fundación Pública Andaluza

Innova Venture S.G.E.I.C., S.A.U.

[Institución] Agencia de Defensa de la Competencia de Andalucía

[Institución] Consejo Audiovisual de Andalucía

[Institución] Consejo de Transparencia y Protección de Datos de Andalucía

Instituto Andaluz de Administración Pública

Instituto Andaluz de Investigación y Formación Agraria, Pesquera, Alimentaria y de la Producción Ecológica

Instituto Andaluz de la Juventud

Instituto Andaluz de la Mujer

Instituto Andaluz de Patrimonio Histórico

Instituto Andaluz de Prevención de Riesgos Laborales

Instituto de Estadística y Cartografía de Andalucía

Inversión y Gestión de Capital Semilla de Andalucía S.I.C.C. S.A.

Parque Científico y Tecnológico Cartuja, S. A

Parque de Innovación Empresarial Sanlúcar la Mayor, S.A.

Parque Tecnológico de Andalucía S.A.

Parque Tecnológico y Aeronáutico de Andalucía, S.L.

Patronato de la Alhambra y Generalife

Red de Villas Turísticas de Andalucía S.A.

Red Logística de Andalucía, S.A.

Servicio Andaluz de Empleo

Servicio Andaluz de Salud

Sociedad Andaluza para el Desarrollo de las Telecomunicaciones, S.A.

Sociedad para la Promoción y Reconversión Económica de Andalucía, S.A.

Venture Invercaria, S.A.

Verificaciones Industriales de Andalucía, S.A.