



Eusko Jaurlaritzaren
Informatika Elkarte

Sociedad Informática
del Gobierno Vasco

Expediente N°: EJIE-065-2020

Servicios de Centro de Operaciones de Seguridad (SOC) para la monitorización y respuesta ante incidentes en BATERA.

Especificaciones de compra / Pliego de condiciones técnicas

Julio de 2020

Este documento es propiedad de Eusko Jauriaritzaren Informatika Elkartea – Sociedad Informática del Gobierno Vasco, S.A. (EJIE). Este documento no puede ser reproducido, en su totalidad o parcialmente, ni mostrado a otros, ni utilizado para otros propósitos que los que han originado su entrega, sin el previo permiso escrito de EJIE. En el caso de ser entregado en virtud de un contrato, su utilización estará limitada a lo expresamente autorizado en dicho contrato. EJIE no podrá ser considerada responsable de eventuales errores u omisiones en la edición del documento.

Versión	Fecha	Resumen de cambios	Elaborado por:	Aprobado por:
1.0	22/07/2020	Versión Inicial	Josu Bagazgoitia	Iñaki Astorkia

Índice

1	Introducción	5
1.1	Perfil de la compañía	5
1.2	Antecedentes	6
2	Objeto y alcance del contrato	7
2.1	Objeto y alcance	7
2.2	Descripción situación actual	8
3	Requisitos vinculados a la solución SIEM	11
	Arquitectura	11
	Seguridad	11
	Volumen de Datos	12
	Correlación	12
	Integración con terceros	13
	Personalización y Facilidad de Uso de la consola de gestión	13
	IoCs, Feeds, MITRE	13
	Integración de Fuentes	14
	Análisis de Vulnerabilidades	14
	Análisis de Comportamiento de Usuarios (UBA)	15
	Automatización de Análisis de Incidentes	15
	Orquestación y Respuesta automática a Incidentes de Seguridad (SOAR)	15
4	Requisitos vinculados a la solución EDR	16
	Arquitectura	16
	Capacidades de detección y respuesta:	16
	Integración con terceros	17
	Características de la Consola:	17
	Características del agente o sensor a instalar en los puestos:	18
	Recolección de Datos	18
5	Alcance y requisitos de los servicios a prestar por el SOC	20
5.1	Introducción al alcance del SOC	20
5.2	Servicios de monitorización, detección y respuesta a incidentes	20
5.3	Servicios que se activan bajo demanda	25
5.4	Condiciones para la prestación del servicio	26
5.5	Generación de Informes de servicio	27
5.6	Organización y configuración del SOC	28
5.7	Mantenimiento y soporte	28
5.8	Integración con los Modelos de operación de EJIE	29
5.9	Niveles de servicio	29
6	Proyecto para la implantación del servicio	31
6.1	Consultoría para el análisis y diseño del servicio	31
6.2	Configuración y puesta en marcha de la solución SIEM	32
6.3	Configuración y puesta en marcha de la solución EDR	32
6.4	Ajuste y acondicionamiento del servicio	33
6.5	Documentación del servicio	33
6.6	Transferencia de conocimiento con el inicio del servicio	34
6.7	Responsabilidades EJIE	34
6.8	Dimensionamiento y alcance inicial del servicio	34

7	Modelo de servicio	36
7.1	Periodo de prestación del servicio.....	36
7.2	Modelo suscripcional de las soluciones SIEM y EDR.....	36
7.3	Modelado del servicio prestado por el SOC.....	37
7.4	Arranque y evolución del servicio	38
7.5	Otras consideraciones	39
7.6	Devolución del servicio.....	39
7.7	Plan de facturación	40
8	Seguimiento del servicio	44
8.1	Responsable del Servicio por parte de EJIE	44
8.2	Responsable del Servicio por parte del adjudicatario.....	44
8.3	Seguimiento y Mejora continua del servicio.....	45

1 Introducción

1.1 Perfil de la compañía

EJIE, Eusko Jauriaritzaren Informatika Elkartea – Sociedad Informática del Gobierno Vasco, es la Empresa pública de servicios de las tecnologías de la información y las comunicaciones (TIC), cuya razón de existir es contribuir a la consecución de un Sector Público Vasco, moderno y eficiente, en el Marco Legal establecido por el Gobierno, con la seguridad y calidad necesarias y con el debido respeto al medio ambiente.

EJIE tiene como meta final la consecución de la satisfacción de sus clientes, siendo el instrumento común de prestación de servicios TIC en el Sector Público Vasco, y comprometiéndose en:

- Construir y mantener con eficiencia y calidad la infraestructura de los Sistemas de Información, posibilitando su continuidad y seguridad.
- Garantizar la interoperabilidad entre las distintas administraciones.
- Servir de apoyo a las necesidades de planificación y realización de la función informática de los Departamentos y Organismos Autónomos del Gobierno, asegurando la cobertura de sus demandas con el compromiso y profesionalidad adecuados a las relaciones contractuales que se establezcan.

Por tanto, EJIE debe ser, un instrumento común de referencia para la prestación de servicios TIC en el Sector Público Vasco:

- Aportando valor añadido.
- Proporcionando soluciones competitivas.
- Transmitiendo confianza a sus clientes.
- Contando con personas cualificadas y comprometidas.

Se puede obtener información más detallada y extensa en nuestra dirección de Internet <http://www.ejie.eus>.

Con fecha 16 de agosto de 2016 se firmó el Acuerdo entre el Ente Público de Derecho Privado Osakidetza y Eusko Jauriaritzaren Informatika Elkartea—Sociedad Informática del Gobierno Vasco, S.A. (EJIE) para la integración del servicio de infraestructuras y operaciones (I.O.) de OSAKIDETZA con el análogo servicio (I.O.) en EJIE, en el marco del acuerdo adoptado por el Consejo de Gobierno sobre el proceso de convergencia en materia de tecnología de la información y comunicación –TIC/ICPS el 27 de julio de 2015 y del Acuerdo de 21 de junio de 2016 relativo a dicho proceso de convergencia por el que se aprueba el documento ejecutivo “plan general de actuación en materia de convergencia TIC/ICPS”.

La actividad objeto de contratación, es necesaria para la prestación de los servicios, competencia de EJIE S.A., y está incluida en los servicios que pueden ser objeto de contratación (según Instrucción Sexta de la Instrucciones sobre buenas prácticas en la contratación de servicios de Gobierno Vasco). Su prestación no puede ser asumida con los recursos humanos y técnicos de que dispone EJIE S.A., siendo además inviable su reorganización.

El presente pliego, como el resto de los documentos de la fase de preparación del contrato, incorporan las debidas garantías para dar cumplimiento a la Instrucción octava de las Instrucciones sobre buenas prácticas en la contratación de servicios de Gobierno Vasco.

1.2 Antecedentes

El contexto actual en materia de Ciberseguridad resulta cada vez más complejo. En un entorno en el que la movilidad y, en consecuencia, los servicios en cloud y el nivel de exposición de los servicios internos es creciente, el nivel de riesgo aumenta proporcionalmente. Por su parte, las redes criminales son cada vez más especializadas y tienden a dirigir y elaborar cada vez más sus ataques.

En consecuencia, EJIE, dentro del proyecto BATERA, se encuentra en una fase de Evolución de los Servicios de Seguridad que ofrece, de cara a mejorar las capacidades ya disponibles y a la incorporación de nuevas capacidades y funcionalidades que permitan hacer frente a la situación actual.

Como punto de partida de esta fase de evolución, se está realizando un Plan de Evolución de Servicios de Seguridad que pretende marcar el camino de BATERA en materia de Ciberseguridad para los próximos 4 años. Para llevar a cabo dicho Plan se utilizarán referencias internacionales en el modelado de la seguridad, como puede ser el “NIST Cyber Security Framework” o la matriz “MITRE ATT&CK”.

Dentro del Plan se han identificado una serie de necesidades a acometer en el corto plazo. En concreto, las necesidades que se han identificado como prioritarias son la contratación de un Centro de Operaciones de Seguridad (SOC) que gestionará los servicios avanzados de: Tecnología SIEM (*Security Information and Event Management*) y de la Plataforma EDR (*Endpoint Detection and Response*).

La diversidad y especialización de las amenazas de seguridad actuales, junto con la complejidad y la envergadura de un entorno IT como BATERA, hacen prácticamente imprescindible disponer de herramientas que permitan centralizar los logs de los diferentes elementos de seguridad y automatizar el análisis de los mismos de cara a la detección de incidentes de seguridad y a la investigación de los mismos, función que realizan las herramientas SIEM. Estas herramientas proporcionan visibilidad en tiempo real para la detección y priorización de amenazas, ofreciendo vigilancia en toda la infraestructura IT y habilitando una gestión de amenazas eficaz, reduciendo y priorizando el número de alertas. La herramienta SIEM será la base, por tanto, del servicio de monitorización de eventos de seguridad.

Por otro lado, la plataforma EDR permitirá hacer una monitorización continua de las actividades de los endpoint (dispositivos finales de usuario), identificando patrones de comportamientos anómalos que puedan constituir una amenaza e, incluso, permitiendo responder ante ellas para detenerla.

Con el fin de que EJIE pueda ofrecer a todas las entidades adheridas a BATERA y resto de organismos del sector público que así lo deseen unos niveles de protección adecuados de su información, así como de los sistemas y comunicaciones que lo conforman, se hace necesaria la contratación de servicios especializados de seguridad, que contemplen la provisión y puesta en marcha de tecnologías SIEM y EDR, así como la disposición de un SOC o Centro de operaciones de Seguridad para la monitorización y respuesta ante incidentes, de acuerdo al alcance y requerimientos técnicos y de servicio solicitados en la presente contratación.

El proyecto contempla como **alcance inicial la prestación de los servicios mencionados para la Red de Gobierno**, siendo objeto del proyecto el poder prestar dichos servicios a otras entidades que así lo soliciten en los plazos de contrato.

2 Objeto y alcance del contrato

2.1 Objeto y alcance

El objeto del presente Pliego de Condiciones Técnicas es la contratación de servicios especializados de seguridad que contemplen la *provisión y puesta en marcha de tecnologías SIEM y EDR, así como la disposición de un Centro de operaciones de Seguridad (en adelante, SOC) para la monitorización y respuesta ante incidentes explotando las tecnologías indicadas*, de acuerdo al alcance y requerimientos técnicos y de servicio solicitados en la presente contratación. Ello permitirá dotar de niveles de seguridad avanzados a las entidades adheridas a BATERA y resto de organismos del sector público que así lo soliciten.

El proyecto deberá considerar, por tanto, el siguiente alcance:

- Provisión y puesta en marcha de una solución SIEM- y de una solución EDR incluyendo los trabajos de consultoría, diseño y configuración necesarios.
- Disposición de un SOC que preste servicios de monitorización de eventos de seguridad y respuesta ante incidentes, explotando para ello las soluciones SIEM y EDR desplegadas, de acuerdo a los requerimientos y alcance de servicios expuesto en el presente documento.
- Relación de trabajos necesarios cuando una entidad u organismo público, esté en BATERA o no, solicite adscribirse al servicio en el periodo de ejecución del contrato.

Como requisitos generales del servicio, el licitador deberá tener en cuenta las siguientes premisas:

- Las soluciones SIEM y EDR se prestarán como un servicio en la nube (SaaS) basado en suscripciones anuales.
 - Ello agilizará la puesta en marcha del servicio, independizándolo de infraestructura hardware y su mantenimiento, y facilitando el escalado del mismo en un entorno multitenant.
 - El adjudicatario deberá garantizar la transferencia del servicio sin interrupción del mismo, con la finalización del contrato, de forma que EJIE pueda explotar a través de otros grupos de trabajo los servicios, tecnologías y configuraciones adoptadas en cuanto se produzca el fin de la presente contratación.
 - En línea con lo indicado, las suscripciones de las licencias serán titularidad de EJIE desde el momento de adquisición, o en su defecto, se deberá garantizar al inicio mediante documento acreditativo de fabricante, que se trasladará la titularidad de las mismas a EJIE con la finalización del contrato.
 - No se admitirá el despliegue de la solución en nube del licitador. Los datos deberán quedar en la nube del fabricante de la solución adjudicataria. Por lo tanto, una vez finalizado el contrato o resuelto anticipadamente, se procederá a traspasarlos, según plan de devolución del servicio (apartado 7.6), por lo que no se admitirán soluciones que impliquen albergue de los datos en nube del licitador si este no es el fabricante de la solución que albergaría los mismos. El fabricante se encargará de las labores de mantenimiento de la plataforma, justificar como son, entre otras, mantenimiento HW, instalación y configuración base del producto en HA, escalado HW en caso de crecimiento, instalación de parches y actualizaciones a nivel de sistema operativo y producto, monitorización del estado de la plataforma.
- El licitador deberá considerar la prestación del servicio en un entorno multitenant, y por tanto deberá presentar un servicio preparado para soportar dicho entorno, en el que las entidades presentan contextos IT diferentes y necesidades en materia de seguridad también diferentes. En este contexto, el licitador deberá considerar también el seguimiento diferenciado del servicio para cada entidad (de acuerdo apartado 2.2.1 donde se describen los tenant).

- El SOC se deberá prestar bajo un modelo 24x7x365, localizado en territorio de la Unión Europea. La solución se albergará en un DataCenter en la Unión Europea para asegurar el cumplimiento de la legislación vigente.

2.2 Descripción situación actual

2.2.1 Arquitectura BATERA

El entorno Batera se basa en infraestructura cloud del fabricante VMware, formando un entorno SDDC (Software-Defined Data Center). La infraestructura NSX permite la generación de un entorno Multi-Tenant que ofrece recursos dedicados (redes, almacenamiento, y otros recursos) a cada entidad, al mismo tiempo que aísla unos de otros. Además, NSX es utilizado para ofrecer los servicios de red (routing, switching, balanceo) y seguridad (firewall, micro-segmentación) en el entorno virtual.

No existe un plan de direccionamiento IPv4 unificado entre las diferentes entidades que se adhieren a Batera. Por este motivo, varias de las redes de clientes y servidores de las diferentes entidades se solapan, lo cual es un hándicap importante en el diseño de Batera y, por consiguiente, en el de cualquier proyecto que se albergue en Batera.

Teniendo estos aspectos en cuenta, cada entidad que se adhiera a Batera tendrá las siguientes características:

- Dispondrá de un tenant individual en la infraestructura de Batera
- El direccionamiento de dicho tenant será propio de la entidad.
- Ese tenant estará conectado con el entorno tradicional de la entidad, no existiendo solape de direccionamiento entre ambos entornos.

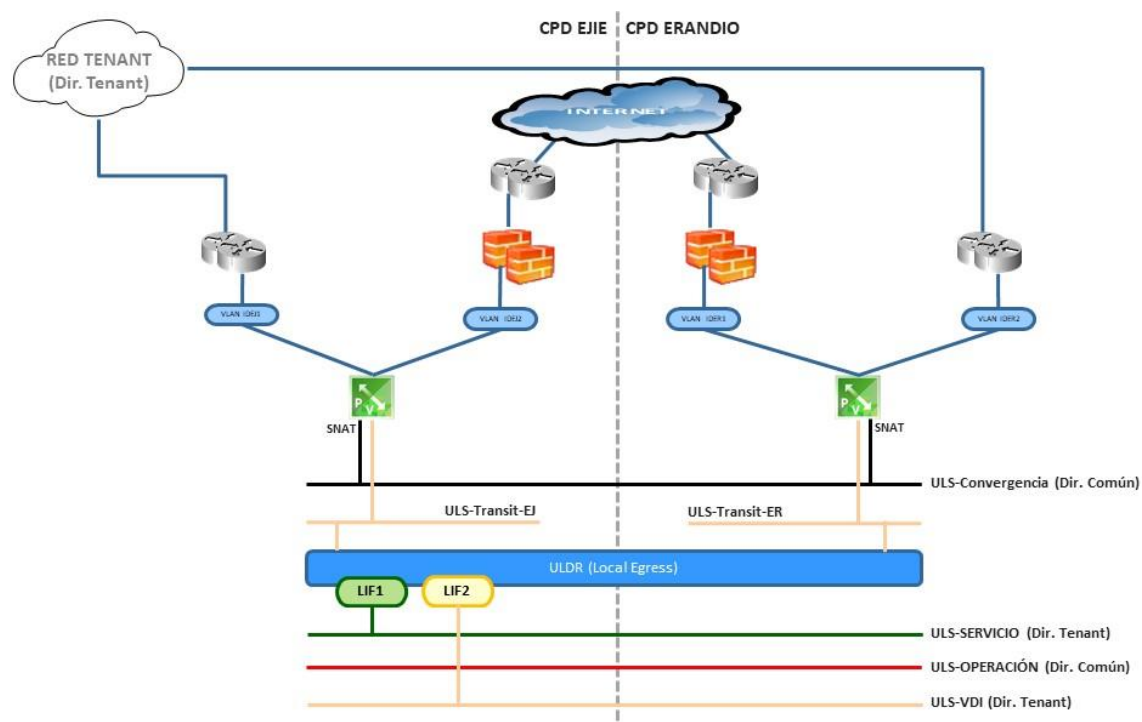
Adicionalmente, existe un tenant que no tiene correspondencia alguna con ninguna entidad, denominado "*tenant de convergencia*":

- Tiene direccionamiento no utilizado en ninguna entidad, que constituye la "*red de convergencia*"
- Está pensado para el consumo común, desde cualquier tenant, de servicios ahí publicados.
- El consumo de los servicios publicados en este tenant se puede realizar desde cualquier puesto de trabajo de cualquier entidad que disponga de un tenant propio en Batera.
- Al existir solapamiento de direcciones, desde este tenant no se pueden iniciar conexiones hacia las redes propias de cada entidad. Por el mismo motivo, las conexiones hacia convergencia se verán detrás de un SNAT.

Adicionalmente, todos los tenants cumplen las siguientes características:

- Aunque los tenants se encuentran aislados, existe una red, denominada "*red de operación*" que se extiende por la totalidad de los tenants. Esta red no es accesible por usuarios y permite la comunicación puntual entre elementos de diferentes tenants.
- Del mismo modo, la "*red de convergencia*" se extiende por todos los tenants, en la cual podrían publicar servicios para el resto de tenants (incluidos ellos mismos).

A continuación, con objeto de reflejar gráficamente lo aquí explicado y añadir algún detalle, se muestra el esquema de un Tenant o Entidad en Batera:



Cada una de las entidades tiene 2 conexiones con Batera, una contra el CPD de EJIE y otra contra el CPD de Erandio. A través de esas conexiones las entidades llegarán a las redes albergadas en Batera, entre las que destacan las siguientes:

- **ULS-Servicio:** Corresponde a la red (o redes) destinada a albergar infraestructura propia de la entidad y, por lo tanto, tendrá un direccionamiento específico de dicha entidad. Un servidor ubicado en esta red podrá ver la IP final de los clientes que accedan al servidor. Además, el servidor podrá acceder a cualquier IP de la entidad.

Si algún servidor lo requiere, podría tener presencia en Internet, tanto en entrada como en salida.

- **ULS-VDI:** A nivel de red es similar a la red de Servicio previa, pero en este caso estará destinada a albergar entornos de VDI de la entidad.
- **ULS-Convergencia:** Se trata de la red común denominada “red de convergencia”, cuyo direccionamiento ha sido elegido de forma que no esté utilizado en ninguna entidad adherida para evitar solapamientos. Su objetivo es albergar servicios comunes que puedan ser consumidos por todas las entidades adheridas.

Sin embargo, al haber solapamiento del direccionamiento de los clientes, al acceder a esta red, el direccionamiento del cliente se oculta detrás de un SNAT. Así, la IP que vería un servidor albergado en Batera sería la misma para todos los clientes de una entidad. Cada entidad tendrá IPs de SNAT diferentes. Desde un servidor albergado en Convergencia no se podrán iniciar conexiones contra IPs específicas de la entidad.

Si algún servidor lo requiere, podría tener presencia en Internet, tanto en entrada como en salida.

- **ULS-Operación:** Se trata de la red común denominada “red de operación”. En este caso el objetivo no es ofrecer servicios comunes por esa red de cara al usuario final, sino que el objetivo es “operar” o gestionar los diferentes servicios a través de esta red de Operación y acceder a servicios internos de infraestructura como pueden ser servidores de actualizaciones, logs, etc. También se puede utilizar para comunicación interna entre elementos de un mismo entorno.

En cuanto al diseño relativo a la alta disponibilidad, Batera es un entorno activo en el CPD de EJIE, siendo el CPD de Erandio un elemento de DR (Disaster Recovery) cuya activación se realiza de forma manual. Por

lo tanto, los entornos se montan de forma que tengan HA y balanceo de carga dentro del CPD de EJIE, ofreciendo el 100% del servicio en dicho CPD, y que dispongan de un mecanismo de DR en el CPD de Erandio. Cuando se trata de componentes virtuales, la propia infraestructura de virtualización proporciona este mecanismo de DR. Cuando se trata de componentes físicos hay que disponer de elementos físicos específicos en Erandio.

Entrando un poco más en detalle en lo relativo al DR:

- Asumiendo que las soluciones de los fabricantes que se despliegan en Batera ya tienen una solución de clúster, no se encuentra activa la función Fault Tolerance de vmware.
- En cuanto a la parte de Disaster Recovery (DR), la solución desplegada en Batera funciona con Cross-Vcenter y SRM. En situación de DR, la máquina al arrancar en el CPD secundario, habrá sufrido un reinicio. Una vez reiniciada, la conectividad es a las mismas redes que en el CPD de EJIE. En cuanto a almacenamiento se hace uso de vsphere replication. Se trata de DR asíncrono.
- Para el equipamiento virtual los equipos en situación de DR mantendrán dirección IP en el momento de arrancar en el CPD secundario. Pero, los equipos físicos de este CPD secundario deberán estar en una subred totalmente diferente a la de los equipos del CPD principal. Es por ello que la oferta deberá detallar claramente el funcionamiento en situación de DR.

Por otra parte, existe un entorno denominado VRF-VRA que constituye la infraestructura base sobre la que se alberga Batera a los diferentes niveles (red, servidores, almacenamiento, etc.). Este entorno dispone de redes de gestión aisladas y específicas para esta infraestructura.

3 Requisitos vinculados a la solución SIEM

En este apartado se indican los requisitos de obligado cumplimiento que tiene que soportar la plataforma SIEM propuesta por el licitador, debiendo quedar debidamente justificado su cumplimiento a través de la propuesta presentada.

Asimismo, todas las funcionalidades y requisitos mínimos solicitados deberán venir licenciados como parte de la solución para todo el periodo del contrato, excepto en aquellos casos en los que se indica explícitamente que no es necesaria su provisión dentro de la configuración mínima del servicio.

La plataforma SIEM deberá cumplir al menos con los siguientes requisitos:

Arquitectura

- La solución SIEM debe ofrecerse en modo servicio (SaaS) en nube mantenida por fabricante. Es decir, todas las labores de instalación, mantenimiento y operación básicas del producto deben ser responsabilidad del fabricante, no del adjudicatario. Entre ellas, instalación y configuración HW, instalación y configuración de los sistemas operativos correspondientes, instalación y configuración básica del producto hasta el momento en que se ofrece como SaaS, instalación de actualizaciones y parches de sistemas operativos y producto, ampliaciones HW necesarias, monitorización básica de la plataforma para asegurar la alta disponibilidad del servicio.
- La solución debe ser MultiTenant, a la vez que debe permitir un trabajo conjunto por parte del SOC. Es decir, la solución debe permitir ofrecer una visión global al SOC que le permita trabajar sobre el conjunto de eventos y configuraciones total, mientras que, a la vez, debe permitir ofrecer una visión a nivel de Tenant que permita realizar configuraciones, informes, indicadores, alarmas, cuadros de mando, etc. específicos de cada Tenant.
- OnPremise sólo se instalarán los elementos mínimos necesarios para permitir el envío de eventos entre las plataformas OnPremise que se monitorizarán con el SIEM y el servicio en nube SaaS, así como posibles elementos para añadir información de contexto a los eventos del SIEM. Los elementos que haya que instalar deberán ser virtualizables en VMWare y se albergarán en la infraestructura de BATERA.

Dada la arquitectura de BATERA, en algún caso puede ser necesario tener colectores de logs diferentes en cada Tenant. La solución debe soportar esta necesidad.

- La consola de gestión de la solución será única y estará basada en Web sin necesidad de Java ni de Flash.
- La solución permitirá realizar una gestión centralizada de todos los componentes albergados en nube y de los componentes para el reenvío de logs a la nube que se instalen OnPremise.
- Al tratarse de una solución en nube, debe ofrecer la posibilidad de hacer Single Sign On (SSO) utilizando proveedores de identidad de terceros (EJIE o el adjudicatario, por ejemplo) en base a estándares. Como mínimo deberá soportar SAML para la realización de SSO.

Seguridad

- La solución se albergará en un DataCenter en la Unión Europea para asegurar el cumplimiento de la legislación vigente.
- Las comunicaciones entre todos los componentes de la solución deberán estar cifradas con algoritmos acreditados por CCN en la guía CCN-STIC-807 (Criptología de empleo en el ENS) en lo correspondiente al nivel alto ([enlace](#) a la serie 800 de guías CCN-STIC, [enlace directo](#) a la guía 807).
- Existirá auditoría de todas las acciones realizadas por todos los usuarios de la solución.
- La solución debe permitir la ofuscación de campos concretos o de parte del texto de ciertos eventos con dos finalidades: Evitar la visualización de cierta información por parte de los analistas y evitar el almacenamiento de información sensible fuera de la organización.

- La solución debe asegurar la integridad de los datos, que deberá poder ser validada mediante algún sistema de hash. Se utilizarán funciones “hash” acreditadas para el nivel alto de cumplimiento del Esquema Nacional de Seguridad según la guía CCN-STIC-807 (Criptología de empleo en el ENS). ([enlace](#) a la serie 800 de guías CCN-STIC, [enlace directo](#) a la guía 807).
- La solución almacenará, como mínimo, los datos en raw.
- La solución debe soportar roles que controlen el acceso tanto a las funcionalidades de la plataforma (administración, informes, cuadros de mando, indicadores) como a los conjuntos de datos de cada Tenant. Esto permitirá ofrecer el servicio en modo MultiTenant. A parte del SOC que operará la solución, EJIE podrá tener acceso a la plataforma.

Volumen de Datos

- En lo relativo a la retención de datos, la solución ofrecerá un mínimo de 3 meses online sobre los que pueda trabajar la herramienta. Además, se retendrá un histórico mínimo de 12 meses. Los datos históricos, ante una necesidad, deben poder ser cargados/importados en la herramienta para una operación “online”.
 - El licitador deberá describir el tratamiento de los datos que realiza la herramienta. Se valorarán positivamente, de acuerdo a los criterios de adjudicación previstos en el PCP, dentro del apartado 28. Criterios de adjudicación, “Descripción de la solución SIEM”, las soluciones en las que solución propuesta trabaje con un periodo de retención de datos on line mayor al especificado, sin coste adicional para EJIE.
- Todo el almacenamiento necesario (online e histórico) para la retención de datos será proporcionado en la nube como parte de la solución de SIEM. No se permiten dependencias de infraestructura del adjudicatario para el almacenamiento de datos.
- La solución debe estar dimensionada para el almacenamiento histórico de todos los datos. Sin embargo, debe ofrecer la posibilidad de decidir qué fuentes se quieren almacenar en modo histórico y cuáles no.
- La solución debe evitar la pérdida de eventos ante picos que superen la licencia en momentos puntuales.
- La solución debe ofrecer a través de componentes propios (sin contar con la configuración de los orígenes de datos) la posibilidad de filtrar los eventos enviados a la plataforma con objeto de poder evitar el envío de grandes cantidades de datos que no aporten valor. Entre otras cosas, debe permitir filtrar el tráfico de una fuente concreta en un momento dado sin tener que desactivar los agentes de integración de esa fuente. También debe permitir filtrar logs específicos dentro de los enviados por una fuente (Por ejemplo, dentro de una fuente como puede ser un proxy de navegación, debe permitir el filtrado de eventos de accesos a URLs concretas).
- Los eventos filtrados no deben ser contabilizados a nivel de licenciamiento.
- Como mínimo en el caso de las plataformas OnPremise, el filtrado de eventos se realizará en origen, sin que esos eventos filtrados consuman ancho de banda.

Correlación

- La solución debe permitir correlar entre sí, como mínimo, la información procedente de logs de las diferentes plataformas origen de datos, flujos de tráfico de red y análisis de vulnerabilidades.
- La solución ofrecerá correlación en tiempo real
- La solución ofrecerá correlación histórica sobre los datos que tenga online. Esta correlación histórica le debe permitir analizar IOC o casos de uso nuevos sobre eventos pasados.
- La solución debe ofrecer casos de uso predefinidos mantenidos y documentados por el fabricante que sean aplicables al menos al 80% de las plataformas de EJIE.

- Las plataformas/fuentes se detallan en el menú “Integración de Fuentes” de este mismo apartado
- La solución debe ofrecer informes predefinidos mantenidos y documentados por el fabricante que sean aplicables al menos al 80% de las plataformas de EJIE.
 - Las plataformas/fuentes se detallan en el menú “Integración de Fuentes” de este mismo apartado
- Durante el tiempo de vida del contrato el fabricante proporcionará actualizaciones periódicas que incluirán nuevas reglas de correlación, casos de uso, informes y alertas predefinidos y documentados por fabricante.
- La solución debe soportar reglas que permitan detectar anomalías en tiempo real como puede ser el cambio repentino de un valor o un suceso (incremento repentino de tráfico o de logins fallidos, por ejemplo).
- La solución debe soportar reglas que permitan detectar anomalías estacionales como puede ser el cambio de un valor o un suceso respecto al que tenía en una fecha previa.
- La solución debe ser capaz de agrupar incidentes relacionados en un único incidente, aunque los eventos estén separados en el tiempo por horas o días.
- La solución debe ser capaz de detectar en tiempo real el uso de nuevos elementos en la red. Como mínimo deberá ser capaz de detectar el uso de una nueva IP en una subred o de un nuevo Usuario.
- La solución debe soportar direccionamiento privado solapado, no mezclando los eventos de un Tenant con los de otro.

Integración con terceros

- La solución debe proporcionar una API REST que permita automatizar diversas tareas de configuración, administración y consulta.

Personalización y Facilidad de Uso de la consola de gestión

- La solución debe ser personalizable, permitiendo crear, como mínimo, vistas, gráficos, filtros y cuadros de mando personalizados visibles para un usuario o compartidos entre varios.
- La solución debe permitir enriquecer los datos con información de contexto general (geolocalización, por ejemplo) y corporativo (datos de directorio activo, por ejemplo).
- La solución debe permitir crear menús contextuales personalizados para facilitar la tarea de los analistas.
- La solución debe permitir realizar consultas avanzadas en lenguajes similares a SQL.
- La solución debe permitir mantener una BBDD de activos en función de los logs y flujos observados (IPs, MACs, Usuarios, etc.).

IoCs, Feeds, MITRE

- La solución debe permitir incorporar feeds de inteligencia con datos sobre amenazas de seguridad que utilice posteriormente en sus correlaciones y búsquedas de eventos de seguridad.
- La solución debe permitir compartir los IoCs con otras herramientas.
- La solución debe permitir importar y exportar IoCs utilizando estándares STIX/TAXII.
- La solución debe clasificar los incidentes o alertas de seguridad detectados en base a la matriz MITRE ATT&CK.

- Se valorarán positivamente, de acuerdo a los criterios de adjudicación previstos en el PCP, dentro del apartado 28. Criterios de adjudicación, “Descripción de la solución SIEM”, las soluciones en las que la herramienta incorpore un feed de inteligencia propio

Integración de Fuentes

- La solución debe permitir la integración de fuentes utilizando diferentes protocolos para la recolección de logs. Como mínimo de permitir los siguientes:
 - Syslog: UDP/TCP – línea única o multilínea
 - SNMP v1, v2 o v3
 - Transferencia de ficheros txt, csv y xml vía FTP, SFTP, HTTP.
 - REST API
 - WMI, MSRPC
- La solución debe detectar y reconocer automáticamente las fuentes syslog más comunes
- La solución debe permitir la integración de flujos de red utilizando diferentes protocolos. Como mínimo debe soportar NetFlow y SFlow (ver punto 7.5)
- La solución debe permitir integrar, interpretar automáticamente y ofrecer reglas de correlación y casos de uso para las siguientes fuentes (al menos el 80% de ellas):
 - Firewalls: FortiNet, CheckPoint, Cisco ASA, VMWare NSX
 - Proxy: McAfee
 - IDS/IPS: McAfee, FortiNet
 - Antivirus: McAfee, BitDefender, TrendMicro
 - EDR: El propuesto en el pliego
 - Correo Electrónico: IronPort, Microsoft Exchange, Office365
 - WAF: F5
 - VPN: F5, Cisco ASA, FortiNet, VMWare NSX
 - Servidores Web y Aplicación: Apache, NGINX, IIS, Weblogic, Tomcat
 - BBDD: Oracle, Microsoft SQL Server, MongoDB
 - Autenticación: LDAP, Active Directory, ADFS, RADIUS, TACACS (Clearpass), OKTA (Cloud), CyberArk (Cloud), Azure AD (Cloud), Oracle OIM
 - DHCP, DNS
 - VMWare ESX
 - Office365
 - PKI: Microsoft
 - Inventario: IPAM (Efficient IP, Infoblox), SCCM, ServiceNow (Cloud)
 - Servidores: Linux/Unix, Windows
 - Routers (Cisco, Juniper), Switches (Cisco, HP/Aruba, Alcatel, Huawei), Wireless APs y Controladoras (Cisco, Aruba, Huawei)
- La solución debe permitir incorporar fuentes personalizadas o no soportadas por defecto.
- La solución debe permitir reenviar logs recibidos
- La solución debe permitir generar alertas en diferentes modos: eMail, SNMP Traps, syslog

Análisis de Vulnerabilidades

- La solución debe permitir incorporar en sus correlaciones los datos procedentes de análisis de vulnerabilidades.

- La solución debe soportar la integración, como mínimo, con los resultados procedentes del analizador de vulnerabilidades que utiliza EJIE: Rapid7 Nexpose

Análisis de Comportamiento de Usuarios (UBA)

- La solución debe disponer de un módulo específico basado en Machine Learning para el análisis de comportamiento de usuarios (UBA). En caso de tratarse de un módulo licenciado, no es requisito obligado su provisión dentro de la configuración mínima del servicio.
 - El licitador deberá especificar, como parte del Modelo Económico, el coste unitario anual asociado a la prestación de este servicio, para que EJIE, si lo considera, proceda con la solicitud de activación del mismo durante el periodo del contrato.
 - Si el licitador considera su provisión como parte del servicio base durante el periodo del contrato, sin coste adicional para EJIE, entonces deberá especificar para este concepto, dentro del Modelo económico, un coste unitario anual de 0€.
 - **Se recuerda que esta información (por ser un dato de carácter objetivo a incluir en el Sobre B) NO se debe INCLUIR dentro de la Propuesta Técnica del Sobre C ya que en caso contrario se procederá a la exclusión de la propuesta presentada.**
- Este módulo debe permitir alertar ante desviaciones de comportamiento habitual de los usuarios.
- Este módulo debe permitir evaluar el riesgo de las actividades de un usuario y alertar ante actividades de riesgo.
- Este módulo debe formar parte de la solución de SIEM, gestionándose y viendo los resultados desde la consola única del SIEM.

Automatización de Análisis de Incidentes

- La solución debe disponer de un módulo basado en Inteligencia Artificial que permita realizar análisis automatizados de los incidentes, reduciendo el tiempo dedicado por los analistas. En caso de tratarse de un módulo licenciado, no es requisito obligado su provisión dentro de la configuración mínima del servicio, pero sí deberá aportarse la descripción correspondiente.
- Este módulo debe formar parte de la solución de SIEM, gestionándose y viendo los resultados a través de la consola única del SIEM.

Orquestación y Respuesta automática a Incidentes de Seguridad (SOAR)

- La herramienta debe permitir la integración con herramientas SOAR para automatizar y orquestar la respuesta frente a incidentes de seguridad.

4 Requisitos vinculados a la solución EDR

En este apartado se indican los requisitos de obligado cumplimiento que tiene que soportar la solución EDR propuesta por el licitador, debiendo quedar debidamente justificado su cumplimiento a través de la propuesta presentada.

Asimismo, todas las funcionalidades y requisitos mínimos solicitados deberán venir licenciados como parte de la solución para todo el periodo del contrato, excepto en aquellos casos en los que se indica explícitamente que no es necesaria su provisión dentro de la configuración mínima del servicio.

Arquitectura

- La solución EDR debe ofrecerse en modo servicio (SaaS) en nube mantenida por fabricante. Es decir, todas las labores de instalación, mantenimiento y operación básicas del producto deben ser responsabilidad del fabricante, no del adjudicatario. Entre ellas, instalación y configuración HW, instalación y configuración de los sistemas operativos correspondientes, instalación y configuración básica del producto hasta el momento en que se ofrece como SaaS, instalación de actualizaciones y parches de sistemas operativos y producto, ampliaciones HW necesarias, monitorización básica de la plataforma para asegurar la alta disponibilidad del servicio. Permitirá crecimiento y escalabilidad según se necesite.
- La solución debe ser MultiTenant. La solución debe permitir ofrecer una visión global, así como permitir ofrecer una visión a nivel de Tenant que permita realizar configuraciones, informes, indicadores, alarmas, cuadros de mando, etc. específicos de cada Tenant.
- Si es necesario instalar algún elemento OnPremise para el envío de eventos de endpoint que por algún motivo no tengan conexión con la solución en nube, los elementos que haya que instalar deberán ser virtualizables en VMWare y se albergarán en la infraestructura de BATERA.
- La arquitectura de la solución estará orientada a minimizar el tráfico de red.

Capacidades de detección y respuesta:

La solución EDR debe disponer las siguientes capacidades:

- Capacidad para detectar malware desconocido (malware avanzado)
- Capacidad para detectar programas potencialmente no deseados - PUP (Potential Unwanted Programs)
- Capacidad para detectar ataques sin archivos, así como troyanos de nueva generación indetectables por los antivirus
- Detección de amenazas de día cero (zero-day)
- Posibilidad de creación de listas blancas y negras
- Posibilidad de ejecutar acciones de respuesta desde la plataforma EDR para contención en caso de detectarse una amenaza
- Capacidad de detección de amenazas avanzadas basada en IOCs y TTPs
- Integración con IOC (Indicadores de compromiso), con posibilidad de crear o modificar IOC y lanzar análisis bajo demanda de un IOC, además de poder exportar o importar IOCs. Se incluye como requisito obligatorio la posibilidad de buscar IOCs en los puestos bajo demanda.
- Clasificación de tácticas, técnicas y procedimientos (TTP) de ATT & CK detectados
- Posibilidad de personalización de políticas, además de disponer de políticas automáticas.
- Posibilidad de remediación a través de la consola. Permitir el aislamiento y la investigación del hosts. Posibilidad de acceso remoto a los equipos. Capacidad de Respuestas automatizadas o manuales en tiempo real.

- Clasificación de todo el software que se ejecuta en el puesto de trabajo, con identificación de software confiable y no confiable.
- Clasificación de todos los procesos en ejecución como malware o goodware
- Para facilitar la investigación y análisis de los incidentes debe proporcionar la siguiente información:
 - Lista de los procesos ejecutados y con identificación del usuario
 - Lista de procesos que se ejecutan en un punto final específico
 - Acceso a los registros de actividad de cada endpoint de forma completa
 - Visualización de las cadenas de ataque de forma gráfica
 - Información de los procesos que acceden a ficheros de datos
 - Conexiones que se producen desde un equipo tanto externas a la red como internas, debe incluir que proceso las realiza
 - Información relacionada con los accesos al registro de Windows
 - Información de los archivos ejecutables y comprimidos descargados de otras ubicaciones
- La solución a desplegar debe soportar la capacidad de detectar versiones de aplicaciones vulnerables en los endpoints.
- Se valorarán positivamente, de acuerdo a los criterios de adjudicación previstos en el PCP, dentro del apartado 28. Criterios de adjudicación, "Descripción de la solución EDR", las soluciones que posibiliten la localización de equipos desprotegidos en la red.
- Se valorarán positivamente, de acuerdo a los criterios de adjudicación previstos en el PCP, dentro del apartado 28. Criterios de adjudicación, "Descripción de la solución EDR", las soluciones que posibiliten la generación de información forense relacionada con los archivos que existan en los equipos con información personal identificable y que sea capaz de buscar los archivos que contengan información de carácter personal según definición de la RGPD.

Integración con terceros

- La solución debe posibilitar su integración con el SIEM ofertado, con capacidad de envío a la plataforma SIEM únicamente los eventos relevantes.
- Asimismo, la solución debe posibilitar su integración vía API con diferentes herramientas de seguridad y automatización.

Características de la Consola:

- Interfaz basada en web con datos en tiempo real y paneles preconfigurados
- Consola, con datos en tiempo real, con soporte de cuadros de mando, herramientas de búsqueda y generación de informes automáticos:
 - Cuadros de mandos, con detalle de incidentes, malware detectado, eventos y alertas generadas
 - Informe ejecutivo con el estado de seguridad global, así como por entidad
 - Posibilidad de personalización de la información a mostrar a través de la consola
- Posibilidad de acceso a la consola en la nube.
- Administración con definición de roles y autenticación doble factor.
- La solución debe permitir la organización de activos en ramas delegadas de administración y la definición de diferentes roles de uso de la plataforma de gestión y registro.
- Posibilidad de descargar informes y la notificación de alertas. Reporting global y por tenant o entidad.

Características del agente o sensor a instalar en los puestos:

- Impacto sobre el rendimiento de CPU menor 5%
- Posibilidad de desplegar el agente manual o mediante herramientas de despliegue centralizado, poder desplegar por grupos de Directorio Activo basado en políticas de dominio, etc
- Desinstalación protegida por contraseña u otra técnica controlada por el administrador
- La empresa licitadora debe garantizar que la herramienta EDR ofertada sea compatible con las soluciones de seguridad actualmente desplegadas como son la solución de antivirus BitDefender para los puestos de trabajo de Batera y soluciones Trendmicro en servidores.
 - El servicio EDR será un complemento a la solución de BitDefender actualmente desplegada en puestos, y convivir con dicha solución.
 - **No se podrá reutilizar la infraestructura de antivirus existente actualmente, incluyendo el agente.**
 - En caso de que la solución propuesta disponga de módulo antivirus (EPP), éste no formará parte de la oferta actual, o, en su defecto, si la tecnología no lo permite, deberá poder quedar desactivado en la solución ofertada.
- La actualización del agente debe poder hacerse planificada a lo largo del tiempo, y así poder evitar saturación de las líneas.
- Soporte para múltiples S.O., como mínimo:
 - Windows server: 2008 R2, 2012R2, 2016, 2019
 - Windows Cliente: Windows 7, Windows 8 y Windows 10
 - MacOS: 10.10 y superiores
 - Linux: RHEL 6.1 superiores, Centos 6.8 y superiores, Ubuntu 16.0 y superiores
 - Entornos de Infraestructura de escritorio virtual (VDI) en Vmware

El licitador deberá especificar todas las compatibilidades soportadas, incluyendo aquellas relativas a sistemas operativos móviles, para su valoración.

- El agente EDR debe soportar enviar los eventos a la nube del producto utilizando la configuración de proxy del sistema, incluyendo configuración basada en ficheros *proxy.pac*

Recolección de Datos

- En lo relativo a la retención de datos, la solución recopilará y almacenará toda la telemetría necesaria (**no solo la relativa a eventos sospechosos**) para poder hacer las investigaciones durante 90 días y posibilidad de recuperación de la información más relevante que será almacenada durante 12 meses como mínimo.

Capacidades de Threat Hunting desde la plataforma:

La plataforma deberá soportar capacidades avanzadas de Threat Hunting para la búsqueda proactiva de amenazas, mediante correlación de históricos y análisis de telemetría e identificación de anomalías, al menos con las siguientes características:

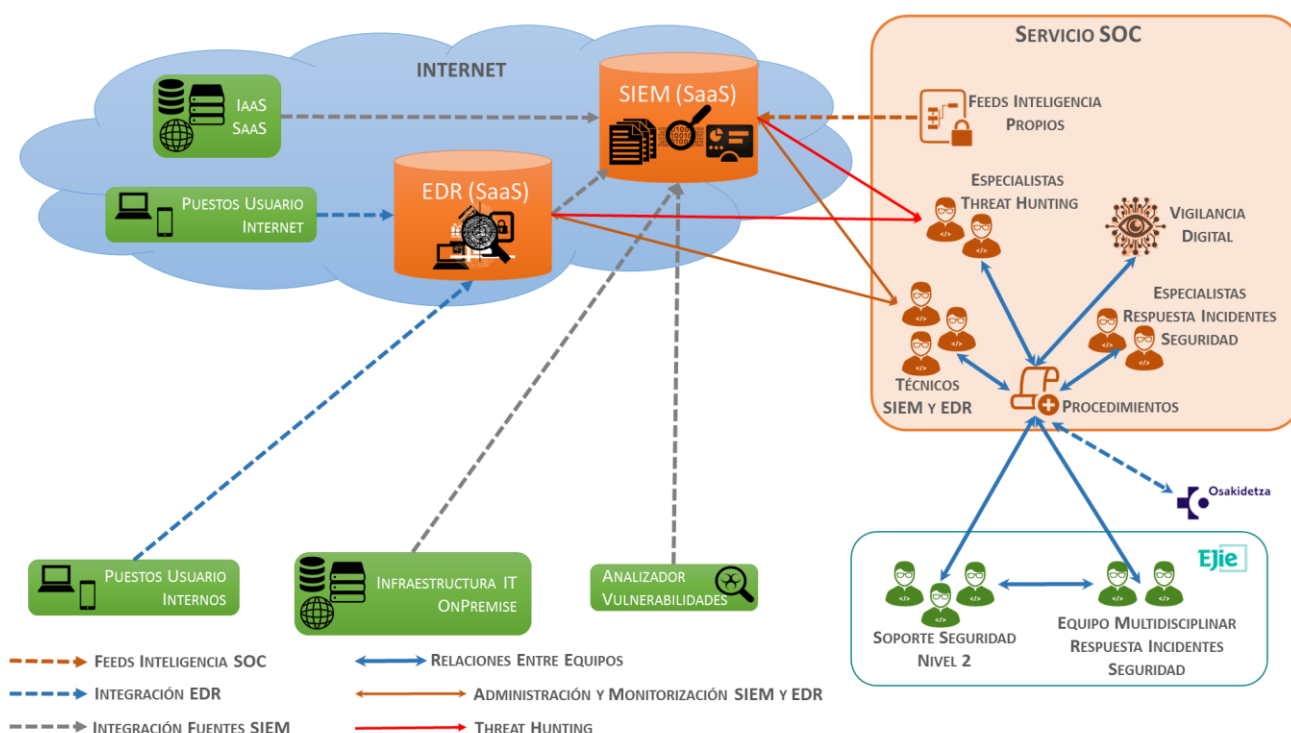
- Capacidad de buscar archivos y procesos, que se ejecutan ahora o en el pasado, en todos los puntos finales gestionados por la herramienta EDR.
- Capacidad de buscar conexiones de red que se ejecutan actualmente en todos los puntos finales gestionados por la herramienta EDR.

- Detección de amenazas avanzadas, ataques en fase temprana, comportamientos anómalos de usuarios y equipos, así como malas prácticas.
- Analizar la actividad sospechosa de los indicios de ataque que se registran de forma continua en la plataforma de Hunting.
- Generar nuevas reglas para detectar nuevas actividades sospechosas en tiempo real, así como implementar detecciones personalizadas y configuraciones de listas de vigilancia.
- Poder incluir listas de vigilancia con feed propias del fabricante, así como de terceros

5 Alcance y requisitos de los servicios a prestar por el SOC

5.1 Introducción al alcance del SOC

A continuación, se presenta, a modo de introducción, la relación de servicios y componentes esperados en el SOC a contratar, cuyo alcance y condiciones de provisión pasan a describirse en los capítulos siguientes, así como la relación entre los diferentes componentes y agentes del servicio.



Con el inicio del contrato, y atendiendo al alcance establecido, se definirá el modelo de relación con los diferentes grupos de seguridad de EJIE y herramientas asociadas.

Asimismo, en caso de adscribirse Osakidetza al servicio en el periodo del contrato, ésta podrá interactuar directamente con el servicio de SOC, de cara a la integración en los procesos de Osakidetza en caso de incidentes de ciber seguridad. Se acordará, igualmente en el inicio de contrato, el modelo de relación a establecer.

5.2 Servicios de monitorización, detección y respuesta a incidentes

El objetivo principal del SOC es el de la monitorización de eventos de seguridad, identificación, detección, alerta temprana y respuesta ante incidentes, apoyándose principalmente en las tecnologías SIEM y EDR desplegadas.

Ello incluye la prestación de los siguientes servicios:

- Monitorización y correlación de eventos en tiempo real, mediante explotación de herramienta SIEM, en modo 24x7x365. La solución deberá disponer de mecanismos de alta disponibilidad que garanticen la prestación del servicio en estas condiciones.

- Identificación, detección y categorización de incidentes. A partir de la información proporcionada por el servicio de monitorización, el adjudicatario deberá, en base a las alertas, identificar y analizar el posible incidente, determinar su alcance y posible escalado. Ello incluye:
 - Recolección y análisis de logs
 - Detección de falsos positivos, antes de reportarlo a siguiente nivel de escalado
 - Clasificación y tipología del incidente
 - Análisis de situación e impacto (evaluación)
 - Propuesta de medidas correctivas o de remediación, en base a la criticidad
 - Documentación de los casos tratados
- Gestión y comunicación de incidentes. Notificación de los incidentes y actividades sospechosas en tiempo real.
 - Una vez identificado y analizado un incidente, se procederá con el registro y escalado del mismo si procede tras la evaluación previa, atendiendo al Procedimiento de gestión y escalado de incidentes que se acuerde con EJIE en el inicio del contrato
 - Existirá integración con los modelos de operación y herramientas de ticketing de EJIE (ServiceNow) para la notificación y reporte del incidente.
 - Con el inicio del contrato, se establecerán conjuntamente los Planes de Respuesta ante incidentes, en base a criterios como criticidad, impacto y tipología del incidente.
 - Con relación a la respuesta ante incidentes, con carácter general será EJIE quien implemente, a través de los grupos de seguridad propios, las acciones de remediación y respuesta que se recomienden.
 - Habrá actuaciones (a definir) de remediación y contención que sí serán realizadas por el adjudicatario, cuando éstas se puedan ejecutar de forma directa desde la consola de EDR, según políticas de remediación acordadas con EJIE.
 - Se definirán casos en los que el servicio EDR actuará directamente aislando los equipos y actuando sobre ellos. Otros casos se tendrán que verificar según los procedimientos establecidos antes de realizar aislamientos.
 - Los *Planes de Respuesta* acordados, así como los *procedimientos de gestión y escalado* de incidentes, quedarán debidamente documentados.
- Dentro del alcance del contrato, el adjudicatario deberá definir un procedimiento particular para la identificación y tratamiento de incidentes críticos que deberá validarse por EJIE:
 - Se entiende por incidente crítico aquel que identifica situación de alto riesgo para la seguridad de los servicios y negocio prestados por EJIE.
 - El SOC será quien, en base a su experiencia y entorno particular de EJIE, defina el procedimiento más adecuado (alcance de tareas a realizar, responsabilidades y asignación, activación de las comunicaciones, coordinación entre grupos, documentación...) para el tratamiento de este tipo de incidentes de alto riesgo. El procedimiento deberá adaptarse para cada tenant.
 - A criterio de EJIE, en función del impacto del incidente y de acuerdo al procedimiento que se defina, se activará el servicio de *Respuesta ante Incidentes Críticos* [ver capítulo 5.3].
 - La notificación de incidentes críticos se realizará bajo el modelo 24x7x365.
 - Se incluirá en el primer año de ejecución del contrato, al menos un ejercicio de simulación de incidente grave, que permita validar el procedimiento de tratamiento de incidentes críticos que se defina.

- Definir diferentes métricas sobre la eficiencia del servicio y niveles de servicio deseables, que puedan ser de interés al objeto del servicio:
 - Ejemplos de métricas e indicadores sobre la eficiencia del servicio: número de incidentes detectados, ratios de falsos positivos, etc.
 - Los niveles de calidad sobre la prestación del servicio (tiempos de notificación, tiempos de atención, tiempos de respuesta...) se establecerán con un valor de inicio, y servirán como referencia para medir la calidad del servicio prestado. [ver capítulo 5.9].
 - Las diferentes métricas y niveles de servicio se medirán y se verificará su cumplimiento con la evolución del servicio.
- Integración del servicio con los *feeds de inteligencia* propios, así como aquellos procedentes de otras fuentes públicas o privadas. Monitorización y análisis de múltiples fuentes de información (públicas y privadas) e investigaciones propias para mejorar la detección y visibilidad de amenazas externas.
- Procedimiento y ajuste de “casos de uso” conocidos. Nuevos casos de uso.
 - Los casos de uso pueden tener dos orígenes:
 - Solicitudes de EJIE para cubrir casos concretos que se necesiten.
 - Propuestas proactivas del adjudicatario en base a su experiencia.
 - Los casos de uso tendrán un proceso de implementación.
 - Los casos de uso quedarán documentados.
 - Se considera que puede llegar a ser necesario configurar un caso de uso semanal. Esto hace unos 50 casos de usos anuales.
- Integración de IOC's en base a feeds de inteligencia propios del fabricante, propios del SOC, externos, etc. Estos IOC's puede ser necesario incorporarlos en otras herramientas de la organización (MISP, FW, Proxy, etc.), por lo que se requiere una trazabilidad de los mismos, indicando que IOC's se añaden/eliminan/modifican a diario.
- Todos los procesos de integración (fuentes, casos de uso, IOC, etc.) tienen que tener unos procedimientos claros de integración por fases que eviten picos de alertas, falsos positivos, etc.
- Definición y configuración de uno o varios Cuadros de Mando sobre las consolas, a los que EJIE tenga acceso, que ofrezcan una visión gráfica en tiempo real de las métricas e indicadores principales del servicio de seguridad:
 - Volumetría de eventos, alarmas e incidentes gestionados.
 - Identificación de incidentes por categorías, criticidad...
 - Ratios de falsos positivos
 - Otros indicadores de seguridad
 - Cumplimiento de los niveles de servicios acordados
 - Etc.

Los cuadros de mando del servicio serán personalizables y permitirán identificar el estado del servicio de seguridad por tenant o entidad. Asimismo, el acceso a los cuadros de mando deberá gestionarse con la definición de usuarios autorizados.

- Generación de informes de servicio, cuyo formato y contenido se acordarán con EJIE con el inicio de la asistencia (ver capítulo 5.5).
- Este servicio será asimismo el responsable de administrar la plataforma SIEM incluyendo:
 - Mantenimiento y escalado a fabricante, cuando sea necesario

- Vigilancia sobre aquellas tareas responsabilidad del fabricante (y participación en las mismas si así lo requiere el fabricante), vinculadas a la instalación, mantenimiento y operación básica del producto como son:
 - Monitorización y estado del sistema (disponibilidad del servicio).
 - Back ups del servicio
 - Instalación de parches y actualizaciones
 - Evolución y escalado de la plataforma en caso de necesidad
 - ..
- Configuraciones base
- Integración de nuevas fuentes en SIEM. Ello incluye, dentro de cada integración:
 - Colaboración en la configuración de la fuente para recogida de los logs
 - Reglas de filtrado previo para evitar EPS que no aporten información útil
 - Configuración de reglas de correlación específicas de esa fuente ya proporcionadas por el fabricante.
 - Configuración de casos de uso específicos de esa fuente ya proporcionados por el fabricante (esto no cuenta como casos de uso de los bloques a consumir mencionados de forma previa)
 - Configuración de paneles y alertas
 - Vigilancia/Monitorización de que se reciben datos de esa fuente.
 - Documentación de las integraciones
- Implementación de reglas de correlación.
- Personalización de consola y cuadros de mando
- Creación de casos de uso
- Gestión de usuarios y roles
- Etc.
- Actividades proactivas de Threat Hunting, para la búsqueda proactiva de amenazas y comportamientos anómalos con la explotación de la telemetría e información obtenida de las fuentes. Se tendrán en cuenta las siguientes consideraciones:
 - Las actividades de Threat Hunting se realizarán tanto sobre EDR como sobre SIEM.
 - Las actividades de Threat Hunting tendrán dos orígenes:
 - Solicitudes de EJIE para cubrir casos concretos
 - Propuestas proactivas del adjudicatario en base a su experiencia y, sobre todo, a su información de Inteligencia disponible.
 - Los casos de Threat Hunting podrán ser genéricos o específicos de entornos concretos (Gobierno, Salud, Justicia, etc.).
 - Se incluye generación de casos para investigación detallada de los indicios de ataque que en el proceso de “priorización de alertas” se consideran un potencial riesgo.
 - En caso de producirse un ataque, identificación completa de impacto, activos y usuarios asociados al ataque, así como identificación de la fase de compromiso.
 - Notificación ante incidentes críticos o potenciales amenazas, con información inicial de resumen, así como información detallada del mismo.
 - Reporte mensual de la actividad realizada, proporcionando informes detallados sobre los hallazgos y resultados del servicio de Threat Hunting utilizando el conocimiento del entorno del

cliente, el conocimiento del panorama de amenazas actual y las fuentes de inteligencia. El servicio se dimensionará de forma que sea posible proporcionar al menos 1 informe periódico mensual, debiendo el adjudicatario poder absorber picos puntuales del servicio (hasta 15 informes al año).

- Proporcionar puntos de control trimestrales de información para revisar la canalización de búsqueda de amenazas y la priorización, procedimientos, telemetría, procesos, flujos de trabajo y tecnologías
- Proporcionar recomendaciones para ajustar las alertas personalizadas e introducir y ajustar nuevas detecciones.
- Explotación de la plataforma EDR en favor de la operación del servicio de seguridad, lo que incluye;
 - Detección y análisis de actividades sospechosas y comportamiento anómalos en endpoints.
 - En caso de endpoints comprometidos, el adjudicatario debe proporcionar asesoramiento inmediato sobre las actividades de remediación.
 - Se definirá un *Plan de Respuesta ante incidentes*, bajo acuerdo con EJIE, que establezca los casos en los que el servicio a través de la consola pueda actuar directamente sobre los equipos aislándolos.
 - Servicios de administración de la plataforma EDR, incluyendo:
 - Vigilancia sobre aquellas tareas responsabilidad del fabricante (y participación en las mismas si así lo requiere el fabricante), vinculadas a la instalación, mantenimiento y operación básica del producto como son:
 - Monitorización y estado del sistema (disponibilidad del servicio).
 - Back ups del servicio
 - Instalación de parches y actualizaciones (relativo a la plataforma)
 - ...
 - Seguimiento del estado del equipamiento instalado, creando paneles, informes, alertas, etc. que asegure que todos los agentes instalados están “enganchados” y actualizados.
 - Atención y seguimiento de incidencias derivadas del agente EDR, derivados de problemas sobre el funcionamiento en puesto.
 - Mantenimiento y escalado a fabricante, cuando sea necesario
 - Integración en SIEM
 - Configuraciones base
 - Configuración de políticas del agente según necesidades
 - Personalización de consola y cuadros de mando
 - Back ups del servicio
 - Gestión de usuarios y roles
 - Instalación de parches y actualizaciones
 - Actualización coordinada de los agentes (el despliegue inicial del agente se realizará con la colaboración y herramientas de EJIE).
 - Evolución y escalado de la plataforma en caso de necesidad
 - Etc.
- Identificación y propuesta de recomendaciones, cambios y otras medidas correctivas con la evolución del servicio, cuya aplicación se considerará a criterio de EJIE. En general, aportaciones a las soluciones y servicios desplegados para la mejora continua del servicio.

- Gestión de la capacidad.
 - Será responsabilidad del SOC avisar a EJIE cuando sea necesaria la adquisición de mayor volumen de suscripciones sobre las plataformas SIEM y EDR, en base a alertas construidas.
 - En el caso del SIEM, se incluye igualmente la vigilancia de los EPS generados por las diferentes fuentes, informando de variaciones atípicas que puedan suponer un consumo excesivo de EPS.

5.3 Servicios que se activan bajo demanda

5.3.1 Servicio especializado de Respuesta ante incidentes críticos

En caso de identificarse un incidente crítico con alto impacto en el negocio y servicios que presta EJIE, además de las tareas sobre el servicio base especificadas en los capítulos previos, EJIE podrá solicitar un servicio especializado de “Respuesta ante incidentes críticos”, que incluya al menos:

- Análisis forense de los eventos, para determinar orígenes del ataque, medios utilizados y objetivos.
- Soporte especializado en la definición de las medidas de contención a aplicar, planes para la recuperación de los sistemas y preservación de evidencias.
 - Incluso podrá considerarse soporte y asesoramiento al despliegue de las medidas de contención indicadas como apoyo a los grupos de trabajo de EJIE.
- Servicios de gestión y coordinación técnica, organizativa, y de negocio de los diferentes grupos de trabajo que puedan estar involucrados, con el objetivo de reducir al mínimo posible los tiempos de recuperación de los sistemas y servicios.
- Servicios de asesoría y asistencia legal como apoyo en la ejecución de medidas legales en caso de incidentes graves de seguridad o acciones derivadas de obligaciones normativas y/o regulatorias.
- Documentación e informe del incidente desde su identificación, impacto, a las medidas para su resolución y ajustes propuestos sobre el global del servicio.

El servicio se podrá prestar de forma remota o in-situ, según el impacto del incidente en cuestión y las necesidades de recuperación de sistemas que se determinen, debiendo el adjudicatario aportar los procesos, herramientas y metodologías necesarias en cada caso.

El servicio se prestará a demanda. En EJIE, el equipo de respuesta a incidentes será un equipo multidisciplinar que decidirá en qué casos hay que recurrir a la activación de este servicio especial por parte del adjudicatario, e incluso si el impacto del incidente lo amerita, presencia in-situ de los expertos correspondientes. Se solicitará previamente a la activación una valoración.

En caso de adscribirse Osakidetza al servicio de seguridad, esta entidad podrá hacer uso directo de este servicio particular, pudiendo interactuar directamente con el SOC, de cara a la integración en los procesos de Osakidetza en caso de incidentes de ciber seguridad.

El licitador deberá realizar una propuesta con relación a este servicio, su alcance, procedimiento y metodologías a aplicar, niveles de servicio ofertados, etc. y describir la relación de *perfiles expertos* (de diferentes disciplinas: legal, experto seguridad, RRHH...) que considere necesario para la prestación de los servicios especializados de respuesta ante incidentes críticos.

Todos los perfiles propuestos dentro del servicio se cotizarán bajo el concepto de “perfil experto/jornada” incluido en el Modelo Económico, e incluirán en el coste ofertado los medios previstos para la prestación de los servicios, incluyendo posibles viajes y desplazamientos necesarios.

5.3.2 Servicio de vigilancia digital

El licitador deberá incluir en su propuesta como parte de los servicios prestados por el SOC, la prestación de un *Servicio de vigilancia digital*, que incluya la revisión de fuentes públicas y privadas para la búsqueda e investigación proactiva de amenazas externas que supongan un riesgo digital a una organización o entidad (afección en dominios, marca y reputación, fugas de información, phishing, ataques en redes sociales...). El

servicio ofertado (alcance, niveles de servicio...) deberá describirse con detalle en la propuesta técnica presentada.

El licitador deberá aportar un coste anual de servicio medido en bloques de 15 “elementos” sobre los que se preste el servicio, pudiendo ser éstos de diferentes tipos:

- Razón social
- Apps móviles
- Web
- Dominios:
 - De la organización
 - De correo
- Marcas de la organización
- Perfiles de redes sociales
- Relación de los medios de comunicación o canales oficiales.
- Direccionamiento público
- Sitio más visitado por los empleados.
- Usuarios VIP
- Etc.

EJIE podrá solicitar su activación en cualquier momento del contrato, definiéndose conjuntamente el alcance de elementos a considerar con la activación del servicio.

Las condiciones de facturación son las establecidas en el capítulo 7.7. del presente documento.

5.4 Condiciones para la prestación del servicio

A continuación, se enumeran las condiciones en las que el SOC deberá prestar los servicios solicitados en el capítulo previo:

- Modelo de atención del servicio:
 - El servicio de Monitorización de incidentes y eventos de seguridad se prestará en modalidad 24x7x365. El adjudicatario deberá disponer de mecanismos de alta disponibilidad sobre las plataformas y servicios que garanticen la prestación del servicio en estas condiciones.
 - Las labores de administración de las plataformas (EDR, SIEM) se realizarán en horario 11x5 de lunes a viernes (de 7am a 6pm de lunes a jueves; de 7am a 4pm los viernes) en línea con los horarios de los grupos de soporte de EJIE, a excepción de:
 - aquellas tareas de operación sobre las plataformas que sean necesarias para la contención de un ataque de seguridad identificado fuera del horario laboral de acuerdo a los *procedimientos de gestión y escalado de incidentes* y niveles de servicio que se acuerden.
 - aquellas tareas programadas que por su impacto en el servicio requieran su desempeño fuera de horario laboral.
 - Los servicios de Threat Hunting se desarrollarán como mínimo de lunes a viernes en horario 8x5.
 - El servicio especializado de *Respuesta ante incidentes críticos* será un servicio que se preste en modo 24x7x365.
- El SOC deberá estar físicamente ubicado en el territorio de la Unión Europea.

- El idioma de atención será el castellano.
- El almacenamiento de datos será en la nube.
 - Los datos deberán albergarse en servidores ubicados en la Unión Europea (cumpliendo la legislación vigente).
 - Se deberá ofertar un periodo de retención acorde a lo especificado en los apartados técnicos de las plataformas SIEM y EDR.
 - El adjudicatario deberá garantizar la disposición de mecanismos que garanticen la disponibilidad de los datos, su autenticidad, su integridad, su privacidad y trazabilidad.
 - En la propuesta técnica, se deberá describir cómo el licitador garantiza dichos aspectos.
- El servicio deberá integrarse con las herramientas de *ticketing* de EJIE (ServiceNow), mediante alertas que se generen de forma automática y/o manual. EJIE garantizará el acceso a dicha herramienta a los técnicos/sistemas correspondientes. (ver capítulo 5.8).
- La prestación de los servicios objeto del presente pliego conlleva el cumplimiento de unos niveles de servicio que se acordarán con EJIE en el inicio del contrato. En caso de incumplimiento se definirán las penalizaciones establecidas a tal efecto (ver capítulo 5.9).
- Para acceder a sistemas en las ubicaciones de EJIE y entidades, EJIE proporcionará los medios para posibilitar el acceso y las comunicaciones entre la infraestructura y sistemas de EJIE y los del adjudicatario.
- El licitador deberá estar en posesión de aquellas certificaciones, autorizaciones y permisos que sean exigibles por la legislación vigente para la prestación de los servicios solicitados.
- El adjudicatario deberá garantizar el cumplimiento de aquellas obligaciones legales establecidas en el ENS (Real Decreto 3/2010 de 8 enero) en lo referido a la adopción de medidas de seguridad de las soluciones tecnológicas o la prestación de servicios ofertados.
- El licitador deberá garantizar el cumplimiento del RGPD. En materia de protección de datos, las instalaciones deberán contar con las medidas de seguridad que apliquen en cada caso, conforme a lo establecido en las disposiciones legales vigentes, garantizando la confidencialidad ante terceros de la información privada de EJIE a la que tengan acceso para el ejercicio de sus funciones.

5.5 Generación de Informes de servicio

Entre los servicios solicitados se incluye el de la generación de informes personalizados relativos al servicio de seguridad prestado durante el plazo de prestación del servicio. Los informes deberán poder reportarse por entidad.

Se identifican al menos:

- Informes automáticos que se generen desde las plataformas (SIEM, EDR) de carácter periódico (diario, semanal)
- Informes mensuales de actividad/seguimiento del servicio donde se especifique:
 - Estadísticas
 - Eventos procesados
 - Resumen de incidentes gestionados
 - Ratios de falsos positivos
 - Alertas generadas
 - Ataques informados
 - Recomendaciones de mejora
 - Evolución del servicio

- Etc.
- Informe específico de incidentes de alto impacto/crítico:
 - Descripción del incidente y su estado.
 - Análisis activos afectados e impacto en el negocio.
 - Análisis forense
 - Propuesta de medidas correctivas.
 - Lecciones aprendidas
 - Etc.
- Informes mensuales con los resultados de las actividades de Threat Hunting, incluyendo posibles recomendaciones.
- Informes de ticketing (incidencias reportadas, estado de las incidencias, medición de ANSs de servicio...)
- Cuadros de mando, indicadores para toma de decisiones.
- Informes trimestrales con las propuestas de mejora derivadas de la vigilancia y evolución del servicio.

La empresa licitadora deberá detallar en su propuesta la relación de informes incluidos con la prestación del servicio (respetando al menos los solicitados en el presente documento), indicando formatos, posibles contenidos, posibilidades de personalización... mostrando ejemplos de cada uno de ellos para su valoración. Igualmente incluirá ejemplos de cuadros de mando con métricas e indicadores de servicio.

5.6 Organización y configuración del SOC

La empresa adjudicataria deberá organizar y dimensionar el equipo de trabajo para cumplir con los requisitos y alcance del servicio establecidos en el presente documento. Asimismo, deberá tener en cuenta que el proyecto de implantación es un proyecto continuo, por lo que la organización deberá ser suficientemente flexible y escalable para adecuarse al crecimiento progresivo del servicio según se incorporen nuevas fuentes a integrar, nuevos *endpoints*, etc. durante el plazo de ejecución del proyecto.

El licitador deberá describir en su propuesta la organización prevista para la prestación de los diferentes servicios de seguridad solicitados, perfiles, rol o función, jerarquías, niveles especialización, así como otras herramientas y recursos propios (colaboración o pertenencia a determinadas asociaciones, fuentes de información, certificaciones...), que aporten valor al servicio prestado.

Igualmente, el licitador deberá describir cómo dar respuesta a aquellas tareas que es necesario acometer para la implantación y puesta en marcha del servicio y las diferentes tecnologías con el inicio del contrato, así como aquellas que deriven del alta de nuevas entidades y organismos que quieran adscribirse al servicio.

5.7 Mantenimiento y soporte

El coste asociado a suscripciones relativas a las soluciones SIEM y EDR llevará implícito los servicios de soporte y mantenimiento de las soluciones, de acuerdo a lo ya referido en los apartados de *Arquitectura* para las plataformas SIEM y EDR, lo que incluye:

- Monitorización de las plataformas.
- Soporte de fabricante para ambas plataformas durante toda la vigencia del contrato
- Mantenimiento correctivo sobre las plataformas ante incidencia o mal funcionamiento de las mismas.
- Acceso a las versiones de software para el mantenimiento evolutivo de las plataformas que conformen la solución. Se requerirá que el sistema esté convenientemente actualizado (libres de

bugs vulnerabilidades, etc). El adjudicatario informará a EJIE de las vulnerabilidades de seguridad que pudieran existir en las suscripciones a las soluciones, incluyendo las valoraciones de su criticidad, y los compromisos de remediación, incluyendo medidas y plazos. En todo caso se respetará lo establecido en el procedimiento para notificaciones de incidentes de seguridad en el PCP.

La oferta que presente el licitador deberá presentar las características del servicio de soporte ofertado.

5.8 Integración con los Modelos de operación de EJIE

El adjudicatario deberá asimismo realizar los trabajos necesarios para garantizar la integración del servicio prestado por el SOC con los modelos de operación y herramientas de ticketing de EJIE, en paralelo a la puesta en marcha de los servicios objeto del proyecto, lo que incluye:

- Definir, en colaboración con EJIE, el Modelo de Servicio en lo relativo a procedimientos de atención, coordinación y escalado, categorización y tratamiento de incidentes que se identifiquen como amenaza.
 - Se incluirá igualmente el procedimiento para seguimiento de incidente notificado a EJIE hasta su cierre y documentación, cuando EJIE sea responsable de la remediación.
- Garantizar (realizando para ello los trabajos necesarios) que el servicio se presta de forma integrada sobre las herramientas de ticketing de EJIE (ServiceNow), mediante alertas que se generen bien de forma automática y/o de forma manual desde el SOC.
 - EJIE garantizará el acceso a la herramienta de ticketing (ServiceNow) a los técnicos/sistemas correspondientes.
- En el modelo deberá acordarse cómo realizar el tratamiento de alertas de indisponibilidad del servicio por parte de EJIE (fallos en las comunicaciones o en activos que generan los eventos, por ejemplo) o fallos de indisponibilidad sobre infraestructura propia del servicio (caso por ejemplo de fallo de colectores de eventos).
- Realizar la medición para seguimiento de los Niveles de servicio (ANSs) acordados para tener una referencia objetiva mensual sobre la calidad del servicio prestado (ver capítulo a continuación).

El licitador deberá realizar una primera propuesta detallada del Modelo de servicio y relacional propuesto, indicando los procesos de coordinación y escalado, tareas para integración de herramientas, aviso de alertas con origen EJIE y con origen el SOC, niveles de servicio a considerar, etc.

5.9 Niveles de servicio

La prestación de los servicios objeto del pliego conllevará el cumplimiento de una serie de niveles de servicio, y la aplicación de penalizaciones en caso de incumplimientos.

En la propuesta, el licitador deberá especificar los valores a los que se compromete con relación, al menos, a los siguientes indicadores:

INDICADOR DE SERVICIO	DESCRIPCIÓN	VALOR OBJETIVO
<i>Tiempo máximo de notificación incidente para su resolución</i>	Tiempo que transcurre desde que una alerta se origina en el sistema (SIEM), ésta es procesada (verificación de incidente categorizado) y se notifica a EJIE para su tratamiento.	*a definir por licitador

<i>Tiempo máximo de notificación incidente categorizado como CRITICO para su resolución –</i>	Tiempo que transcurre desde que una alerta se origina en el sistema (SIEM), ésta es procesada, se confirma como CRITICA y se notifica a EJIE para su tratamiento.	*a definir por licitador
<i>Eficacia en el diagnóstico de incidentes</i>	% de incidentes correctamente categorizados	>95%
<i>Eficacia en la notificación</i>	% de falsos positivos	<5%
<i>Tiempo máximo de asignación de Perfil Experto- caso de SERVICIO RESPUESTA INCIDENTE CRITICO</i>	Tiempo que transcurre desde solicitud por parte de EJIE de activación del Servicio para Respuesta ante incidentes críticos hasta la disposición de al menos de un recurso que inicie actividad	< 2 horas
<i>Tiempo máximo de respuesta para la aplicación correcta de medidas correctivas o recomendaciones de ajuste</i>	Tiempo que transcurre desde que se valida por parte de EJIE la introducción de un cambio o ajuste sobre el servicio y se inician los trabajos asociados a ese cambio.	*a definir por licitador
<i>Desviación máxima sobre los tiempos de entrega de informes de seguimiento periódicos</i>	Desviación máxima permitida sobre los plazos de entrega acordados para los informes periódicos de seguimiento de servicio	<2d

El licitador deberá realizar una propuesta de los valores objetivo a los que se compromete para los indicadores trasladados (respetando o mejorando aquellos para los que se aporta valor), y añadir los que considere para realizar un adecuado control sobre la calidad del servicio. Esta información será objeto de valoración dentro del Plan de Control de Calidad del servicio que deberá proporcionar el licitador.

En paralelo a la puesta en marcha de la solución, el adjudicatario deberá por tanto trabajar en la implantación y posterior medición de los Niveles de Servicio acordados. EJIE y adjudicatario llegarán a un acuerdo sobre el momento temporal en que se empiecen a gestionar de forma efectiva los niveles de servicio, una vez superada una primera fase de estabilización del servicio.

Con el seguimiento del servicio, se analizará el cumplimiento de los valores objetivo-comprometidos, se determinarán las penalizaciones asociadas si procede, y e igualmente se podrán introducir recomendaciones de ajuste (sobre los valores acordados, incorporando nuevos indicadores, etc.) en función de la necesidades y evolución del servicio, que deberán validarse por EJIE.

6 Proyecto para la implantación del servicio

La empresa adjudicataria deberá considerar, entre los servicios a prestar, el proyecto para la implantación y puesta en marcha de las plataformas SIEM y EDR sobre los que operará el servicio de seguridad.

Para la puesta en marcha de los servicios, se identifican al menos los siguientes trabajos a realizar por la empresa adjudicataria, que se detallan a continuación:

- Consultoría para definir la arquitectura y diseño del servicio.
- Configuración y puesta en marcha inicial de la solución SIEM.
- Configuración y puesta en marcha inicial de la solución EDR.
- Configuración y ajuste del servicio, tras aprendizaje del entorno.
- Documentación de la solución.

El adjudicatario deberá considerar que la implantación es un proceso continuo, integrando nuevas fuentes, nuevos endpoints...con vigencia en los plazos de ejecución del contrato. Así, el servicio y las plataformas quedarán operativas una vez realizados los trabajos necesarios de puesta en marcha para incluir una primera entidad en el servicio, debiendo, para las siguientes entidades y organismos, realizarse los trabajos de diseño, consultoría y configuración necesarios sobre las plataformas para la incorporación del nuevo entorno.

El coste de la implantación lo asumirá íntegramente el adjudicatario a través de los servicios prestados desde el SOC. No obstante, cuando sea una entidad u organismo que actualmente no esté en BATERA el que solicite la adscripción del servicio, los trabajos relativos a la consultoría, definición y puesta en marcha inicial del servicio para dicha entidad se cotizarán de forma independiente a los servicios prestados por el SOC.

6.1 Consultoría para el análisis y diseño del servicio

El adjudicatario deberá realizar un análisis detallado sobre las características de la infraestructura a monitorizar y el entorno IT de BATERA/entidad, que le permitan proceder con el diseño y definición de la arquitectura de la solución a desplegar.

- El adjudicatario será responsable de definir y recopilar, en colaboración con EJIE/entidad, el conjunto de datos necesarios para entendimiento del entorno IT objeto del proyecto. Esto es: infraestructura LAN/WAN, soluciones de seguridad ya desplegadas, controladores de dominio, servidores, puestos de trabajo y características, etc.
- Con la información anterior, el adjudicatario podrá:
 - Identificar y determinar, en colaboración con EJIE, las posibles fuentes a integrar (tipología de fuentes, volúmenes...)
 - Conocer el volumen de endpoints y sus características
 - Realizar un primer dimensionamiento (eventos por segundo, número de endpoints) de la solución
 - Definir la arquitectura y diseño de la solución a desplegar
- El diseño deberá tener en cuenta posibles limitaciones y requerimientos IT sobre la infraestructura del EJIE/entidad, incluyendo el relativo despliegue de colectores y recolección de eventos.
- Por último, el adjudicatario deberá elaborar un Plan de implantación, a validar por EJIE, para el despliegue y configuración de los servicios, una vez identificados y realizados los trabajos previos.

6.2 Configuración y puesta en marcha de la solución SIEM

El adjudicatario deberá proceder con la provisión e instalación de la infraestructura necesaria, así como con la configuración de la plataforma SIEM, de acuerdo al diseño y dimensionamiento establecido, y atendiendo al Plan de implantación validado. Ello incluye:

- Despliegue y configuración inicial del sistema
- Instalación y provisión de infraestructura para recolección de los logs (colectores), si procede
- Integración de las fuentes de logs y flujos, y recolección de eventos.
 - Las configuraciones necesarias sobre las fuentes a integrar para el envío de logs y flujos a la plataforma SIEM serán responsabilidad de EJIE, que contará con el apoyo del adjudicatario para la definición de las configuraciones a adoptar.
 - La solución EDR deberá integrarse como una fuente más.
- Implantación de reglas de correlación y casos de uso.
- En una primera fase, el adjudicatario realizará un *testeo del entorno y de la solución desplegada*, que permitirán un primer ajuste de la monitorización. Esto es:
 - Comprobación de configuración e integración de todos los componentes.
 - Comprobación de conectividad y recepción de logs. Verificar de envío de logs por parte de las diferentes fuentes.
 - Análisis de comportamiento sobre eventos recibidos y resultados de la correlación, chequeo sobre la generación de alarmas previstas, falsos positivos, etc.
 - Respuesta de la consola de servicio: visualización de alarmas e indicadores, informes...

6.3 Configuración y puesta en marcha de la solución EDR

Al igual que en el caso de la solución SIEM, una vez conocidos el volumen y características de los endpoints a integrar en la solución EDR, el adjudicatario deberá proceder con la configuración de la plataforma EDR y provisión de los servicios/infraestructura necesarios. Ello incluye:

- Configuración inicial del sistema
- Antes de proceder con el despliegue de la solución para cada uno de los endpoints solicitados, el adjudicatario deberá realizar un piloto productivo con un número representativo de equipos de cada entidad, que permita verificar aspectos tales como:
 - La convivencia con la solución actual de Antivirus (BitDefender en puesto de trabajo, Trendmicro en servidores) sin incidencias.
 - El comportamiento de la solución considerando diferentes sistemas operativos, diferente tipología de endpoints, etc.
 - La verificación de la correcta aplicación de las políticas de remediación acordadas.
 - Definición de los procedimientos adecuados para el despliegue de los agentes en los endpoints.
 - Etc.

El piloto estará en producción el periodo necesario para garantizar el ajuste de las configuraciones requeridas. Se deberán documentar los resultados de los pilotos tras las pruebas satisfactorias y el correcto funcionamiento de los sistemas.

Por último, el adjudicatario deberá realizar un piloto para despliegue de agentes en endpoints por cada entidad que solicite adscribirse al servicio.

- Una vez verificados los puntos anteriores y realizados los ajustes necesarios, se procederá con el despliegue progresivo al resto de equipos:
 - El adjudicatario proporcionará el software de agente y creará el paquete de configuración para su distribución.
 - EJIE será el responsable de la distribución de dicho agente en puestos una vez superado el piloto.
 - El adjudicatario realizará tareas de coordinación y seguimiento de dichos despliegues en colaboración con los grupos de soporte correspondientes.
- Al igual que en el caso del despliegue de la solución SIEM, se establecerá una primera fase de *testeo del entorno y de la solución desplegada*, que permita un ajuste posterior de la configuración, alertas, políticas de telemetría (reducir falsos positivos) etc.
- Por último, se garantizará la integración del EDR como una fuente más del SIEM.

6.4 Ajuste y acondicionamiento del servicio

Una vez operativas las plataformas SIEM y EDR, y realizado el testeo de las configuraciones preliminares establecidas, el adjudicatario deberá introducir los ajustes adicionales para un mejor acondicionamiento y personalización de la solución atendiendo a parámetros y políticas corporativas: incorporación nuevas reglas y casos de uso, configuración de cuadros de mando, inclusión de nuevas alertas, métricas e indicadores de interés, inclusión de nuevas políticas de remediación, definición de informes...

En paralelo a la puesta en marcha de la solución, el adjudicatario deberá trabajar en la integración de la operación del servicio con los modelos de operación y herramientas de ticketing de EJIE (ServiceNow), de forma que superado un periodo inicial de arranque y una vez estabilizado el servicio, sea posible medir indicadores de calidad relativos a los niveles de servicio establecidos.

6.5 Documentación del servicio

El adjudicatario deberá documentar la solución desplegada y servicio configurado, al menos:

- La arquitectura y configuración de las soluciones desplegadas para ambas tecnologías (SIEM, EDR), incluyendo:
 - Análisis técnico realizado
 - Fuentes integradas
 - Catálogo de reglas aplicadas
 - Casos de uso
 - Características de los endpoints integrados
 - Políticas de telemetría, políticas de remediación y acciones de respuesta acordadas.
 - Configuración de las consolas y cuadros de mando, indicadores, alertas configuradas, informes automáticos definidos...
- Documentación técnica (oficial) con las características de las soluciones desplegadas, manuales técnicos y operativos, etc.

La documentación deberá mantenerse actualizada con la evolución del servicio (mejoras introducidas, nuevas políticas, nuevas reglas de correlación...) e integración de nuevas entidades.

6.6 Transferencia de conocimiento con el inicio del servicio

Adicionalmente, con el arranque del servicio, EJIE podrá solicitar sesiones para la transferencia de las soluciones y servicio desplegado, orientadas principalmente al conocimiento de uso de las consolas, interpretación de alertas e indicadores, y generación de informes. Se considera al menos el siguiente contenido:

- Introducción a las tecnologías SIEM y EDR desplegadas
- Descripción del alcance del servicio prestado
- Presentación de las diferentes consolas, cuadros de mando, informes. Indicadores y alertas, uso de las consolas, búsquedas, generación de reportes...
 - Uso de las consolas.
 - Presentación e interpretación de los resultados de la Monitorización
 - Conocimiento de las métricas e indicadores
 - Reporting y modelos de informes

Se estiman en el plazo del contrato un máximo de 3 sesiones de transferencia, con un mínimo, en cada sesión, de 3 jornadas de 6 horas por jornada. El licitador deberá considerar la asistencia, en cada sesión, del entorno de 12 personas (personal de EJIE y/o de las diferentes entidades adscritas al servicio).

El adjudicatario deberá entregar manuales y documentación relativa a los temas tratados en las diferentes sesiones.

La transferencia de conocimiento tendrá lugar en las instalaciones que especifique EJIE.

6.7 Responsabilidades EJIE

Con relación a la puesta en marcha, implantación y evolución del servicio, EJIE será responsable de:

- La instalación de los agentes en los *endpoints*, una vez establecida de forma conjunta los procedimientos más adecuados para el despliegue de los agentes, según tipologías de equipos.
- Las configuraciones necesarias sobre la infraestructura propia para posibilitar el envío de logs, flujos, telemetría...a las diferentes plataformas.
- Disponer los medios para posibilitar el acceso y las comunicaciones entre la infraestructura y sistemas de EJIE y los del adjudicatario.
- Validar los cambios y recomendaciones de ajuste propuestos por el adjudicatario sobre las soluciones desplegadas.

6.8 Dimensionamiento y alcance inicial del servicio

Con carácter general, el adjudicatario deberá prestar los servicios solicitados para aquellas entidades y organismos públicos que así lo soliciten (estén o no adheridas a BATERA) en el periodo de ejecución del contrato.

El proyecto contempla como **alcance inicial la prestación del servicio para la Red de Gobierno**, con el siguiente dimensionamiento.

	GOBIERNO
ENDPOINTS	9.000
EPS (eventos por segundo)	4.000

A la fecha de formalización del contrato se adquirirán suscripciones sobre la plataforma SIEM y sobre la plataforma EDR para **3.000EPS** (Eventos por Segundo) y **3.000 endpoints**, respectivamente, que se incrementarán en el volumen adecuado de acuerdo al progreso en la implantación del servicio.

El objetivo del proyecto es el de posibilitar la prestación del servicio a otras entidades en los plazos de contrato, entre ellas entidades adheridas a BATERA, como pueden ser Osakidetza y Justizia. Se indica a continuación, y únicamente a modo de referencia, la volumetría estimada para estas entidades, sin que ello implique compromiso de ejecución por parte de EJIE.

	OSAKIDETZA	JUSTIZIA
ENDPOINTS	23.000	3.000
EPS	9.750	1.250

Se recuerda que el servicio en su conjunto (plataformas, SOC) deberá ser escalable, de acuerdo a las condiciones establecidas en el presente contrato, pudiendo EJIE solicitar el alta de nuevas suscripciones/ampliación del servicio siempre que sea viable en los plazos de proyecto y que, con la previsión añadida de nuevos servicios y suscripciones, no se supere el importe máximo de licitación al finalizar el periodo del contrato.

7 Modelo de servicio

7.1 Periodo de prestación del servicio

El servicio se prestará hasta 31/12/2023, con un plazo estimado de duración de 38 meses.

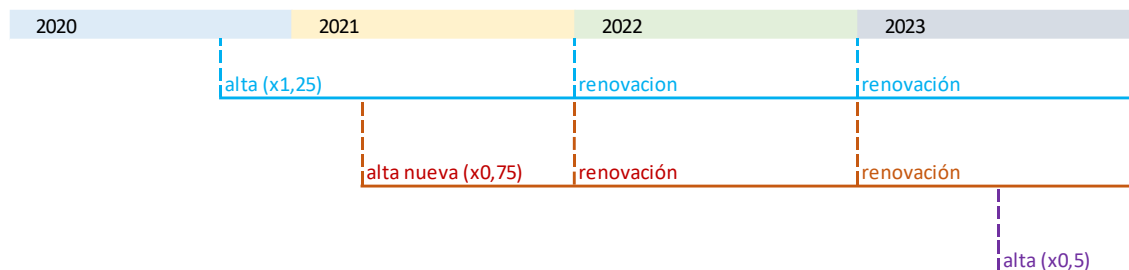
7.2 Modelo suscriptorial de las soluciones SIEM y EDR

Las soluciones SIEM y EDR se prestarán como un servicio en la nube basado en suscripciones anuales al servicio. A continuación, se describe el modelo suscriptorial solicitado para ambas soluciones y al que deberá dar respuesta el adjudicatario durante la vigencia del contrato.

- Las suscripciones deberán incluir todos los servicios y funcionalidades vinculados a las plataformas solicitados como obligatorios a través de la siguiente contratación.
- En ambos casos (SIEM, EDR) la titularidad de las suscripciones será de EJIE desde el momento de adquisición, o en su defecto, se deberá garantizar al inicio mediante documento acreditativo de fabricante, que se trasladará la titularidad de las mismas a EJIE con la finalización del contrato.
- La suscripción de la herramienta SIEM se realizará en base al número de eventos por segundo objeto de monitorización, medidos en bloques de 1000 eventos por segundo*. Las suscripciones se solicitarán en base a **bloques enteros, redondeando al número entero superior con el fin de garantizar la prestación del servicio.** Así, por ejemplo, en el caso de monitorización de 1.300EPS, se contratarían 2.000 suscripciones (2 bloques de 1.000EPS).
- La suscripción de la herramienta EDR se realizará en base al número de endpoints objeto de monitorización sobre la plataforma EDR medidos en bloques de 1000 endpoints. Las suscripciones se solicitarán en base a **bloques enteros, redondeando al número entero superior con el fin de garantizar la prestación del servicio,** aplicándose los mismos criterios que en el punto anterior.
- El tratamiento con relación al alta y renovación de suscripciones (SIEM y EDR) será el siguiente:
 - EJIE podrá solicitar altas nuevas en todo el periodo del contrato.
 - Como criterio general, toda alta solicitada tendrá asociada una duración de un año.
 - En caso de altas que tengan lugar a lo largo de cualquiera de los años de contrato, estas se regularizarán hasta el fin de año de adquisición y su coste se calculará como la parte proporcional al precio anual ofertado. Es decir, si el alta se produce, por ejemplo, el 01/10/2022, en esa anualidad se abonará por la cantidad de 0,25 veces el coste anual ofertado.
 - La renovación de la suscripción durante la siguiente anualidad se producirá de manera automática, salvo que EJIE indique lo contrario. El adjudicatario deberá realizar un aviso previo antes de la renovación, para conocimiento y toma de decisión de EJIE.
 - Como excepción: a la fecha de formalización del contrato se adquirirán suscripciones sobre la plataforma SIEM y sobre la plataforma EDR para 3.000EPS y 3.000 endpoints. En caso de que esta primera adquisición se realice antes de la finalización del año 2020, se procederá con la adquisición de las suscripciones hasta 31/12/2021, abonándose la parte proporcional correspondiente.

() En el presente expediente, los conceptos vinculados al SIEM se dimensionan en base a Eventos Por Segundo (EPS) o Flujos por Minuto (FPM). En caso de que la solución SIEM propuesta no se licencie en base a estos parámetros, será responsabilidad del licitador realizar la equivalencia a Eventos Por Segundo en los conceptos que así se requiera, siendo OBLIGATORIO presentar la equivalencia realizada.*

Como ejemplo se muestra el siguiente gráfico:



En el momento de realizar la solicitud de altas, deberá confirmarse que, con el volumen de altas solicitadas hasta la fecha y las nuevas, no se superará el importe máximo de licitación con las renovaciones que estas altas implicarían al finalizar el periodo del contrato.

7.3 Modelado del servicio prestado por el SOC

El adjudicatario deberá considerar incluidos en los costes del servicio prestado por el SOC la relación de servicios solicitados en la presente contratación (ver capítulo 5), a excepción de aquellos solicitados a demanda. El servicio se estructurará de la siguiente forma:

- *Servicios de monitorización, administración y operación de la plataforma SIEM*, relativo a la relación de servicios de seguridad prestados por el SOC mediante la explotación de dicha plataforma, incluyendo aquellos relativos a la administración y operación de la misma, así como los servicios de despliegue, implantación y evolución del servicio que estén relacionados:
 - Monitorización y correlación de eventos en tiempo real
 - Identificación y detección de incidentes, notificación, escalado
 - Definición de métricas y alertas
 - Configuración de cuadros de mando e informes
 - Administración y operación de la plataforma
 - integración nuevas fuentes, nuevas reglas...
 - Mejoras sobre el servicio
 - Etc.

Como criterio general, estos servicios se dimensionarán en base al número de bloques enteros de 1.000 eventos por segundo que se estén monitorizando en cada periodo, redondeándose al **número entero más cercano**. A modo de ejemplo:

- Si se monitorizan en el servicio 5.600EPS, entonces el servicio de SOC se dimensionará para un volumen de 6.000EPS.
 - Si se monitorizan en el servicio 5.250EPS, entonces el servicio de SOC se dimensionará para un volumen de 5.000EPS.
- *Servicios de monitorización, administración y operación de la plataforma EDR*, relativo a la relación de servicios de seguridad prestados por el SOC mediante la explotación dicha plataforma, incluyendo aquellos relativos a la administración y operación de la misma, así como los servicios de despliegue, implantación y evolución del servicio que estén relacionados:
 - Detección de actividades sospechosas en endpoints

- Planes de contención desde consola
- Actividades de Threat Hunting (aunque se considera un servicio a prestar con carácter general desde el SOC, este servicio, desde el punto de vista de facturación, se incluirá dentro de los servicios de operación y explotación de plataforma EDR).
- Administración y operación de la plataforma, integración nuevos endpoints, nuevas políticas de telemetría...
- Configuración de cuadros de mando e informes
- Mejoras sobre el servicio
- Etc.

Como criterio general, estos servicios se dimensionarán en base al número de bloques enteros de 1.000 endpoints objeto de la monitorización en cada periodo, **redondeándose al número entero más cercano**, siguiendo los mismos criterios de dimensionamiento y escalado que los indicados en el caso del SIEM.

7.4 Arranque y evolución del servicio

7.4.1 Arranque del servicio

Con idea de absorber la relación de trabajos vinculados a la puesta en marcha de plataformas, se considerará en el arranque la prestación de un servicio de SOC dimensionado para la monitorización de 3.000EPS y 3.000 endpoints, adquiriéndose las suscripciones correspondientes.

7.4.2 Evolución del servicio

Una vez que las plataformas y el servicio del SOC esté operativo y se genere la ingesta de eventos por segundo, se producirán, durante el periodo del contrato, revisiones mensuales sobre el dimensionamiento y evolución del servicio.

- Con relación a la evolución de las suscripciones sobre las plataformas SIEM y EDR:
 - Gestión de la Capacidad. Será responsabilidad del SOC alertar a EJIE cuando sea necesaria la adquisición de mayor volumen de suscripciones, con idea de que EJIE, si está de acuerdo, proceda con la solicitud de nuevas altas, teniendo en cuenta las siguientes consideraciones:
 - La plataforma SIEM deberá poder absorber picos de servicio por encima de lo contratado.
 - En caso de que se superen las suscripciones contratadas durante 4 o más días consecutivos, el SOC deberá alertar a EJIE para valorar la adquisición de nuevas suscripciones. Asimismo, se establecerán alertas sobre las plataformas para control de este aspecto.
 - La contratación efectiva a un nuevo bloque de suscripción se realizará en base a lo establecido en el capítulo 7.2.
- Con relación al dimensionamiento de los servicios prestados por el SOC:
 - Alineado con el punto anterior, a partir del incremento sostenido durante 4 o más días consecutivos sobre el número de eventos por segundo que se estén monitorizando respecto al mes anterior, se procederá con la revisión conjunta del dimensionamiento de los Servicios de monitorización, administración y operación de la plataforma SIEM, escalando de forma progresiva los recursos si es necesario.
 - Para el dimensionamiento de los servicios en bloques de servicio y su evolución, se tendrá en cuenta lo establecido en el capítulo 7.3.

- Se considera que existe necesidad de adecuar recursos, si durante 4 o más días consecutivos se supera el valor requerido que permite evolucionar al siguiente bloque de servicios.
- En el caso de los recursos destinados al SOC para la prestación de los Servicios de monitorización, administración y operación de la plataforma EDR, se procederá a la revisión y posterior regularización cuando se produzca un incremento tal sobre el número de endpoints que se requiera evolucionar al siguiente bloque de servicios, atendiendo a lo establecido en el capítulo 7.3.
- El licitador deberá explicar en su propuesta (Plan para la Evolución del Servicio) cómo garantiza el dimensionamiento y escalado PROGRESIVO de recursos del SOC con la evolución del servicio atendiendo a lo indicado en los puntos anteriores, para su valoración.
- La incorporación de nuevas fuentes y endpoints cuando una entidad ya está adscrita al servicio o se trate de una entidad BATERA se acometerán como actividades regulares a realizar por el SOC, y se ajustarán con la evolución mensual del servicio de acuerdo a lo indicado previamente.
- En las reuniones mensuales de seguimiento deberá revisarse la proyección económica del proyecto en el plazo del contrato, con el fin de poder determinar las capacidades reales de evolución y crecimiento del servicio.

7.4.3 Adscripción de nuevas entidades al servicio

Cualquier entidad y organismo público, esté adherido a o no a BATERA, podrá solicitar la adscripción al servicio durante la vigencia del contrato.

- Se recuerda que el servicio en su conjunto (plataformas, SOC) deberá ser escalable, de acuerdo a las condiciones establecidas en el presente contrato, pudiendo EJIE solicitar el alta de nuevas suscripciones/ampliación del servicio siempre que sea viable en los plazos de proyecto y que, con la previsión añadida de nuevos servicios y suscripciones, no se supere el importe máximo de licitación al finalizar el periodo del contrato.
- Con la adscripción al servicio de una nueva entidad, la empresa adjudicataria deberá considerar la ejecución de todas aquellas tareas necesarias para asegurar la correcta puesta en marcha del servicio considerando el entorno de la entidad (capítulo 6).
- No obstante, cuando una entidad u organismo que actualmente no esté en BATERA sea el que solicite la adscripción del servicio, los trabajos relativos a la consultoría, definición y puesta en marcha inicial del servicio para dicha entidad se cotizarán de forma independiente a los servicios prestados por el SOC (concepto *Alta de entidad no BATERA*).

7.5 Otras consideraciones

Para los casos en que se solicite la monitorización de flujos se aplicarán las mismas condiciones que las establecidas en los capítulos previos 7.2, 7.3 y 7.4, aplicándose la equivalencia correspondiente entre el bloque de 10.000 Flujos por Minuto y el bloque de 1.000 Eventos por Segundo. Dicha equivalencia se solicita asimismo como parte del Modelo Económico.

7.6 Devolución del servicio

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

Se identifican al menos las siguientes condiciones para su devolución:

- Las suscripciones vinculadas a los sistemas y tecnologías ofertadas serán titularidad de EJIE desde el momento de adquisición, o en su defecto, se deberá garantizar al inicio mediante documento

acreditativo de fabricante, que se trasladará la titularidad de las mismas a EJIE con la finalización del contrato.

- El adjudicatario deberá garantizar la disponibilidad de la última configuración activa de los sistemas y plataformas SIEM y EDR, para su explotación posterior por parte de EJIE.
 - Todas las configuraciones de reglas de correlación, casos de uso, políticas, etc. quedarán configuradas en el SIEM y EDR (modelo SaaS), de forma que sea posible su explotación por parte de EJIE cuando el adjudicatario deje de proveer el servicio.
- El adjudicatario deberá garantizar la disponibilidad de los logs atendiendo a los periodos de retención de logs establecidos, y condiciones de almacenamiento (on line, históricos).
- El adjudicatario deberá garantizar la disponibilidad de los elementos físicos necesarios (p.e colectores de eventos) que formen parte de la solución tecnológica desplegada.
- El adjudicatario deberá realizar la entrega de toda documentación técnica y administrativa necesaria para el traspaso del servicio.
- Asimismo, durante el último mes de servicio, 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...garantizando con ello una transición efectiva del servicio con el inicio del siguiente contrato.

Por lo tanto, el adjudicatario deberá considerar como parte del alcance de los servicios solicitados, la ejecución de todas las tareas que sean necesarias para garantizar la continuidad del servicio por parte de EJIE cuando se produzca la finalización del contrato.

Por último, el adjudicatario deberá garantizar el borrado de información sensible en los sistemas propios del adjudicatario que no pasen a ser explotados por EJIE con la transferencia del servicio, certificando mediante documento escrito la ejecución de dichos trabajos.

En caso de que el adjudicatario no garantice la entrega del servicio en las condiciones establecidas en el presente pliego, no se procederá con la última factura del servicio.

El licitador deberá describir en su propuesta técnica (Plan de transferencia del Servicio) el alcance, plazos y procedimiento propuesto para realizar de forma efectiva la transferencia del servicio con la finalización del contrato, sin pérdidas de datos ni configuración, y sin interrupción del servicio, y garantizando las mismas capacidades operativas y funcionales de los sistemas actuales.

7.7 Plan de facturación

A continuación, se describe el plan de facturación propuesto durante la vigencia del contrato, atendiendo al Modelo de Servicio y sus condiciones de evolución.

7.7.1 Conceptos de cuota variable

Entre los conceptos de cuota variable se encuentran aquellos relativos a las nuevas suscripciones/renovaciones de servicio correspondientes a las plataformas tecnológicas (SIEM, EDR) y aquellos relativos a los servicios prestados desde el SOC, vinculados en ambos casos al volumen y dimensionamiento de la solución en cada momento.

7.7.1.1 Facturación de los servicios de SOC

Las condiciones de pago serán las siguientes:

- Los servicios de SOC se abonarán mensualmente (a mes vencido) en función de los costes unitarios ofertados de acuerdo al Modelo Económico y el dimensionamiento del servicio en cada periodo (mes).
 - Los Servicios de monitorización, administración y operación de la plataforma SIEM se abonarán en base al número de bloques enteros de 1.000 eventos por segundo que se

estén monitorizando en cada periodo, redondeándose al número entero más cercano, de acuerdo a las condiciones establecidas en el capítulo 7.3. A modo de ejemplo:

- Si se monitorizan en el servicio 5.600EPS, entonces se abonarán 6 bloques de 1000EPS.
- Si se monitorizan en el servicio 5.250EPS, entonces se abonarán 5 bloques de 1000EPS.
- Los *Servicios de monitorización, administración y operación de la plataforma EDR* se abonarán en base al número de bloques enteros de 1.000 endpoints que se estén monitorizando en cada periodo, de acuerdo a las condiciones establecidas en el capítulo 7.3, siguiendo los ejemplos establecidos en el punto anterior.
 - El servicio de Threat Hunting se facturará dentro de este concepto, aunque se considera un servicio a prestar con carácter general desde el SOC.
- El número medio de eventos por segundo y endpoints que se monitorizan son parámetros que se revisarán mensualmente con la evolución del servicio. En caso de darse un incremento respecto al mes previo se procederá con la revisión de la facturación, y escalado si procede, de acuerdo a lo establecido en el capítulo 7.4.
- Con idea de absorber la relación de trabajos vinculados a la puesta en marcha de plataformas, se considerará una primera factura mensual de servicios de SOC considerando la monitorización de 3.000EPS y 3.000 endpoints, que evolucionará de acuerdo a los criterios establecidos de forma previa.
- La última factura mensual del servicio estará sujeta a la ejecución con garantías de la devolución del servicio de acuerdo a las condiciones establecidas en el capítulo 7.5.

7.7.1.2 Facturación las suscripciones SIEM y EDR

Las condiciones de pago serán las siguientes:

- Las suscripciones y su renovación tendrán un carácter anual, salvo el año de adquisición que será la parte proporcional hasta 31 de diciembre de dicho año.
 - Como excepción: a la fecha de formalización del contrato se adquirirán suscripciones sobre la plataforma SIEM y sobre la plataforma EDR para 3.000EPS y 3.000 endpoints. En caso de que esta primera adquisición se realice antes de la finalización del año 2020, se procederá con la adquisición de las suscripciones hasta 31/12/2021, abonándose la parte proporcional correspondiente.
- El pago se realizará en el mes en que se haya producido dicha solicitud/renovación.
- El importe de facturación se calculará en función de las nuevas altas/renovaciones de suscripciones que se hayan producido en el mes, de acuerdo a los costes unitarios ofertados en el Modelo Económico.
 - Las suscripciones se solicitarán en base a bloques enteros de 1.000EPS (SIEM) y 1.000 endpoints (EDR), redondeando al número entero superior con el fin de garantizar la prestación del servicio.
 - Así, por ejemplo, en el caso de monitorización de 1.300EPS, se contratarían 2 bloques de suscripciones de 1.000EPS.
 - y en el caso de monitorización de 1.900EPS, se contratarían igualmente 2 bloques de suscripciones de 1.000EPS.
 - La solicitud tanto de nuevas altas como de renovaciones estará sujeta a validación por parte de EJIE, tras notificación por parte del SOC.

- Se tendrán en cuenta el resto de las condiciones establecidas en el capítulo 7.2 con relación al modelo de suscripción solicitado. Para la evolución del servicio y escalado de las suscripciones se seguirán las condiciones establecidas en el capítulo 7.4.

7.7.1.3 Otras consideraciones

- Para los casos en que se solicite la monitorización de flujos se aplicarán las mismas condiciones de facturación que las establecidas en los capítulos previos, aplicándose la equivalencia correspondiente entre el bloque de 10.000 Flujos por Minuto y el bloque de 1.000 Eventos por Segundo para determinar las unidades (volumen) a considerar para facturar aquellos conceptos que se definen en base a bloques de 1.000 EPS según Modelo Económico.

Dicha equivalencia se solicita como parte del Modelo Económico.

- En caso de que la solución SIEM propuesta no se licencie o dimensione en base a Eventos por Segundo/Flujos por Minuto, será responsabilidad del licitador realizar la equivalencia a Eventos Por Segundo/Flujos por Minuto en los conceptos económicos que así se requiera, siendo OBLIGATORIO presentar la equivalencia realizada dentro de la propuesta.

7.7.2 Conceptos de cuota fija

Cuando sea una entidad u organismo que actualmente no esté en BATERA el que solicite la adscripción del servicio, los trabajos relativos a la consultoría, definición y puesta en marcha inicial del servicio para dicha entidad se cotizarán de forma independiente a los servicios prestados por el SOC (concepto *Alta de entidad no BATERA* en el Modelo Económico).

El pago será único, al cumplimiento del hito de su implantación, testeo, y documentación, previa aprobación por parte de EJIE, de acuerdo al coste ofertado para este concepto.

7.7.3 Conceptos a solicitud

7.7.3.1 Activación de módulos licenciados sobre las plataformas SIEM

Este capítulo se refiere a los siguientes conceptos, de los que deberá especificarse en el Modelo Económico el coste unitario anual (medido en base a bloques de 1.000 EPS) asociado a la prestación de dicho servicio:

- SIEM: Análisis de Comportamiento de Usuarios (UBA)

Se aplicarán las mismas condiciones que en el caso de las suscripciones SIEM:

- EJIE podrá solicitar el alta de la licencia del módulo correspondiente en todo el periodo del contrato.
- Su dimensionamiento estará alineado con el de las suscripciones SIEM contratadas, es decir, mismo número de bloques de 1.000EPS.
- Como criterio general, toda alta solicitada tendrá asociada una duración de un año, abonándose para la primera anualidad la parte proporcional al precio anual ofertado según momento de adquisición del servicio para EJIE y sus clientes, hasta 31 de diciembre de dicho año. EJIE determinará la renovación o no del servicio en cada caso, tras alerta previa por parte de adjudicatario de la necesidad de renovación.

7.7.3.2 Servicio de Respuesta a Incidentes Críticos

El importe correspondiente a las actividades de *Respuesta ante incidentes críticos*, siempre que haya habido solicitud formal por parte de EJIE, se abonará en un pago único, en base al número de jornadas de *Perfil Experto* efectivamente consumidas en la resolución del incidente, de acuerdo al coste ofertado para este concepto, y una vez verificado el cumplimiento de los servicios solicitados por parte de EJIE.

7.7.3.3 Servicio de vigilancia digital

Las condiciones de facturación para este servicio serán las siguientes:

- EJIE podrá solicitar la activación de este servicio en cualquier momento del contrato, teniendo el servicio una duración anual.
- El licitador deberá aportar en el Modelo Económico un coste anual de servicio medido en bloques de 15 “elementos” sobre los que se preste el servicio.
- La facturación del servicio sería mensual (a mes vencido), por bloques enteros de 15 “elementos”, de acuerdo a la parte proporcional correspondiente a una mensualidad calculada a partir del coste unitario anual ofertado.
- Durante el periodo de ejecución del contrato el volumen de bloques de 15 “elementos” sobre los que prestar el servicio, podrá verse modificado en caso de nuevas solicitudes de servicio.
- La renovación del servicio durante la siguiente anualidad se producirá a solicitud EJIE, tras alerta previa por parte de adjudicatario.

7.7.4 Otras condiciones

La adjudicación y formalización del contrato no supone en modo alguno el derecho del contratista adjudicatario de cobrar el importe total de adjudicación, ya que se trata de un presupuesto con facturación variable en base al resultado de los servicios efectivamente prestados por el contratista, aplicando a los mismos los precios unitarios según oferta adjudicada.

8 Seguimiento del servicio

8.1 Responsable del Servicio por parte de EJIE

EJIE designará un **Responsable del Servicio** que velará por el cumplimiento del alcance y objeto del contrato, lo que incluye la ejecución de las siguientes tareas:

- Realizar el seguimiento y evaluación del progreso para la implantación y puesta en marcha del servicio.
- Verificar el cumplimiento del alcance y requisitos establecidos para la prestación del servicio, y que el personal asignado por el adjudicatario para la ejecución de los servicios cuenta con los medios, capacitación técnica y soporte necesarios para la correcta ejecución de las tareas.
- Monitorizar el avance global de los servicios objeto del contrato y evaluar los resultados obtenidos en materia de seguridad y detección de amenazas.
- Analizar y validar, si procede, los cambios, recomendaciones de ajuste y en general propuestas de mejora del servicio que proponga el adjudicatario. Revisar la evolución sobre la implantación de las propuestas aprobadas.
- Verificar el cumplimiento de los acuerdos de nivel de servicio (ANS) adoptados, y determinar la necesidad de aplicación de las penalizaciones correspondientes en caso de incumplimiento.
- Validar los cambios y recomendaciones de ajuste propuestos por el adjudicatario sobre los acuerdos de nivel de servicio (ANS) y su adaptación a la evolución de los servicios.
- Trasladar solicitudes de ampliación del servicio, con la incorporación de nuevas entidades.
- Realizar seguimiento a la proyección económica del contrato y facturación del servicio.

8.2 Responsable del Servicio por parte del adjudicatario

Por parte del adjudicatario se definirá la figura del **Responsable del Servicio**, como responsable principal en la prestación de los servicios solicitados. Este perfil formará parte activa del equipo de trabajo del SOC que preste servicios a través del presente contrato, y ejercerá entre otras las siguientes funciones principales:

- Ser el interlocutor principal con EJIE para el presente contrato, actuando a su vez como responsable único del proyecto.
- Velar por el cumplimiento del alcance y niveles de servicio acordados.
- Garantizar que los recursos dispuestos en el SOC y su organización se adecua a las necesidades requeridas para la prestación de los servicios durante el plazo de ejecución del proyecto.
- Ejercer el mando y responsabilidad sobre el equipo del SOC propuesto.
- Liderar la resolución de cualquier cuestión relacionada con los servicios objeto del contrato.
- Atender a las reuniones de seguimiento periódicas que se establezcan, y otras de carácter extraordinario cuando la situación lo requiera.
- En base al seguimiento periódico del servicio e informes de actividad presentados, realizar las propuestas para la mejora continua del servicio en los plazos de ejecución del proyecto.

8.3 Seguimiento y Mejora continua del servicio

El adjudicatario deberá considerar al menos los siguientes mecanismos para el control y seguimiento del servicio:

- El adjudicatario elaborará *Informes mensuales de actividad/seguimiento* del servicio de seguridad con el resumen de eventos procesados, alertas generadas, ratio falsos positivos, etc. (ver capítulo 5.5), lo que permitirá, por un lado, medir la actividad y eficiencia de los servicios de seguridad contratados y, por otro lado, garantizar el adecuado dimensionamiento del servicio.
 - Se recuerda que los informes mensuales deberán reflejar los datos diferenciados por entidad.
- De forma adicional, el adjudicatario deberá presentar *informes mensuales con el estado de las diferentes suscripciones y de la proyección económica* del proyecto en el plazo del contrato, con el volumen de suscripciones y renovaciones involucradas hasta la fecha de elaboración del informe, con el fin de poder determinar las capacidades reales de evolución y crecimiento del servicio.
- Igualmente, se mantendrán reuniones mensuales de seguimiento para el análisis de las actividades realizadas por el SOC, donde se trabajarán, entre otros, los siguientes aspectos:
 - Análisis del cuadro de mando con las alertas e indicadores principales del servicio en tiempo real.
 - Conclusiones derivadas de los diferentes informes periódicos de actividad:
 - *Informes mensuales de actividad/seguimiento.*
 - *Informes de Threat Hunting.*
 - *Incidentes críticos en el periodo.*
 - *Informes mensuales con el estado de las diferentes suscripciones y de la proyección económica.*
 - Estado de los niveles de servicio acordados y su cumplimiento.
 - Otros
- Por último, trimestralmente, el adjudicatario realizará propuestas de mejora que redunden en una mejora en la calidad y eficiencia del servicio de seguridad prestado (cambios en políticas, nuevas reglas, mecanismos correctivos...) cuya adopción deberá ser autorizada por EJIE, pero que en ningún caso supongan modificación de los servicios, mejoras no establecidas en el pliego de condiciones particulares, ni nuevos precios.

El licitador establecerá en su propuesta un Plan de Seguimiento y control de Calidad con las metodologías, procedimientos, indicadores, etc. propuestos para el seguimiento, mejora y optimización de los servicios prestados.