Eusko Jaurlaritzaren
Informatika Elkartea

Sociedad Informática
del Gobierno Vasco

EJIE-076-2024

Suministros y Servicios para la evolución del grupo de servicios de Monitorización y Respuesta de Seguridad Avanzada.

Especificaciones de compra / Pliego de condiciones técnicas

Junio de 2024

Mediterráneo, 14 • 01010 Vitoria-Gasteiz • Posta-kutxatila / Apartado: 809 • 01080 Vitoria-Gasteiz • Tel. 945 01 73 00* • Fax. 945 01 73 01 • www.ejie.eus

Este documento es propiedad de Eusko Jaurlaritzaren 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	31/05/2024	Versión Inicial	Javier González Tavera	Josu Bagazgoitia Saez De Vicuña

Índice

1 Introducción 4

1.1 Perfil de la compañía 4
1.2 Antecedentes 5

2 Situación actual y necesidad 6

3 Objeto y Lotes del contrato 7

4 LOTE 1: Equipamiento del fabricante CrowdStrike 8

4.1 Situación actual y necesidad 8
4.2 Justificación de la tecnología 8
4.3 Objeto 9
4.4 Alcance 10
4.5 Garantía y soporte del fabricante 11

5 LOTE 2: Servicios de Soporte del grupo de servicios de Monitorización y Respuesta de Seguridad Avanzada (SOC) 13

5.1 Situación actual y necesidad 13
5.2 Objeto 13
5.3 Alcance 13
5.4 Requisitos de los servicios a prestar por el SOC 16

6 LOTE 3: Servicios Especializados de Respuesta y Evaluación de laCiberSeguridad 42

6.1 Situación actual y necesidad 42
6.2 Objeto 42
6.3 Alcance 42
6.4 Requisitos de los Servicios Especializados de Respuesta y Evaluación de laCiberSeguridad 44

1 Introducción

1.1 Perfil de la compañía

EJIE, Eusko Jaurlaritzaren 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 Jaurlaritzaren 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

En 2020 EJIE publicó el pliego EJIE-065-2020 con objeto de iniciar el camino de la Monitorización y Respuesta de Seguridad Avanzada. Desde entonces, durante los 3 últimos años, EJIE ha estado trabajando en el desarrollo del **grupo de servicios de Monitorización y Respuesta de Seguridad Avanzada,** que trata de ofrecer a las entidades adheridas a BATERA, para complementar el objetivo final del conjunto de Servicios de Seguridad ofrecidos por EJIE, que es prevenir los CiberIncidentes y, en caso de producirse, ser capaces de responder de manera adecuada.

En este contexto, se han constatado que el elemento principal que ha proporcionado cierto nivel de seguridad en la organización ha sido la plataforma de EDR (Endpoint Detection and Response). Asimismo, se ha detectado la necesidad de evolución en algunos aspectos del servicio SOC y de la plataforma de SIEM, con el objetivo de que el grupo de servicios sea más efectivo y escalable.

En paralelo, a lo largo de este periodo, las amenazas en materia de ciberseguridad han seguido evolucionando y, con objeto de adaptarse a las mismas, EJIE ha llevado a cabo un Plan de Evolución de CiberSeguridad en el cual se ponen de manifiesto una serie de necesidades que, en el ámbito de la Monitorización y Respuesta de Seguridad, están alineadas con las ya mencionadas previamente.

Con el fin de que EJIE pueda adaptarse a las nuevas necesidades en materia de CiberSeguridad y continuar ofreciendo a todas las entidades adheridas a BATERA y resto de organismos del sector público que así lo deseen un nivel de seguridad adecuado, en el marco del Plan de Evolución de los Servicios de Seguridad, se hace necesaria la contratación de servicios especializados de seguridad, que contemplen la **evolución del grupo de servicios de Monitorización y Respuesta de Seguridad Avanzada, tanto a nivel de plataformas como a nivel de servicios**, de acuerdo al alcance y requerimientos técnicos y de servicio solicitados en la presente contratación.

2 Situación actual y necesidad

En el anexo denominado Anexo I_PCT_Reservado.docx se incluye la información correspondiente a la situación actual y necesidad del presente expediente.

Esta información se considera **confidencial**, por lo cual los licitadores interesados en recibir estos datos deberán seguir las instrucciones indicadas en el **Apartado: "20.Confidencialidad" del PCP** del presente expediente y procedimiento de la claúsula 66.5 del PCP.

3 Objeto y Lotes del contrato

El objeto del presente Pliego de Condiciones Técnicas, en el marco del Plan de Evolución de los Servicios de Seguridad, consiste en la contratación de servicios especializados de seguridad, que contemplen la *evolución del grupo de servicios de Monitorización y Respuesta de Seguridad Avanzada, tanto a nivel de plataformas como a nivel de servicios*, de acuerdo al alcance y requerimientos técnicos y de servicio solicitados en la presente contratación. Esto permitirá a EJIE adaptarse a las nuevas necesidades detectadas en materia de Ciberseguridad en el ámbito de la Monitorización y Respuesta y continuar ofreciendo dichos servicios a las entidades adheridas a BATERA y resto de organismos del sector público que así lo soliciten.

El presente expediente comprende diferentes aspectos dentro del mismo grupo de servicios, por lo que se ha dividido en los siguientes lotes:

- **LOTE 1**: Equipamiento del fabricante CrowdStrike. Se trata del suministro de las suscripciones correspondientes a la renovación y evolución de la Plataforma central para la Monitorización y Respuesta de Seguridad Avanzada.
  De este modo, el adjudicatario deberá suministrar las suscripciones y su soporte de fabricante asociado, correspondiente a la solución actual del fabricante CrowdStrike y a su evolución en línea con lo detallado en el apartado correspondiente a este lote (LOTE 1: Equipamiento del fabricante). Asimismo, se podrán adquirir nuevas suscripciones durante la vigencia del contrato.

- **LOTE 2:** Servicios de Soporte del grupo de servicios de Monitorización y Respuesta de Seguridad Avanzada (en adelante, SOC). Se trata de un equipo de Soporte de Nivel 2 integrado plenamente en EJIE[1], al igual que el resto de los grupos de Soporte existentes, que se centrará principal pero no exclusivamente en la Plataforma correspondiente al LOTE 1, quedando el alcance del servicio detallado en el apartado correspondiente a este lote (LOTE 2: Servicios de Soporte del grupo de servicios de Monitorización y Respuesta de Seguridad Avanzada (SOC)).

- **LOTE 3:** Servicios Especializados de Respuesta y Evaluación de la CiberSeguridad. Se trata de un conjunto de servicios que se requiere que sean aislados de los servicios de Seguridad ya existentes, bien por nivel de especialización, bien por considerarse una “evaluación” de los servicios existentes. Este LOTE incluye servicios de DFIR (Digital Forensics and Incident Response), Ciber Ejercicios para entrenar el protocolo de respuesta a incidentes en casos de crisis, así como servicios de Red Team que permitan testear las capacidades de EJIE para protegerse, detectar y responder a Ciber Ataques, quedando detallado el alcance en el apartado correspondiente a este lote (LOTE 3: Servicios Especializados de Respuesta y Evaluación de laCiberSeguridad.).

Durante la ejecución del proyecto podrían existir relaciones y dependencias entre lotes y con otros servicios y equipos. Los responsables del proyecto en EJIE serán los encargados de coordinar su ejecución, siendo obligación de los adjudicatarios de cada lote garantizar el trabajo en equipo (comunicación y colaboración) para el correcto avance y ejecución de las tareas designadas en cada momento siguiendo las indicaciones de EJIE.

[1] Grupo de Soporte que sigue las directrices de EJIE en cuanto a metodología, procedimientos, herramientas y con una dedicación exclusiva, todo ello cumpliendo los requisitos indicados en el presente PCT.

4 LOTE 1: Equipamiento del fabricante CrowdStrike

4.1 Situación actual y necesidad

La situación actual y necesidad en materia de tecnología se ha explicado en el apartado “2 Situación actual y necesidad”.

Resumiendo lo expuesto previamente, se concluye que la actual plataforma de EDR del fabricante CrowdStrike constituye el elemento sobre el cual se debe construir la “Plataforma de Seguridad única” sobre la que centralizar los servicios de Monitorización y Respuesta de Seguridad Avanzada ofrecidos por EJIE.

4.2 Justificación de la tecnología

Con objeto de cubrir la necesidad expuesta previamente de una “Plataforma de Seguridad” orientada a la Monitorización, Detección y Respuesta, se opta por la solución que proporciona el fabricante CrowdStrike.

La justificación de esta tecnología se basa en los siguientes puntos:

- A nivel de EDR, la renovación de la solución existente manteniendo la tecnología y la configuración actual que es sólida y estable, ha sido sometida a varias pruebas con resultado satisfactorio y responde a las necesidades del Servicio. Esto hace que se reduzca el tiempo dedicado a la recogida de requisitos, diseño, pilotos y pruebas complejas, así como el tiempo de implementación y ejecución, traduciéndose todo ello en menor coste y mejor servicio.
- El despliegue de EDR que está dando servicio actualmente en EJIE se ha llevado a cabo en los últimos 3 años y alcanza a más de 48.000 Endpoints (Puestos de trabajo y servidores). Sustituir este producto por otro equivalente generaría varios inconvenientes:
    - Migración de un producto a otro, lo cual supone pagar licencias de ambos productos durante un tiempo hasta que se consigue finalizar la migración. En experiencias previas con migraciones de antivirus (producto de características similares) este proceso de migración supone varios años de trabajo.
    - Durante el tiempo de convivencia hay que gestionar dos plataformas, con las implicaciones que tiene a nivel de recursos humanos (técnicos que dominen ambos entornos) y de calidad del servicio (los equipos no migrados no contarán con las diferentes novedades hasta no estar en el nuevo entorno).
    - La migración constituiría un proyecto en sí mismo, con una dedicación y un coste
- A nivel de nuevas necesidades, los fabricantes del mercado que están realizando la evolución de sus herramientas a “Plataformas de Seguridad” que cubren las necesidades planteadas son los correspondientes a productos EDR. Esto es debido a que son las herramientas que disponen de la telemetría más abundante y relevante a nivel de Seguridad. No tendría ningún sentido replicar la información de un EDR a otro sistema puesto que supondría un coste económico muy significativo.
- El fabricante CrowdStrike, dentro de la solución ya productiva en EJIE, ofrece módulos para cubrir las necesidades ya descritas surgidas hasta el momento, todas ellas utilizando además los agentes ya desplegados en la actualidad. Esto implica que el tiempo necesario para la implantación de las nuevas funcionalidades es prácticamente inmediato, repercutiendo en la mejora del servicio en el corto plazo. Por lo cual se considera necesario dar continuidad al proceso de evolución con el suministro de nuevos módulos/elementos manteniendo el fabricante actual, ya que incorporar un nuevo fabricante, implicaría afección en los siguientes ámbitos:
    - Afección en el ámbito técnico:

- La introducción de nuevos fabricantes, diferente al actual, imposibilita realizar ciertas correlaciones o detecciones de amenazas (incluyendo, por ejemplo, acciones de Threat Hunting), por no disponer de toda la telemetría de seguridad en un único punto.
- La propia integración de una posible nueva tecnología considerando las soluciones actuales, caso de ser viable, impacta en los procesos de migración y planificación de proyecto. Se genera una dificultad real en fase de despliegue al disponerse de varias tecnologías SIEM/XDR/EDR diferentes que deberán convivir, lo que lleva implícito la necesidad de ejecución de trabajos adicionales, como son integraciones más complejas vinculadas a los procesos de despliegue y migración.

Adicionalmente, si se requiere integrar una fuente con varias tecnologías se multiplica el trabajo de integración a realizar.

- Por último, en caso de desplegarse diferentes tecnologías, las capacidades globales de las nuevas soluciones podrían verse limitadas, dependiendo de la evolución tecnológica que cada fabricante proyecte sobre su solución. Existe, por tanto, un riesgo en el medio plazo de tener que dar respuesta mediante soluciones particulares a la integración de nuevos servicios, contribuyendo a incrementar la heterogeneidad de los servicios.

- Afección en el ámbito organizativo:
  - Se incrementa la complejidad y esfuerzo a realizar para el despliegue y la operación y mantenimiento de la solución (en el día a día) derivado de:
    - La necesidad de realizar una gestión paralela sobre tecnologías/soluciones de fabricantes diferentes contra plataformas distintas.
    - La necesidad de definir procedimientos de operación y mantenimiento que tengan en cuenta ambas tecnologías, atendiendo a los modelos de relación y modelo de garantías del propio fabricante. .
    - La necesidad de disponer de recursos expertos adicionales sobre la nueva tecnología, así como de garantizar la formación de los recursos actuales en el corto plazo.
- Afección en el ámbito económico:
  - Un sobrecoste por duplicar la telemetría en varios servicios SaaS.
  - Un mayor coste en recursos, capacitación y esfuerzo, tanto en la puesta en marcha de la nueva infraestructura como en la operación y mantenimiento posterior, de acuerdo con lo ya mencionado en los puntos anteriores.

En resumen, el presente lote contempla la adquisición de equipamiento del mismo fabricante que el actual (CrowdStrike), con el fin de facilitar la explotación y operación de la solución, garantizando los tiempos de respuesta actuales sin costes adicionales.

4.3 Objeto

Este lote tiene por objeto la contratación de los suministros del fabricante CrowdStrike necesarios para la renovación y ampliación de la plataforma actual según el listado de suministros descrito en el alcance del lote.

De este modo, el adjudicatario deberá suministrar las suscripciones y su soporte de fabricante asociado correspondiente al Alcance Inicial descrito en el alcance del lote. Asimismo, se podrán adquirir nuevas suscripciones del listado de suministros durante la vigencia del contrato, según el modelo de suscripción descrito en el alcance.

4.4 Alcance

A continuación, se describe el alcance del Lote 1 a través del presente expediente.

4.4.1 Catálogo de Suministros

En el anexo denominado Anexo I_PCT_Reservado.docx se incluye la información correspondiente al catálogo de suministros del Lote 1 del presente expediente.

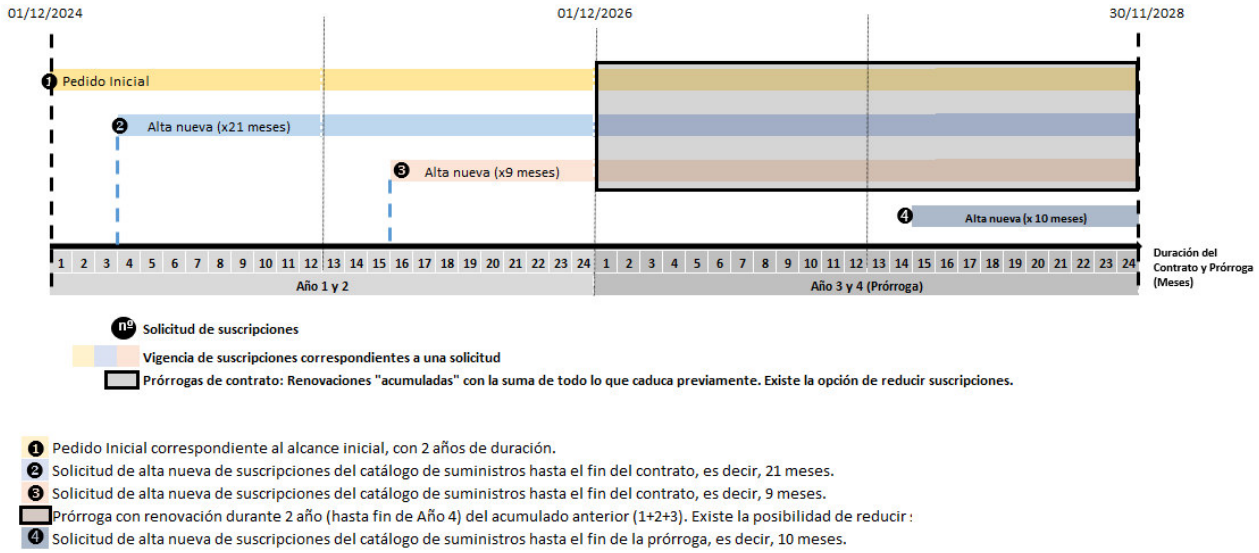
Esta información se considera **confidencial**, por lo cual los licitadores interesados en recibir estos datos deberán seguir las instrucciones indicadas en el **Apartado: "20.Confidencialidad" del PCP** del presente expediente y procedimiento de la claúsula 66.5 del PCP.

4.4.2 Modelo de Suscripción

El tratamiento con relación al alta y renovación de suscripciones será el siguiente:

- La solicitud tanto de nuevas altas como de renovaciones en la posible prórroga estará sujeta a validación por parte de EJIE.
- EJIE podrá solicitar altas nuevas durante toda la vida del contrato inicial y de la posible prórroga.
- 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 se realizará en base a las unidades definidas en cada ítem del catálogo de suministros. Se podrán adquirir bloques del tamaño que se necesite en cada caso, debiendo respetar el número mínimo en el alta inicial indicado en cada ítem.
- Como criterio general, toda alta solicitada tendrá duración hasta final del contrato inicial o de la posible prórroga.
    - El pedido inicial, asociado al alcance inicial, comenzará su vigencia el día 1 de diciembre de 2024, teniendo una duración las suscripciones correspondientes de 2 años hasta el día 30 de noviembre de 2026.
    - En caso de altas que tengan lugar a lo largo de cualquiera de los años de contrato o de la posible prórroga, estas se regularizarán hasta el fin del contrato (fin de año 2 o fin de año 4 según sea contrato inicial o prórroga respectivamente) y su coste se calculará como la parte proporcional al precio anual ofertado. Es decir, si el alta se produce, por ejemplo, el 01/03/2025, se abonará por la cantidad 1,75 veces el coste anual ofertado.
    - 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 del contrato inicial ni de la posible prórroga con las renovaciones que estas altas implicarían.
    - La renovación de la suscripción durante la prórroga se producirá de manera automática en caso de ejecutarse la prórroga, salvo que EJIE indique lo contrario. El adjudicatario deberá realizar un aviso previo antes de la renovación, con al menos 2 meses de antelación, para conocimiento y toma de decisión por parte de EJIE. Podría darse el caso de reducirse el número de licencias en la ejecución de la prórroga.
    - La facturación de las suscripciones será única por el importe completo hasta fin de contrato inicial o posible prórroga, en el momento en que la solicitud sea atendida por el adjudicatario y las suscripciones estén activas. Esto aplica a todo tipo de solicitud, incluyendo pedido inicial y renovación en la posible prórroga, correspondiendo estos dos casos a facturaciones de 2 años de suscripción completos.

Como ejemplo se muestra el siguiente gráfico:



1 Pedido Inicial correspondiente al alcance inicial, con 2 años de duración.
2 Solicitud de alta nueva de suscripciones del catálogo de suministros hasta el fin del contrato, es decir, 21 meses.
3 Solicitud de alta nueva de suscripciones del catálogo de suministros hasta el fin del contrato, es decir, 9 meses.
Prórroga con renovación durante 2 año (hasta fin de Año 4) del acumulado anterior (1+2+3). Existe la posibilidad de reducir :
4 Solicitud de alta nueva de suscripciones del catálogo de suministros hasta el fin de la prórroga, es decir, 10 meses.

En todo caso, el Adjudicatario asume que no existe ningún tipo de compromiso por parte de EJIE de agotamiento del presupuesto licitado y/o, en su caso, precio del contrato, más allá del correspondiente al Alcance Inicial descrito a continuación.

En el contexto de la renovación de licencias vigentes, es imprescindible garantizar que las renovaciones que se produzcan durante la ejecución de este contrato ofrezcan al menos las mismas funcionalidades proporcionadas por el fabricante en la actualidad. Es decir, si el fabricante introduce un nuevo modelo de licenciamiento (incluyendo cambios de nombres de SKUs o separaciones de funciones en SKUs diferentes), el adjudicatario debe adquirir las nuevas licencias necesarias que presten como equivalente al menos las funcionalidades que EJIE tenga adquiridas en cada momento. Asimismo, deberá actualizar el catálogo de suministros, manteniendo los mismos precios.

4.4.3 Alcance Inicial

En el anexo denominado Anexo I_PCT_Reservado.docx se incluye la información correspondiente al Alcance Inicial del Lote 1 del presente expediente.

Esta información se considera **confidencial**, por lo cual los licitadores interesados en recibir estos datos deberán seguir las instrucciones indicadas en el **Apartado: "20.Confidencialidad" del PCP** del presente expediente y procedimiento de la cláusula 66.5 del PCP.

4.5 Garantía y soporte del fabricante

El contratista adjudicatario deberá incluir junto con la renovación de suscripciones, la garantía y soporte de fabricante de acuerdo con las siguientes condiciones:

- Todas las suscripciones objeto de suministro deberán disponer de garantía de fabricante durante la duración del contrato o la posible prórroga.
- El tipo de soporte contratado por el licitador con el fabricante deberá ser, para todas las suscripciones, el tipo Essential (RR.HOS.ENT.ESTL)
- Este tipo de soporte incluye, al menos, servicio de TAM y ejercicios de Training por parte del fabricante.

- Se incluye el software necesario para garantizar las diferentes funcionalidades y tecnologías solicitadas, incluyendo el soporte de fabricante a lo largo del periodo indicado.
- El soporte de fabricante debe incluir, sin coste adicional, el acceso a las actualizaciones de parches, alertas de seguridad, y nuevas versiones de software durante el periodo de garantía. El suministro de la actualización incluirá tanto las licencias y software como los manuales y la documentación técnica del fabricante asociado.
- El soporte de fabricante deberá permitir lanzar consultas y gestionar incidencias en 24x7 durante la vigencia del contrato. Este servicio será para todas las suscripciones contratadas e irá incluido en el coste unitario de suscripción.

Los licitadores deberán presentar justificación de cumplimiento de garantías solicitadas para el suministro, mediante declaración responsable correspondiente (modelo Anexo VIII del PCP), de acuerdo con las condiciones establecidas en el PCP.

Dentro de los servicios incluidos en las suscripciones, se contará con soporte directo de fabricante para revisiones periódicas de la plataforma, recomendaciones, conocimiento de nuevas funcionalidades y roadmap previsto, así como para otro tipo de tareas de Mantenimiento Preventivo que permitan sacar el máximo partido a la Plataforma a todos los niveles, todo ello a través de la figura del TAM. Esta figura realizará reuniones periódicas (al menos mensuales) con EJIE y estará disponible para atender a las necesidades (consultas, etc.) que EJIE necesite trasladarle directamente o a través de sus soportes de nivel 2.

Así mismo, durante este periodo, EJIE tendrá la posibilidad, si así lo requiere, de realizar la apertura de casos y gestiones directamente con el fabricante a través de sus equipos de soporte Nivel 2 (LOTE 2 del presente pliego). En este sentido, el adjudicatario deberá habilitar los procedimientos necesarios para esta gestión (cambios de titularidad o cualquier otra modificación necesaria para este fin).

5 LOTE 2: Servicios de Soporte del grupo de servicios de Monitorización y Respuesta de Seguridad Avanzada (SOC)

5.1 Situación actual y necesidad

En el anexo denominado Anexo I_PCT_Reservado.docx se incluye la información correspondiente a la situación actual y necesidad del Lote 2 del presente expediente.

Esta información se considera **confidencial**, por lo cual los licitadores interesados en recibir estos datos deberán seguir las instrucciones indicadas en el **Apartado: "20.Confidencialidad" del PCP** del presente expediente y procedimiento de la cláusula 66.5 del PCP.

5.2 Objeto

Este lote tiene como objeto ofrecer los Servicios de Soporte del grupo de servicios de Monitorización y Respuesta de Seguridad Avanzada (en adelante, SOC). Se trata de un equipo de Soporte de Nivel 2 integrado plenamente en EJIE [2], al igual que el resto de los grupos de Soporte existentes, que se centrará principal pero no exclusivamente en la Plataforma correspondiente al LOTE 1, quedando el alcance del servicio detallado más adelante.

5.3 Alcance

5.3.1 Tecnologías

El grupo de Soporte SOC se pretende que sea un grupo de Nivel 2 dedicado a un ámbito específico dentro de los servicios de seguridad, que es el de la Monitorización y Respuesta Avanzada de Seguridad, por lo que el alcance de las tecnologías abarca todas las tecnologías presentes y futuras que EJIE incorpore en dicho ámbito.

La tecnología principal en la que estará centrado este equipo es la del fabricante CrowdStrike (LOTE 1 del presente pliego), pero se requiere que el equipo tenga asimismo conocimientos transversales de Seguridad que le permitan realizar labores de analista de ciberseguridad, automatizaciones e integraciones con otras tecnologías, propuestas de evolución en la materia que pueden implicar a otras tecnologías, etc... Asimismo, a lo largo de la vida del contrato, puede ser necesario que asuman el Nivel 2 de otras tecnologías siempre en el ámbito de la Monitorización y Respuesta Avanzada de Seguridad.

EJIE dispone de soportes avanzados, que denominaremos de tercer nivel, con sus principales proveedores tecnológicos. El servicio gestionará los distintos soportes de tercer nivel con los que EJIE cuenta dentro de su ámbito, coordinando conjuntamente las acciones que garanticen el correcto funcionamiento de los sistemas.

En el caso del fabricante CrowdStrike, el propio servicio de SOC deberá contar con los requisitos necesarios para poder tratar directamente con el fabricante como si de un Nivel 3 se tratara. Deberá poder gestionar la

[2] Grupo de Soporte que sigue las directrices de EJIE en cuanto a metodología, procedimientos, herramientas y con una dedicación exclusiva, todo ello cumpliendo los requisitos indicados en el presente PCT.

plataforma SaaS, abrir casos directamente con el fabricante y realizar todas las gestiones necesarias que garanticen el correcto funcionamiento del entorno sin necesidad de un Nivel 3 adicional.

5.3.2 Ámbito

El ámbito se limita a los Servicios de Monitorización y Respuesta Avanzada de Seguridad ofrecidos por EJIE a todos los clientes que se adscriban a dichos servicios. Estos servicios son los ya mencionados previamente en la descripción de la situación actual, pero podrían ampliarse o modificarse a lo largo de la duración del contrato.

5.3.3 Servicios

Como se ha explicado previamente, el objetivo final de los servicios de Seguridad de EJIE y, en consecuencia, de los servicios de Monitorización y Respuesta de Seguridad Avanzada ofrecidos por EJIE es tratar de prevenir los CiberIncidentes y, en caso de producirse, ser capaz de responder a ellos de la mejor manera posible.

5.3.3.1 Hitos Principales

Para lograr los objetivos ya adelantados se consideran fundamentales los siguientes hitos a lograr por el SOC:

- **Consolidación de CrowdStrike como "Plataforma de Seguridad" en el ámbito de la Monitorización, Detección y Respuesta**.
  Para lograr este hito, el SOC gestionará por completo la plataforma de CrowdStrike y llevará a cabo todas las acciones necesarias para que se convierta en el elemento central de Monitorización de la Seguridad en EJIE, persiguiendo la integración de todas las infraestructuras posibles, la explotación de la plataforma para sacarle el máximo partido a todas sus funcionalidades, trabajando en la automatización creciente de respuestas tanto a nivel de contextualización como de prevención y contención. Todo ello según las buenas prácticas marcadas por el fabricante y en línea con los acuerdos de políticas, configuraciones, nomenclaturas, procesos, etc. a los que se llegue con EJIE

- **Consolidación del SOC como el grupo de referencia en relación a la Monitorización y Respuesta de Seguridad Avanzada y, específicamente, en relación a los CiberIncidentes.**
  Dentro de esta línea el SOC trabajará para ser el grupo al que recurrir tanto para detectar incidentes de seguridad (preventiva y proactivamente) como para gestionar la respuesta ante ellos, sustituyendo a SecOps en este último rol de grupo de referencia en el servicio CSIRT para todos los CiberIncidentes gestionados por EJIE.

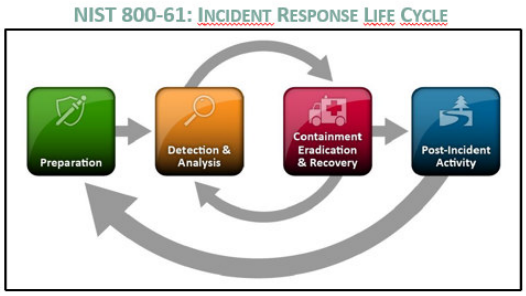
5.3.3.2 Fases del Servicio

El servicio ofrecido por el SOC pasará por varias fases, considerándose las siguientes las principales que se detallarán en el apartado 5.4.2.1.2 Fases de la Transición:

- **Transición SOC.**
- **Incorporación de nuevos módulos al Servicio**.
- **Incorporación de nuevos equipos de Hezkuntza al Servicio (EDR).**
- **Transición SecOps-CSIRT.**
- **Servicio Estable.**

5.3.3.3 Líneas de Trabajo

En cuanto a líneas de trabajo, acorde al cumplimiento del ENS y a las recomendaciones del NIST, EJIE se rige por el siguiente protocolo para la Gestión de Incidentes de Seguridad o CiberIncidentes:





Las principales líneas de trabajo en las que trabajará el SOC responderán a las diferentes fases de este protocolo, destacando:

1. **PREPARACIÓN**

   En esta fase, el SOC trabajará en todas las **medidas preventivas** que pueda ofrecer a través de las herramientas que gestione, centrándose principalmente en todas las derivadas de la Plataforma de CrowdStrike.

   A destacar, liderazgo en despliegues de ***EDR***; liderazgo en integración de fuentes en ***SIEM/XDR*** y explotación de la plataforma para activación/creación/configuración de casos de uso; liderazgo en la integración de todas las fuentes de los módulos de ***Identidad***; liderazgo en colaboración con SecOps en la explotación y aprovechamiento de los módulos de ***gestión de vulnerabilidades*** ofrecidos por la Plataforma; liderazgo en general en la puesta en marcha y aprovechamiento de los diferentes módulos disponibles en la Plataforma de CrowdStrike; liderazgo en la integración con herramienta ITSM de EJIE (***ServiceNow***); liderazgo destacado sustituyendo a SecOps en el Equipo de Respuesta a CiberIncidentes (***CSIRT***). En todo momento se entiende liderazgo como la toma de iniciativa en las diferentes tareas, impulsándolas y "tirando del carro", sin olvidar la ejecución de todas las tareas derivadas que correspondan en la plataforma de CrowdStrike.

2. **DETECCIÓN, ANÁLISIS E IDENTIFICACIÓN**

   En esta fase, el SOC trabajará en la detección, análisis e identificación de CiberIncidentes detectados principal, pero no exclusivamente, a través de la Plataforma de CrowdStrike.

   A destacar, explotación de la Plataforma para ***automatizar y optimizar el triaje, la contextualización y la clasificación de las alertas*** para ser capaces de atender al servicio según los SLAs establecidos; responsabilidad en el ***análisis e identificación de los ciberincidentes*** detectados en la Plataforma de CrowdStrike o en otros orígenes y del escalado al equipo correspondiente a través de ITSM, todo ello según marque el protocolo de Gestión de CiberIncidentes (CSIRT) a todos los niveles (procedimientos, prioridades, urgencias,…); liderazgo en la atención a incidentes derivados de tareas de ***Threat Hunting*** del fabricante CrowdStrike o de otros grupos (SecOps fundamentalmente), así como realización de actividades propias de Threat Hunting.

3. **CONTENCIÓN, MITIGACIÓN Y RECUPERACIÓN**

   En esta fase, el SOC participará principalmente en tareas de contención para que un ciberincidente no se expanda y en la mitigación para tratar de minimizar su impacto.

A destacar, liderazgo en tareas de contención (automáticas y manuales) de equipos a través del EDR; liderazgo en integraciones con otros elementos de seguridad para automatización (***SOAR***) de respuestas directas (bloqueos de IOCs, etc.) o indirectas (integraciones con ITSM u otros elementos para que otros equipos actúen rápidamente, por ejemplo); liderazgo en la explotación de la Plataforma para determinar los "paths" de ataque y poder mitigar los CiberIncidentes.

4. **ACTIVIDAD POST-CIBERINCIDENTE**

   En esta fase, el SOC participará principalmente en todas las tareas que estén a su alcance para, en caso de que vuelva a repetirse el incidente, detectarlo y detenerlo antes de que se complete.

   A destacar, liderazgo en la incorporación de fuentes a la Plataforma para centralizar la detección (casos en que los ciberincidentes no se originen en la Plataforma); liderazgo en la creación/modificación/adaptación de casos de uso para mejora la detección (casos en los que las fuentes estén integradas pero no se haya detectado nada); liderazgo en el análisis y respuesta ante ciberincidentes, bien manual o mediante automatizaciones (casos en los que se haya detectado el incidente pero no se haya hecho nada o lo que se haya hecho no haya sido suficiente).

Como se ha comentado previamente, estas son las líneas inicialmente definidas, pudiendo incorporarse nuevas líneas de trabajo a lo largo de la vida del contrato o modificarse las existentes.

5.3.4 Disponibilidad

- El servicio se ofrecerá en régimen de 24x7 (24 horas, 7 días a la semana) los 365 días del año, detallándose el Horario del Servicio en el apartado 5.4.3.4

5.4 Requisitos de los servicios a prestar por el SOC

En este apartado se recopilan una serie de requisitos de obligado cumplimiento que debe satisfacer la propuesta del licitador. **La oferta del licitador no se debe limitar a indicar el cumplimiento o no de los diferentes requisitos y a la explicación de los mismos**. El licitador debe presentar una propuesta global de servicio en la que, teniendo en cuenta dichos requisitos, explique el modo en que va a ofrecer el servicio de SOC.

5.4.1 Requisitos Globales

5.4.1.1 ITIL

EJIE, en su objetivo de ofrecer Servicios como un medio de entregar valor a los clientes, se basa en las buenas prácticas ITIL para la gestión de todos sus Servicios TI.

Adicionalmente, se hace uso de metodologías ágiles que se están promoviendo principalmente en las fases de Gestión de la Demanda y de Proyectos (Gestión de Iniciativas) para la entrega de servicios y productos, así como en las fases de Evolución de los Servicios TI.

En la línea de las buenas prácticas ITIL, el Servicio de Soporte contratado deberá participar en las principales fases del Ciclo de Vida de un Servicio IT, enumerándose a continuación dichas fases y los procesos a gestionar en cada una de ellas:

- Estrategia del Servicio
    - Definición de la estrategia.
    - Gestión del porfolio de los servicios.
    - Gestión de la demanda.
    - Gestión financiera.
    - Gestión de la relación de las ramas del negocio.

- Diseño del Servicio.
    - Monitorización y reporte del nivel de servicio.
    - Gestión del rendimiento.
    - Gestión de la disponibilidad.
    - Gestión de la capacidad.
    - Backup y recuperación.
    - Continuidad del servicio de TI y recuperación de desastres.
    - Seguridad.

- Transición del Servicio.
    - Gestión del Cambio.
    - Gestión de la Configuración.
    - Gestión de Activos.
    - Gestión de Licencias.
    - Gestión de Versiones/Entregas.
    - Gestión del Conocimiento.
    - Gestión de la Documentación.

- Operación del Servicio.
    - Gestión de Incidencias.
    - Gestión de Problemas.
    - Operación y administración.
    - Mantenimiento.
    - Gestión de Peticiones.
    - Gestión de Eventos.

- Mejora Continua del Servicio.

5.4.1.2 Herramientas de Gestión

De acuerdo al modelo de gestión de EJIE, se dispone en la actualidad de una serie de herramientas de gestión de servicios IT que también serán de aplicación para la gestión de los servicios objeto del presente pliego. La herramienta principal para esta gestión considerando los alcances ITSM, ITBM, e ITOM es ServiceNow, que es consumida por los servicios técnicos de EJIE, los servicios profesionales de entidades de EJ/GV y organismos públicos a los que EJIE da servicio, así como por los servicios técnicos contratados por EJIE. En relación a este modelo de gestión, cabe indicar los siguientes aspectos:

- El contratista adjudicatario deberá hacer uso de estas herramientas de EJIE registrando la información que se defina.
- EJIE definirá, cuantificará y proporcionará al adjudicatario los elementos necesarios para acceder a la citada plataforma ServiceNow u otras que considere de aplicación: licencias, credenciales, procedimientos, etc.
- De manera genérica estas aplicaciones serán accesibles desde Internet.
- Deberá existir colaboración por parte del operador adjudicatario para la definición y modelado de los diferentes servicios dentro de los sistemas de gestión de EJIE (ServiceNow), atendiendo a la definición del Catálogo de Servicios y tarificaciones realizada en el presente expediente, manteniendo la coherencia con la implementación ya realizada de servicios en producción.

- El contratista adjudicatario deberá realizar la entrega de la información requerida en los formatos y modelos establecidos para facilitar la carga en ServiceNow, y en general compatibles con las herramientas de gestión de EJIE
- Se requiere que el adjudicatario se responsabilice de la actualización en ServiceNow de las líneas o servicios contratados (actualización de la CMDB) según modelos definidos.
- El adjudicatario deberá velar por la calidad de los datos introducidos en la plataforma de EJIE y estos deberán estar totalmente alineados con cualquier otra información manejada por el adjudicatario en relación con los servicios prestados.
- Para realizar los contrastes de información que el adjudicatario estime oportuno, EJIE proporcionará los roles que considere adecuados para explotar la información en la plataforma ServiceNow de EJIE (acceso a informes relacionados con los servicios prestados)
- EJIE se reserva el derecho de controlar y auditar regularmente la información que el adjudicatario introduce en la plataforma, existiendo la posibilidad de aplicar penalidades asociadas a incumplimientos.

5.4.1.3 Condiciones de Seguridad

EJIE S.A. proporcionará acceso a sus sistemas informáticos y entregará la información, software y documentación necesaria para poder llevar a cabo los Servicios especificados, debiendo la empresa adjudicataria comprometerse a no utilizar para otros fines que los recogidos en el presente Pliego de Condiciones Técnicas, así como a no extraerla, cederla, publicarla o venderla total o parcialmente, ni en soporte informático ni en papel, debiendo proceder a la devolución de los soportes de la información facilitados por EJIE, S.A: , así como a la descarga de la misma de los equipos informáticos (si existieran), una vez se dé por concluido el trabajo. Queda terminantemente prohibido:

- El uso de estos recursos para actividades no relacionadas con el propósito del negocio, o bien con la extralimitación en su uso.
- Los equipos y/o aplicaciones que no estén especificados como parte del Software o de los Estándares de los Recursos Informáticos propios de EJIE o bajo supervisión de EJIE. Todos los ordenadores personales que se conecten a la red corporativa serán de las marcas y modelos homologados. El proveedor pondrá a disposición de EJIE dichos equipos para que se les instale el software necesario. Todos los ordenadores personales a los que EJIE les haya instalado software se llevarán a EJIE para que se formatee el disco duro a la finalización del servicio a EJIE.
- El proveedor se compromete a informar periódicamente a EJIE de los activos de información con los que proporciona el servicio.

Serán también de obligado cumplimiento las “Políticas de Seguridad para personal de empresas proveedoras” (accesible en la web www.ejie.eus). El servicio objeto del presente pliego se proporcionará desde las oficinas de la adjudicataria, de modo que:

- Según el apartado “Aplicabilidad de las Políticas Específicas de Seguridad para Proveedores” de dichas políticas:
  - El lugar de ejecución del servicio tendrá la consideración de “remoto”.
  - La propiedad de las infraestructuras TIC utilizadas tendrá la consideración “del proveedor”.
  - El “nivel de acceso” a los sistemas de EJIE tendrá la consideración de “con acceso privilegiado”.
- Serán de aplicación las políticas específicas de seguridad según la tabla del apartado 3.1, entre ellas las correspondientes a “seguridad física” (apartado 3.4).
- EJIE, tal como se indica en el apartado 2.6.c se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.

La adjudicataria además se compromete al cumplimiento y a proporcionar la información solicitada en el documento “Políticas de Seguridad para personal de Empresas proveedoras – Anexo - Infraestructura TIC y Seguridad física y del entorno” que se encuentra en el Anexo Seguridad de dicho documento. Esta

información será utilizada en las auditorías que se realizarán periódicamente. Será obligación de la adjudicataria proporcionar esta información anualmente y ante cualquier cambio significativo en su contenido.

Asimismo, la empresa adjudicataria está obligada a cumplir todas las reglas de seguridad referidas en el apartado “Reglas de la seguridad” del PCP.

El servicio objeto del presente pliego realizará labores de administración sobre los entornos responsabilidad de EJIE. EJIE se reserva el derecho de exigir al adjudicatario la implantación de medidas de seguridad específicas que deberá acometer en el plazo de 6 meses, suponiendo el incumplimiento de esa implantación la penalización correspondiente especificada en el PCP.

Como referencia, sin que suponga un compromiso inicial, se especifican los siguientes ejemplos de posibles elementos a exigir:

- El proveedor deberá proporcionar, bajo solicitud de EJIE, dispositivos hardware que permitan la identificación y el acceso a los sistemas con suficientes garantías. Estos dispositivos podrán ser:
  - Teléfono móvil corporativo (Android o iOS), con sistema operativo actualizado, capaz de utilizar la APP del servicio de IDaaS implantado.
  - Dispositivos hardware homologados por EJIE:
    - Compatibles FIDO FIDO Alliance - Open Authentication Standards More Secure than Passwords y Okta https://www.okta.com).
- El proveedor deberá proporcionar, bajo solicitud de EJIE, la utilización por parte de los administradores de equipos específicos (físicos o virtuales) securizados utilizados exclusivamente para las labores de administración, debiendo utilizar equipos diferentes para sus labores no administrativas (email, navegación, ofimática, etc.). Como referencia, en algunos ámbitos este tipo de soluciones se denominan Estaciones de Acceso Privilegiado (PAW).
- El proveedor deberá proporcionar a los administradores equipos securizados con tecnologías EDR y EPP.

5.4.2 Requisitos Específicos

5.4.2.1 Requisitos de Proyecto de Transición

El licitador deberá realizar su propuesta de proyecto de transición, a validar en fase de ejecución por EJIE, teniendo en cuenta la información de situación actual y los requisitos mínimos solicitados en este pliego.

El proyecto de transición lo asumirá el adjudicatario como parte del servicio, sin coste adicional al del “equipo permanente” del SOC.

5.4.2.1.1 Transición del Servicio

Como ya se ha adelantado, la empresa adjudicataria deberá considerar, entre los servicios a prestar, el proyecto de transición desde la solución actual descrita en apartados previos (2 y 5.1) a una solución basada en la “Plataforma de Seguridad de CrowdStrike”.

Así, se identifican, al menos, los siguientes trabajos a realizar por la empresa adjudicataria:

- **Módulos EDR**

  Análisis de situación, propuestas de activación y configuración de módulos no existentes hasta el momento, propuestas de mejora sobre los módulos existentes hasta el momento.

A tener en cuenta que se incorporarán una cantidad significativa tanto de equipos con el agente EDR completo como equipos con una versión del agente ligero.

- **Módulos de Exposición**

Análisis de situación, propuestas de activación y configuración de módulos no existentes hasta el momento, propuestas de mejora sobre los módulos existentes hasta el momento.

En este caso se realizará la sustitución del producto actual de análisis de vulnerabilidades por un nuevo módulo en CrowdStrike, por lo que la adjudicataria deberá considerar las migraciones/adaptaciones correspondientes.

- **Módulos de Identidad**

Análisis de situación, propuestas de activación y configuración al tratarse de un módulo no existente hasta el momento.

A tener en cuenta que en la actualidad el análisis de eventos de identidad se realiza en el actual SIEM, por lo que la adjudicataria deberá considerar la migración/equivalencia/adaptación de los casos de uso, informes y dashboards de los que se disponga actualmente.

- **Módulos de SIEM-XDR**

Análisis de situación, propuestas de activación, diseño, configuración, integración, etc. teniendo cuenta que en este caso hay que realizar una migración desde la solución de SIEM existente en la actualidad. Este módulo requerirá elementos on-premise cuya responsabilidad será del SOC y que se tendrán que tener en cuenta dentro de la propuesta del licitador (diseño, instalación, configuración, etc.), del mismo modo que habrá que considerar todas las integraciones con elementos externos, etc.

A tener en cuenta que este elemento es fundamental que esté disponible en los plazos establecidos en el apartado 5.4.2.1.2.

- **Módulos de Automatización**
  - Análisis de situación, propuestas de activación, configuración e integración.
  - A tener en cuenta que en la actualidad se realizan algunas automatizaciones básicas que habrá que migrar, si aplica.
  - Resulta crítico, como ya se ha adelantado, la integración y automatización de la integración con ServiceNow para, desde el primer momento, ofrecer el servicio completamente integrado en los sistemas de EJIE.
- **Tareas de Threat Hunting**

Análisis de situación, propuestas de acción.

5.4.2.1.2 Fases de la Transición

El servicio ofrecido por el SOC pasará por varias fases, considerándose las siguientes las principales, aunque el licitador tendrá que hacer su propuesta específica:

- **Transición SOC:**
  Durante esta fase, que tendrá una duración máxima de 1 mes, se deberá realizar una transición del actual servicio ofrecido por el SOC (CrowdStrike, Splunk, Nivel 1 y Nivel 2) actual al nuevo modelo de Servicio (CrowdStrike y Nivel 2).
  Esta fase se realizará durante el último mes del Servicio actual. Es fundamental que cuando el Servicio actual finalice su servicio, el impacto en el “Servicio de SOC” sea mínimo, para lo cual el licitador deberá hacer su propuesta de transición teniendo en cuenta que el nuevo servicio se ofrecerá por completo sobre ServiceNow cuando finalice esta fase.
  Durante esta fase, en caso de no existir licencias definitivas para alguno de los módulos, el adjudicatario hará uso de las licencias temporales que serán proporcionadas por el LOTE1.

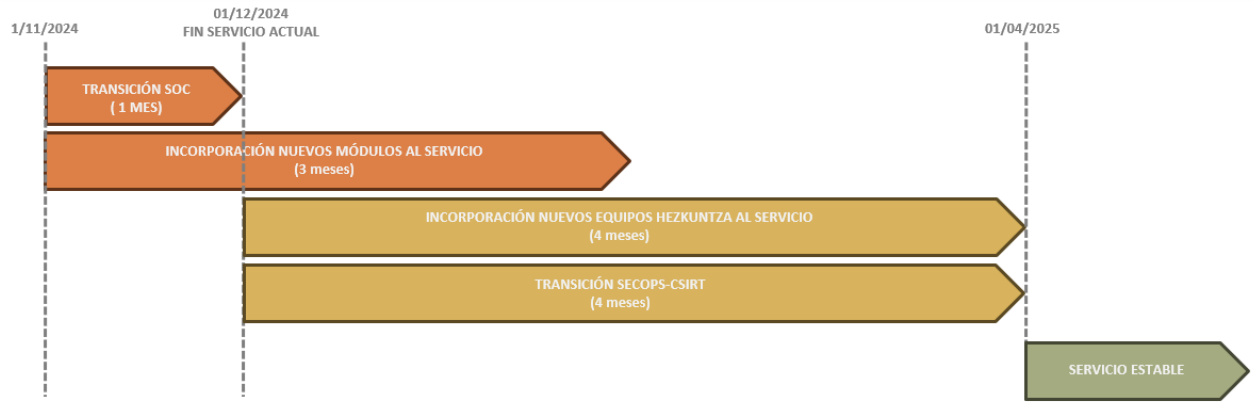
- **Incorporación de nuevos módulos al Servicio:**
  Durante esta fase, que tendrá una duración máxima de 3 meses (a comenzar 1 mes antes de la finalización del Servicio actual), se deberán diseñar, activar, configurar y poner en marcha los nuevos módulos que se incorporan a la Plataforma de Seguridad (LOTE 1 del presente pliego).
  El licitador deberá proponer el plan de incorporación de los diferentes módulos al servicio. Para ello deberá tener en cuenta que, al menos, al finalizar esta fase:
  - Los módulos equivalentes al actual SIEM deberán estar en un nivel de despliegue equivalente al actual (mínimo fuentes actuales y casos de uso equivalentes). Este hito es prioritario y debería alcanzarse lo antes posible, idealmente en el momento de finalizar el servicio actual. A posteriori, o idealmente ya en esta fase, se deberá evolucionar el nivel del servicio con automatizaciones de respuestas, nuevas fuentes, etc.
  - Los módulos nuevos (identidad, exposición) deberán estar incorporados al servicio completamente.
  - Al finalizar esta fase deberán estar finalizadas las configuraciones/automatizaciones que permitan “sustituir el nivel 1”. Esto supondrá que únicamente se producirán llamadas a la guardia del SOC cuando se produzca un CiberIncidente que, según el Procedimiento de Gestión de CiberIncidentes (CSIRT) implique un escalado a dicha guardia.

- **Incorporación de nuevos equipos de Hezkuntza al Servicio (EDR):**
  Durante esta fase, que tendrá una duración máxima de 4 meses (a comenzar desde la finalización del servicio de SOC actual), el nuevo servicio llevará a cabo el Onboarding de unos 20.000 equipos de Hezkuntza al servicio de EDR general.
  Se trata de los equipos (puestos y servidores) que NO corresponden a equipos de alumnos dentro de Hezkuntza.
  Adicionalmente, durante esta fase se incorporarán también unos 60.000 equipo de alumnos al servicio de EDR básico, participando el nuevo servicio en las tareas que le correspondan.

- **Transición SecOps-CSIRT:**
  Durante esta fase, que tendrá una duración máxima de 4 meses (a comenzar desde la finalización del servicio de SOC actual), el servicio deberá haber asumido la función de realiza el equipo de SecOps en el actual procedimiento de Gestión de CiberIncidentes.

- **Servicio Estable:**
  Superados los 4 primeros meses (a comenzar desde la finalización del servicio de SOC actual), se considera que el servicio será estable y se ofrecerá cumpliendo todos los requisitos que se indicarán en apartados posteriores. En esta fase, además del servicio habitual, será el momento de posible incorporación/onboarding de nuevos clientes, de mejora continua, etc.

En el siguiente esquema se reflejan las principales fases comentadas previamente:



El adjudicatario deberá cumplir los plazos establecidos, aplicándose una penalización con código 5 en caso de incumplimiento de plazos en alguna de las fases.

5.4.2.2 Requisitos Estratégicos

Como ya se ha comentado, el objetivo principal del SOC es el de la monitorización de eventos de seguridad, identificación, detección, alerta temprana y respuesta ante ciberincidentes, apoyándose principalmente en la "Plataforma de Seguridad" de CrowdStrike desplegada (LOTE 1).

A continuación, se resumen los principales **aspectos estratégicos** a tener en cuenta a la hora de plantear el servicio:

- **Orientación al Servicio**: El servicio del SOC se enmarca, como ya se ha explicado, dentro del conjunto de servicios de Monitorización y Respuesta de Seguridad Avanzada que ofrece EJIE en su porfolio de servicios de Seguridad. Como tal, debe existir una orientación al servicio con todo lo que ello implica a nivel de procesos, procedimientos, herramientas ITSM, documentación (para mayor detalle verificar apartado 5.4.3.7 Gestión Documental del Servicio), etc., debiendo el SOC adaptarse a lo que se le solicite para cumplir los requisitos que pueda exigir EJIE durante el contrato. En este sentido, a tener en cuenta EJIE trata de certificar sus servicios en la ISO 20.000.
- **CSIRT**: Existe un Protocolo de Gestión de CiberIncidentes que cuenta con la Plataforma de Seguridad y con el servicio del SOC como elementos fundamentales para el tratamiento de los Incidentes de Seguridad.
  El SOC participará tanto como grupo principal involucrado en el protocolo, como en la definición y evolución de dicho Protocolo en base a su experiencia y a los avances del servicio que ofrezca.
  El SOC sustituirá el rol que actualmente realiza SecOps en la gestión de todos los CiberIncidentes. Así, al menos, la responsabilidad del SOC en la gestión de los CiberIncidentes incluirá la recepción, análisis, contextualización, registro, categorización de apertura y cierre, determinación de impacto y urgencia y el escalado a grupos resolutores después de determinar qué grupos deben ser los resolutores o gestores de siguiente nivel (ciberincidentes graves) y, según el caso, incluirá incluso el seguimiento del ciberincidente hasta determinar su resolución y cierre, siendo partícipe en las actividades post-incidente con objeto de realimentar el procedimiento.
  En este rol, el SOC también participará en los escalados de los ciberincidentes a comités de crisis o a servicios DFIR (Digital Forensics and Incident Response) especializados, participando en labores de seguimiento y coordinación si fuera necesario según el caso.
- **Plataforma de Seguridad única**: EJIE ha tomado la decisión de centralizar la mayor parte de sus procesos de Monitorización, Detección y Respuesta de Seguridad en una única plataforma: **CrowdStrike**.
  Así, el SOC deberá liderar de forma proactiva la consolidación de esa plataforma, procurando la centralización e integración de todos los posibles eventos de seguridad en esta Plataforma.
- **Multitenant**: Habiendo tomado EJIE la decisión estratégica de evolucionar hacia una "Plataforma de Seguridad" única, ésta es una plataforma Multitenant y el servicio deberá plantearse como tal, dedicando un Tenant "hijo" a cada una de las entidades que se adhieran al servicio.
  Así EJIE podrá ofrecer a cada entidad un servicio a su medida sin impactar en el resto de entidades adheridas: Configuraciones, Acceso a sus datos, Dashboards, Informes, etc.
  Aunque esta situación es así actualmente para las grandes entidades, esto supondrá ajustes para acomodar las entidades más pequeñas al nuevo paradigma.
- **Servicio Gestionado**: El conjunto de servicios de Monitorización y Respuesta de Seguridad Avanzada que ofrece EJIE a través del SOC al resto de entidades se trata de un servicio gestionado. Las entidades tendrán acceso en modo lectura a su Tenant dentro de la plataforma para explotar la información como consideren oportuno, siendo responsabilidad del SOC la gestión completa de la Plataforma para ofrecer el servicio.
  Así, el SOC, además de sus tareas internas implícitas al servicio, deberá ofrecer un catálogo de servicios para poder atender las necesidades asociadas a la plataforma que puedan solicitar los clientes: Configuraciones, dashboards, informes, etc.
- **ServiceNow**: La herramienta de ITSM corporativa de EJIE es ServiceNow. Sólo se permiten integraciones con el ServiceNow corporativo desde productos propiedad de EJIE, por lo que la "Plataforma de Seguridad" de CrowdStrike deberá tener una integración directa con ServiceNow. Será

responsabilidad del SOC la configuración de esa integración en el extremo de CrowdStrike y las configuraciones necesarias para que los CiberIncidentes lleguen a ServiceNow y así puedan integrarse dentro de todo el protocolo de gestión de CiberIncidentes de EJIE.
Del mismo modo, toda la gestión de peticiones, incidencias, etc. que apliquen al SOC se realizarán a través de esta herramienta, disponiendo el SOC de un grupo dentro de esta herramienta al igual que el resto de grupos de Soporte de Nivel 2 de EJIE.
Además de ServiceNow, puede darse el caso de que haya algún cliente trabajando con su herramienta ITSM (Osakidetza con Service Manager, al menos) que haya que atender en su propia herramienta. El SOC deberá asumir esta situación mientras no se unifiquen todas las herramientas ITSM.

- **CCN-CERT**: Como ya se ha comentado, EJIE debe cumplir una serie de normativas a nivel nacional e internacional (ENS, GDPR, entre otras) que hacen que, a nivel estratégico, la gestión de Incidentes de Seguridad se haya decidido que se va a ajustar lo máximo posible al modelo definido por el Consejo Nacional de Ciberseguridad (guía nacional de notificación y gestión de ciberincidentes) para así poder atender los requisitos existentes en este ámbito.
  Esto, a efectos prácticos para el SOC, tiene implicaciones fundamentalmente en la clasificación (categoría, impacto y urgencia) de los Incidentes de Seguridad en ServiceNow y en el procedimiento de respuesta a CiberIncidentes implementado y en el que el SOC tendrá un rol principal.
- **Automatización**: Se considera estratégico hacer un esfuerzo en automatización, IA y en cualquier otra tecnología/herramienta que permita reducir hasta eliminar la carga de trabajo de poco valor añadido que tenga realizar el SOC: identificación, clasificación, contextualización, escalado, contención, etc.
  Así, el SOC deberá liderar proactivamente todas las tareas de automatización cuyo origen sean los procesos de Monitorización de Seguridad, siendo el responsable de las automatizaciones en el extremo de la Plataforma de Seguridad y cooperando con otros posibles grupos de soporte de otros entornos sobre los que se realicen las automatizaciones.
  Asimismo, el SOC será responsable de automatizar el escalado de CiberIncidentes desde la “Plataforma de Seguridad" al equipo correspondiente en ServiceNow, siendo el primer objetivo **evitar un Nivel 1** en el SOC, sustituyéndolo por automatización.
- **Soporte Nivel 2 + guardias 24x7**: Se considera fundamental que el SOC sea un grupo de soporte de nivel 2 como el resto de grupos de soporte de EJIE con todo lo que ello implica a nivel de procesos ITIL, herramientas, etc.. Esto asegurará que el equipo conoce el entorno de EJIE y sus clientes, conoce y colabora mano a mano con el resto de los grupos de EJIE y, en definitiva, está integrado en EJIE.
  El SOC atenderá en 24x7 mediante guardias los posibles incidentes de seguridad que se produzcan fuera de horas, siendo el equipo de Operación el que active dichas guardias en respuesta a incidentes recibidos vía automatización-integración de la Plataforma de Seguridad con ServiceNow.
  Así, será responsabilidad del SOC **sustituir el Nivel 1 por automatización** y asegurarse de que se escalan a ServiceNow sólo los CiberIncidentes realmente relevantes haciendo uso de las automatizaciones pertinentes.
- **Autonomía**: La seña de identidad del SOC debe ser la Excelencia en el servicio que ofrece tanto a nivel técnico como a nivel de gobernanza. Así, aunque EJIE disponga de responsables del servicio que gobiernen el servicio, el Soporte SOC debe ser un grupo autónomo, para lo cual debe demostrar dominio técnico en materia de seguridad, iniciativa/proactividad, gran implicación y capacidad de colaboración tanto con EJIE como con otros grupos de soporte, dada la transversalidad de su trabajo.
- **Colaboración**: Como ya se ha avanzado, el SOC deberá colaborar con cualquier equipo de trabajo que EJIE solicite a lo largo de la duración del contrato. Esta colaboración se realizará, al menos, a través de las herramientas ITSM e ITBM proporcionadas por EJIE (ServiceNow, ServiceManager) y de las herramientas de comunicación corporativas (Teams), aunque podría requerirse el uso de otras herramientas. Se identifican, al menos, los siguientes grupos con los que podría tener que colaborar el SOC:
  - **Niveles 1**: CAU EJIE y clientes finales, Operación/Gertu EJIE, SASU EJIE y otros clientes, Referentes en EJIE y clientes finales (informáticos, SAFIs,….)
  - **Niveles 2**: Grupos de soporte de las diferentes pilas de servicios de EJIE
  - **Niveles 3**: Soportes de fabricantes contratados por EJIE
  - **Otros**: Responsables de Seguridad de EJIE y clientes finales, Funcionales y/o equipos de desarrollo de EJIE o clientes finales.

  Entre las tareas de colaboración se incluyen tareas de transferencia del conocimiento que se pueden solicitar al SOC para EJIE, para sus clientes o para otros grupos de soporte según cada necesidad específica.

- **Estabilidad:** Para que el SOC pueda ofrecer un servicio de calidad se requiere que se ofrezca un servicio estable, sin rotación de personal. Es por ello que la adjudicataria deberá tener este punto en cuenta y se impondrán penalizaciones por excesiva rotación de los componentes presentados en la oferta técnica, reservándose EJIE, en último término, el derecho a su rescisión por incumplimiento reiterado. En este mismo sentido, y consensuado con EJIE, se fomentará la promoción interna en caso de bajas laborales de recursos adscritos al servicio.

5.4.2.3 Requisitos sobre la Plataforma de Seguridad de CrowdStrike

A continuación, se recopilan algunos de los requisitos principales del servicio en relación a la "Plataforma de Seguridad" de CrowdStrike:

- Gestión completa de la "Plataforma de Seguridad" de CrowdStrike (LOTE 1) y de todos los módulos disponibles presentes y futuros de la misma, incluyendo, al menos:
    - Diseño, configuración, mantenimiento y operación de la plataforma y de cada uno de sus módulos según las buenas prácticas de fabricante y según los acuerdos alcanzados con EJIE.

      Se incluye la puesta en marcha, con todo lo que implique, de los nuevos módulos que se activan en este pliego (ver LOTE 1) y los que se puedan activar a lo largo del contrato.
    - Gestión de usuarios y roles teniendo en cuenta el carácter multitenant de la solución.
    - 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).
        - Backups del servicio.
        - Despliegue de parches y actualizaciones.
        - Evolución y escalado de la plataforma en caso de necesidad.
    - Escalado a fabricante, cuando sea necesario.
    - Revisión, análisis y actuación en consecuencia de los informes presentados por el TAM del fabricante.
    - Seguimiento del estado de la plataforma y de todos sus módulos con el fin de asegurar que todos los servicios están activos y funcionando adecuadamente: Agentes EDR activos, fuentes SIEM o módulo de Identidad reportando, por ejemplo.
    - Evolución de la plataforma y de sus módulos (actualizaciones, nuevas funcionalidades, nuevos módulos) según vaya avanzando el roadmap de la misma y en línea con los seguimientos con fabricante y con EJIE.
    - Ejecución de procesos de "Onboarding" de nuevas entidades al servicio, con todo lo que implique a nivel de plataforma y módulos a los que se adhiera la entidad.
    - Generación y explotación de métricas, indicadores, informes y dashboards según las necesidades de EJIE y según las propuestas del SOC con objeto tanto de determinar el nivel del servicio como el estado de cada una de las entidades según lo determinado por la Plataforma y sus módulos.
    - Tratamiento completo de los ciberincidentes generados en los diferentes módulos según corresponda: Detección, filtrado, clasificación, contextualización, investigación, escalado, seguimiento, respuesta, etc.

      Todo ello tratando de minimizar el trabajo de poco valor añadido en base a automatizaciones.
    - Automatización de todas las tareas que se puedan automatizar, fundamentalmente aquellas que no aporten valor y todas aquellas que permitan mejorar el servicio en calidad, velocidad de respuesta, etc.

- Tareas de Threat Hunting sobre el conjunto de datos de la Plataforma, con sus informes y gestión correspondientes.
- Integración de IOCs en base a feeds de inteligencia. Aunque los IOCs que proporcione el propio fabricante de la Plataforma pueden ser suficientes, es importante disponer de esta posibilidad e implementar esa integración con objeto de cumplir normativa o de integrar en redes de interés, como puede ser la Red Nacional de SOCs, CyberZaintza, o similares.
- Gestión de las suscripciones y capacidad: El SOC será responsable del seguimiento del número de suscripciones consumidas por los diferentes módulos de la Plataforma y del escalado a EJIE para la adquisición de nuevas suscripciones.
  También será responsabilidad del SOC analizar el origen de los consumos de suscripciones/GB de ingesta/etc. por si se debieran a una anomalía o fallo de configuración.

Aunque la gestión completa de la plataforma será responsabilidad del SOC, puede haber otros grupos de soporte (SecOps, AT Seguridad, SASU, …) o los propios clientes que requieran accesos a la plataforma con diferentes roles. En general serán accesos de sólo lectura para consumo de logs, dashboards, informes, etc., pero podría darse el caso de que haya colaboraciones con otros grupos que realicen configuraciones sobre la plataforma. Del mismo modo, podrá haber grupos del entorno de Seguridad que colaboren con el servicio del SOC en la definición de posibles mejoras, supervisión de configuraciones, integraciones, seguimiento de ciberincidentes, indicadores, etc... El SOC colaborará en todo caso con todos los grupos implicados dada la naturaleza transversal de su labor.

- En el caso particular del módulo de SIEM/XDR, además de lo indicado a nivel de plataforma:
  - Integración de nuevas fuentes, colaborando en el filtrado de logs para evitar subir a la plataforma información que no aporte valor a nivel de Seguridad.
  - Implementación de casos de uso, correlaciones, etc. que permitan detectar ciberincidentes de manera automática.

5.4.2.4 Requisitos de Seguimiento

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, todo ello teniendo en cuenta los requisitos establecidos en este pliego.

5.4.2.4.1 Niveles de Servicio

A continuación, se indican diferentes niveles de servicio que el adjudicatario deberá cumplir a lo largo del contrato. Los valores (tiempo, umbrales, etc.) de los niveles de servicio son objeto de revisión y ajuste de forma cuatrimestral a lo largo de la vida del contrato.

5.4.2.4.1.1 Niveles de servicio ante incidencias

A continuación, se definen los conceptos a tener en cuenta para los niveles de servicio ante incidencias:

- Se entiende por tiempo de respuesta del servicio, el tiempo transcurrido desde la notificación de la avería a la adjudicataria, dentro del horario de cobertura, hasta el momento en el que el personal técnico de la adjudicataria comienza a proceder con el diagnóstico de la misma.
- Se entiende por tiempo de resolución del servicio, el tiempo que va desde la notificación de la avería a la adjudicataria, dentro del horario de cobertura, hasta el momento en que la avería está reparada o el servicio en funcionamiento.

Se deben cumplir los siguientes tiempos de respuesta y resolución según la siguiente clasificación:

- **Críticas y graves:** incidencias en el equipamiento que impidan o degraden el uso del servicio, resultando en incidencias por parte del usuario final.
- **Leves:** incidencias que no impiden el funcionamiento del servicio, pero que degradan su uso de manera leve, sin suponer incidencias de usuario final.
- **Consultas:** consultas técnicas en el ámbito de las tecnologías especificadas.

La siguiente tabla muestra los tiempos máximos a cumplir por el adjudicatario:

	Críticas y graves	**Leves**	**Consultas**
Tiempos de respuesta	15 minutos	15 minutos	-
Tiempos de resolución	4 horas (restauración) servicio)	24 horas	96 horas

5.4.2.4.1.2 Niveles de servicio ante ciberincidentes

A continuación, se definen los conceptos a tener en cuenta para los niveles de servicio ante ciberincidentes:

- Se entiende por tiempo de respuesta del servicio, el tiempo transcurrido desde la notificación del ciberincidente a la adjudicataria, dentro del horario de cobertura, hasta el momento en el que el personal técnico de la empresa adjudicataria comienza a proceder con el diagnóstico de la misma.
- Se entiende por tiempo de asignación/escalado del servicio, el tiempo que va desde la notificación del ciberincidente a la empresa adjudicataria, dentro del horario de cobertura, hasta el momento en que el ciberincidente, después de ser analizado y diagnosticado, es escalado/asignado al grupo que debe escalar la incidencia o aplicar un procedimiento de resolución de ciberincidente.

Se deben cumplir los siguientes tiempos de respuesta y asignación/escalado según la siguiente clasificación (impacto y urgencia están alineados con los criterios del CCN-CERT):

PRIORIDAD		IMPACTO				
		1- CRÍTICO (L5)	2 - MUY ALTO (L4)	3- ALTO (L3)	4 - MEDIO (L2)	5 - BAJO (L1)
PELIGROSIDAD URGENCIA	1 - CRÍTICO (L5)	1	1	1	2	3
	2 - MUY ALTO (L4)	1	1	1	2	3
	3 - ALTO (L3)	1	1	1	2	3
	4 - MEDIO (L2)	2	2	2	3	4
	5 - BAJO (L1)	3	3	3	4	4

PRIORIDAD:
4 – Baja (8x5)
3 – Moderada (8x5)
2 – Alta (24x7)
1 – Crítica (24x7)
1 – Crítica (24x7 + GiG)
1 – Crítica (24x7 + GiG + Comité de Crisis)

- **Prioridad Alta y Crítica:** Según tabla impacto y urgencia. CiberIncidentes que se atienden en 24x7.
- **Prioridad Baja y Moderada:** Según tabla impacto y urgencia. CiberIncidentes que se atienden en Horario Habitual.

	Crítica	**Alta**	**Moderada y Baja**
Tiempos de respuesta	15 minutos	15 minutos	15 minutos
Tiempos de escalado/asignación	2 horas	4 horas	8 horas

5.4.2.4.1.3 Acuerdos de Nivel de Servicio (ANS)

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.

El licitador podrá ofrecer otros ANS que complementen a los anteriores que serán valorados, durante la fase de adjudicación, de acuerdo con los criterios indicados en el pliego de condiciones particulares:

Proceso	**Descripción**	**Objetivo**	**Período de Cómputo**	**Código de penalización**
Mejora continua	% de tiempo del Servicio dedicado a Mejora Continua	>20%	Mensual	2
Mejora continua	Nº de automatizaciones (hasta automatizar todo lo viable)	>=3	Trimestral	4
Mejora continua	Nº de integraciones (hasta integrar todo lo viable)	>=2	Trimestral	4
Gestión de cambios	Nº de Intervenciones sobre los sistemas realizadas sin registrar un cambio	<1	Mensual	1
Gestión de eventos	Nº de eventos de la herramienta de monitorización modelados para la generación de incidencias automáticas en la herramienta de ticketing del Servicio (hasta tener monitorizado todo lo viable)	>=1	Trimestral	1
Gestión de CiberIncidentes	Tiempo entre ciberincidente y asignación a grupo resolutor en ServiceNow. Prioridad Media/Baja.	< 8h Horario Laboral	Mensual	1

Gestión de CiberIncidentes	Tiempo entre ciberincidente y asignación a grupo resolutor en ServiceNow. Prioridad Alta.	< 4h 24x7	Mensual	2
Gestión de CiberIncidentes	Tiempo entre ciberincidente y asignación a grupo resolutor en ServiceNow. Prioridad Crítica.	< 2h (24x7)	Mensual	3
Gestión de CiberIncidentes	Nº CiberIncidentes detectados sin logs en la Plataforma de Seguridad	<= 2	Mensual	2
Gestión de CiberIncidentes	Nº CiberIncidentes (detectables en Plataforma de Seguridad) detectados por CAU (llamada de usuario) antes que por SOC (plataforma seguridad).	<= 2	Mensual	2
Gestión de CiberIncidentes	N.º Ciberincidentes detectados en Plataforma de prioridad Alta o Crítica que no se envían a ServiceNow para escalar a guardia en 24x7	<= 1	Mensual	4
Gestión de CiberIncidentes	Nº acciones de Threat Hunting	>= 1	Mensual	2
Gestión de incidencias	% de incidencias reabiertas	< 3%	Mensual	1
Gestión de incidencias	% de incidencias críticas y graves asignadas antes de 15 minutos	>= 90%	Mensual	1
Gestión de incidencias	% de incidencias críticas y graves resueltas antes de 4 horas	>= 95%	Mensual	2
Gestión de incidencias	% de incidencias leves resueltas antes de 24 horas	>= 95%	Mensual	1
Gestión de incidencias	N.º cambios que generan incidencias críticas o graves	<1	Mensual	1
Gestión de incidencias	No atención al chat de Responsables de Incidencias Graves en Teams	<1	Mensual	3
Gestión de incidencias	N.º de quejas de clientes o asistencia técnica por resolución de incidencias o ciberincidentes críticas o graves	<1	Mensual	4
Gestión de incidencias o CiberIncidentes	Llamadas al 24x7 no atendidas o no contestadas en plazo (30 minutos).	<1	Mensual	4

Gestión de incidencias o CiberIncidentes	No presencia en EJIE del 24x7 si fuera necesario en plazo (1 hora).	<1	Mensual	4
Gestión de incidencias o CiberIncidentes	Incidencias con más de 5 días sin justificar	< 4	Mensual	1
Gestión de peticiones	% de peticiones que finalizan en plazo (según catálogo)	>= 90%	Mensual	2
Gestión de peticiones	% de peticiones que generan incidencias	<= 1 %	Mensual	3
Gestión de peticiones	Tiempo de integración de nueva fuente de datos en SIEM-XDR	<= 10 días laborables	Mensual	2
Gestión de peticiones	Tiempo de integración de nuevo caso de uso en SIEM-XDR	<= 5 días laborables	Mensual	2
Gestión de peticiones	Tiempo de integración de nuevo elemento para automatización vía SOAR	<= 10 días laborables	Mensual	2
Gestión de peticiones	Tiempo de implementación de nueva automatización en SOAR	<= 5 días laborables	Mensual	2
Gestión de peticiones	Tiempo de realización de estimación de equipo SOC puntual	<= 5 días laborables	Mensual	2
Gestión de peticiones	Tiempo de incorporación de equipo SOC puntual	<= 10 días laborables	Mensual	2
Gestión de peticiones	Peticiones de catálogo sin procedimiento operativo asociado	<1	Trimestral	1
Gestión de peticiones	% de peticiones que se registran en la categoría “Otros” del Catálogo	<=10%	Trimestral	1
Gestión de problemas	Tiempo medio para terminar un problema crítico	<=15 días	Mensual	3
Gestión de problemas	Tiempo medio para terminar un problema no crítico	<=40 días	Mensual	2
General	Cumplimiento plan entregables	100%	Mensual	2
Gestión de versiones y entregas	Cumplimiento Política de Parches	>=95%	Trimestral	2
Mantenimiento	Nº de análisis de los informes preventivos realizados en más de una semana desde su entrega a soporte	<1	Trimestral	1

Mantenimiento	N.º de incidencias registradas por la no aplicación de las medidas correctivas incluidas en informes preventivos	<1	Trimestral	3
Documentación	N.º de plataformas administradas sin documentar	<1	Semestral	2
Transferencia del conocimiento	N.º de recursos en incumplimiento de solvencia durante el contrato (caducidad de certificaciones)	<=1	Mensual	4
Transferencia del conocimiento	N.º de miembros del equipo sin haber recibido un mínimo de 20 horas de formación externa	<1	Anual	4
Transferencia del conocimiento	Personal del Equipo Técnico de Seguridad sin certificación correspondiente en vigor a los tres meses del arranque del servicio existiendo un compromiso de obtención en el Plan de Formación del Servicio	<1	Mensual	4
Estrategia del Servicio	N.º de recursos por debajo del dimensionamiento ofertado por la adjudicataria	<1	Mensual	4
Estrategia del Servicio	N.º de perfiles rechazados justificadamente por EJIE para una sustitución	<=1	Mensual	4
Estrategia del Servicio	Tiempo mínimo de solape entre un recurso entrante y uno saliente	>=15 días	Mensual	4
Estrategia del Servicio	% de rotación de recursos del servicio sobre el dimensionamiento ofertado por la adjudicataria (redondeando al alza)	<30%	Semestral	4

5.4.2.4.2 Informes y Cuadros de Mando

Además de la documentación propia del servicio, el SOC deberá generar una serie de informes y cuadros de mando de seguimiento, valorándose positivamente la generación automática de los mismos o, al menos, de todo el contenido estadístico/volumétrico de forma que el tiempo de dedicación a la generación de los informes sea mínimo y el tiempo que se dedique sea al análisis y extracción de conclusiones. La adjudicataria deberá detallar su propuesta de entregables y cuadros de mando, identificándose, al menos, los siguientes:

- Informes/Dashboards Automáticos de la Plataforma de Seguridad.
  A considerar el requisito estratégico de Multitenant y la necesidad de disponer de los diferentes indicadores de seguridad del servicio.
- Informes de seguimiento para los diferentes comités de seguimiento.

- Informes de CiberIncidentes relevantes.

  Según lo que se solicita en el Procedimiento de Gestión de Ciberincidentes, y relacionado con los requisitos del CCN-CERT a nivel de informes/notificaciones.

5.4.2.4.3 Comités de Seguimiento

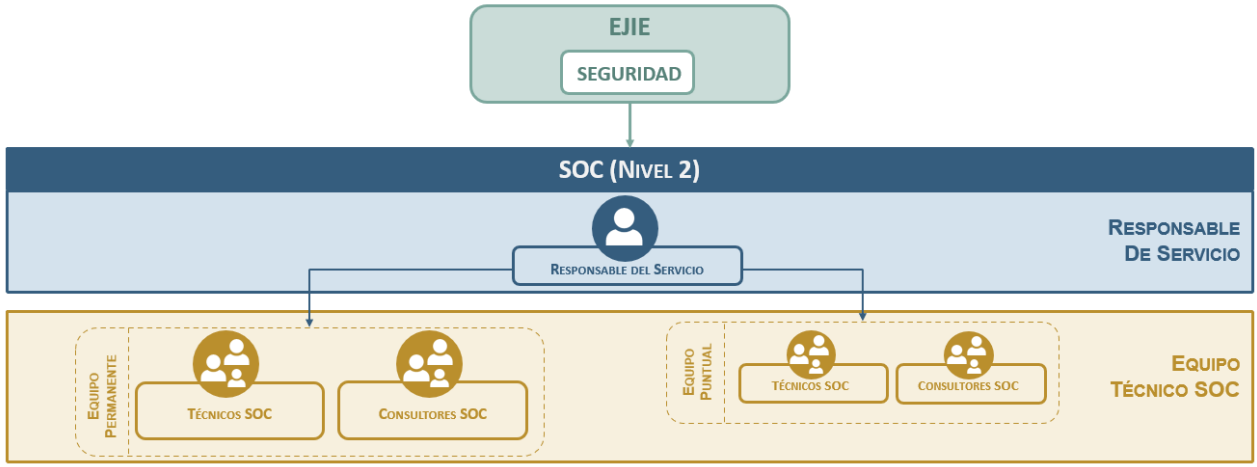
Para llevar a cabo el seguimiento del servicio existirán una serie de comités de seguimiento. La adjudicataria deberá detallar su propuesta específica de comités indicando el objetivo, frecuencia, participantes, entregables, etc. Se considera que, al menos, deberán existir los siguientes comités:

- **Operativo**: Orientado al seguimiento del día a día del SOC.
- **Ejecutivo/Estratégico**: Orientado al seguimiento del estado general del SOC y de la evolución del mismo, así como de los hitos principales del avance del servicio.
- **Directivo**: Orientados al seguimiento con los diferentes responsables jerárquicos en EJIE.

5.4.3 Planificación y Organización del Servicio SOC

5.4.3.1 Organigrama del Servicio

Teniendo en cuenta que se trata de un grupo de Soporte de nueva creación, en principio, no se establece por parte de EJIE ningún organigrama del Servicio más allá de los siguientes puntos (el número de recursos pintado en el esquema no es vinculante):



Como se observa en el esquema:

- El servicio dependerá del grupo de Seguridad dentro de EJIE.
- **Responsable del Servicio**: Deberá existir la figura de un Responsable del Servicio dentro del equipo.
- **Equipo Permanente**: Se determina que existirá un número de técnicos que formarán parte del equipo de forma continua a lo largo del contrato, existiendo dos perfiles de especialización de técnicos que se han denominado “Técnicos SOC” y “Consultores SOC”.
- **Equipo Puntual**: Como se ha adelantado previamente, el licitador deberá poder acometer, sin afección al servicio, la incorporación de nuevas entidades al servicio u otro tipo de actividades puntuales que

requieran una carga de trabajo superior a la habitual. Para ello deberá contar con personal que pueda incorporarse de manera puntual al servicio para realizar este tipo de actividades no habituales. Del mismo modo que en el equipo permanente, existen los mismos perfiles de especialización.

La empresa adjudicataria deberá organizar el equipo de trabajo y asignar los roles que considere a cada perfil para cumplir con los requisitos y alcance del servicio establecidos en el presente documento. Asimismo, deberá tener en cuenta que el Servicio de SOC 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 funcionalidades, nuevas entidades, etc. durante el plazo de ejecución del contrato, pudiendo requerirse a lo largo del contrato la incorporación de técnicos permanentes adicionales a los que se indicarán en el dimensionamiento inicial del servicio.

5.4.3.2 Equipo de trabajo

5.4.3.2.1 Roles y ámbito de responsabilidad

El licitador deberá describir en su propuesta la organización prevista para la prestación del servicio solicitado, perfiles, roles, funciones, jerarquías, niveles especialización, tareas, etc. Asimismo, describirá el modo en que activará los técnicos con participación puntual ante situaciones que requieran mayor carga de trabajo.

Igualmente, el licitador deberá describir cómo dar respuesta a aquellas tareas que es necesario acometer para la transición del servicio actual y la puesta en marcha del “nuevo” servicio y las diferentes tecnologías con el inicio del contrato. El licitador debe tener en cuenta que pasará de un servicio con un Nivel 1 en 24x7 a un servicio en el que no existe ese Nivel 1, lo cual, hasta que el SOC automatice y tunee la integración y filtrado de ciberincidentes puede suponer un número destacable de llamadas a la guardia 24x7 del Nivel 2.

5.4.3.2.2 Dimensionamiento

Los recursos con los que se dimensione inicialmente el servicio dependerán de las ofertas presentadas, pero se considera, y por tanto es un requisito mínimo, que para cubrir los perfiles planteados al menos es necesario que el **equipo permanente inicial** tenga la capacidad equivalente a 6.800 horas de dedicación en un periodo de un año:

Perfil	Dedicación Mínima (horas/año)
Responsable del Servicio (Equipo Permanente)	700
Consultor SOC (Equipo Permanente)	2.700
Técnico SOC (Equipo Permanente)	3.400
TOTAL	**6.800**

(*) El Responsable del Servicio podrá desempeñar también el perfil de Consultor SOC, siempre y cuando cumpla con la solvencia exigida para dicho perfil.

Con la intención de fomentar la estabilidad del grupo de trabajo y el mantenimiento de la calidad global del servicio, a lo largo de la vigencia del contrato, podrán imponerse penalizaciones por excesiva rotación de los componentes presentados en la oferta técnica, reservándose EJIE, en último término, el derecho a su rescisión por incumplimiento reiterado. En este mismo sentido, y consensuado con EJIE, se fomentará la promoción interna en caso de bajas laborales de recursos adscritos al servicio.

Como se ha adelantado, pueden darse situaciones temporales en las que se requiera incorporar a personal de lo que se ha denominado "**equipo puntual**" dentro del equipo técnico del SOC. La incorporación de este personal se dará bajo las siguientes condiciones:

- La necesidad de una carga de trabajo adicional podrá iniciarse tanto por parte de EJIE como por parte del propio SOC ante diferentes situaciones, siendo las más típicas la incorporación de nuevas entidades o la integración de nuevos módulos o funcionalidades.
- El equipo permanente de SOC realizará una estimación de los recursos necesarios: N.º Recursos, Perfil, Duración (en jornadas) de la necesidad, Datos de los técnicos propuestos (Experiencia y certificaciones al menos).
  El plazo máximo para realizar la estimación desde el momento de la solicitud por parte de EJIE será de 5 días laborables.
- EJIE deberá autorizar la incorporación de recursos puntuales tras analizar y aprobar la estimación propuesta por el SOC permanente.
- El plazo máximo de incorporación de los recursos puntuales desde el momento en que se autorice la estimación será de 10 días laborables.
- Si hiciera falta ampliar la estimación inicial, el SOC realizará una nueva estimación y EJIE volverá a realizar el proceso de análisis y aprobación correspondiente. La necesidad de ampliación deberá estar claramente justificada por parte del SOC.
- La adjudicataria llevará un control de todas las dedicaciones de recursos por parte del "equipo puntual" del SOC.
- La adjudicataria llevará un control económico para evitar que con las nuevas incorporaciones se supere el importe máximo de licitación del contrato inicial o de la posible prórroga.

La facturación de estos recursos se realizará según se indique en el PCP en base a los precios para cada uno de los perfiles que se determinarán en el modelo económico.

Como ya se ha adelantado, a lo largo del contrato, podría determinarse la necesidad de **incorporar personal** con el rol técnico o consultor de SOC **al equipo permanente**. La incorporación de este personal se dará bajo las siguientes condiciones:

- La necesidad de incorporar personal adicional al equipo permanente podrá iniciarse tanto por parte de EJIE como por parte del propio SOC.
- El equipo permanente de SOC realizará un análisis y justificación de la necesidad.
  El plazo máximo para realizar el análisis y justificación desde el momento de la solicitud por parte de EJIE será de 15 días laborables.
- EJIE deberá autorizar la incorporación de recursos permanentes tras analizar la justificación preparada por el SOC permanente.
- El plazo máximo de incorporación de los recursos permanentes desde el momento en que se autorice la estimación será de 30 días laborables.
- La adjudicataria llevará un control económico para evitar que con las nuevas incorporaciones se supere el importe máximo de licitación del contrato inicial o de la posible prórroga.

La facturación de estos recursos se realizará según se indique en el PCP en base a los precios para cada uno de los perfiles que se determinarán en el modelo económico.

5.4.3.2.3 Dedicación

Idealmente, todos los recursos adscritos al equipo permanente servicio que se utilicen para cubrir el mínimo de horas exigidas tendrán una dedicación del 100% durante toda la ejecución del contrato.

No obstante, se permite que el Responsable del Servicio y un Consultor tengan una dedicación menor, siempre y cuando esta no sea inferior a 700 horas y 1000 horas respectivamente. En estos casos, el adjudicatario deberá reportar mensualmente la dedicación de los técnicos no dedicados al 100% al servicio según modelo proporcionado por EJIE.

5.4.3.2.4 Lugar de trabajo

Por regla general, los recursos adscritos al servicio deberán prestar sus servicios y desarrollar sus trabajos desde la ubicación o ubicaciones designadas en la oferta, que en ningún caso podrá ser en ubicaciones de EJIE y/o de las entidades cliente de EJIE, tanto si se plantea una única ubicación (única principal) como si se plantean varias (principal + adicionales), con objeto de garantizar una correcta comunicación y coordinación dentro del equipo y las sinergias entre los diferentes roles.

Los requisitos asociados al lugar de trabajo se encuentran en el PCP del presente pliego.

5.4.3.3 Actualización tecnológica

En el transcurso de la ejecución del contrato el servicio deberá recepcionar las nuevas tecnologías/módulos que vayan surgiendo a lo largo de su vigencia, fijándose para cada una los plazos en los que se deberán asumir. Adicionalmente la adjudicataria deberá formar y, si procediera, certificar durante ese plazo a un mínimo de los técnicos adscritos al servicio. La certificación a obtener será aquella que EJIE estime necesaria para garantizar una gestión óptima de la nueva tecnología/módulo implantado. El incumplimiento de este punto será objeto de penalización.

En el caso particular de la plataforma de seguridad de CrowdStrike, además de las certificaciones correspondientes solicitadas en la solvencia del pliego de condiciones particulares, el adjudicatario deberá certificar, al menos, a 2 componentes del equipo permanente en las nuevas certificaciones que CrowdStrike publique y correspondan a módulos que estén en uso en EJIE, disponiendo de un plazo de 6 meses para ello.

Además del cumplimiento efectivo de los requisitos de solvencia exigidos en el pliego de condiciones particulares, se deberá garantizar su mantenimiento a lo largo del contrato. En el caso de que no se llegue a las adaptaciones requeridas podrá conllevar la aplicación de las penalizaciones establecidas.

Sin perjuicio de lo anterior, durante la vigencia del contrato, y ante la identificación de una deficiencia o necesidad estratégica, EJIE podrá solicitar a la adjudicataria del servicio adaptar/certificar a un determinado número de recursos en tecnologías existentes. La adaptación/certificación, nivel de la misma, número de recursos afectados y plazo máximo de obtención se establecerán de mutuo acuerdo entre EJIE y la adjudicataria siendo, en todo caso, responsabilidad y obligación de la adjudicataria la adaptación/certificación de los recursos sin coste asociado para EJIE.

5.4.3.3.1 Plan de Formación y actualización tecnológica

El objetivo de este plan es plasmar la planificación relativa a la formación de los integrantes del servicio al inicio y durante el transcurso del mismo velando en todo momento por su transversalidad y reflejando la vigencia de las certificaciones que la acreditan.

Como parte de la oferta presentada, el licitador deberá presentar un Plan de Formación y actualización tecnológica que, al menos, deberá contener:

- Objetivos.
- Descripción de la metodología de formación que seguirá la adjudicataria con sus trabajadores detallando, al menos, la formación inicial y la formación continua asociada al proyecto en relación a su ámbito, tipología, formato, contenido, fases, personal docente y forma de evaluación de su aprovechamiento.
- Compromiso, planificación, mapa de conocimiento y cronograma de certificaciones. Desde EJIE se exige la realización de **al menos 20 horas de formación externa** anuales por cada miembro del equipo de trabajo.
- Estrategia de cara al aseguramiento de la transversalidad evitando nichos de conocimiento.

El mapa de conocimiento deberá ofrecer una instantánea del dominio de las tecnologías/módulos existentes en el servicio con objeto de detectar posibles lagunas de conocimiento que pudieran tener un impacto pernicioso en el soporte al Servicio. Deberá indicar las fechas de caducidad de las certificaciones de fabricante en él incluidas y actualizarse ante cualquier modificación del equipo de trabajo adscrito al servicio o, en su defecto, cuatrimestralmente

5.4.3.4 Horario del Servicio

El servicio se ofrecerá en régimen de 24x7x365 (24 horas, 7 días a la semana) los 365 días del año, siendo los niveles de actuación los siguientes:

- **Horario habitual** (salvo festivos de ámbito nacional y autonómico. Los festivos locales y provinciales computarán dentro del horario habitual):
  - Jornada partida: lunes a jueves: 7:00h a 18:00h. Viernes: 7:00h a 16:00h.
  - Jornada continua: lunes a viernes: 7:00h a 16:00h.
- **Horario extendido**:
  - Horario no incluido en el horario habitual durante los días laborables, las 24 horas de los fines de semana y los festivos de ámbito nacional y autonómico.

5.4.3.4.1 Requerimientos en horario habitual

El adjudicatario deberá organizar al SOC para que, durante el horario habitual, el servicio esté atendido constantemente.

El adjudicatario deberá proporcionar un teléfono de contacto único que permita contactar con los técnicos asociados al servicio, independientemente de la oficina designada en la que estén ubicados.

El adjudicatario deberá asegurar que ese teléfono será atendido en todo momento por alguno de los técnicos asociados al servicio durante el horario habitual.

5.4.3.4.2 Requerimientos en horario extendido

Deberá garantizarse una disponibilidad 24x7x365 fuera del horario habitual de EJIE para la atención de incidencias y/o incidentes de seguridad y/o intervenciones planificadas. El coste asociado a esta disponibilidad estará incorporado en el coste horario de los diferentes perfiles.

Se debe contemplar el servicio en horario extendido, fijándose 3 niveles de actuación:

- Soporte de atención telefónica.
- Acceso vía Internet/VPN.
- Presencia in situ.

El **tiempo de respuesta** deberá ser como máximo de 30 minutos desde que se solicita una actuación, independientemente del método utilizado para la resolución de la incidencia. El **tiempo de presencia in situ**, si fuera necesario, deberá ser como máximo de 1 hora.

Este servicio fuera de horas **deberá ser atendido por los mismos técnicos** que conforman el servicio en "Horario Habitual".

El adjudicatario deberá proporcionar un teléfono de guardia único que permita contactar con los técnicos asociados de guardia, independientemente del técnico o técnicos que estén ofreciendo el servicio de guardia. Idealmente, el teléfono podría ser el mismo que el solicitado para la atención en horario habitual.

Con objeto de que el servicio de guardia no reciba llamadas de personas no autorizadas y de que el número sólo sea conocido por estas personas autorizadas, el servicio de teléfono de guardia deberá ofrecer la posibilidad de filtro llamante (listas blancas/listas negras) y la posibilidad de ocultación del número de teléfono final del técnico de guardia en llamadas iniciadas por este. A tal fin, tendrá que rellenar en el *Anexo II: Compromiso de Adscripción de medios* del PCP una tabla de adscripción de medios materiales para reflejar el medio que ponga a disposición de EJIE para este servicio.

A continuación, se amplía el detalle correspondiente a las diferentes intervenciones fuera del "Horario habitual"

- Las operaciones y asistencias que requieran los servicios objeto del expediente y que exijan la parada de alguna máquina o de alguno de los servicios que presta, se planificarán de acuerdo con el personal técnico de EJIE en un horario convenido y que menos afecte al funcionamiento de dichos servicios.

  Dichas intervenciones podrán realizarse fuera del "Horario Habitual", en horario nocturno y/o festivo.
- La atención a incidencias o incidentes de seguridad / ciberincidentes que tengan cierta criticidad según el Protocolo de Gestión de CiberIncidentes, se deberán atender en 24x7 fuera del "Horario habitual", para lo cual se llamará al teléfono de guardia del servicio.
- Se estima un total de **250 horas de intervenciones extraordinarias/llamadas a guardia al año incluidas en el importe total de la oferta**:
  - Esta bolsa de horas englobará las horas de intervenciones planificadas, así como las horas dedicadas a la resolución de incidencias o ciberincidentes fuera del "Horario Habitual".

    Sin embargo, las llamadas a guardia que EJIE considere que deba atender un SOC de Nivel 1 NO computarán en esta bolsa de horas y deberán ser asumidas por el adjudicatario, ya que se considerará que se producen por errores originados por el propio SOC.

- Dentro del “Horario Extendido” e independientemente del horario y/o día de la intervención/incidencia, se descontará una hora de la bolsa por cada hora empleada en los trabajos.
- Las horas correspondientes a intervenciones planificadas se realizarán con autorización de EJIE. La adjudicataria deberá presentar informe de propuesta y seguimiento de las mismas que deberá ser aprobado por EJIE.
- La adjudicataria mantendrá un informe de seguimiento del consumo de la bolsa de horas.
- Las horas no consumidas anualmente se sumarán a las horas del año siguiente.
- Mejora: la ampliación del número de horas incluidas (según lo indicado en el apartado de criterios de adjudicación del PCP).

  Se recuerda que la información que corresponda a un dato de carácter objetivo (Archivo Electrónico De Fórmula) no se debe INCLUIR dentro de la Propuesta Técnica del Archivo Electrónico De Criterios De Juicio De Valor, ya que en caso contrario se procederá a la exclusión de la propuesta presentada.
- En caso de superar este número de horas, las siguientes se facturarán en base al precio presentado por la adjudicataria que también será valorado (apartado criterios de adjudicación del PCP).
- Durante el servicio de guardia se velará por el cumplimiento de los ANS pactados con EJIE relativos al proceso de Gestión de Incidencias o CiberIncidentes.
- Por cada intervención planificada y por cada llamada recibida en el teléfono de guardia la adjudicataria se compromete a seguir los procesos de gestión de cada tipo de intervención definidos por EJIE, destacando los correspondientes a la gestión vía ITSM y al Modelo de Comunicación de EJIE.

5.4.3.4.3 Plan de Cobertura Horaria del Servicio

El objetivo de este plan es reflejar la propuesta de la adjudicataria para satisfacer, tanto la cobertura del servicio en horario habitual, como el requisito de disponibilidad 24x7 en horario extendido en la prestación del servicio exigido por EJIE. Como parte de la oferta presentada el licitador deberá presentar su propuesta estratégica para cumplir con los horarios exigidos.

5.4.3.5 Planes de Transición

El objetivo de estos planes es reflejar la estrategia a seguir en las transiciones de entrada y salida del servicio garantizando en todo momento la continuidad del mismo sin suponer gasto adicional para EJIE.

Como parte de la oferta presentada, el licitador deberá presentar su propuesta para los siguientes planes de transición:

5.4.3.5.1 Plan de Transición de entrada al Servicio

Antes del comienzo de la prestación efectiva del servicio por parte de la nueva adjudicataria, esta se obliga a colaborar con el proveedor saliente, bajo la supervisión de EJIE, para llevar a cabo la transición del servicio. Esta fase es la que se ha denominado “Transición SOC” en el apartado 5.3.3.2.

Se habrá de tener en cuenta lo siguiente:

1. No se trata de una transición entre dos servicios exactamente iguales, por lo que la adjudicataria deberá tener esto en cuenta a la hora de plantear su plan de transición, que incluye un cambio de tecnología en alguno de los servicios a traspasar.
2. La fase de transición comprenderá desde **un mes** antes al comienzo de la prestación efectiva del servicio por parte de la nueva adjudicataria hasta el momento en que el proveedor saliente le transfiera efectivamente la responsabilidad del servicio.
3. Durante esta fase el servicio seguirá siendo prestado y las responsabilidades asociadas al mismo ejercidas por el proveedor saliente.
4. Se llevará a cabo una reunión de lanzamiento en la que se analizará el plan de salida del servicio del proveedor saliente y el plan de entrada al servicio de la nueva adjudicataria para ajustarlos a los objetivos, necesidades, situación actual y calendarios de traspaso del servicio. También se presentarán los equipos que participarán en la fase de transición y se constituirán los equipos y comités de gobernanza de la misma.
5. La nueva adjudicataria coordinará y ejecutará el traspaso del servicio con el proveedor saliente de manera que se garantice en todo momento la continuidad del mismo.
6. El proveedor saliente realizará la transferencia de conocimiento, herramientas y procedimientos que sean necesarios.
7. En lo posible, el traspaso de actividad se realizará progresivamente.
8. La aprobación de la finalización del periodo de transición se realizará por parte de EJIE cuando se considere probada y garantizada la transición del servicio.
9. Ningún coste asociado a esta fase podrá ser repercutido a EJIE ni por el proveedor saliente ni por la nueva adjudicataria.

Por tanto, se deberán desarrollar en el plan, al menos, los siguientes aspectos:

- Metodología propuesta.
- Equipos y comités necesarios.
- Recursos necesarios.
- Calendario propuesto.
- Estrategia de transición.
- Documentación, procedimientos y herramientas objeto de traspaso.

5.4.3.5.2 Plan de Transición de salida del Servicio

Antes de la finalización del contrato o, en su caso, de sus prórrogas la adjudicataria se obliga a prestar apoyo al nuevo proveedor, en caso de que este sea distinto a la adjudicataria del presente pliego, bajo la supervisión de EJIE, para llevar a cabo la transición del servicio. Se habrá de tener en cuenta lo siguiente:

1. La fase de transición comprenderá desde un mes antes al comienzo de la prestación efectiva del servicio por parte del nuevo proveedor hasta el momento en que la actual adjudicataria le transfiera efectivamente la responsabilidad del servicio.
2. Durante esta fase el servicio seguirá siendo prestado y las responsabilidades asociadas al mismo ejercidas por la actual adjudicataria.
3. Se llevará a cabo una reunión de lanzamiento en la que se analizará el plan de salida del servicio de la actual adjudicataria y el plan de entrada al servicio del nuevo proveedor para ajustarlos a los objetivos, necesidades, situación actual y calendarios de traspaso del servicio. También se presentarán los equipos que participarán en la fase de transición y se constituirán los equipos y comités de gobernanza de la misma.

4. El nuevo proveedor coordinará y ejecutará el traspaso del servicio con la actual adjudicataria de manera que se garantice en todo momento la continuidad del mismo.
5. La actual adjudicataria realizará la transferencia de conocimiento, herramientas y procedimientos que sean necesarios.
6. En lo posible, el traspaso de actividad se realizará progresivamente.
7. La aprobación de la finalización del periodo de transición se realizará por parte de EJIE cuando se considere probada y garantizada la transición del servicio.
8. Ningún coste asociado a esta fase podrá ser repercutido a EJIE ni por el nuevo proveedor ni por la actual adjudicataria.

Por tanto, se deberán desarrollar en el plan, al menos, los siguientes aspectos:

- Metodología propuesta.
- Equipos y comités necesarios.
- Recursos necesarios.
- Calendario propuesto.
- Estrategia de transición.
- Documentación, procedimientos y herramientas objeto de traspaso.

5.4.3.6 Garantía de la disponibilidad del Servicio

En todo caso y circunstancia, la adjudicataria debe obligarse a garantizar la disponibilidad del servicio. Para ello debe reflejar la estrategia, políticas o mecanismos de actuación habilitados frente a contingencias materiales provocadas por desastres, emergencias, falta de respuesta en el plazo, etc. y de recursos humanos que puedan poner en riesgo la prestación óptima del servicio a fin último de garantizar su prestación y calidad en cualquier circunstancia.

5.4.3.6.1 Plan de Continuidad de Negocio y Plan de Contingencia

A continuación, se enumeran los requisitos que los proveedores han de cumplir para asegurar la prestación del servicio:

- El proveedor deberá disponer de un plan de continuidad de negocio que asegure la provisión del servicio en modo contingencia, ante cualquier caso que imposibilite la ejecución normal (o preestablecida) del servicio. Este plan deberá tener identificadas a todas las personas y roles necesarios para su correcta ejecución.
- El proveedor deberá contar con un plan de pruebas (simulacros) exhaustivo que cubra todos los aspectos de continuidad vinculados a la provisión del servicio. Estas pruebas estarán programadas y su ejecución estará acompañada de la generación de evidencias necesaria para poder aportarlo ante una puntual solicitud de EJIE o para su revisión en las auditorías a proveedores.
- El proveedor deberá contar, si procede, con planes de mejora derivados de las pruebas realizadas.
- Se deberá disponer de un canal de comunicación especial en el que el proveedor informará a EJIE de manera urgente de cualquier incidente que active el plan de continuidad del servicio e informará periódicamente mientras se encuentre en situación de contingencia. Así mismo, se comunicará a EJIE el final de la situación de contingencia y cuando el servicio se encuentre, de nuevo, en funcionamiento normal
- El proveedor deberá disponer de una política de continuidad del proveedor que esté alineada con el servicio prestado a EJIE.

Teniendo lo anterior en cuenta, como parte de la oferta el licitador deberá presentar un plan de contingencia que, al menos, y sin implicar que sean las únicas situaciones de contingencia que se puedan dar, deberá contener su propuesta sobre:

- Indisponibilidad, planificada o no, de la utilización de los emplazamientos físicos habitualmente utilizados para la entrega del servicio (oficinas, etc.).
- Indisponibilidad, planificada o no, de elementos tecnológicos habitualmente utilizados para la entrega del servicio (redes de comunicaciones, hardware, software, licencias, etc.).
- Indisponibilidad por brechas de seguridad (malware, campañas de phising, etc.).
- Bajas médicas no planificadas de personal asociado al servicio por un período superior a una semana.
- Bajas médicas no planificadas de personal asociado al servicio, de carácter indefinido o permanente.
- Bajas laborales no planificadas, bien de carácter temporal o permanente.
- Bajas laborales planificadas, bien de carácter temporal o permanente.
- Ausencias planificadas por periodos vacacionales.

También se deberá indicar la forma de garantizar, en todo momento, la disponibilidad de un equipo mínimo adecuado para la prestación óptima del servicio y el método propuesto para la asunción automática de responsabilidades de los roles clave del servicio (Responsable del Servicio) ante indisposiciones, bajas médicas o laborales, vacaciones…etc.

5.4.3.7 Gestión Documental del Servicio

La empresa adjudicataria deberá documentar la solución desplegada y servicio configurado, completando la documentación necesaria para el modelado de los nuevos offerings y actualización de los servicios de **Monitorización y Respuesta de Seguridad Avanzada**, incluyendo, al menos:

- Descripción y diseño de la solución.
- Documentación del servicio para su operación
- Documentación técnica (oficial) con las características de las soluciones desplegadas, manuales técnicos y operativos, etc.
- Otros Entregables: Otra documentación que pueda complementar a la anterior (Plan de Calidad, Mapa de Red, Fichero Albergue, DFW…).

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

Para el seguimiento del servicio, EJIE pondrá a disposición una plataforma de gestión documental, accesible a todas las personas usuarias autorizadas, y donde se mantendrá actualizada de forma diaria la documentación del servicio. Esta herramienta será de especial relevancia principalmente como herramienta de información sobre los avances del servicio, y herramienta de intercambio para la validación de la documentación del servicio durante la ejecución del contrato.

El adjudicatario y EJIE deberán interactuar directamente contra la Plataforma de gestión indicada, siendo el adjudicatario el responsable último del registro y volcado de la documentación que se vaya generando.

6 LOTE 3: Servicios Especializados de Respuesta y Evaluación de laCiberSeguridad.

6.1 Situación actual y necesidad

La situación actual y necesidad en el ámbito del tratamiento de los CiberIncidentes más graves se ha explicado en el apartado “2 Situación actual y necesidad”.

Resumiendo lo expuesto previamente, se concluye que se requiere madurar en diversos aspectos relacionados todo el ciclo de Gestión de CiberIncidentes, para lo cual se hace necesario contar con Servicios Especializados de Respuesta y Evaluación de la CiberSeguridad.

6.2 Objeto

Este lote tiene por objeto ofrecer una serie de Servicios Especializados de Respuesta y Evaluación de laCiberSeguridad. Se trata de un conjunto de servicios que se requiere que sean aislados de los servicios de Seguridad ya existentes, bien por nivel de especialización, bien por considerarse una “evaluación” de los servicios existentes. Este LOTE incluye, al menos, servicios de DFIR, Ciber Ejercicios para entrenar el protocolo de respuesta a incidentes en casos de crisis, así como servicios de Red Team que permitan testear las capacidades de EJIE para protegerse, detectar y responder a Ciber Ataques.

6.3 Alcance

6.3.1 Ámbito

El ámbito de los servicios a contratar se limita a EJIE y a los Clientes adscritos a sus Servicios de Seguridad, siendo los principales clientes (por volumen de usuarios y puestos/servidores), aunque no los únicos, Gobierno Vasco, Osakidetza, Justizia y Educación.

6.3.2 Servicios

Se requieren servicios a ejecutar bajo demanda por el adjudicatario, dentro del ámbito de la Evaluación de la Seguridad y de la Respuesta Especializada a CiberIncidentes críticos. Los servicios pueden ser de diferentes tipos, requiriéndose, al menos, los siguientes tipos:

- **DFIR (Digital Forensics and Incident Response)**
  Se trata de servicios especializados de CiberSeguridad a activar cuando se produce un CiberIncidente crítico con muy alto impacto que supone una situación de Crisis y para el que se requiere ayuda externa para determinar el origen del incidente y/o para responder al mismo.

- **Ciber Ejercicios**
  Se trata de servicios especializados que se activan bajo demanda para entrenar y mejorar el Procedimiento de Gestión de CiberIncidentes en sus diferentes fases y en diferentes situaciones simuladas.

- **Ejercicios de Red Team**
  Se trata de servicios especializados que se activan bajo demanda para poner a prueba el nivel de seguridad de una entidad simulando un ataque externo o interno de forma que se determine la capacidad de detección y respuesta del equipo de Seguridad (Blue Team).

6.3.3 Modelo de Servicio

El licitador deberá hacer su propuesta de servicio teniendo en cuenta las siguientes condiciones:

- El Servicio Principal que se solicita y que se verá reflejado en el Alcance Inicial es el servicio de DFIR.
- Para el servicio DFIR se plantean los siguientes costes:
  - Coste Fijo Anual: Se entiende que este coste es el necesario para "estar disponible y preparado" para atender a la posible llamada de EJIE. Este coste se verá reflejado en el modelo económico.
  - Coste Horas: Es el coste asociado a las horas consumidas en el servicio. Se solicitarán en el Alcance Inicial una serie de horas mínimas disponibles. Cuando estas horas se consuman, se podrán ampliar a lo largo del contrato en base al coste/hora que se reflejará en el modelo económico.
- Las horas disponibles para DFIR, en caso de no consumirse, se podrán utilizar en el resto de servicios que el licitador proponga (al menos los reflejados en el apartado 6.3.2). El plazo para consumir las horas no consumidas será hasta, al menos, 3 meses una vez finalizado el plazo de duración del servicio.
  Si se consumen las horas disponibles DFIR, se adquirirán nuevas horas para utilizar en DFIR u otros servicios.
- El índice de conversión horas DFIR por horas de otro tipo de servicios será, como máximo de 1. Es decir, como máximo, se computará 1 hora DFIR por cada hora de otro tipo de servicios.
- Las horas de DFIR se podrán empezar a utilizar en cualquiera de los otros servicios propuestos, como máximo, a partir del mes 6 completo del primer año de contrato, es decir, como máximo, a partir del 1/6/2025 (recordar que el servicio comienza el 1/12/2024).
- Cuando EJIE quiera utilizar las horas en servicios diferentes al DFIR, se seguirá un procedimiento similar al siguiente, pudiendo el licitador proponer su propio procedimiento a consensuar con EJIE:
  - EJIE le solicitará al adjudicatario una estimación del servicio requerido, indicando el servicio/objetivo en cada caso.
  - El adjudicatario presentará una propuesta del servicio con la estimación correspondiente. El tiempo máximo para presentar esta estimación será de 10 días laborables.
  - EJIE analizará la propuesta y, si la considera adecuada, la autorizará.
  - El adjudicatario planificará y realizará los servicios solicitados ajustándose a la propuesta. El tiempo máximo para comenzar los servicios una vez autorizados será de 10 días laborables.
  - Si hiciera falta ampliar el número de horas estimadas, se requerirá volver a repetir del proceso de estimación y aprobación, debiendo estar claramente justificada la necesidad de ampliación de horas.

Se recuerda que la información que corresponda a un dato de carácter objetivo (Archivo Electrónico De Fórmula) no se debe INCLUIR dentro de la Propuesta Técnica del Archivo Electrónico De Criterios De Juicio De Valor, ya que en caso contrario se procederá a la exclusión de la propuesta presentada.

6.3.4 Alcance Inicial

El **alcance inicial** del Servicio consiste en la disponibilidad de:

Servicio	Horas
DFIR	100 horas

6.4 Requisitos de los Servicios Especializados de Respuesta y Evaluación de laCiberSeguridad

6.4.1 Requisitos globales del servicio

6.4.1.1 Condiciones de Seguridad

EJIE S.A. proporcionará acceso a sus sistemas informáticos y entregará la información, software y documentación necesaria para poder llevar a cabo los Servicios especificados, debiendo la empresa adjudicataria comprometerse a no utilizar para otros fines que los recogidos en el presente Pliego de Condiciones Técnicas, así como a no extraerla, cederla, publicarla o venderla total o parcialmente, ni en soporte informático ni en papel, debiendo proceder a la devolución de los soportes de la información facilitados por EJIE, S.A: , así como a la descarga de la misma de los equipos informáticos (si existieran), una vez se dé por concluido el trabajo. Queda terminantemente prohibido:

- El uso de estos recursos para actividades no relacionadas con el propósito del negocio, o bien con la extralimitación en su uso.
- Los equipos y/o aplicaciones que no estén especificados como parte del Software o de los Estándares de los Recursos Informáticos propios de EJIE o bajo supervisión de EJIE. Todos los ordenadores personales que se conecten a la red corporativa serán de las marcas y modelos homologados. El proveedor pondrá a disposición de EJIE dichos equipos para que se les instale el software necesario. Todos los ordenadores personales a los que EJIE les haya instalado software se llevarán a EJIE para que se formatee el disco duro a la finalización del servicio a EJIE.
- El proveedor se compromete a informar periódicamente a EJIE de los activos de información con los que proporciona el servicio.

Serán también de obligado cumplimiento las “Políticas de Seguridad para personal de empresas proveedoras” (accesible en la web www.ejie.eus). El servicio objeto del presente pliego se proporcionará desde las oficinas de la adjudicataria, de modo que:

- Según el apartado “Aplicabilidad de las Políticas Específicas de Seguridad para Proveedores” de dichas políticas:
  - El lugar de ejecución del servicio tendrá la consideración de “remoto”.
  - La propiedad de las infraestructuras TIC utilizadas tendrá la consideración “del proveedor”.
  - El “nivel de acceso” a los sistemas de EJIE tendrá la consideración de “con acceso privilegiado”.
- Serán de aplicación las políticas específicas de seguridad según la tabla del apartado 3.1, entre ellas las correspondientes a “seguridad física” (apartado 3.4).
- EJIE, tal como se indica en el apartado 2.6.c se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.

La adjudicataria además se compromete al cumplimiento y a proporcionar la información solicitada en el documento “Políticas de Seguridad para personal de Empresas proveedoras – Anexo - Infraestructura TIC y Seguridad física y del entorno” que se encuentra en el Anexo Seguridad de dicho documento. Esta información será utilizada en las auditorías que se realizarán periódicamente. Será obligación de la adjudicataria proporcionar esta información anualmente y ante cualquier cambio significativo en su contenido.

Asimismo, la empresa adjudicataria está obligada a cumplir todas las reglas de seguridad referidas en el apartado “Reglas de la seguridad” del PCP.

El servicio objeto del presente pliego realizará labores de administración sobre los entornos responsabilidad de EJIE. EJIE se reserva el derecho de exigir al adjudicatario la implantación de medidas de seguridad específicas que deberá acometer en el plazo de 6 meses, suponiendo el incumplimiento de esa implantación la penalización correspondiente especificada en el PCP.

Como referencia, sin que suponga un compromiso inicial, se especifican los siguientes ejemplos de posibles elementos a exigir:

- El proveedor deberá proporcionar, bajo solicitud de EJIE, dispositivos hardware que permitan la identificación y el acceso a los sistemas con suficientes garantías. Estos dispositivos podrán ser:
  - Teléfono móvil corporativo (Android o iOS), con sistema operativo actualizado, capaz de utilizar la APP del servicio de IDaaS implantado.
  - Dispositivos hardware homologados por EJIE:
    - Compatibles FIDO FIDO Alliance - Open Authentication Standards More Secure than Passwords y Okta https://www.okta.com).
- El proveedor deberá proporcionar, bajo solicitud de EJIE, la utilización por parte de los administradores de equipos específicos (físicos o virtuales) securizados utilizados exclusivamente para las labores de administración, debiendo utilizar equipos diferentes para sus labores no administrativas (email, navegación, ofimática, etc.). Como referencia, en algunos ámbitos este tipo de soluciones se denominan Estaciones de Acceso Privilegiado (PAW).
- El proveedor deberá proporcionar a los administradores equipos securizados con tecnologías EDR y EPP.

6.4.2 Requisitos específicos del Servicio

En este apartado se recopilan una serie de requisitos de obligado cumplimiento que debe satisfacer la propuesta del licitador. **La oferta del licitador no se debe limitar a indicar el cumplimiento o no de los diferentes requisitos y a la explicación de los mismos**. El licitador debe presentar una propuesta global de servicio en la que, teniendo en cuenta dichos requisitos, explique su servicio completo.

Como se ha adelantado en el Alcance del servicio, el Servicio principal que se demanda es el **servicio DFIR**. Sin embargo, se demandan una serie de servicios adicionales que podrán ser solicitados por EJIE bajo demanda. El licitador deberá hacer su **propuesta completa de servicios** adicionales dentro del ámbito de este LOTE, debiendo presentar, al menos, los servicios correspondientes a la realización de **Ciber Ejercicios** y ejercicios de **Red Team.**

El licitador expondrá en su propuesta los diferentes servicios que ofrece y el modo en el que se consumirán dichos servicios bajo demanda de EJIE, siempre teniendo en cuenta los requisitos y el alcance solicitados para este LOTE.

Se recuerda que la información que corresponda a un dato de carácter objetivo (Archivo Electrónico De Fórmula) no se debe INCLUIR dentro de la Propuesta Técnica del Archivo Electrónico De Criterios De Juicio De Valor, ya que en caso contrario se procederá a la exclusión de la propuesta presentada.

En todo caso, los servicios se podrán prestar de forma remota o in-situ, según cada caso, debiendo el adjudicatario aportar los procesos, herramientas y metodologías necesarias en cada caso.

Los servicios se facturarán en base al concepto COSTE HORA SERVICIO DFIR incluido en el modelo económico y dicho concepto incluirá todos los medios previstos para la prestación de los servicios, incluyendo posibles viajes y desplazamientos necesarios. El adjudicatario llevará un control del consumo de horas del contrato e informará a EJIE del mismo y de la posible necesidad de ampliación de horas, siempre con justificación y con necesidad de validación por parte de EJIE según lo establecido en el Modelo de Servicio.

6.4.2.1 Requisitos Servicio DFIR

En caso de identificarse un incidente crítico con alto impacto en el negocio y servicios que presta EJIE, EJIE podrá solicitar bajo demanda en horario **24x7x365** la participación de un servicio especializado de DFIR, que incluya al menos:

- Análisis forense, para determinar orígenes del ataque, medios utilizados y objetivos: Al menos se deberá determinar Qué, Cómo, Cuándo, Quién y Por qué.
- 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.

6.4.2.2 Requisitos Ciber Ejercicios

A lo largo del contrato se podrá solicitar, a demanda en horario 8x5, la realización de una serie de Ciber Ejercicios que incluyan, al menos:

- Simulación de situaciones para entrenar el Procedimiento de Respuesta a CiberIncidentes con el objetivo de determinar la idoneidad del propio Procedimiento, resultando en su modificación/adaptación si así fuera necesario, cubriendo al menos los siguientes aspectos:
    - Flujo y Modelo de Gestión de los CiberIncidentes.
    - Modelo de Escalado.
    - Modelo de Comunicación.
    - Modelo de Gestión de Crisis.
    - Aspectos legales.
- Simulación de situaciones para entrenar el Procedimiento de Respuesta a CiberIncidentes con el objetivo de entrenar la respuesta de los diferentes actores en EJIE en situaciones de crisis:
    - Nivel técnico.
    - Nivel operativo.
    - Nivel ejecutivo.
- Simulación de situaciones concretas para determinar la capacidad de respuesta de EJIE incluyendo, al menos, los siguientes supuestos:
    - Ransomware en EJIE.
    - Ransomware en Cliente adherido a servicios de EJIE.
    - Compromiso de proveedor crítico para EJIE.
- Documentación asociada a los Ciber Ejercicios que sirva como base para mejoras en este ámbito.

6.4.2.3 Requisitos Red Team

A lo largo del contrato se podrá solicitar, a demanda en horario 8x5, la realización de ejercicios de Red Team que incluyan, al menos:

- Ataques simulados que permitan evaluar el nivel de protección de EJIE y su capacidad de detección y respuesta.
- Ataques simulados que permitan entrenar a los equipos de Seguridad para mejorar la prevención, detección y respuesta frente a posibles ataques.
- Ataques simulados orientados a sectores específicos de los clientes de EJIE: Gobierno, Sector Sanitario, Justicia, Medios de Comunicación, Transporte, etc.
- Documentación asociada a los ejercicios que sirva como base para mejoras en este ámbito.

6.4.3 Requisitos de Seguimiento

6.4.3.1 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.

El licitador podrá ofrecer otros ANS que complementen a los anteriores que serán valorados, durante la fase de adjudicación, de acuerdo con los criterios indicados en el pliego de condiciones particulares:

Servicio	Descripción	Objetivo	Período de Cómputo	Tipo de penalización
DFIR	Tiempo de Respuesta para comenzar a trabajar en un CiberIncidente	< 3 horas	Mensual	2
DFIR	Llamadas sin atender en 24x7x235	< 1	Mensual	2
Todos menos DFIR	Tiempo en preparación de propuesta de servicio con estimación desde la solicitud del servicio por parte de EJIE.	< 10 días laborables	Mensual	1
Todos menos DFIR	Tiempo en comenzar a ejecutar servicio una vez autorizado por EJIE.	< 10 días laborables	Mensual	1

6.4.3.2 Informes y Cuadros de Mando

Se deberá generar una serie de informes y cuadros de mando de seguimiento del servicio. La empresa licitadora deberá detallar su propuesta de entregables y cuadros de mando, identificándose, al menos, los siguientes:

- Informes/Dashboards asociados al servicio.
- Informes de seguimiento para los diferentes comités de seguimiento.

- Informes de los servicios prestados.

6.4.3.3 Gestión Documental del Servicio.

Se deberá generar una serie de documentación relacionada con el servicio. La empresa licitadora deberá detallar su propuesta de documentación, identificándose, al menos, los siguientes:

- Descripción del servicio.
- Catálogo de Peticiones.
- Procedimiento para las solicitudes
- Documentación asociada a los servicios.

La documentación deberá mantenerse actualizada con la evolución del servicio (mejoras introducidas…)

Para el seguimiento del servicio, EJIE pondrá a disposición una plataforma de gestión documental, accesible a todas las personas usuarias autorizadas, y donde se mantendrá actualizada de forma diaria la documentación del servicio. Esta herramienta será de especial relevancia principalmente como herramienta de información sobre los avances del servicio, y herramienta de intercambio para la validación de la documentación del servicio durante la ejecución del contrato.

La empresa adjudicataria y EJIE deberán interactuar directamente contra la Plataforma de gestión indicada, siendo el adjudicatario el responsable último del registro y volcado de la documentación que se vaya generando.

6.4.3.4 Comités de Seguimiento

Para llevar a cabo el seguimiento del servicio existirán una serie de comités de seguimiento. La empresa licitadora deberá detallar su propuesta específica de comités indicando el objetivo, frecuencia, participantes, entregables, etc. Se considera que, al menos, deberán existir los siguientes comités:

- **Operativo**: Orientado al seguimiento del día a día del Servicio.
- **Ejecutivo/Estratégico**: Orientado al seguimiento del estado general del servicio y de la evolución del mismo, así como de los hitos principales del avance del servicio.
- **Directivo**: Orientados al seguimiento con los diferentes responsables jerárquicos en EJIE.

6.4.3.5 Equipo de Trabajo

El equipo de trabajo propuesto por el adjudicatario deberá estar formado por personal técnico con categoría profesional y nivel de especialización adecuados a las necesidades planteadas en el presente lote.

El equipo de trabajo del adjudicatario estará dirigido por un Responsable del Servicio que deberá contar con disponibilidad para atender sin demora los requerimientos de los responsables designados por EJIE. El responsable del servicio deberá contar con capacidad suficiente para tomar las decisiones que se adopten sobre las prestaciones contratadas sin que estas puedan verse afectadas por la falta de capacidad decisoria, ya sea legal o formal. Este Delegado será el único interlocutor principal con la Dirección del Servicio de EJIE. Dispondrá de teléfono móvil, para facilitar su localización, y correo electrónico.

El dimensionamiento del equipo deberá realizarse acorde a la metodología planteada por el licitador, a los tiempos y planificaciones establecidas y a los requerimientos mínimos expuestos en el presente lote.

En cualquier caso, el adjudicatario será el responsable de garantizar los medios durante la ejecución del proyecto y éstos deberán adecuarse en todo momento para cumplimiento de los hitos y plazos establecidos.

Un aspecto clave para el dimensionamiento de recursos y organización es, no solo la ejecución de los trabajos, sino también la necesidad de elaboración de documentación (informes finales, actas de servicio…) requerida durante el servicio.

El dimensionamiento del equipo de trabajo deberá realizarse considerando el tiempo necesario para la ejecución de las tareas para lograr el alcance del contrato. El dimensionamiento y dedicación final de estos recursos estará sujeto a la organización del servicio por parte del adjudicatario para cumplimiento de los plazos previstos.

El adjudicatario pondrá a disposición el personal técnico adecuado con la preparación y experiencia necesarias, con el dimensionamiento y dedicaciones requeridas, para llevar a cabo las tareas requeridas para la ejecución del contrato.

A continuación, se especifican los roles mínimos identificados a los que deberá dar respuesta la empresa adjudicataria para la ejecución del presente contrato, y que se acompañarán del equipo de trabajo necesario para la ejecución de los trabajos solicitados en los plazos requeridos:

- **Responsable del Servicio,** mencionado previamente**,** que será el responsable último del contrato y de la disposición de los medios y su coordinación para cumplimiento de los objetivos del servicio (plazos, calidad, alcance...), y con los conocimientos y capacidades solicitados en el PCP.

6.4.3.6 Seguimiento por parte de la Empresa Adjudicataria

La empresa adjudicataria será el responsable principal de controlar la ejecución de los trabajos, estableciendo para ello, todos los mecanismo y procedimientos necesarios que garanticen el cumplimiento de la planificación, la correcta operatividad y la calidad del servicio.

Uno de los aspectos más críticos del servicio es la necesidad de coordinación de los trabajos con los siguientes agentes posible:

- EJIE.
- Los diferentes Proveedores, que EJIE considere.
- Entidades involucradas en el servicio.

Asimismo, la empresa adjudicataria designará un Responsable de Servicio como interlocutor principal con EJIE para el control del servicio que tendrá una participación activa.

El Responsable del servicio se responsabilizará de las siguientes tareas principales:

- Realizará la coordinación y seguimiento continuo del servicio y velará por mantener el plan de ejecución de trabajos periódicamente actualizado, considerando en todo momento la integración de sus tareas (planes de trabajo, pruebas, etc.) con aquellas que involucren a EJIE (y soportes).
- Será el responsable por parte de la empresa adjudicataria de disponer de los medios necesarios y organizar los recursos y equipo de trabajo para garantizar el cumplimiento del plan, y definirá metodologías para control de riesgos y definición de propuestas de mitigación de los mismos que garanticen los resultados esperados en proyecto en plazos y calidad técnica.
- Organizará el conjunto de recursos necesarios para la ejecución de los trabajos siempre con el objetivo de cumplir la planificación definida.
- Podrá tener, a consideración de EJIE, interlocución directa con otros involucrados del proyecto por parte de EJIE como son los grupos de soporte.
- Realizará reportes de avance de proyecto.
- Definirá metodologías para identificación y control de riesgos y definición de propuestas de mitigación de estos.

- Asistirá, junto con los técnicos que se estime conveniente, a las reuniones de seguimiento y técnicas que convoque EJIE, y con la periodicidad que se designe.
- Garantizará que toda la información y documentación del proyecto se encuentra en todo momento actualizada en la plataforma de gestión que a tal efecto disponga EJIE.
- Realizará el seguimiento periódico sobre la calidad de los servicios solicitados y será el responsable de garantizar el cumplimiento de los acuerdos de nivel de servicio asociados.