Eusko Jaurlaritzaren
Informatika Elkartea

Sociedad Informática
del Gobierno Vasco

Servicios de Soporte Seguridad de EJIE

Especificaciones de compra / Pliego de condiciones técnicas

Junio 2021

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	11/06/2021	Versión Inicial	Josu Bagazgoitia	Aritza Iratzagorria

Índice

1 Introducción....4
2 Objeto del contrato....5
3 Alcance del contrato....6
3.1 Tecnologías....6
3.2 Ámbito....6
3.3 Disponibilidad....6
4 Requisitos del Servicio....8
4.1 Requisitos globales del Servicio....8
4.2 Requisitos específicos del Servicio....25
4.3 Procedimiento y Calidad....35
5 Planificación y organización del servicio....46
5.1 Organigrama del Servicio....46
5.2 Equipo de trabajo....48
5.3 Carga de trabajo....53
5.4 Actualización tecnológica....54
5.5 Horario del Servicio....55
5.6 Interconexión con BATERA....57
5.7 Planes de Transición....57
5.8 Garantía de la disponibilidad del Servicio....59
6 Condiciones de Seguridad/Generales....61
7 Anexo I – Entorno tecnológico....63
7.1 Sistemas....63
8 Anexo II – Centros dentro del ámbito....65
9 Anexo III – Catálogo de servicio de referencia....66

1 Introducción

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

En julio de 2015, el Consejo de Gobierno aprobó la iniciativa que pone en marcha el denominado proceso de convergencia en materia de Tecnologías de la Información y la Comunicación (TIC).

El objeto de esta iniciativa, bautizada con el nombre de «BATERA», es llevar a cabo un proceso de convergencia en materia TIC, circunscrita a las instalaciones y otros elementos relacionados (como son las Infraestructuras, Comunicaciones, Puesto de trabajo y Servicios corporativos unificados). Así mismo se consideró que EJIE era el organismo más apropiado para ser el órgano gestor que determine en cada momento los proyectos y el modelo a seguir para prestar los servicios de la iniciativa «BATERA», así como la operación de los mismos.

Estos nuevos proyectos tecnológicos construirán nuevos servicios corporativos que, una vez construidos, facilitarán que las diferentes entidades y organismos de Gobierno los puedan consumir y se comience con los proyectos de convergencia de las mismas.

2 Objeto del contrato

El objeto del contrato es la adquisición del **Servicio de Soporte de Seguridad de EJIE** comprendiendo la operación, soporte y evolución dentro del ciclo de vida tanto de los servicios convergentes ofrecidos desde BATERA como de los servicios "legacy" utilizados por diversos departamentos, entidades y organismos dependientes del Gobierno Vasco.

Los objetivos que deben primar en el suministro de este servicio son:

- Garantizar un servicio de calidad.
- Optimizar la disponibilidad y utilización de los recursos puestos en juego.
- Flexibilidad para asumir nuevas competencias y tecnologías.
- Integración con los procesos de EJIE.
- Mejora continua de los Servicios, Infraestructuras, Procesos y Procedimientos objeto del contrato.
- Consolidación del proceso de convergencia y desarrollo de los Servicios de Seguridad ofrecidos por BATERA.
- Establecimiento de la Seguridad como un elemento Transversal a la Organización, fomentando la colaboración entre el equipo de Seguridad y el resto de departamentos con el objetivo de mantener la Organización segura, es decir, implantar un enfoque SecOps.

La prestación de los servicios solicitados en este pliego conlleva el cumplimiento de los **Acuerdos de Nivel de Servicio** (ANS en adelante) entre EJIE y la empresa adjudicataria, que tendrán los ajustes necesarios en función de la ejecución de los servicios. Dichos ANS estarán alineados con las necesidades actuales de EJIE, siendo necesario su constante seguimiento para garantizar el servicio prestado y con la suficiente flexibilidad para que permita su actualización en función de cambios o nuevos requerimientos de EJIE.

Se requerirá un mínimo de 30.600 horas anuales para la prestación del servicio.

3 Alcance del contrato

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

3.1 Tecnologías

El alcance de las tecnologías abarca la totalidad de las infraestructuras de seguridad de las que EJIE es responsable y que se encuentran especificadas en el *Anexo I – Entorno Tecnológico* del presente documento.

A lo largo del presente contrato se podrán ir incrementando o decrementando las tecnologías de las que EJIE se responsabilice. Por lo que, de manera periódica se irán revisando los mismos, y aplicando las modificaciones previstas en el PCP.

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

Adicionalmente, al constituir la Seguridad un elemento transversal según el enfoque SecOps, el servicio colaborará en la definición y mejora de aspectos de Seguridad del resto de departamentos, principalmente otras pilas [1]del Área de Servicios Convergentes y otras pilas tecnológicas (Desarrollo, etc.).

3.2 Ámbito

El ámbito se limita principalmente a las infraestructuras de la Red Corporativa Administrativa del Gobierno Vasco (RCAGV), Batera, Osakidetza, Justizia y Hezkuntza, pero podrá verse ampliado durante el ciclo de vida del contrato con la incorporación de nuevas infraestructuras a mantener.

En el *Anexo II – Centros dentro del ámbito* se detallan las sedes dentro del alcance donde se encuentra desplegado el equipamiento que conforma las infraestructuras mencionadas. En dicho desglose se incluyen tanto CPDs de las diferentes entidades como centros asociados a su red de acceso.

Sin perjuicio de lo anterior, el servicio deberá igualmente suministrarse a cualquier otra sede de nueva apertura, así como a otros clientes que puedan incorporarse al servicio durante la vigencia del contrato objeto de este expediente. La actualización de sedes se realizará de forma periódica, con comunicación con la suficiente antelación a la adjudicataria, y en su caso, aplicando las modificaciones previstas en el PCP.

3.3 Disponibilidad

El servicio se ofrecerá en régimen de 24x7 (24 horas, 7 días a la semana) los 365 días del año, siendo los niveles de actuación los siguientes:

[1] Cuando se habla de “pila” se está haciendo referencia a verticales dentro de una organización jerárquica, es decir, a otras áreas o a otros departamentos dentro de un área.

- 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.

En el horario extendido el tipo de atención podrá ser:

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

4 Requisitos del Servicio

4.1 Requisitos globales del Servicio

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 Servicios TI, sin perjuicio del 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.

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, siendo las cinco siguientes:

- Estrategia del Servicio
- Diseño del Servicio.
- Transición del Servicio.
- Operación del Servicio.
- Mejora Continua del Servicio.

Los procesos a gestionar, así como sus respectivas tareas a realizar, por el Servicio dentro de cada una de estas cinco fases se detallan en los siguientes apartados.

4.1.1 Estrategia del Servicio

Los procesos principales de la fase de Estrategia del Servicio son los siguientes:

- 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

En el ámbito de la Seguridad, el proveedor colaborará en todos ellos proporcionando información clave por parte de especialistas que ayude en la toma de decisiones.

4.1.1.1 Definición de la estrategia

Este proceso es el responsable de definir los Servicios (visión y misión) a nivel estratégico, definiendo objetivos, políticas, métricas, indicadores y evolución o roadmap de los servicios.

4.1.1.2 Gestión del porfolio de los servicios

Este proceso es el responsable de definir la forma en que los Servicios serán ofrecidos por BATERA a sus clientes. En el ámbito de la Seguridad los servicios se ofrecerán, en general, como valor añadido de otros servicios básicos ofrecidos por BATERA.

4.1.1.3 Gestión de la demanda

El objetivo de este proceso es predecir y regular la demanda para optimizar el uso de los recursos y poder proporcionar los servicios ofrecidos con la calidad acordada.

4.1.1.4 Gestión financiera

Este proceso es el que se encarga de las valoraciones económicas relacionadas con los servicios con el objetivo de publicar unas tarifas para los Servicios que se ofrecen a los clientes que cubran los costes asociados.

4.1.1.5 Gestión de la relación de las ramas del negocio

Este es el proceso que establece y mantiene la relación entre EJIE y sus clientes. Identifica las necesidades cambiantes de los clientes con objeto de ser capaz de reaccionar y poder cubrirlas.

4.1.2 Diseño del Servicio

Los procesos principales para el Diseño del servicio son los siguientes:

- 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.

4.1.2.1 Monitorización y reporte del nivel de servicio.

El proceso para la Monitorización y reporte del nivel de servicio corresponde a las tareas asociadas con la monitorización y los servicios de reporte relacionados con los acuerdos de nivel de servicio (ANS). Adicionalmente, el proveedor podría facilitar información sobre la administración del sistema (por ejemplo, métricas de rendimiento, estadísticas…etc.) en un formato que sea acordado con EJIE, que resulte representativo y diseñado para el mismo. Los siguientes puntos identifican los roles y responsabilidades relevantes que el proveedor debe realizar para desarrollar los niveles de servicio y monitorización:

- Mantener y documentar el manual de procedimientos del servicio de monitorización y reporte siguiendo los requerimientos y las políticas definidas.
- Reportar un ANS de rendimiento y mejora de resultados.
- Medir, analizar y proporcionar informes de gestión sobre el rendimiento en relación con los ANS.
- Realizar reuniones de mejora de ANS para revisarlos y recomendar mejoras.
- Implementar mejoras para los planes ANS.
- Otorgar acceso a EJIE para visualizar el rendimiento del sistema, informes de monitorización de ANS, así como el acceso a datos relevantes.

4.1.2.2 Gestión del Rendimiento

El proceso de Gestión del Rendimiento engloba las tareas asociadas con la gestión y el ajuste de los componentes de la pila de servicio para un rendimiento óptimo. Los siguientes puntos identifican los roles y responsabilidades relevantes que el proveedor debe realizar para desarrollar la Gestión del rendimiento:

- Monitorización del rendimiento de los servicios de TI y de los componentes de TI de apoyo.
- Evaluación de los resultados de los informes.
- Realización de análisis de tendencias.
- Proporción de recomendaciones para la mejora continua del rendimiento.
- Realización de actividades de ajuste.
- Actualización periódica (al menos anualmente).

Los siguientes puntos identifican los roles de gestión del rendimiento y las responsabilidades que el proveedor debe realizar:

- Mantener y documentar los procedimientos de gestión del rendimiento siguiendo los requisitos y políticas previamente definidos.
- Realizar la optimización de los componentes de la pila de servicio para mantener un rendimiento óptimo de acuerdo con los procedimientos de la Gestión del Cambio.
- Administrar los recursos de componentes de la pila de servicio (por ejemplo, dispositivos y tráfico) para cumplir con las especificaciones de los ANS en términos de disponibilidad y rendimiento.
- Proporcionar monitorización y reportes de rendimiento, la utilización y la eficiencia de los componentes de la pila de servicio basados en un marco de tiempo y secuencia definidos (por ejemplo, mensualmente).
- Evaluar, identificar y recomendar de forma proactiva configuraciones o cambios en configuraciones que mejoren el rendimiento.
- Llevar a cabo un análisis de tendencias para recomendar cambios para mejorar el rendimiento basado en el marco de tiempo especificado (por ejemplo, mensualmente).
- Desarrollar y proporcionar planes de mejora según sea necesario para satisfacer los ANS basados en el marco de tiempo definido (por ejemplo, mensualmente).
- Implementar planes de mejora para coordinar con terceros, según sea necesario.
- Proporcionar asesoramiento y apoyo técnico al personal de soporte y desarrollo de aplicaciones según sea necesario.

4.1.2.3 Gestión de la Disponibilidad

El objetivo de la Gestión de la Disponibilidad es comprender los requisitos generales de disponibilidad de las necesidades de negocio de EJIE y planificar, medir, supervisar y esforzarse continuamente por mejorar la disponibilidad de la Infraestructura de TI, los servicios y la organización de TI de soporte para garantizar que estos requisitos se cumplan de forma coherente. Se centra en ofrecer mejoras de disponibilidad que ofrecen beneficios de negocio medibles. La Gestión de la Disponibilidad abarca la evaluación, diseño, implementación, medición y gestión de la disponibilidad de Infraestructura de TI desde un componente y una perspectiva de extremo a extremo (es decir, servicios), incluyendo metodologías y herramientas nuevas o modificadas de Gestión de Servicios de TI, modificaciones o actualizaciones de los sistemas y componentes de infraestructura de TI. El objetivo del proceso de Gestión de la Disponibilidad es optimizar la capacidad de la infraestructura de TI, los servicios y la organización de apoyo para ofrecer un nivel de disponibilidad sostenido que permita a EJIE satisfacer sus objetivos de negocio.

Las actividades clave del proceso de Gestión de la Disponibilidad son las siguientes:

- Determinar los requisitos de disponibilidad de unidades de negocio (generalmente como parte del desarrollo del ANS) para un servicio de TI nuevo o mejorado y formular los criterios de diseño de

disponibilidad y recuperación para la infraestructura de TI para garantizar que los servicios de TI estén diseñados para proporcionar los niveles apropiados.

- Determinar las funciones críticas del negocio, así como el impacto derivado del fallo del componente de TI. Cuando sea apropiado, revisar los criterios de diseño de disponibilidad para proporcionar información adicional para prevenir o minimizar el impacto al negocio.
- Identificar oportunidades para optimizar la disponibilidad de la Infraestructura de TI para ofrecer mejoras costo-efectivas que proporcionen beneficios empresariales tangibles.
- Establecer medidas y reportes de disponibilidad, confiabilidad y mantenibilidad que reflejen las perspectivas de la empresa, del usuario final y de la organización de soporte de TI.
- Monitorizar y analizar las tendencias de la disponibilidad, confiabilidad y mantenibilidad de sistemas y componentes de TI.
- Revisar el servicio de TI, la disponibilidad de sistemas y componentes, identificando niveles inaceptables y adoptando medidas correctivas apropiadas para abordar los déficits de disponibilidad.
- Investigar las razones subyacentes de la disponibilidad inaceptable y proporcionar recomendaciones para la resolución.
- Producir y mantener un Plan de Disponibilidad orientado hacia el futuro que priorice y planifique mejoras generales de la disponibilidad de TI para mejorar la disponibilidad general de componentes de Servicios de TI e Infraestructura para asegurar que los requerimientos de disponibilidad del negocio existente y futuro sean los acordados.
- Proporcionar información de disponibilidad de TI: informes para asegurar que los niveles acordados de disponibilidad, confiabilidad y mantenibilidad se midan y monitoricen continuamente.

Los siguientes puntos identifican los roles y responsabilidades de la Gestión de la Disponibilidad que deben ser adquiridas por el cliente y por el proveedor.

- Implementar los procedimientos de gestión de la disponibilidad acordados.
- Proporcionar acceso de lectura sin restricciones a EJIE y al personal designado a todos los datos y registros de disponibilidad actuales e históricos de la base de conocimiento.
- Participar con EJIE en la definición de las medidas de disponibilidad y los requisitos de presentación de informes.
- Asegurar que se implementan herramientas y prácticas de medición de disponibilidad.
- Participar en las sesiones de revisión de la Gestión de Problemas según corresponda, específicamente aquellos problemas relacionados con cortes de sistemas críticos.
- Monitorizar la disponibilidad real de TI lograda frente a los objetivos y asegurar que los déficits se aborden con prontitud y efectividad.
- Llevar a cabo sesiones de revisión de la evaluación de la disponibilidad y proporcionar recomendaciones de mejora justificadas por costes.
- Producir y mantener un Plan de Disponibilidad que priorice y planifique mejoras de disponibilidad de TI aprobadas.
- Proporcionar informes de disponibilidad de TI para asegurar que los niveles acordados de disponibilidad, confiabilidad y mantenibilidad se miden, reportan y monitorizan de manera continua.

4.1.2.4 Gestión de la Capacidad

El proceso de Gestión de la Capacidad comprende las tareas asociadas a asegurar que la capacidad de las pilas de Servicio coincida con la evolución de las demandas del negocio del EJIE de la manera más rentable y oportuna. El proceso abarca lo siguiente:

- Supervisar el rendimiento de los servicios de TI y de los componentes de TI de apoyo.
- Comprender las demandas actuales y pronosticar las necesidades futuras.
- Desarrollar planes de capacidad que satisfagan la demanda y los ANS.
- Desarrollar modelos y realizar simulaciones para gestionar la capacidad.
- Realizar evaluaciones de riesgo de las recomendaciones de capacidad.
- Desarrollar e implementar un plan de capacidad que incluya el impacto financiero de las pilas de Servicio.

- Realizar las actividades de ajuste necesarias.

Los siguientes puntos identifican las funciones y responsabilidades relevantes de Gestión de la Capacidad que el proveedor debe realizar:

- Mantener y documentar los procedimientos de Gestión de la Capacidad que cumplan los requisitos y se adhieran a las políticas definidas.
- Desarrollar un plan de capacidad periódico (usualmente anual), incluyendo actualizaciones trimestrales.
- Desarrollar e implementar modelos de capacidad y ejecutar simulaciones para validar el plan de capacidad.
- Evaluar los impactos de la capacidad al agregar, eliminar o modificar aplicaciones y componentes de infraestructura.
- Supervisar continuamente el uso de los recursos de TI para permitir la identificación proactiva de los problemas de capacidad y rendimiento.
- Capturar información de tendencias y pronosticar futuros requisitos de capacidad de clientes basados en umbrales definidos por el cliente.
- Evaluar los incidentes / problemas relacionados con la capacidad y formular recomendaciones para su resolución.
- Recomendar cambios en la capacidad para mejorar el rendimiento del servicio.
- Evaluar el impacto / riesgo y el coste de los cambios de capacidad.
- Mantener los niveles de capacidad para optimizar el uso de los recursos de TI existentes y minimizar los costes de EJIE para ofrecer servicios cumpliendo los ANS acordados.
- Asegurar que exista una capacidad adecuada dentro del entorno de TI para satisfacer los ANS y requisitos, teniendo en cuenta las variaciones diarias, semanales y estacionales en las demandas de capacidad.

4.1.2.5 Backup y Recuperación

El proceso de Backup y Recuperación engloba las actividades asociadas con la provisión de capacidades de copia de seguridad y recuperación de acuerdo con los programas y requisitos de EJIE. El proveedor debe demostrar que cumplirá o excederá los requisitos de Backup y Recuperación de EJIE. Los siguientes puntos identifican las funciones y responsabilidades relevantes de Backup y Recuperación que el proveedor debe realizar:

- Recomendar las mejores prácticas para las estrategias, políticas, procesos y procedimientos de backup y recuperación.
- Mantener y documentar los procedimientos de backup y recuperación que se adhieren a los requisitos y políticas de EJIE.
- Definir requisitos y políticas de supervisión y generación de informes de copia de seguridad y recuperación.
- Administrar el inventario de medios de copia de seguridad (cinta, disco, óptico y otro tipo de medios), incluyendo el orden y la distribución de los medios.
- Realizar copias de seguridad del componente de la pila del servicio y la rotación asociada de los medios según sea necesario.
- Archivar medios de datos en una ubicación segura fuera de sitio.
- Asegurar la capacidad continua para recuperar los datos archivados de los medios como se especifica (compatibilidad hacia atrás del equipo de respaldo más reciente).
- Probar los medios de copia de seguridad para garantizar la recuperación incremental y completa de los datos y asegurar que la integridad del componente de la pila de servicio, según lo requiera o solicite EJIE.
- Recuperar archivos, sistema de archivos u otros datos requeridos de los medios de copia de seguridad, según sea requerido o solicitado por EJIE.

4.1.2.6 Continuidad de servicios TI y Recuperación de Desastres

Los procesos de Continuidad de servicios de TI y Recuperación de Desastres (DR) son las tareas asociadas con el suministro de dichos servicios para proporcionar aplicaciones cliente y su infraestructura asociada (por ejemplo, CPU, servidores, red, dispositivos de datos y salida, dispositivos de usuario final…etc.). Las aplicaciones cliente y la infraestructura asociada recibirán servicios de DR de acuerdo con el plan de continuidad de negocio de EJIE. El proveedor debe demostrar que cumplirá o excederá los requisitos de Continuidad de servicios de TI y Recuperación de Desastres del Cliente. Los siguientes puntos identifican las funciones y responsabilidades del proceso de Continuidad de servicios TI y DR que el proveedor debe realizar:

- Cuando sea necesario, ayudar al EJIE en otras actividades de continuidad de TI y gestión de emergencias.
- Mantener y documentar un plan de DR detallado para cumplir con los requisitos de Continuidad de Servicio de TI y DR. Incluir planes de datos, replicación, copias de seguridad, administración de almacenamiento y operaciones de contingencia que proporcionen la recuperación de los sistemas de EJIE dentro de los marcos de tiempo de requisito de recuperación establecidos después de que un desastre afecte al uso de los servicios por parte de EJIE.
- Realizar pruebas de DR programadas por políticas de EJIE.
- Revisar e informar los resultados de la prueba de DR a EJIE.
- Desarrollar un plan de acción para abordar los resultados de las pruebas DR.
- Implementar el plan de acción y proporcionar un estado continuo hasta la terminación.
- Coordinar con EJIE durante una situación de DR de proveedor según las políticas y procedimientos de DR.
- Proporcionar acceso a EJIE a la continuidad de los servicios de TI y a los sistemas y datos de notificación y monitorización de DR.

4.1.2.7 Seguridad

El proceso de Seguridad son las tareas asociadas con el mantenimiento de la seguridad física y lógica de todos los componentes de la pila de servicio (hardware y software), protección de datos, virus, protección de acceso y otros servicios de seguridad en cumplimiento con los requisitos de seguridad de EJIE. Los siguientes puntos identifican las funciones y responsabilidades relevantes de seguridad que el proveedor debe realizar:

- Generales:
    - Mantenerse al día con las actuales tendencias de seguridad, amenazas y vulnerabilidades comunes, así como políticas de seguridad, procedimientos y mejores prácticas.
    - Llevar a cabo autoevaluaciones para identificar los agujeros de control o seguridad.
    - Implementar planes de seguridad física y lógica coherentes con las políticas de seguridad de usuario y los estándares de la industria.
    - Denunciar infracciones de seguridad a directivas cliente por EJIE.
    - Resolver violaciones de seguridad por políticas de cliente.
    - Revisar todos los parches de seguridad relevantes para el entorno de TI y clasificar la necesidad y la velocidad con la que deben instalarse los parches de seguridad según lo definido por las políticas de seguridad y la administración del cambio.
    - Instalar los parches de seguridad por proceso y procedimientos de Gestión del Cambio del cliente, incluyendo la adquisición de la aprobación del cliente requerida.
    - Mantener toda la documentación requerida para las evaluaciones de seguridad, auditorías y pruebas de control y control interno.
    - Permitir auditorías de seguridad de terceros.
    - Implementar en el servicio un programa de concienciación sobre seguridad.

  - Asegurar que todo el personal del proveedor complete el entrenamiento de seguridad requerido por EJIE, basado en roles de seguridad de información definidos por EJIE.
- Seguridad física. Se centra en los controles de acceso físicos implementados para garantizar la seguridad de los datos de EJIE y el proveedor, instalaciones y sus sistemas de gestión asociados.
- La seguridad de los datos consiste en las actividades asociadas con la clasificación, gestión, seguridad y encriptación de los datos confidenciales y el almacenamiento de los medios que contienen esos datos.
- El proveedor proporcionará servicios de Detección/Prevención de Intrusión basados en la Red y servicios de Detección/Prevención de Intrusión basados en Host utilizando hardware y software propiedad de EJIE. El proveedor también realizará una monitorización interna de amenazas para actividades maliciosas y/o sospechosas.
- Los servicios de Gestión de Incidentes de Seguridad son las actividades asociadas con la identificación, clasificación, gestión y notificación de un evento de seguridad.
- Los servicios de Cumplimiento y Auditoría de Seguridad son las actividades para identificar los estándares que EJIE debe cumplir y modificar prácticas, políticas y procedimientos para permitir su cumplimiento.

4.1.3 Transición del Servicio

Los procesos principales para la Transición del Servicio son los siguientes:

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

4.1.3.1 Gestión del Cambio

El proceso de Gestión del Cambio comprende las tareas para asegurar que se usan métodos y procedimientos estandarizados para el manejo eficiente y rápido de todos los cambios, para minimizar el impacto del cambio en la calidad del Servicio y, en consecuencia, mejorar las operaciones cotidianas de EJIE.

La Gestión del Cambio cubre todos los aspectos de la gestión, de la introducción e implementación de todos los cambios que afectan a todas las pilas tecnológicas y en cualquiera de los procesos de gestión, herramientas y metodologías diseñados y utilizados para soportar los componentes de las pilas.

Las actividades de Gestión del Cambio están interrelacionadas y son complementarias con la Gestión de Versiones y la Gestión de la Configuración, así como con la Gestión de Incidencias y la Gestión de Problemas.

Las principales tareas del proceso de Gestión del Cambio incluyen:

- Determinación de métricas para evaluar la efectividad de un cambio.
- Solicitud de cambio (RFC).
- Seguimiento.
- Priorización.

- Asignación de responsabilidad.
- Evaluación de impacto/riesgo.
- Participación en la continuidad del servicio de TI y planificación de los “disaster recovery”.
- Coordinación del Comité de gestión del Cambio (CAB).
- Revisión/aprobación.
- Establecer y administrar el calendario de cambios aprobados.
- Implementación.
- Verificación (prueba).
- Cierre.

Los siguientes puntos identifican las funciones y responsabilidades más relevantes dentro del servicio de Gestión del Cambio que el proveedor realizará:

- Mantener y documentar los procedimientos de Gestión del Cambio según las tareas del proceso de Gestión del Cambio descritos anteriormente.
- Participar en la evaluación del riesgo para que el cambio sea introducido sin ser probado completamente.
- Ser consultado e informado de revisiones y auditorías de control de calidad de Gestión del Cambio de procesos y de registros de Gestión del Cambio.

4.1.3.2 Gestión de la Configuración

El proceso de Gestión de la Configuración se compone de las tareas asociadas con la provisión de un modelo lógico de los activos de servicios (incluyendo licencias de software) y sus relaciones mediante la identificación, control, mantenimiento y verificación del hardware, software y documentación instalados (contratos de mantenimiento, documentos ANS, etc.).

Los objetivos son dar cuenta de todos los activos y configuraciones de TI, proporcionar información precisa sobre las configuraciones, proporcionar una base sólida para la administración de incidencias, problemas, cambios y versiones, y verificar los registros de configuración en la infraestructura y corregir cualquier excepción. Los siguientes puntos identifican las funciones y responsabilidades más relevantes de Gestión de la Configuración que el proveedor realizará:

- Mantener y documentar el procedimiento de Gestión de la Configuración para que cumplan con los requisitos y se adhieran a las políticas definidas.
- Instalar y mantener herramientas de gestión de configuración asociadas a la pila tecnológica.
- Introducir / cargar datos de configuración en la base de datos de configuración asociadas a la pila tecnológica.
- Establecer interfaces de procesos para la Gestión de Incidencias y Problemas, Gestión del Cambio, Soporte Técnico, Mantenimiento y Gestión de Activos.
- Establecer controles de autorización apropiados para modificar los elementos de configuración y verificar el cumplimiento de licencias de software.
- Mantener procedimientos para establecer líneas de base de configuración como puntos de referencia para reconstrucciones y proporcionar la capacidad de volver a estados de configuración estables.
- Proporcionar un informe de deficiencia y las medidas adoptadas para abordar los problemas identificados.
- Ser informado de la auditoría de la gestión de la configuración y la precisión de los datos de configuración.

4.1.3.3 Gestión de Activos

El proceso de Gestión de Activos comprende las tareas asociadas con el proceso de la gestión y seguimiento continuos del ciclo de vida de los componentes existentes de la Pila Tecnológica de Servicio (por ejemplo, hardware, software, licencias de software, mantenimiento…etc.) y sus atributos (contratos, proveedores, números de serie, etc.). Los siguientes puntos identifican las funciones y responsabilidades más relevantes de Gestión de Activos que el proveedor debe realizar:

- Mantener y gestionar un sistema de gestión de activos que cumpla los requisitos del cliente y se adhiera a las políticas definidas.
- Gestionar el ciclo de vida de todos los activos desde la identificación, ordenación de pedidos, inventario, instalación y mantenimiento hasta la eliminación.
- Actualizar registros de activos dentro del alcance relacionados con todas las actividades de cambio aprobadas.
- Ser consultado para proporcionar un plan de remediación de la Gestión de Activos para las deficiencias encontradas.
- Participar en los informes de auditoría y los planes de remediación de la información de la gestión de inventario de activos.
- Ser informado de la auditoría de calidad periódica del sistema de Gestión de Activos.

4.1.3.4 Gestión de Licencias de software

El proceso de Gestión de Licencias de software comprende las tareas asociadas con la identificación, adquisición y eliminación, así como la gestión y seguimiento continuos del software y sus licencias correspondientes. Los siguientes puntos identifican las funciones y responsabilidades más relevantes del proceso de Gestión de Licencias de software que el proveedor debe realizar:

- Recomendar mejoras a los requisitos y políticas de gestión de licencias de software.
- Mantener y documentar procedimientos de Gestión de Licencias de software que cumplan con los requisitos y se adhieran a políticas definidas como asignadas a la Gestión de Activos.
- Administrar y mantener (por ejemplo, monitorizar, rastrear el estado, verificar, auditar, realizar el cumplimiento del contrato) licencias de software y medios a través del ciclo de vida de la licencia de software.
- Desarrollar y mantener el inventario de todas las licencias de software dentro del sistema de Gestión de Activos.
- Informar a EJIE sobre cualquier excepción a los términos y condiciones del vendedor, incluyendo incumplimiento de licencia.
- Proporcionar a EJIE informes y recomendaciones para usar en la toma de decisiones de adquisición y descontinuación de software.
- Proporcionar recomendaciones para adquirir licencias adicionales, recomendar alternativas o restringir el uso cuando sea necesario y apropiado, para restaurar o continuar manteniendo el cumplimiento de las licencias.
- Identificar y reportar problemas de cumplimiento de licencias a EJIE y proporcionar recomendaciones para resolver el problema de cumplimiento.
- Gestionar y realizar auditorías y conciliar el número de licencias con el número de instalaciones, según lo solicitado por EJIE.
- Proporcionar recomendaciones a EJIE para resolver cualquier problema de conciliación de software.

4.1.3.5 Gestión de Versiones/Entregas

El proceso de Gestión de Versiones/Entregas se preocupa por implementar los cambios a los servicios de TI definidos y cubre tanto el software como el hardware. Las tareas de Gestión de Versiones son actividades que tienen una visión holística de un cambio en un servicio para garantizar que los aspectos técnicos y no técnicos de una versión relacionados con el software y el hardware cambian.

Estos cambios se pueden implementar desplegando una combinación de nuevas aplicaciones o software de infraestructura y/o hardware actualizado o nuevo, o simplemente haciendo cambios en la documentación, como horas de servicio o arreglos de soporte. Los procesos y actividades de Gestión de Versiones están relacionados entre sí y son complementarios con el proceso de Gestión del Cambio, así como la Gestión de la Configuración y la Gestión de Problemas.

La gestión de Versiones incluye las siguientes actividades:

- Establecer políticas y procedimientos estandarizados de gestión de versiones.
- Gestionar la planificación y la programación global del calendario general de versiones, así como para las versiones individuales.
- Establecer y administrar la documentación de versiones.
- Gestionar los procesos de diseño, creación y configuración de la versión.
- Liberar y gestionar pruebas.
- Planificar el despliegue incluyendo planes de calidad y planes de marcha atrás.
- Comunicar, preparar y formar la versión.
- Gestionar el despliegue/distribución e instalación de todos los elementos de una versión.
- Documentar cada versión y actualizar la base de datos de gestión de configuración (CMDB).

Las versiones también pueden consistir en una serie de correcciones de problemas y mejoras a los servicios de TI existentes. También pueden ser servicios de migración como actividades asociadas con la instalación de componentes de TI nuevos o mejorados (por ejemplo, hardware, software [sistema operativo] y componentes de red).

Una versión consiste en el software nuevo requerido y cualquier hardware nuevo o modificado necesario para implementar los cambios aprobados. Las versiones se dividen generalmente en:

- Versiones mayores de software y actualizaciones de hardware o reemplazos, que normalmente contiene grandes áreas de nueva funcionalidad. Normalmente, actualización principal reemplaza todas las actualizaciones menores anteriores, las revisiones y las correcciones de emergencia.
- Versiones menores de software y actualizaciones de hardware, que contiene normalmente pequeñas mejoras y correcciones, algunos de los cuales ya han sido emitidos como correcciones de emergencia. Normalmente, una actualización o actualización secundaria reemplaza todas las correcciones de emergencia anteriores.
- Software y correcciones de hardware de emergencia, normalmente contiene las correcciones a un pequeño número de problemas conocidos.

Los siguientes puntos identifican las funciones y responsabilidades más relevantes de Gestión de Versiones/Entregas que el proveedor realizará:

- Establecer y mantener un entorno o entornos seguros apropiados en los que todas las versiones autorizadas de todos los programas informáticos, y donde todos los repuestos de hardware estén almacenados y contabilizados.
- Mantener copias maestras de todas las versiones nuevas del software y del elemento de configuración de actualización.
- Asegurar que todos los repuestos de hardware están protegidos reflejados en la(s) base(s) de administración de configuración(s).
- Desarrollar planes de calidad y planes de marcha atrás según sea apropiado para cada versión.
- Asegurar que todos los entornos de prueba necesarios estén disponibles y configurados adecuadamente para admitir pruebas de la versión.
- Revisar los planes de prueba de aceptación de la versión.
- Instalar mejoras en la arquitectura técnica o servicios proporcionados.

- Instalar componentes de la pila de servicio nuevos o mejorados (por ejemplo, hardware, software, middleware, utilidades, redes, periféricos, configuraciones) de acuerdo con los procedimientos de gestión de cambios de EJIE.
- Realizar actualizaciones de componentes de la pila de Servicio como resultado de nuevas y mejoradas aplicaciones y arquitecturas y planes y requisitos de actualización de EJIE (por ejemplo, hardware, software, middleware, utilidades, redes, periféricos, configuraciones).
- Instalar la infraestructura física según sea necesario de acuerdo con los procedimientos de Gestión del Cambio de EJIE.
- Realizar la migración y conversión de datos mediante métodos electrónicos o manuales como resultado de la implementación o migración (por ejemplo, bases de datos, repositorios de administración de sistemas de red, tablas de direcciones, Bases de Información de Gestión [MIB]).
- Realizar pruebas apropiadas en todas las instalaciones, movimientos, agregados y cambios por requerimientos, de acuerdo con los procedimientos de la Gestión del Cambio de EJIE.
- Administrar y programar el entorno de prueba de integración.
- Instalar equipos, software o servicios nuevos y mejorados para transitar sin problemas al entorno existente, basándose en los requisitos definidos en las especificaciones y en los documentos de diseño.
- Realizar modificaciones y ajustes de rendimiento o mejoras en el software del sistema y utilidades como resultado de cambios en las normas de arquitectura o adiciones y mejoras del entorno.
- Probar las nuevas versiones de hardware y software soportados para garantizar que el rendimiento y la funcionalidad requeridos se mantengan en conformidad con requerimientos de servicio de EJIE.
- Documentar las verificaciones post-despliegue, planes de marcha atrás y resultados.
- Proporcionar al personal técnico de TI de EJIE y los usuarios finales formación relacionada con la implementación de nuevos productos y servicios por requerimientos.

4.1.3.6 Transferencia del Conocimiento

El proceso de Transferencia del Conocimiento distingue los siguientes dos tipos que la empresa adjudicataria proporcionará:

- Transferencia de conocimientos para la mejora de habilidades a través de la instrucción a su propio personal. EJIE proporcionará la información y documentación precisa sobre en el entorno técnico y de negocio de EJIE para facilitar la transferencia de este conocimiento.
- Transferencia de conocimiento derivado de la efectiva prestación del objeto del contrato para servicios propios o contratados por EJIE con el propósito expreso de explotar las funciones y características del entorno informático de EJIE. Los métodos de entrega pueden incluir instrucciones en sesiones o reuniones tanto individuales como colectivas tipo webinar o similares.

Los siguientes puntos identifican las funciones y responsabilidades más relevantes de formación y Transferencia de Conocimiento que la empresa adjudicataria debe realizar:

- Mantener y documentar procedimientos de Transferencia del Conocimiento para asegurar que el personal técnico adscrito al servicio entienda los componentes técnicos clave.
- Desarrollar, documentar y entregar, para su personal, los requisitos de formación que apoyen la provisión continua de servicios a EJIE, incluyendo cursos de actualización según sea necesario e instrucción sobre nuevas funcionalidades.
- Realizar formaciones entre su personal según sea necesario para mantenerse al día con los sistemas, software, características y funciones para las que se presta asistencia técnica, con el fin de mejorar el rendimiento del Servicio.
- Proporcionar materiales de formación continua, o realizar sesiones tipo webinar o similares derivados del objeto del contrato, para otros servicios propios o contratados por EJIE tales como CAU, operación u otros, según lo definido por EJIE.
- Proporcionar materiales de formación continua, o realizar sesiones tipo webinar o similares derivados del objeto del contrato, para entidades cliente de EJIE, según lo definido por EJIE.

4.1.3.7 Documentación

El proceso de Documentación comprende las tareas asociadas con el desarrollo, revisión, mantenimiento, reproducción y distribución de información de la pila del servicio en forma impresa y electrónica. Los siguientes puntos identifican las funciones y responsabilidades relevantes de la Documentación que el proveedor debe realizar:

- Proporcionar resultados en formato acordado para apoyar las actividades a lo largo del ciclo de vida de los servicios, tal como se especifica en la pila del servicio.
- Documentar especificaciones y configuraciones del sistema (por ejemplo, topología de interconexión, configuraciones, diagramas de red, diagrama de flujo de datos, mapas del sistema, etc.).
- Mantener y documentar los procedimientos operativos estándar (por ejemplo, arranque, conmutación por error/recuperación de desastres, procesamiento por lotes, copia de seguridad, peticiones de catálogo recurrentes, herramientas más utilizadas, etc.)
- Mantener y documentar los procedimientos operativos avanzados necesarios para la gestión de las herramientas y plataformas administradas desde el Servicio.
- Mantener y documentar, bajo los procedimientos para ello establecidos, el trabajo realizado por el Servicio en la plataforma de gestión de servicios TI que aplique en cada caso ya sea con relación a Incidencias, Problemas, Peticiones, Base de Datos de Conocimiento, Base de Datos de Activos, etc.

4.1.4 Operación del Servicio

Los procesos principales para la Operación del Servicio son los siguientes:

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

4.1.4.1 Gestión de Incidencias

El proceso de Gestión de Incidencias se encarga de las actividades asociadas con la restauración de la operación de servicio normal lo más rápido posible y minimizar el impacto adverso en las operaciones de negocio del cliente, asegurando así que se mantienen los mejores niveles posibles de calidad y disponibilidad del servicio.

Las principales tareas del proceso de Gestión de Incidencias incluyen:

- Detección y grabación de incidentes.
- Clasificación de incidentes y apoyo inicial.
- Investigación y diagnóstico de incidentes.
- Escalado de incidentes.
- Resolución y recuperación de incidentes.
- Cierre del incidente.

Los siguientes puntos identifican las funciones y responsabilidades más relevantes de Gestión de Incidencias que el proveedor realizará:

- Mantener y desarrollar procedimientos de Gestión de Incidencias que soporten los requisitos de soporte de la Gestión de Incidencias de EJIE.
- Resolver incidencias en el primer contacto de acuerdo con el Manual de Procedimientos, los documentos de base de datos de conocimiento y las bases de datos de configuración.
- Registrar todas las llamadas/consultas que lleguen.
- Identificar, filtrar y clasificar eventos e incidencias a un nivel de prioridad y manejar de acuerdo con los procedimientos acordados de respuesta a incidencias.
- Diagnosticar y resolver incidencias. Cuando sea posible, implementar acciones correctivas apropiadas para errores conocidos (por ejemplo, soluciones para problemas no resueltos conocidos).
- Escalar los incidentes al grupo de servicios de nivel siguiente apropiado dentro de los fabricantes, EJIE o un proveedor de servicios de terceros, tan pronto como esté claro que la incidencia no puede ser resuelta sin ayuda adicional o cuando se requiera para cumplir con los requisitos de nivel de servicio y los tiempos de respuesta.
- Monitorizar y rastrear el progreso de la resolución de incidencias hasta el cierre final y registrar/actualizar el estado del registro de las incidencias según corresponda.
- Proporcionar asistencia técnica y de procesos de expertos para aplicaciones dentro del ámbito de aplicación en el Nivel 2 y escalar al recurso de Nivel 3 según sea necesario.
- Proveer asistencia de Nivel 2 a consultas sobre las características, funciones y uso de software para todo el hardware y software dentro del alcance.
- Proporcionar soporte de Nivel 2 para aplicaciones de software en la lista de aplicaciones compatibles.
- Comprobar que todos los registros (por ejemplo, el inventario, el activo y los registros de Gestión de la Configuración) se actualizan para reflejar la incidencia finalizada/resuelta.
- Ayudar a los usuarios con preguntas relacionadas sobre funcionalidades del software dentro del alcance.
- Documentar soluciones para resolver incidencias en la base de conocimientos. Actualizar con precisión toda la información pertinente a los problemas.
- Notificar al personal designado por EJIE de todas las incidencias de Prioridad 1 y Prioridad 2 dentro del plazo designado.
- Mantener registros actuales e históricos de todas las incidencias y la resolución de las mismas durante la vigencia del contrato y proporcionar capacidades de generación de informes y tendencias.
- Resolver problemas, diagnosticar y resolver incidencias para todo el software con garantía y sin garantía.
- Participar en la identificación, escalado y resolución extremo a extremo de las incidencias, y en el proceso de cierre, incluyendo la gestión de tickets de escalado a terceros.
- Determinar, si es posible, si se debe abrir un problema para resolver una incidencia.
- Seguimiento del estado actual de cualquier incidencia y su registro de problemas correspondiente para asegurar que los problemas identificados sean registrados y resueltos.
- Asegurar que las actividades de resolución de incidencias se ajusten a los procedimientos definidos de Gestión del Cambio.
- Revisar periódicamente el estado de los incidentes abiertos y no resueltos y los problemas conexos, así como los progresos realizados en los problemas registrados.
- Participar en las sesiones de revisión de la gestión de problemas según corresponda.
- Llevar a cabo sesiones de revisión de incidencias y proporcionar listado y estado del mismo categorizado por impacto.
- Coordinar con otros grupos de soporte de Nivel 2 de EJIE para adquirir y transferir conocimientos sobre resoluciones de incidencias y problemas y registrar este conocimiento adquirido en la base de conocimientos para facilitar una mayor capacidad para el servicio de Nivel 1 de EJIE.
- Realizar un seguimiento con los usuarios finales que informaron del incidente para verificar que el incidente fue resuelto a satisfacción del usuario final.
- Cerrar los incidentes que se resolvieron satisfactoriamente.
- Proporcionar informes de la Gestión de Incidencias, según sea necesario.

La clasificación de incidencias está tipificada actualmente en Críticas, Altas, Medias y Bajas.

4.1.4.2 Gestión de Problemas

El proceso de Gestión de Problemas se encarga de minimizar el impacto adverso de incidencias y problemas en el negocio, causado por errores dentro de la infraestructura de TI, y para prevenir la repetición de incidencias relacionadas con estos errores determinando la causa subyacente desconocida, asegurando que se inician acciones para mejorar o corregir la situación.

El proveedor proporcionará servicios de gestión de problemas reactivos diagnosticando y resolviendo problemas en respuesta a uno o más incidentes que han sido reportados a través de la Gestión de Incidencias. Proporcionará un manejo proactivo de problemas para identificar y resolver problemas y errores conocidos antes de que ocurran las incidencias, incluyendo realizar actividades de análisis predictivo, donde sea práctico, identificar posibles problemas futuros, desarrollar planes de mitigación recomendados e implementar acciones y procesos correctivos de mitigación aprobados. El proveedor también mantendrá, actualizará y difundirá información sobre problemas y las soluciones y resoluciones apropiadas, de manera que el número y el impacto de incidentes que ocurran dentro de la infraestructura de TI del cliente se reduzca con el tiempo.

Las principales tareas de la Gestión de Problemas son:

- Control de problemas.
- Control de errores.
- Prevención proactiva de problemas.
- Realización de grandes revisiones de problemas.
- Entrega de informes de gestión de problemas.

El proveedor también es responsable de asegurar que las resoluciones a los problemas se implementan a través de los procedimientos de control apropiados, especialmente la Gestión del Cambio y la Gestión de Versiones. El proveedor debe coordinar las actividades de Gestión de Problemas con los distintos equipos dentro del proveedor, EJIE y los proveedores de terceros responsables de realizar las actividades de Gestión de la Configuración, Gestión de la Disponibilidad, Gestión de la Capacidad, Gestión de Continuidad de Servicio de TI y Gestión de Nivel de Servicio.

Los siguientes puntos identifican las funciones y responsabilidades relevantes de la Gestión de Problemas que el proveedor deberá realizar:

- Mantener y documentar procedimientos apropiados y metodologías que apoyen los requisitos y políticas de la Gestión de Problemas aprobados y que cumplan con los requisitos de EJIE.
- Asegurar que las actividades de Gestión de Problemas se ajusten a los procedimientos definidos de Gestión del Cambio establecidos en el Manual de Procedimientos.
- Coordinar con los equipos apropiados de Gestión de Incidencias y tomar posesión de las actividades de Gestión de Problemas de todos los problemas determinados para residir en el área de responsabilidad del proveedor (por ejemplo, detección, registro, RCA, etc.).
- Coordinar, escalar y realizar un seguimiento de las actividades de Gestión de Problemas dentro de EJIE y terceras partes relacionadas con los problemas determinados para residir en todas las áreas responsabilidad del proveedor.
- Señalar todos los incidentes que requieran que se realicen el estudio de causa raíz según procedimientos acordados.
- Asegurar que los problemas recurrentes relacionados con el área de responsabilidad del proveedor se revisen mediante procedimientos RCA (Root Cause Analysis).

- Realizar análisis proactivos de tendencias de incidencias y problemas y otros elementos de datos para identificar situaciones recurrentes que son o puedan ser indicativas de problemas futuros y puntos de fallo.
- Perseguir e informar sobre problemas, tendencias y fallos e identificar las consecuencias asociadas a los mismos.
- Desarrollar y recomendar acciones correctivas o soluciones para abordar incidencias y problemas recurrentes, así como estrategias de mitigación y acciones a tomar para evitar posibles problemas identificados a través del análisis de tendencias.
- Identificar, desarrollar, documentar y recomendar soluciones adecuadas para detectar errores conocidos de problemas no resueltos, y notificar a Gestión de Incidencias y a todas las demás partes interesadas apropiadas sobre su disponibilidad si se aprueba. Documentar la solución en la base de conocimientos.
- Coordinar y monitorizar el estado de las actividades de RCA realizadas por EJIE y proveedores de terceros (es decir, de otras áreas de servicios de TI).
- Documentar y actualizar la base de conocimiento de Gestión de Problemas con información sobre acciones, actividades y estado de resolución de problemas (por ejemplo, causa raíz, errores conocidos, soluciones alternativas, etc.) y notificar a todos los interesados apropiados sobre la disponibilidad de información.
- Coordinar con EJIE y proveedores de servicios terceros para asegurar que el conocimiento sobre problemas relacionados con otras áreas de servicios de TI sea capturado y registrado en la base de conocimiento centralizada de Gestión de Problemas.
- Asegurar que las actividades de resolución de problemas se ajusten a los procedimientos definidos de Gestión del Cambio establecidos en el Manual de Procedimientos.
- Proporcionar informes de estado detallando la causa raíz y el procedimiento para corregir los problemas recurrentes, según lo determine EJIE.
- Realizar reuniones de revisión de la Gestión de Problemas y proporcionar listado y estado de las mismas clasificadas por impacto.
- Revisar periódicamente el estado de los incidentes abiertos y los problemas conexos, así como los progresos realizados en la solución de los problemas.
- Crear la documentación de RFC con las acciones correctivas recomendadas que se deben tomar para resolver un problema y enviar a EJIE para su revisión y aprobación.
- Realizar sesiones periódicas de revisión proactiva de la Gestión de Problemas.
- Proporcionar informes de gestión de problemas según se requiera.

4.1.4.3 Operación y Administración

El proceso de Operación y Administración comprende las tareas asociadas con la provisión de una infraestructura de TI estable y con procedimientos efectivos y eficientes para asegurar que los servicios de TI cumplan con los objetivos y requerimientos de los ANS acordados. Los siguientes puntos identifican las funciones y responsabilidades relevantes de Operaciones y Administración que el proveedor debe realizar:

- Mantener y documentar procedimientos de Operaciones y Administración que cumplan con los requisitos y se adhieran a las políticas definidas.
- Desarrollar documentación operacional (es decir, libros de ejecución, listas de contactos, scripts de operaciones, etc.) que cumpla con los requisitos de EJIE.
- Coordinar con EJIE para implementar herramientas de administración para supervisar las aplicaciones de Infraestructura de TI y cliente.
- Instalar y configurar o utilizar herramientas de administración de tal manera que las incidencias, problemas y eventos sean identificados, reportados y resueltos proactivamente de acuerdo con los ANS acordados.
- Realizar una monitorización de eventos de servicios de TI para detectar condiciones anormales o alarmas, registrar condiciones anormales, analizar la condición y tomar medidas correctivas.
- Administrar software y hardware para cumplir con los ANS, minimizar el tiempo de inactividad y minimizar los requerimientos de recursos de EJIE.
- Gestionar y coordinar a subcontratistas y terceros para cumplir con los ANS.

- Desarrollar y proporcionar informes operacionales (diarios, semanales, mensuales) que proporcionen estado de las actividades operacionales, problemas de producción y métricas operativas clave.
- Proporcionar a EJIE o cualquier proveedor permitido una copia de documentación suministrada por terceros (incluyendo actualizaciones de los mismos).

4.1.4.4 Mantenimiento

El proceso de Mantenimiento comprende las tareas asociadas con el mantenimiento y la reparación de software y hardware incluyendo los servicios de "parcheado". La plataforma instalada y los niveles de versión del producto no deben estar detrás del nivel de versionado especificado por EJIE. Los siguientes puntos identifican las funciones y responsabilidades relevantes de Mantenimiento que el proveedor debe realizar:

- Mantener y documentar los procedimientos de mantenimiento que cumplan con los requisitos y se adhieran a las políticas definidas.
- Desarrollar calendarios de mantenimiento.
- Asegurar una cobertura de mantenimiento apropiada para todos los componentes de la torre del servicio.
- Proporcionar el mantenimiento y parcheado en las ubicaciones definidas por EJIE, incluyendo el envío de técnicos a la ubicación del servicio si es necesario.
- Realizar (y/o coordinar con el proveedor de mantenimiento de terceros, si procede) diagnósticos y mantenimiento en los componentes de la torre de servicio.
- Realizar un análisis del impacto y/o aplicabilidad de los parches y/o Service Packs proporcionados por fabricante, de acuerdo con las políticas y requisitos de EJIE.
- Revisar todos los parches relevantes para el entorno de TI y clasificar la necesidad y la velocidad a la que deben instalarse los parches de seguridad, según lo definido por las políticas y la Gestión del Cambio.
- Instalar los parches siguiendo los procedimientos de administración del cambio de EJIE y bajo su aprobación.
- Instalar (y/o coordinar con el proveedor de mantenimiento de terceros, si procede) los Service Packs, las versiones de mantenimiento de software y firmware, etc.
- Realizar la distribución de software y el control de versiones relacionado con el mantenimiento, tanto electrónico como manual.
- Reemplazar (y/o coordinar con el proveedor de mantenimiento de terceros, si procede) piezas defectuosas, incluido el mantenimiento preventivo, de acuerdo con las tasas de tiempo medio entre fallos publicadas por el fabricante.

4.1.4.5 Evolución Tecnológica

El proceso de Evolución Tecnológica comprende las tareas asociadas con la modernización del entorno de TI de forma continua, para asegurar que los componentes del sistema permanezcan actualizados con las plataformas tecnológicas de la industria. Los siguientes puntos identifican las funciones y responsabilidades relevantes de Evolución Tecnológica que el proveedor debe realizar:

- Recomendar procedimientos y planes de gestión del ciclo de vida de evolución tecnológica adecuados para respaldar los requisitos del negocio de EJIE.
- Realizar las tareas necesarias para cumplir con los planes de evolución tecnológica.
- Proporcionar informes de gestión sobre el progreso de los planes de evolución tecnológica.

4.1.4.6 Gestión de Peticiones

El proceso de Gestión de Peticiones comprende las tareas para cumplir las peticiones de servicio (por ejemplo, solicitudes de cambio de contraseña o información). Los siguientes puntos identifican las funciones y responsabilidades relevantes de Gestión de Peticiones que el proveedor debe realizar:

- Mantener y documentar los procedimientos de Gestión de Peticiones que cumplan con los requisitos y se adhieran a las políticas definidas.
- Realizar las tareas necesarias para cumplir la solicitud.
- Proponer añadir nuevos servicios al catálogo en base a un análisis de todas las solicitudes recibidas.
- Proporcionar informes de gestión sobre el progreso y uso de los servicios.

4.1.4.7 Gestión de Eventos

El proceso de Gestión de Eventos comprende las tareas para asegurar que los elementos de Configuración (CI) y los servicios sean monitorizados constantemente, así como descartar y categorizar eventos antes de decidir qué acciones son las adecuadas. Se considera un desencadenante muy importante de actividades en la Gestión de Incidencias y la Gestión de Problemas. Los siguientes puntos identifican las funciones y responsabilidades relevantes de Gestión de Eventos que el proveedor debe realizar:

- Mantener y documentar los procedimientos de Gestión de Eventos que cumplan con los requisitos y se adhieran a las políticas definidas.
- Mantener mecanismos y reglas de monitorización de eventos. Establecer y mantener los mecanismos para generar reglas efectivas para los procesos de descarte y correlación de eventos.
- Clasificar y categorizar los eventos. Clasificar aquellos eventos que se pueden obviar, y asignar categorías a los que son significativos.
- Correlar eventos y seleccionar las respuestas según clasificación y categoría. Interpretar el significado de un evento y elegir una respuesta adecuada.
- Revisar y cerrar eventos. Verificar que los eventos hayan sido manejados adecuadamente y si se pueden cerrar.
- Analizar los eventos de manera que se identifiquen tendencias y patrones que puedan sugerir medidas correctivas necesarias.

4.1.5 Mejora Continua del Servicio

El proceso de Mejora Continua del Servicio engloba las tareas asociadas al análisis, medición, revisión y adaptación de los procesos inherentes al ciclo de vida de cada servicio TI con la intención de minimizar errores, optimizar la utilización de los recursos disponibles y cumplir con los parámetros de calidad del servicio con vocación de excelencia adecuando los requisitos tecnológicos y organizativos a los resultados de negocio. Este proceso se desarrolla de manera transversal al Servicio e implica a toda la organización siendo una parte intrínseca de la cultura de la misma.

Para lograrlo, es necesario identificar oportunidades de mejora y realizar las tareas necesarias para conseguir dichas mejoras. A tal efecto se adoptarán y adaptarán los procesos, servicios e infraestructuras de TI para alinearlos con las necesidades cambiantes del negocio y, así, incrementar su efectividad y rentabilidad.

El proveedor deberá formalizar, ejecutar y automatizar aquellas tareas de mantenimiento, adecuación y optimización que le sean encomendadas asegurando el correcto rendimiento de las tecnologías estratégicas y estándares que se detallan en el *Anexo I – Entorno tecnológico*.

Así mismo, como parte de las labores a desarrollar por el proveedor, se identificarán acciones proactivas de mejora en los sistemas administrados que den lugar a un incremento en la calidad del servicio suministrado por EJIE a sus clientes y usuarios. Estas acciones serán estructuradas en el **Plan de Transformación** que, cubriendo la totalidad del contrato, aglutine las líneas maestras que van a gobernar la Mejora Continua del Servicio y de las infraestructuras que lo componen, así como indicadores objetivos que permitan evaluar su grado de cumplimiento. A su vez, cuando así se requiera, de este plan general podrán derivar otros planes de mejora más específicos contando con la colaboración de otros grupos de EJIE siempre y cuando los beneficios para EJIE lo justifiquen.

Para la correcta gestión de la Mejora Continua se deberán tener en cuenta los siguientes conceptos clave:

- Definición de factores críticos a evaluar (CSF).
- Definición de indicadores que permitan evaluar los factores críticos (KPI).
- Retorno de la inversión (ROI): refleja la diferencia entre los beneficios y la cantidad invertida.
- Valor de la inversión (VOI): refleja valor añadido que no constituye un beneficio económico y que se obtiene a largo plazo.

Los objetivos a alcanzar en este proceso aún se pueden concretar más en:

- Revisar, analizar y hacer las recomendaciones de mejora para cada proceso, servicio o infraestructura de TI.
- Revisar y analizar el grado de cumplimiento de los ANS acordados.
- Identificar e implementar mejoras que aumenten el ROI y VOI de los servicios TI, sin sacrificar la satisfacción del cliente.
- Mejorar la calidad de los servicios, incorporando nuevos procesos adaptados a los requisitos del cliente, aumentando la eficiencia y efectividad.

4.2 Requisitos específicos del Servicio

4.2.1 Estrategia del Servicio

La Seguridad en BATERA se considera un aspecto fundamental y fundacional de cualquier Servicio ofrecido. La Seguridad se quiere dejar de ver como un conjunto de equipamiento específicos y se quiere transitar hacia una visión transversal de la Seguridad en la que toda la Organización, empezando por las pilas tecnológicas, esté implicada y sea responsable de la misma (Enfoque SecOps). Asimismo, se quiere evolucionar a una visión en forma de “Servicios de Seguridad” asociados a otros servicios básicos ofrecidos por BATERA como pueden ser Hosting, Puesto de Trabajo, Identidad, etc.

En esa línea, el adjudicatario colaborará en esa transición al constituir el grupo de Soporte de Seguridad el equipo alrededor del que pivoten todas las iniciativas relacionadas con la seguridad, requiriendo, por lo tanto, un alto grado de colaboración con otros equipos y un alto grado de conocimientos en materia de seguridad que permita realizar recomendaciones en diferentes tipos de tecnología.

En esta nueva visión, las responsabilidades principales del adjudicatario serán:

- La Operación de los servicios de seguridad cuya responsabilidad directa es del adjudicatario, incluidos en el Anexo I – Entorno Tecnológico. Las tareas más relevantes se describen en otros apartados.
- La participación en la Estrategia y en la Definición de todos los Servicios de Seguridad, incluyendo aquellos de los que no sea responsable directo (IDaaS, por ejemplo) o de servicios que no sean específicamente entornos de Seguridad (Hardening de Puesto de Trabajo, por ejemplo).

- La participación en diferente medida en función de su responsabilidad final en el Diseño, la Transición y la Mejora continua de los Servicios de Seguridad y en las diferentes Demandas y Proyectos relacionadas con la Seguridad y que llegarán o se tratarán preferentemente a través del Área de Gestión de Iniciativas. Las tareas más relevantes se describen en otros apartados.
- La Vigilancia de Seguridad (Vulnerabilidades, Auditorías…) y la Gestión de la Respuesta a Incidentes de Seguridad (Procedente del SOC o de otras fuentes), en relación directa con otros implicados en estas actividades, como núcleo central dentro del enfoque SecOps.

4.2.2 Gestión de incidencias

4.2.2.1 Niveles de servicio ante incidencias

Será responsabilidad del Servicio la identificación, gestión, seguimiento y resolución de todas las incidencias que afecten a los entornos de los que sea responsable, definidos inicialmente en el *Anexo I - Entorno Tecnológico*. Deberán contemplarse todos los desplazamientos que pudieran ser necesarios para cubrir estos objetivos.

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.
- Dada la siguiente clasificación de las incidencias:
    - Críticas: Incidencias que impidan o degraden el uso del servicio, resultando en indisponibilidad total del servicio.
    - Alta: Incidencias que impidan o degraden el uso del servicio, resultando en incidencias masivas por parte del usuario final.
    - Media: Incidencias que impidan o degraden el uso del servicio, resultando en incidencias puntuales por parte del usuario final.
    - Baja: incidencias que no impiden el funcionamiento del servicio, pero que degradan su uso de manera leve, sin suponer incidencias de usuario final.

  la siguiente tabla muestra los tiempos máximos, a cumplir por la adjudicataria en las resoluciones, según la severidad de las incidencias:

Tiempos máximos	Críticas	Alta	Media	Baja
Respuesta	15 minutos en horario habitual y 30 minutos en horario extendido			
Resolución	2 horas horario habitual y 4 horas en horario extendido	4 horas	12 horas	24 horas

Los técnicos adscritos al Servicio además de tener que personarse en los centros dentro del ámbito (*Anexo II – Centros dentro del ámbito*) en horario habitual para la sustitución de equipos/módulos que provoquen

incidencias o degradaciones del servicio también deberán realizar estas labores en horario extendido cuando las incidencias afecten a sedes o infraestructuras categorizadas como críticas/graves. A mayores, si alguna de estas actuaciones implica la intervención de técnicos asociados a un soporte de nivel 3, estos deberán ser acompañados y supervisados en sus tareas por un técnico adscrito al Servicio.

4.2.2.2 Reposición de equipos averiados

En caso de avería, la adjudicataria deberá llevar a cabo la sustitución del equipamiento afectado en todos los centros del ámbito del expediente o nuevos que se adhieran haciendo uso de los contratos de tercer nivel que disponga EJIE o utilizando equipos en stock de EJIE para tal efecto.

La adjudicataria deberá llevar la gestión y el control del stock de repuestos, realizar propuestas de ampliación ante la indisponibilidad de activos, y proponer incorporar al stock nuevos modelos.

Todos los traslados deberán estar incluidos en la oferta presentada.

4.2.3 Gestión de peticiones

El catálogo de referencia inicial se encuentra especificado en el *Anexo III – Catálogo de servicios de referencia.* Se trata de catálogos vivos que se mantendrán actualizados junto con la evolución de los entornos tecnológicos tendiendo, en la medida de lo posible, a su consolidación en un único catálogo transversal. La existencia de dichos catálogos no implica que tareas fuera de los mismos no deban atenderse.

La adjudicataria deberá gestionar todas las solicitudes (incluidas las de equipamiento) procedentes de los centros y personarse en ellos en caso de ser necesario.

4.2.3.1 Instalación/desinstalación de equipamiento

La adjudicataria deberá llevar a cabo la instalación de equipamiento de seguridad en cualquiera de los centros del ámbito del expediente o nuevos que se adhieran.

Se entienden englobadas en esta casuística las acciones derivadas de nuevas necesidades y el mantenimiento evolutivo de las infraestructuras por cierre de centros, variación en las necesidades, variaciones en la capacidad, obsolescencia tecnológica, etc.

Del mismo modo, se deberá encargar de la desinstalación de equipamiento en desuso u obsoleto. En el primer caso, deberá ser convenientemente almacenado para su reutilización, mientras que en el segundo caso, se deberá sustituir por uno de capacidades iguales o superiores procediendo al reciclaje del equipamiento retirado según normativa vigente de protección del medio ambiente.

En cualquier caso, la instalación/desinstalación de equipamiento no implica únicamente las tareas de traslado, instalación física, configuración y parametrización de los equipos. En este sentido, se considerarán responsabilidades de la adjudicataria la puesta en marcha efectiva del servicio soportado por tal

equipamiento, la actualización del inventario y la documentación de gestión asociada (léase diagramas de red, bastionado entre otras), el etiquetado, la gestión de versiones software y licencias, la gestión de los contratos de mantenimiento y soporte nivel 3 en vigencia, la adición a herramientas de monitorización, el backup, la automatización, etc., así como la limpieza, paletizado y envío si procede del equipamiento que se desinstale.

Para algunas de estas tareas la adjudicataria dispondrá del apoyo de otros soportes técnicos de EJIE (principalmente Instalaciones), de soportes de nivel 3, de integradores tecnológicos y cualesquiera otros proveedores de servicios contratados por EJIE.

Todos los traslados deberán estar incluidos en la oferta presentada sin sobrecoste para EJIE.

4.2.3.2 Auditorías

La adjudicataria se compromete a personarse físicamente en sede de cliente para realizar y/o formar parte junto a cliente y posibles terceras partes implicadas en auditorías de las siguientes tipologías en las que pueda haber infraestructura bajo su responsabilidad:

1. Revisión física de los CPDs al menos una vez por semestre.
2. Revisión física de salas y armarios de comunicaciones en sedes remotas.

En el marco de las auditorías EJIE podrá solicitar, entre otras, las siguientes revisiones:

- Estado de los equipamientos de seguridad en términos de alarmas, sobrecalentamiento, ruidos sospechosos, etc.
- Retirada de equipamiento en desuso u obsoleto.
- Estado del conexionado, capacidad y redundancia de los elementos de seguridad.
- Estado de la alimentación y redundancia eléctrica de los elementos de seguridad.
- Condiciones ambientales de las salas en términos de temperatura, humedad, etc.

Como parte de estas auditorías se generarán informes descriptivos de la situación de la infraestructura. De su análisis podrán derivar otros informes correctivos que serán llevados a cabo dentro de las tareas de mantenimiento que se detallarán en siguientes puntos del expediente.

4.2.4 Gestión de activos

4.2.4.1 CMDB y ciclo de vida del CI

El concepto clave con relación a la gestión del inventario y el ciclo de vida de los activos es la base de datos de la gestión de configuración (CMDB por sus siglas en inglés). En ella se refleja el estado y los detalles de cada elemento de configuración (CI por sus siglas en inglés) que forma parte de las infraestructuras que componen el Servicio. Su actualización y mantenimiento resultarán cruciales para el correcto desarrollo del Servicio por lo que se deberá seguir escrupulosamente y con rigurosidad la política de “Modelado de la CMDB” durante la gestión de los activos ya estén estos desplegados (equipos en producción) o almacenados (equipos en stock). A tal efecto, la adjudicataria se compromete a mantenerla actualizada a

lo largo del contrato aglutinando en ella el inventario de equipamiento (padres e hijos) de todas las infraestructuras del Servicio y a proponer a EJIE las mejoras oportunas conducentes a su optimización.

4.2.4.2 Auditoría inicial

Con objeto de agilizar el conocimiento y control del entorno del que es responsable, el adjudicatario realizará una auditoría inicial durante los primeros 4 meses de los activos de los que sea responsable que incluirá:

- Visita a los CPDs para localización e identificación de los activos físicos.
- Revisión del listado total de activos, verificando, al menos: Existencia en CMDB, Existencia en Mapas de red y Documentación, Monitorización, Disponibilidad de backup, existencia de herramienta administrativa y acceso a la misma.

4.2.5 Gestión de eventos

Será responsabilidad de la adjudicataria la:

- Definición de la monitorización necesaria para garantizar la continuidad del Servicio plasmada en la línea base de monitorización.
- Monitorización continua del estado de los servicios:
  - Deberá administrar, gestionar, configurar y evolucionar las herramientas que EJIE ponga a su disposición.
- Implantación de nuevas plataformas si procede para garantizar la continuidad del Servicio.
- Monitorización continua de los recursos de sistemas implicados en cada servicio.
- Ingeniería asociada a la correlación de eventos y generación de alarmas.
- Aplicación y evolución de la línea base de monitorización dictada por EJIE.

La adjudicataria deberá integrar los sistemas objeto de este contrato con las diferentes plataformas de monitorización en diferentes entornos para la gestión de las alertas 24x7 identificadas durante la definición de la monitorización. Será necesaria la colaboración estrecha con otros soportes de EJIE para la ejecución de las tareas anteriormente citadas. Las herramientas de monitorización disponibles y las plataformas con las que se deben integrar se detallan en *Anexo I – Entorno tecnológico*.

4.2.6 Mantenimiento

4.2.6.1 Mantenimiento correctivo

Será responsabilidad de la adjudicataria el mantenimiento correctivo para la resolución de incidencias (in situ o en remoto) generadas por problemas o mal funcionamiento de los equipos incluidos en contrato, incluyendo las tareas necesarias hasta conseguir la restauración del servicio y otras asociadas a la gestión de incidencias y mejora continua, como pueden ser:

- Coordinación con los grupos de soporte y resto de proveedores que participan en el mantenimiento de la solución.
- Administración de los sistemas objeto del contrato y de los servicios ofrecidos a través de estos sistemas.
- Trabajos de reconfiguración de equipos.
- Reparación y/o sustitución de elementos averiados.
- Instalación/desinstalación de equipos, según necesidad.

- Instalación de software por: fallo, vulnerabilidades publicadas que afecten, necesidad de actualización detectada en el mantenimiento preventivo o por indicación del fabricante.
- Pruebas para verificación de la reposición del servicio.
- Escalado a fabricantes.
- Registro, seguimiento y documentación de la incidencia hasta su resolución.
- Elaboración de informes o partes de intervención o averías, a petición de EJIE.

4.2.6.2 Mantenimiento evolutivo hardware

Será responsabilidad de la adjudicataria el mantenimiento evolutivo hardware de los activos a administrar, para ello se participará en la toma de decisiones de compra de nuevo equipamiento ante reposiciones por rotura de stock, nuevas necesidades o sustitución de equipamiento por obsolescencia tecnológica.

La tendencia deseada será la de un parque lo más homogéneo posible, en ciclo de vida de producto, con soporte nivel 3 y/o fabricante en vigor y amoldado al uso que se le esté dando. En este punto también se tendrán en cuenta las posibles necesidades futuras a corto y medio plazo, en especial para sustituciones de hardware averiado o desbordado en capacidad y nuevas implementaciones, siguiendo siempre las recomendaciones y mejores prácticas sugeridas por la industria y los propios fabricantes obteniendo, en todo caso, el acuerdo y autorización por parte de EJIE para su implantación. Para las infraestructuras críticas existen mantenimientos preventivos contratados con proveedores de nivel 3. Ante cualquier deficiencia detectada durante los preventivos o en el día a día, se deberá notificar a EJIE inmediatamente para su pronta subsanación.

4.2.6.3 Mantenimiento evolutivo software

Será responsabilidad de la adjudicataria el mantenimiento evolutivo del software desplegado en los activos a administrar. La tendencia deseada será la de un parque actualizado y homogéneo siguiendo siempre las recomendaciones y mejores prácticas sugeridas por la industria y los propios fabricantes/desarrolladores del software en cuestión y obteniendo, en todo caso, el acuerdo y autorización por parte de EJIE para su implantación. Para las infraestructuras críticas existen mantenimientos preventivos contratados con proveedores de nivel 3. A mayores, se deberá seguir o, si no existiera, elaborar una política de Gestión de Versiones consensuada con EJIE que deberá ser implementada de acuerdo con el proceso de Gestión del Cambio. Ante cualquier deficiencia detectada durante los preventivos o en el día a día, se deberá notificar a EJIE inmediatamente para su pronta subsanación.

4.2.6.4 Mantenimiento preventivo

Será responsabilidad de la adjudicataria realizar acciones preventivas a partir de inspecciones y/o mediciones periódicas orientadas a mejorar el rendimiento y/o disponibilidad del servicio.

Por otra parte, también será responsabilidad de la adjudicataria el análisis pormenorizado de los informes preventivos periódicos contratados por EJIE a los soportes de nivel 3 con objeto de valorar si es necesario aplicar las medidas correctivas incluidas en ellos para evitar un potencial impacto en la infraestructura y, por ende, en los servicios.

En caso de optar por la implementación de las correcciones propuestas se priorizarán aquellas cuya no aplicación pudieran derivar en un mayor impacto. En caso de rechazar su aplicación, será necesario argumentar la decisión de manera objetiva y reflejarlo por escrito.

Se aprovechará el estudio de los informes preventivos para revisar que el anexo asociado a la tecnología analizada incluye todo el parque existente en ese momento y que ha sido chequeado en su totalidad por parte del soporte de nivel 3. También se contrastará la información relevante en él contenida con la anotada para esa tecnología en cuestión (p. ej. fechas fin de soporte).

En caso de que se detecten carencias en los informes preventivos analizados, la adjudicataria deberá trasladárselo a EJIE para tomar las medidas oportunas.

4.2.7 Documentación

Al comienzo del contrato desde EJIE se proporcionará a la adjudicataria un listado de documentos estratégicos a mantener actualizados durante el mismo.

Toda la documentación generada a lo largo del contrato será propiedad de EJIE y, por tanto, a su discreción y bajo su responsabilidad, podrá ser difundida a terceras partes con las que mantenga relación contractual.

4.2.7.1 Topología de red

La adjudicataria se compromete a mantener permanentemente actualizados y generar, si no existieran, los siguientes diagramas de red (tanto lógicos como físicos) con la herramienta y formato designado por EJIE:

- Nivel alto global del conjunto de infraestructuras de seguridad.
- Nivel alto global por cada infraestructura.
- Detalle de cada infraestructura
- Etc.

Estos diagramas serán aprobados por el responsable designado por EJIE y almacenados en la ubicación que EJIE disponga a tal efecto.

4.2.7.2 Procedimientos operativos

La adjudicataria se compromete a mantener permanentemente actualizados y generar, si no existieran, los procedimientos operativos tipo “How-To” para, al menos, las tareas incluidas en el *Anexo III – Catálogo de servicio de referencia* de modo que supongan de facto la base de datos de conocimiento para los técnicos del Servicio en relación con las peticiones más frecuentes.

Por otra parte, la adjudicataria deberá automatizar aquellas tareas más frecuentes susceptibles de ser entregadas al servicio de explotación para que sean ejecutadas por Operación con la idea de aligerar la carga de trabajo que supongan estas tareas al propio servicio.

4.2.7.3 Plataformas administradas

La adjudicataria se compromete a mantener permanentemente actualizada y generar, si no existieran, la documentación de gestión relativa a las plataformas que se explotan desde el Servicio. Se tomará como referencia el *Anexo I – Entorno tecnológico*.

4.2.8 Otros requisitos específicos

A continuación, se detallan otros requisitos específicos objeto de este expediente además de todos los expuestos anteriormente:

4.2.8.1 Perito Acreditado

Bajo demanda y ante un incidente de seguridad que lo requiera EJIE podrá solicitar servicios de un perito acreditado para la realización de un informe pericial que pueda ser necesario en la gestión de algún incidente de seguridad.

En la oferta se incluirán los servicios de la realización de UN INFORME AL AÑO por parte de un perito acreditado. Si algún año no se hace el informe, se acumulará la posibilidad de realizarlo al año siguiente.

Se desea que los informes obtenidos cumplan con la normativa UNE 197001:2011 o equivalente (“UNE 197001:2011. Criterios generales para la elaboración de informes y dictámenes periciales”).

El perito debe estar suficientemente acreditado y cumplir con las competencias para el análisis forense de las evidencias electrónicas definidas en la norma UNE 71506:2013 ó equivalente (“Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas.”).

4.2.8.2 Servicios en Cloud

La adjudicataria, además de todas las incidencias y peticiones relacionadas con su ámbito, deberá también detectar, escalar, coordinar y realizar el seguimiento de todas las incidencias y peticiones relacionadas con Servicios en nube en los que se basen Servicios de Seguridad bajo su responsabilidad (ver Anexo I – Entorno Tecnológico)

Del mismo modo, siendo los Servicios en Cloud un recurso de uso y relevancia creciente, la adjudicataria deberá promover por parte de sus técnicos la especialización en materia de Seguridad en este tipo de ámbitos y el Servicio tendrá que colaborar en la definición de la Seguridad de servicios en Cloud, tanto si están bajo su responsabilidad, como si no lo están, en la línea de Seguridad transversal que se ha comentado previamente.

4.2.8.3 Automatización y Delegación

En un entorno como BATERA, con un volumen creciente de usuarios y clientes, y en un ámbito absolutamente cambiante como es la Seguridad, la automatización y la delegación de funciones adquiere un papel protagonista de cara, por una parte, a conseguir servicios sostenibles y lo suficientemente dinámicos y, por otra parte, a que los técnicos del Soporte Seguridad se dediquen a aportar valor y no a realizar labores repetitivas o exentas de valor añadido.

En esta línea, la adjudicataria deberá promover varias líneas de actuación:

- A la hora de definir y diseñar Servicios se tendrá en mente la Operación posterior del mismo con objeto de minimizar los recursos necesarios para atender peticiones administrativas o, en su defecto, para poder delegar las peticiones a grupos de soporte de Nivel 1.
- Se analizarán las peticiones que se atienden actualmente con objeto de reducir progresivamente el volumen que debe ser atendido por técnicos de Soporte Seguridad actuando en varias líneas:
    - Reducirlas en base a automatizaciones
    - Simplificarlas o documentarlas para que puedan ser atendidas por grupos de soporte de Nivel 1
- Se trabajará de forma prioritaria en la automatización de configuraciones, despliegues o cualquier otra tarea recurrente con objeto de lograr un entorno más dinámico, con mejores tiempos de respuesta y autónomo, evitando dependencias de actuaciones manuales.
  Esta automatización adquiere especial importancia en ámbitos críticos relacionados con la seguridad como son los ámbitos de respuesta a incidentes o de actualización de IOCs, por ejemplo. En este sentido, la adjudicataria se compromete a trabajar de forma estrecha con el SOC, principalmente a través de su Área SecOps, en la generación de casos de uso para el SIEM y automatización de respuesta a eventos procedentes del mismo o de otras herramientas proporcionadas por el SOC.
- Se trabajará en la automatización progresiva de todo tipo de cuadros de mando, indicadores, informes, etc. que actualmente se realizan de forma manual. Esta automatización es la única vía sostenible para conseguir ofrecer la información tanto de forma interna como de forma externa a los clientes, segmentada y en fechas predefinidas e incluso “online” en algunos casos, como por ejemplo los cuadros de mando.

Las automatizaciones se realizarán mediante el uso de las herramientas que administra el servicio, las que se vayan incorporando a lo largo de la vigencia del contrato, y/u otras ofrecidas por la adjudicataria como parte de su oferta. Sin limitar el ámbito de actuación, se tomará como referencia inicial de las plataformas susceptibles de automatización las incluidas en el *Anexo I – Entorno tecnológico***.**

La adjudicataria, del mismo modo, colaborará de forma activa con el soporte de automatización y otros terceros con quienes EJIE mantenga relación contractual para la generación de automatismos en herramientas no administradas o explotadas directamente desde el Servicio.

4.2.8.4 Presencia in situ en actuaciones de terceros

Dada la criticidad del entorno, EJIE podrá solicitar dentro del ámbito de este contrato la realización de ciertos trabajos de mantenimiento, configuración o acompañamiento tanto dentro como fuera del horario habitual.

De tal modo, podrá solicitar la presencia in situ como medida de carácter preventivo en actuaciones de terceros que pudieran afectar a los servicios mantenidos. Entre los ejemplos de estas actuaciones están:

- Intervenciones de operadores de telecomunicaciones, integradores, soportes de tercer nivel y/u otros proveedores contratados por EJIE o sus clientes para instalar/modificar/desinstalar aplicaciones, servidores y otro tipo de máquinas que se conecten a la red de acceso o de Datacenter.

4.2.8.5 Colaboración

Sin perjuicio de otras posibles colaboraciones, durante la ejecución del contrato, la adjudicataria colaborará con los siguientes equipos, preferentemente a través de herramientas ITSM e ITBM:

- Niveles 1:
  - CAU EJIE y clientes finales
  - SOC EJIE
  - Operación EJIE
  - SASU EJIE
  - Referentes en EJIE y clientes finales (informáticos, SAFI, etc.)

- Niveles 2:
  - Grupos de Soporte de otras pilas de Servicios Convergentes

- Niveles 3:
  - Soportes de fabricantes contratados por EJIE.

- Otros:
  - Responsables de Soporte Seguridad de EJIE
  - Responsable de Seguridad de EJIE
  - Responsables de Seguridad de clientes finales
  - Funcionales y/o Equipos de desarrollo de EJIE o de clientes finales.

Durante la ejecución del contrato EJIE podrá exigir a la adjudicataria colaboración con cualquier departamento de EJIE que así la requiera.

De forma puntual y con un preaviso suficiente se podrá solicitar a la adjudicataria la realización de formaciones internas a EJIE, sus clientes y/o a terceras partes con las que EJIE mantenga relación contractual. La metodología, ámbito, tipología, formato, contenido, fases, personal docente y forma de evaluación de aprovechamiento de estas formaciones internas será consensuado entre EJIE y la adjudicataria para cada caso concreto.

4.2.8.6 Proyectos estratégicos

Durante el transcurso del contrato la adjudicataria deberá abordar, entre otros, los siguientes proyectos estratégicos en colaboración con EJIE:

- Acompañamiento y colaboración en la ejecución del Plan Director de Seguridad de EJIE.
- Definición/Estrategia de Servicios de Seguridad ofrecidos por BATERA.
- Establecimiento de un enfoque SecOps para hacer de la Seguridad algo transversal responsabilidad de toda la Organización.
- Consolidación de la convergencia:
  - Migración a Servicios Convergentes (Baterización)
  - Cierres de CPDs legacy
  - Equipo técnico orientados a tecnología convergente en vez de a clientes específicos
  - Optimización de los catálogos de servicios existentes y consolidación de los mismos en un único catálogo transversal.
  - Etc.
- Optimización e implementación de la política de monitorización transversal.

- Optimización e implementación de la política de configuración transversal.
- Optimización e implementación de la política de backup transversal.
- Optimización e implementación de la política de Gestión de Activos (CMDB).

4.3 Procedimiento y Calidad

El desarrollo del Servicio y su calidad deberá gobernarse de acuerdo a unos Acuerdos de Nivel de Servicio (ANS) que sirvan para medir el grado de calidad del mismo, un Plan de Calidad que desarrolle las estrategias y procedimientos implantados para la consecución de los ANS y unas reuniones periódicas que permitan evaluar la marcha del Plan de Calidad, el grado de cumplimiento de los ANS y permitir la toma de decisiones necesarias para mitigar desviaciones y mejorar continuamente la calidad del servicio.

Los niveles de servicio ofertados deberán cumplir, como mínimo, los indicados en este pliego. Adicionalmente el licitador podrá ofrecer otros ANS que complementen a los anteriores. Estos ANS, junto con sus penalizaciones asociadas, serán revisados por la adjudicataria y EJIE. En cualquier caso, si a criterio de EJIE fuera necesario para mejorar el servicio que presta a sus clientes, durante estas revisiones los ANS podrán ser actualizados, añadidos o retirados. El incumplimiento de dichos niveles será penalizado según lo dictado en el pliego de condiciones particulares.

El licitador deberá proponer un Plan de Calidad que garantice la correcta ejecución del servicio prestado y seguimiento del mismo.

Este plan deberá contemplar, al menos, los siguientes entregables:

- Plan de seguimiento del servicio. Incluyendo propuestas de cuadros de mando, informes, etc.
- Planteamiento de actividades de mejora continua del servicio debidamente formalizado en el Plan de Transformación.

La adjudicataria deberá asistir a reuniones de seguimiento periódicas según lo establecido en el presente pliego. Sin perjuicio de lo anterior, podrán establecerse más reuniones específicas debidamente justificadas promovidas/requeridas tanto por EJIE como por la adjudicataria. En lo posible, estas reuniones adicionales deberán planificarse con la antelación suficiente e indicar las personas convocadas y el orden del día a tratar.

4.3.1 Niveles de servicio

Tal y como se indicaba en la introducción, los ANS ofertados deberán cumplir, como mínimo, los indicados a continuación. 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	Tipo de penalización
Mejora continua	% de tiempo del Servicio dedicado a Mejora Continua	>20%	Mensual	3
Mejora continua	Nº de Peticiones genéricas promovidas a paquetizadas	>=1	Trimestral	3
Mejora continua	Nº de altas nuevas en la BBDD de conocimiento para operadores/clientes/técnicos en relación con incidencias frecuentes	>=1	Trimestral	3
Mejora continua	Nº de altas nuevas en la BBDD de conocimiento para operadores/clientes/técnicos en relación con tareas paquetizadas	>=1	Trimestral	3
Mejora continua	Nº de nuevos paneles propuestos en las herramientas del Servicio (u optimización de los existentes)	>=1	Trimestral	3
Gestión de cambios	Nº de Intervenciones sobre los sistemas realizadas sin registrar un cambio	<1	Mensual	3
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	>=1	Trimestral	3
Gestión de incidencias	% de incidencias reabiertas	< 3%	Mensual	2
Gestión de incidencias	% de incidencias con prioridad Crítica y Alta asignadas antes de 15 minutos	>= 90%	Mensual	1
Gestión de incidencias	% de incidencias críticas resueltas en horario habitual antes de 2 horas	>= 95%	Mensual	1
Gestión de incidencias	% de incidencias críticas resueltas en horario extendido antes de 4 horas	>=95%	Mensual	1
Gestión de incidencias	% de incidencias altas resueltas antes de 4 horas	>= 95%	Mensual	2
Gestión de incidencias	% de incidencias medias resueltas antes de 12 horas	>= 95%	Mensual	2
Gestión de incidencias	% de incidencias bajas resueltas antes de 24 horas	>= 95%	Mensual	2

Gestión de incidencias	Nº cambios que generan incidencias críticas o graves	<1	Mensual	1
Gestión de incidencias	No atención al chat de Responsables de Incidencias Graves	<1	Mensual	1
Gestión de incidencias	Nº de quejas de clientes o asistencia técnica por resolución de incidencias críticas o graves	<1	Mensual	1
Gestión de incidencias	Llamadas al 24x7 no atendidas o no contestadas en plazo (30 minutos).	<1	Mensual	1
Gestión de incidencias	No presencia en EJIE del 24x7 si fuera necesario en plazo (1 hora).	<1	Mensual	1
Gestión de incidencias	Incidencias con más de 5 días sin justificar	< 4	Mensual	2
Gestión de incidencias	Cumplimiento plan entregables	100%	Mensual	2
Gestión de la disponibilidad	% de disponibilidad de los servicios de Seguridad	>99%	Mensual	3
Gestión de peticiones	Cumplimiento plan entregables	100%	Mensual	3
Gestión de peticiones	% de peticiones que finalizan en plazo	>= 90%	Mensual	3
Gestión de peticiones	% de peticiones que generan incidencias	<= 1 %	Mensual	3
Gestión de peticiones	Peticiones de catálogo sin procedimiento operativo asociado	<1	Trimestral	3
Gestión de peticiones	% de peticiones que se registran en la categoría “Otros” del Catálogo	<=10%	Trimestral	3
Gestión de problemas	Tiempo medio para terminar un problema crítico	<=15 días	Mensual	2
Gestión de problemas	Tiempo medio para terminar un problema no crítico	<=40 días	Mensual	2
Gestión de problemas	Cumplimiento plan entregables	100%	Mensual	2
Gestión de problemas	% de problemas reabiertos	<5%	Trimestral	2
Gestión de problemas	% de problemas críticos o altos con solución definitiva	>80%	Semestral	2
Gestión de problemas	% de problemas con solución definitiva	>60%	Trimestral	2
Gestión de problemas	% de problemas repetitivos / proactivos	>15%	Trimestral	2

Gestión de problemas	% incidencias graves repetidas con respecto al total de incidencias graves solucionadas	<25%	Mensual	2
Gestión de versiones y entregas	Cumplimiento Política de Parches	>=95%	Trimestral	3
Mantenimiento	Nº de análisis de los informes preventivos realizados en más de una semana desde su entrega a soporte	<1	Trimestral	3
Mantenimiento	Nº de incidencias registradas por la no aplicación de las medidas correctivas incluidas en informes preventivos	<1	Trimestral	2
Documentación	Nº de plataformas administradas sin documentar	<1	Semestral	3
Documentación	% de documentos desactualizados del listado de documentos estratégicos marcados por EJIE	<=20%	Trimestral	3
Transferencia del conocimiento	Nº de recursos en incumplimiento de solvencia durante el contrato (caducidad de certificaciones, acuerdos EJIE/Adjudicataria para nuevas tecnologías recepcionadas o tecnologías preexistentes)	<=1	Mensual	4
Transferencia del conocimiento	Nº de miembros del equipo sin haber recibido un mínimo de 40 horas de formación externa	<1	Anual	4
Transferencia del conocimiento	Personal del Equipo Técnico de Seguridad sin certificación correspondiente en vigor a los seis meses del arranque del servicio existiendo un compromiso de obtención en el Plan de Formación del Servicio	<1	Mensual	4
Transferencia del conocimiento	Nº total de Técnicos de Seguridad cuyo tiempo de dedicación al tratamiento de incidencias y peticiones de una misma infraestructura exceda el 70%	<=2	Mensual	4
Gestión de la seguridad	Entrega Informes Trimestrales de Riesgos	≥4	Trimestral	3
Gestión de capacidad	Entrega Informes Trimestrales de Estado	≥4	Trimestral	3

Gestión de capacidad	N.º de incidencias críticas debidas a carga en los sistemas no detectadas con antelación	<2	Mensual	1
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)	<10%	Trimestral	4

Habrá indicadores de incidencias, peticiones y problemas con variables de tiempo que se medirán desde que las incidencias/peticiones/problemas son abiertos en el proceso buscando que el Servicio se involucre en su mejora mediante la colaboración con otros servicios que participen en él.

Los indicadores podrán ser solicitados individualmente para cada entidad de Gobierno Vasco y/o globales siendo obligación de la adjudicataria su cumplimiento en todos ellos.

Estos indicadores tendrán una revisión periódica a lo largo de la vigencia del contrato.

4.3.2 Plan de Calidad

Como se indicaba en la introducción, el plan de calidad se compone de diferentes secciones y entregables de los que el licitador tendrá que aportar propuesta en su oferta. A continuación, se listan las características mínimas que deberá cumplir cada sección o entregable. Será valorado, durante la fase de adjudicación, el formato y contenido propuesto de acuerdo con los criterios indicados en el pliego de condiciones particulares.

4.3.2.1 Plan de Seguimiento del Servicio

4.3.2.1.1 Cuadro de mando semanal del Servicio

El objetivo de este entregable es disponer de un resumen semanal relativo al estado del servicio que refleje por cada proceso ITIL los eventos más relevantes desde un punto de vista operativo.

Como parte de la oferta presentada el licitador deberá presentar una propuesta de cuadro de mando semanal que, al menos, deberá contener:

- Indicadores de incidencias.
- Indicadores de problemas.
- Indicadores de peticiones.
- Indicadores de próximas intervenciones.
- Indicadores de incidentes de seguridad.
- Indicadores de vigilancia de seguridad.

Los indicadores propuestos por la adjudicataria serán aprobados y complementados por EJIE. Su valoración se realizará de acuerdo con los niveles de servicio mínimos exigidos en el presente pliego y a los que se comprometa la adjudicataria en su oferta. En cualquier caso, tanto indicadores como niveles de servicio se deberán adaptar, a lo largo de la vigencia del contrato, a las necesidades que EJIE considere oportunas para el correcto desarrollo del servicio y su mejora continua.

4.3.2.1.2 Cuadro de mando mensual de Iniciativas (Demandas y Proyectos)

El objetivo de este entregable es disponer con carácter mensual de una visión global del grado de avance de todas las iniciativas (demandas, proyectos,…) en curso (tanto los impulsados desde el propio Servicio como aquellos en los que se colabora) así como describir los nuevos proyectos de próxima ejecución.

Como parte de la oferta presentada, el licitador deberá presentar una propuesta de cuadro de mando de proyectos que, al menos, deberá contener:

- Indicadores de iniciativas en curso impulsados desde el servicio.
- Indicadores de iniciativas en curso en los que el servicio colabora.
- Descripción de iniciativas de próxima ejecución.

Los indicadores propuestos por la adjudicataria serán aprobados y complementados por EJIE. Su valoración se realizará de acuerdo con los niveles de servicio mínimos exigidos en el presente pliego y a los que se comprometa la adjudicataria en su oferta. En cualquier caso, tanto indicadores como niveles de servicio se deberán adaptar, a lo largo de la vigencia del contrato, a las necesidades que EJIE considere oportunas para el correcto desarrollo del servicio y su mejora continua.

4.3.2.1.3 Cuadro de mando mensual de Estado de la Seguridad

El objetivo de este entregable es disponer con carácter mensual de una visión global del estado de la Seguridad (tanto de elementos responsabilidad del Servicio como de otros servicios) de las diferentes entidades adheridas a BATERA.

Como parte de la oferta presentada, el licitador deberá presentar una propuesta de cuadro de mando de Seguridad que, al menos, deberá contener:

- Indicadores de cada uno de los Servicios de Seguridad ofrecidos por BATERA

- Indicadores relativos al Roadmap Global de Seguridad que incluye las iniciativas impulsadas en cada uno de los Servicios de Seguridad ofrecidos por BATERA
- Indicadores relativos a los incidentes de Seguridad [Destacados respecto al resto de Servicios de Seguridad por su entidad]
- Indicadores relativos a la Vigilancia de Seguridad (Vulnerabilidades y Auditorías) [Destacados respecto al resto de Servicios de Seguridad por su entidad]

Los indicadores propuestos por la adjudicataria serán aprobados y complementados por EJIE. Su valoración se realizará de acuerdo con los niveles de servicio mínimos exigidos en el presente pliego y a los que se comprometa la adjudicataria en su oferta. En cualquier caso, tanto indicadores como niveles de servicio se deberán adaptar, a lo largo de la vigencia del contrato, a las necesidades que EJIE considere oportunas para el correcto desarrollo del servicio y su mejora continua.

Durante la vigencia del contrato los informes requeridos podrán ser independientes por entidades y organismos dependientes del Gobierno Vasco y/o global al servicio, a decidir por EJIE en cada caso.

4.3.2.1.4 Informe mensual del Servicio

El objetivo de este entregable es disponer con carácter mensual de una visión global del rendimiento del servicio desde un punto de vista ejecutivo.

Como parte de la oferta presentada el licitador deberá presentar una propuesta de informe mensual que, al menos, deberá contener:

- Resumen ejecutivo de volumetrías de incidencias, peticiones y problemas.
- Resumen ejecutivo del Estado de la Seguridad último mes.
- Gestión de incidencias último mes.
- Gestión de problemas último mes.
- Gestión de peticiones último mes.
- Mejora continua proyectos y procesos último mes.
- Gestión de la dedicación último mes.
- Cumplimiento de los ANS.

Durante la vigencia del contrato los informes requeridos podrán ser independientes por entidades y organismos dependientes del Gobierno Vasco y/o global al servicio, a decidir por EJIE en cada caso.

4.3.2.1.5 Informe de Capacidad

El objetivo de este entregable es analizar la capacidad asociada a servicios TI proporcionados por el Servicio con objeto de valorar si está correctamente dimensionada para cubrir la demanda actual y futura con el coste y plazos más razonables posible.

Como parte de la oferta presentada, el licitador deberá presentar una propuesta de Informe de Capacidad que, al menos, deberá contener:

- Equipamiento en stock disponible.
- % utilización de recursos hardware (CPU, memoria, almacenamiento).
- % utilización de licencias cuando aplique.

Durante la vigencia del contrato los informes requeridos podrán ser independientes por entidades y organismos dependientes del Gobierno Vasco y/o global al servicio, a decidir por EJIE en cada caso.

4.3.2.1.6 Informe cuatrimestral del Servicio

El objetivo de este entregable es disponer con carácter cuatrimestral de una visión global del rendimiento del Servicio desde un punto de vista ejecutivo y del grado de cumplimiento del Plan de Transformación.

Como parte de la oferta presentada, el licitador deberá presentar una propuesta de informe cuatrimestral que, al menos, deberá contener:

- Resumen ejecutivo de volumetrías de incidencias, peticiones y problemas.
- Resumen ejecutivo del Estado de la Seguridad últimos cuatro meses.
- Gestión de incidencias últimos cuatro meses.
- Gestión de problemas últimos cuatro meses.
- Gestión de peticiones últimos cuatro meses.
- Gestión de la dedicación últimos cuatro meses.
- Cumplimiento de los ANS durante los últimos cuatro meses.
- Grado de cumplimiento del Plan de Transformación.

Durante la vigencia del contrato los informes requeridos podrán ser independientes por entidades y organismos dependientes del Gobierno Vasco y/o global al servicio, a decidir por EJIE en cada caso.

4.3.2.1.7 Auditoría CPD

El objetivo de este entregable es conocer el estado físico y ambiental del equipamiento de Datacenter del Servicio para valorar con posterioridad si aplica realizar alguna medida correctiva sobre el mismo.

Como parte de la oferta presentada el licitador deberá presentar una propuesta de informe de auditoría CPD que, al menos, deberá contener:

- Parámetros ambientales a evaluar.
- Parámetros a evaluar en racks que albergan equipos de seguridad.
- Parámetros físicos a evaluar en dispositivos de seguridad.
- Parámetros a evaluar en cableados.
- Parámetros a evaluar en cuanto a la alimentación eléctrica.
- Metodología de evaluación de cada parámetro.

4.3.2.2 Plan de Transformación

El objetivo de este entregable es detallar las líneas maestras que van a gobernar la Evolución y Mejora Continua del Servicio y de las Infraestructuras e incluir indicadores objetivos que permitan evaluar su grado de cumplimiento.

Como parte de la oferta presentada, el licitador deberá presentar una propuesta de Plan de Transformación inicial que, al menos, deberá contener:

- Definición de factores críticos sobre los que se desarrollará el plan.
- Justificación del porcentaje de asignación de recursos de las diferentes áreas del servicio a ejecución del plan.
- Indicadores objetivos de seguimiento de la evolución y grado de cumplimiento del plan.

El plan definitivo, junto con los objetivos de cumplimiento se consensuarán con EJIE a partir de la propuesta final presentada por la adjudicataria.

4.3.3 Reuniones de seguimiento

Como se indicaba en la introducción, la adjudicataria deberá asistir a las reuniones de seguimiento periódicas listadas a continuación amén de las adicionales que se puedan establecer de forma discrecional.

	Objetivo	Participantes EJIE	Entregables	Participantes Adjudicataria
Seguimiento del Servicio (semanal)	Analizar el rendimiento del Servicio desde un punto de vista operativo a partir de los indicadores relativos a incidencias, peticiones, problemas e intervenciones gestionados por el Servicio	Responsables del Servicio de EJIE	Cuadro de Mando Semanal	Responsable del Servicio Responsable de Estrategia Responsable SecOps Responsable Operación
Seguimiento del Servicio (mensual)	Analizar el rendimiento del Servicio desde un punto de vista ejecutivo a partir de los indicadores relativos a incidencias, peticiones, problemas y proyectos gestionados por el Servicio	Responsables del Servicio de EJIE	Informe Mensual del Servicio	Responsable del Servicio Responsable de Estrategia Responsable SecOps Responsable Operación
Seguimiento de Proyectos (mensual)	Analizar el grado de avance de todos los proyectos en curso y de los futuros	Responsables del Servicio de EJIE	Cuadro de Mando Mensual de Proyectos	Responsable del Servicio Responsables de Área

Seguimiento de Estado de la Seguridad (mensual)	Analizar el Estado de la Seguridad	Responsables del Servicio de EJIE	Cuadro de Mando Mensual de Estado de la Seguridad	Responsable del Servicio Responsable de Estrategia Responsable SecOps Responsable Operación
Seguimiento del Servicio (cuatrimestral)	Analizar el rendimiento del Servicio desde un punto de vista ejecutivo y del grado de cumplimiento del Plan de Transformación	Responsables del Servicio de EJIE	Informe Cuatrimestral del Servicio	Responsable del Servicio
Reuniones de Operación (mensual)	Analizar incidencias relevantes o recurrentes elevadas a Operación de EJIE por parte de las herramientas de monitorización de los diferentes soportes	Área de Operación de EJIE	N/A	Responsable de Operación
Reuniones de Soportes (mensual)	Analizar incidencias relevantes o recurrentes asociadas a los diferentes soportes	Área de Gestión de Incidencias de EJIE	N/A	Responsable de Operación
Reuniones de Procesos (mensual)	Analizar la gestión de los diferentes Soportes en el ámbito de Procesos y establecer las directrices a seguir para su correcta implementación	Área de Procesos de EJIE	N/A	Responsable de Procesos

4.3.4 Metodología aplicable y entorno tecnológico

EJIE dispone de procedimientos y normativas propios para la gestión de los procesos que deberán cumplirse. La empresa adjudicataria deberá asumir y adecuarse a las herramientas y los procesos de trabajo predefinidos (Gestión de Incidencias, Gestión de Peticiones, Gestión del Cambio, etc.) para poder desarrollar su trabajo. Se valorará positivamente toda mejora aportada a dichas normativas.

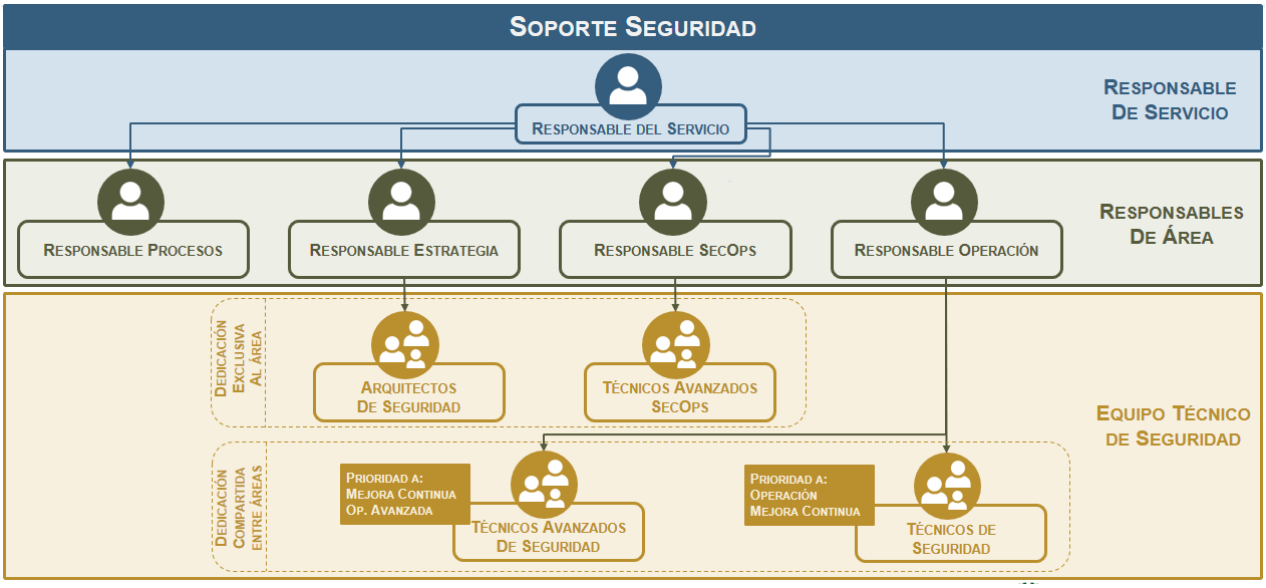
En cualquier caso, reseñar que la metodología principal de gestión TI por la que se rige EJIE es ITIL y el entorno tecnológico aplicable y las herramientas y equipamientos que lo conforman pueden consultarse en *Anexo I – Entorno tecnológico*. Adicionalmente, EJIE está incorporando el uso de metodologías Ágiles en el ámbito de la entrega de Productos y Servicios y, en lo que a Seguridad específicamente se refiere, quiere implementar un enfoque SecOps.

Dentro del sentido del proyecto BATERA dichas plataformas irán convergiendo durante el contrato.

5 Planificación y organización del servicio

5.1 Organigrama del Servicio

El equipo de trabajo encargado de construir el entorno objeto de este contrato deberá respetar el siguiente organigrama jerárquico (el número de recursos pintados por cada rol no es vinculante salvo en el caso de los roles de Responsable):



Tal y como se observa en la anterior figura, el Servicio estará dirigido por un **Responsable de Servicio** que junto con el responsable de EJIE del Servicio de Seguridad se encargarán de la gestión del servicio y de velar por el buen funcionamiento del mismo. La empresa adjudicataria, por tanto, deberá comunicar por escrito la designación de una persona de su organización encargada de ejercer dichas facultades de Dirección en lo referente al servicio contratado, responsabilizándose frente a EJIE de las personas que prestan el servicio.

En el siguiente nivel de la jerarquía se encuentran los **Responsables de Área**. Se pretende que haya tres áreas técnicas enfocadas a objetivos o fases del ciclo de vida del Servicio diferenciadas, pero que deben colaborar estrechamente entre ellas constituyendo un Soporte de Seguridad único, a saber:

- **Estrategia**: Éste área tiene, entre sus objetivos principales de la fase de Estrategia, colaborar con EJIE en la Definición de los Servicios de Seguridad ofrecidos por BATERA (tanto los que sean responsabilidad del Servicio como los que no lo sean). Entre los aspectos a definir se encuentran las Características de los Servicios, Políticas, Roadmap (de Productos y de Configuración), Indicadores de Seguridad y Procesos (Seguimiento, Evolución, Entregas…).
  Otros de sus objetivos principales será la ejecución del Roadmap de Seguridad de los servicios de los que sean responsables, así como la participación en las diferentes Iniciativas (Demandas, Proyectos, Entregas…) que surjan, como pueden ser en la incorporación de nuevos Servicios o en la evolución de los mismos, colaborando en el Diseño, Despliegue y en la Transición de esas Iniciativas para su entrega a Operación.
- **Operación**: Esta área tiene, entre sus objetivos principales, llevar a cabo la Operación de todos los Servicios de los que Soporte Seguridad es responsable.

- **SecOps**: Esta área tiene, entre sus objetivos principales, colaborar con EJIE en la implantación de un enfoque SecOps en la Organización, es decir, un enfoque en el que la Seguridad sea algo transversal responsabilidad de toda la Organización. En esa línea, éste área se encargará, al menos, de la vigilancia de la seguridad (alertas de vulnerabilidades, auditorías de seguridad, etc.), de la respuesta a incidentes de seguridad (reportados desde el SOC después de filtrar los eventos del SIEM en cuya definición de casos de uso esta área participará de forma especial, o procedentes de otros actores) y de la coordinación con el resto de grupos y departamentos con el fin de lograr el objetivo común de la Seguridad de la Organización.

Adicionalmente, como se ha comentado en apartados previos, la Mejora Continua es un elemento común que estará presente en todas las áreas, en cada una de ellas aplicando a las tareas propias del área.

Por cada una de las áreas habrá un Responsable que ejercerá el liderazgo en lo relativo a su Área:

- El **Responsable de Operación** ejercerá de líder de la fase ITIL de Operación de todos los Servicios responsabilidad del Soporte de Seguridad.
- El **Responsable de SecOps** ejercerá el liderazgo del enfoque SecOps que se quiere dar a la Seguridad de la Organización.
- El **Responsable de Estrategia** liderará al Soporte en las fases ITIL de Estrategia en lo relativo a todos los Servicios de Seguridad ofrecidos por BATERA.
- El **Responsable de Procesos**, por su parte, ejercerá de referente transversal dentro del Servicio en lo relativo al paradigma ITIL siendo responsable durante el periodo de vigencia del contrato de su correcta implementación a lo largo de los siguientes cinco fases principales que modelan el Soporte: Estrategia, Diseño, Transición, Operación y Mejora Continua.

En el siguiente nivel de la jerarquía se encuentra el **Equipo Técnico de Seguridad**. Se trata de un equipo técnico formado por personal con cuatro perfiles diferenciados:

- **Técnicos de Seguridad**: Perfiles de Seguridad con una orientación principalmente a la Operación y Mejora continua de los Servicios de Seguridad, pero sin perjuicio de participar ocasionalmente, con la tutela de los técnicos avanzados, en labores propias de éstos.
- **Técnicos Avanzados de Seguridad y Técnicos Avanzados SecOps**: Perfiles especializados de Seguridad con gran experiencia, conocimientos globales y transversales de seguridad que les permite ejercer, a parte de las tareas Operativas más avanzadas, tareas más específicas de Diseño, Transición y Mejora continua de Servicios, así como tareas propias de SecOps.
- **Arquitectos de Seguridad**: Perfiles altamente cualificados en materia de seguridad global, con un conocimiento profundo y transversal de la seguridad, y altamente especializados en ciertas tecnologías que les permite participar en la Estrategia, Diseño, Transición y Mejora Continua de los Servicios de Seguridad.

Con el objetivo de que las tareas Operativas no ocupen a todos los técnicos disponibles y no impidan en consecuencia el desarrollo de las tareas del resto de áreas, la organización de los perfiles del equipo técnico de Seguridad será como se muestra en el esquema:

- Arquitectos de Seguridad y Técnicos Avanzados SecOps: Tendrán dedicación exclusiva al área al que pertenezcan.
- Técnicos de Seguridad y Técnicos Avanzados de Seguridad: Tendrán dedicación prioritaria a las labores del Área de Operación del que dependerán (Operación Básica y Mejora Continua los Técnicos de Seguridad, Operación Avanzada y Mejora Continua los Técnicos Avanzados de Seguridad).
  Sin embargo, estos perfiles podrán participar en las tareas de otras áreas cuando así se requiera.
  La dedicación compartida de cada técnico con otras áreas será coordinada entre el responsable del servicio y los responsables de las áreas en base a las necesidades y prioridades marcadas por EJIE en cada momento.

Como complemento a lo anterior, es conveniente indicar que el responsable jerárquico de cada rol será el marcado por las flechas, salvo los Técnicos de Seguridad y Técnicos Avanzados de Seguridad, cuyo

responsable de base es el Responsable de Operación, pero que podrían depender de otros Responsables cuando están realizando tareas para otras áreas, por lo que quedaría de la siguiente manera:

- Responsable del Servicio: Responsable máximo por lo que no tiene superior jerárquico. Actúa como responsable jerárquico directo de los Responsables de Área.
- Responsable de Procesos: Su responsable es el Responsable del Servicio y no tiene subordinados.
- Responsable de Operación: Su responsable es el Responsable del Servicio y ejerce de responsable de los Técnicos de Seguridad y Técnicos Avanzados de Seguridad cuando estén trabajando para su Área.
- Responsable de SecOps: Su responsable es el Responsable del Servicio y ejerce de responsable de los Técnicos Avanzados SecOps y de los Técnicos Avanzados de Seguridad y Técnicos de Seguridad que tengan dedicación compartida cuando estén asignados a dicho Área.
- Responsable de Estragia, Diseño y Transición: Su responsable es el Responsable del Servicio y ejerce de responsable de los Arquitectos de Seguridad y de los Técnicos Avanzados de Seguridad y Técnicos de Seguridad que tengan dedicación compartida cuando estén asignados a dicho Área.

Por último, comentar que el equipo de trabajo deberá cubrir la totalidad de los roles recién descritos sin posibilidad de que existan roles compartidos. Relacionado con lo anterior, en todos los casos los roles de "Responsable" del organigrama deberán ser cubiertos por un único recurso.

5.2 Equipo de trabajo

5.2.1 Roles y ámbito de responsabilidad

Sin perjuicio de todo tipo de tareas que EJIE pueda requerir dentro de la provisión del Servicio de Soporte Seguridad a lo largo del contrato, así como de todos los procesos, tareas, etc. expuestas en el apartado de "Requisitos del Servicio", se detallan a continuación las tareas y consideraciones más relevantes a ejecutar por parte de los diferentes roles:

5.2.1.1 Aspectos comunes a todos los integrantes del servicio

Existen una serie de aspectos que todos los integrantes del Servicio deben tener siempre en mente para aplicarlos en su ámbito de responsabilidad, no eximiendo esto de que se establezcan controles específicos por parte del propio servicio para verificar que todo se cumple como está establecido:

- Orientación a Servicios: Todos los integrantes deben ser conscientes y estar implicados en la Oferta de Servicios de Seguridad de Calidad a los Clientes adscritos a BATERA. Los Servicios son ofrecidos por BATERA, no por grupos específicos, por lo que es de vital importancia la colaboración activa y proactiva entre equipos y departamentos para lograr el objetivo común.
- Servicios Convergentes: Aunque se sigue dando soporte a sistemas Legacy, el objetivo es consolidar la Convergencia y, por lo tanto, ofrecer servicios transversales. Los integrantes tendrán una orientación a los servicios convergentes, evitando la orientación a clientes específicos.
- Multidisciplinariedad: Como se ha comentado en varias ocasiones la Seguridad es transversal y, como tal, su alcance es muy amplio, demandando de todos los participantes en el servicio un conocimiento muy variado. Tanto responsables como técnicos del equipo deben velar, cada uno a su nivel, por que los integrantes del equipo sean multidisciplinares y puedan dar soporte al mayor número posible de tecnologías bajo su responsabilidad, evitando técnicos especialistas únicamente en tecnologías concretas.

- Mejora Continua: Autoevaluación continua de todas las actividades dentro de su ámbito de responsabilidad con el fin de implementar las medidas de ajuste o mejora necesarias. Adicionalmente, propondrán libremente mejoras no específicas de su ámbito de responsabilidad que serán escaladas dentro de la jerarquía del servicio y evaluadas en consecuencia.
- Automatización y Delegación: Como parte de la búsqueda de la Mejora Continua, los integrantes del servicio tenderán hacia y trabajarán en la automatización de todo lo que sea posible automatizar (configuraciones, procesos, informes, indicadores, respuestas a eventos, etc.) con las herramientas a su alcance en su ámbito de responsabilidad (scripts, herramientas de automatización, etc.).
  Asimismo, teniendo en cuenta que uno de los objetivos del Servicio de Soporte es aportar valor (evitando la dedicación a tareas repetitivas, por ejemplo), se trabajará siempre, cada uno en su ámbito de responsabilidad, teniendo en mente la administración sostenible de los entornos creando configuraciones, documentaciones, procedimientos, etc. permitan delegar administración a los Niveles 1 disponibles (CAU, SASU, etc.)
- Cumplimiento de ANS: En todo momento se tendrán en mente los ANS asociados a su ámbito de responsabilidad con el objetivo de cumplirlos escrupulosamente.
- Gestión del Conocimiento: Todos los integrantes generarán conocimiento en su ámbito de responsabilidad en forma de documentos, procedimientos, esquemas, etc. que alojarán en los repositorios o BBDD de conocimientos que EJIE ponga a su disposición.
  Del mismo modo, estudiarán la documentación existente y se encargarán de la actualización de la misma dentro de su ámbito de responsabilidad.
- Líneas Base: Todos los integrantes del servicio deben ser conscientes de la existencia de unos mínimos que deben cumplir todos los activos bajo su responsabilidad y trabajarán para que así sea, colaborando al nivel que les corresponda en el cumplimiento en todo momento de las políticas establecidas por parte de EJIE (línea base de Configuración, HA, políticas de Backup, políticas de Monitorización, CMDB, Gestión de identidades de administración, Herramientas administrativas, Niveles 3, etc.).
- Herramientas ITSM e ITBM: Fomento del uso de las herramientas ITSM e ITBM disponibles para la recepción de todo tipo de incidencias, peticiones, tareas, demandas, proyectos, etc. que haya que llevar a cabo, tanto externas como internas.
- Modelo de Comunicación: Cumplimiento del Modelo de Comunicación establecido por EJIE para todas las comunicaciones iniciadas desde el Servicio. Este modelo especifica tanto aspectos comunes como aspectos específicos de los roles de Responsable.
- Reuniones: Existe un plan reuniones de seguimiento al que deberán asistir los participantes predefinidos. Adicionalmente, todos los integrantes del equipo deberán asistir a las reuniones virtuales o presenciales convocadas por los cauces preestablecidos en las que se requiera su presencia.
- Unidad de Equipo: El Servicio de Soporte Seguridad debe verse como un único equipo dentro de la organización, por lo que todos los integrantes deberán conocer a grandes rasgos los ámbitos de responsabilidad del equipo y de los diferentes participantes, colaborando activamente entre ellos según los protocolos establecidos dentro del equipo.
- Intervenciones: Todos los miembros del equipo deberán encargarse de las tareas asociadas a su ámbito de responsabilidad en la ejecución de intervenciones. Entre otros, creación y/o revisión de runbooks o planes de trabajo.
  Las intervenciones se realizarán en los horarios que EJIE estime conveniente para minimizar el impacto en los Servicios.
  En las intervenciones que EJIE estime oportuno, se podrá reclamar presencia in situ como medida de carácter preventivo, pudiendo ser intervenciones propias o intervenciones de terceros que puedan impactar en elementos bajo responsabilidad del Servicio.
- Análisis de Informes: Todos los miembros del equipo, cada uno en su ámbito de responsabilidad, deberá analizar informes de terceros que puedan desencadenar acciones de mejora, como pueden ser los Informes reportados por los Niveles 3 de forma periódica, resultados de auditorías de seguridad, publicaciones relativas a vulnerabilidades de seguridad, “release notes” publicada por fabricantes, etc.

5.2.1.2 Aspectos comunes a todos los Responsables

- Colaboración y Prioridades: Los diferentes responsables colaborarán para ofrecer un servicio global de Calidad, promoviendo la colaboración e interacción entre áreas para que todas ellas cumplan sus objetivos. Se encargarán de la priorización y provisión de los recursos necesarios para completar en tiempo y forma aquellas tareas o proyectos en su ámbito de responsabilidad que desde EJIE se marquen como prioritarios a lo largo del contrato.
  Asimismo, la dedicación de los recursos con dedicación compartida será coordinada entre el responsable del servicio y los responsables de las áreas en base a las necesidades y prioridades marcadas por EJIE en cada momento.
- Servicios de Seguridad: Los responsables velarán por la calidad de los Servicios bajo su ámbito de responsabilidad y, en esa línea, serán los garantes de mantener vivos y actualizados todos los aspectos relativos a los mismos, entre los cuales se encuentran: descripciones, políticas, roadmap, indicadores-informes-dashboards, procesos y procedimientos de seguimiento y control, evolución, entregas, gestión de incidencias e incidentes de seguridad, procesos de onboarding en el servicio, catálogo de servicios en herramientas ITSM, documentación, etc.
- Seguimiento de Aspectos Destacados: Como responsables, serán los encargados de liderar y hacer seguimiento especial de los aspectos más destacados de los Servicios bajo su ámbito de responsabilidad de cara a, entre otras cosas, poder realizar los seguimientos oportunos con EJIE. Algunos de los aspectos destacados más relevantes serían las incidencias graves, incidentes de seguridad, problemas, intervenciones, eventualidades fuera de lo habitual, etc.
- Mejora Continua: Los diferentes responsables del Servicio velarán de forma especial por la mejora continua de los aspectos bajo su área de responsabilidad. Entre las labores a realizar en esta línea, harán revisiones periódicas de los Acuerdos de Nivel de Servicio (ANS).
- Prevención: Reporte a EJIE ante cualquier eventualidad detectada relativa a su ámbito de responsabilidad que pueda poner en riesgo el Servicio y para la cual no exista ya un procedimiento claro de actuación. Posteriormente se trabajará en la creación de los procedimientos correspondientes para tratar posteriores eventos similares.
- Incidencias Graves: Seguimiento de las Incidencias Graves asignadas a Seguridad relativas a su ámbito de responsabilidad y cumplimiento escrupuloso del protocolo para el tratamiento de las mismas establecido desde el área de Gestión de Incidencias de EJIE.
  Asimismo, participación en los grupos de responsables conformados en la herramienta colaborativa de EJIE para agilizar la resolución de Incidencias Graves, así como revisión de las Actas de Incidencias Graves relativas a la infraestructura bajo su responsabilidad.
- Escalado: Los responsables deberán hacer un seguimiento especial a los problemas e incidencias irresolubles en primera instancia en su ámbito de responsabilidad, escalando internamente dentro del servicio y promoviendo la apertura de casos a los Soportes de Nivel 3 si así aplica sin esperar a que la situación se extienda en el tiempo, teniendo siempre en cuenta los ANS establecidos y lo establecido por el área de Gestión correspondiente de EJIE.
  Asimismo, abrirán problemas de forma proactiva relativos a su área de responsabilidad para prevenir que desemboquen en incidencias.
- Formación: La capa de Responsables velará porque la Formación y Certificaciones de su equipo cumple, al menos, lo exigido en la solvencia. En ese sentido, velará por el cumplimiento y actualización del Plan de Formación. Asimismo, será e que, durante los procesos de formación o transferencias de conocimiento en los que participen sus equipos, el Servicio no se resienta.
  Adicionalmente, supervisará que las transferencias de conocimiento a EJIE o a terceros exigidas a la adjudicataria se realizan con plenas garantías y con los recursos necesarios a nivel de personal y documentación.

5.2.1.3 Aspectos comunes al Área de Gestión de Procesos

- Referente ITIL: Éste área ejercerá de referente transversal dentro del Servicio en lo relativo al paradigma ITIL siendo responsable durante el periodo de vigencia del contrato de su correcta implementación a lo largo de los siguientes cinco fases principales que modelan el Soporte: Estrategia, Diseño, Transición, Operación y Mejora Continua
  De forma especial colaborará con el resto de Responsables en el seguimiento de ANS.

- Servicios de Seguridad: Éste área velará por el cumplimiento de los procesos establecidos en la definición de los Servicios de Seguridad ofrecidos por BATERA.
- Vigilancia y Seguimiento: Éste área será la encargada de vigilar que se cumplen los diferentes modelos y procedimientos de gestión establecidos por EJIE con el fin de evitar incumplimientos y malas prácticas a todos los niveles: comunicación, herramientas ITSM, servicios de guardia, gestión de incidencias graves, etc.
  Asimismo, se encargará de revisiones periódicas aleatorias para verificar que el Servicio está cumpliendo las Líneas Base establecidas.
- Catálogos de Servicio ITSM: Análisis de uso de catálogos con objeto de optimizarlos.
- Entregables: Éste área participará de forma especial en el diseño y optimización de los entregables asociados el Servicio.

5.2.1.4 Aspectos comunes al Área de Estrategia

- Definición de Servicios de Seguridad: Éste área será la encargada de participar en la definición de todos los Servicios de Seguridad ofrecidos por BATERA, tanto los que son responsabilidad suya como los que no lo son directamente. En esta línea, participará en la definición de los diferentes aspectos del servicio tanto a petición de EJIE como de forma proactiva, por ejemplo, en el diseño de una nueva solución para un servicio, en la decisión de compra de un nuevo equipamiento, propuesta de un nuevo indicador, etc.
- Entrega a Operación: Éste área será la encargada de velar por que la entrega a Operación se realice según la normativa establecida por EJIE (documentación, líneas base, etc.). Ésta labor la realizará tanto para iniciativas que partan del propio servicio (a través del Plan de Transformación, por ejemplo), como para iniciativas externas como pueden ser, entre otros, proyectos para responder a demandas, para incorporar nuevos servicios o para evolucionar servicios ya existentes en los que esta área participará activamente.
- Procesos ITIL: Éste área será el encargado de participar en todos los procesos ITIL asociados a la fase de Estrategia de todos los Servicios de Seguridad. Asimismo, participará en los procesos asociados a las fases de Diseño, Transición y Mejora Continua de servicios nuevos o evolucionados de forma que, cuanto se complete la entrega al área de Operación, ésta pueda continuar con todos los procesos según la normativa de EJIE.
- Consultoría: Éste área será la encargada de las diferentes labores de consultoría que puedan ser solicitadas por EJIE en el ámbito de la Seguridad.
- Metodologías Ágiles: Sin perjuicio del uso de las herramientas ITSM e ITBM propias de la organización y del uso de la metodología ITIL implantado en EJIE, éste área hará uso de metodologías Ágiles con objeto de dinamizar la entrega de Servicios, versiones, etc.

5.2.1.5 Aspectos comunes al Área de SecOps

- SecOps: Éste área se encargará de liderar el tránsito hacia un enfoque SecOps de la Organización según el cual la Seguridad pasa a ser algo transversal responsabilidad de toda la Organización y no únicamente del equipo de Seguridad.
- Vigilancia de Seguridad: Éste área será la encargada liderar la vigilancia de la Seguridad en la Organización. En esta línea, entre sus tareas más relevantes se encuentran:
  - Recepción, análisis y gestión de las alertas de Vulnerabilidades procedentes de terceros (BCSC, CCN-CERT, INCIBE, etc.)
  - Recepción, análisis y gestión de las auditorías de Seguridad tanto internas como realizadas por terceros.
  - Recepción, análisis y gestión de las alertas procedentes el Nivel 1 SOC contratado por EJIE. Estas alertas procederán principalmente del correlador de eventos de seguridad (SIEM) y del EDR que reportan al SOC.

- Coordinación Interdepartamental: Éste área será la encargada, con objeto de gestionar los aspectos mencionados en el punto anterior, de coordinar las acciones derivadas de esos eventos. Esta coordinación implicará la colaboración con otros grupos de soporte de Servicios Convergentes (incluyendo las Áreas de Estrategia y Operación de Soporte Seguridad), con niveles 1 (CAU, SASU, SOC, etc.), con equipos de desarrollo, asistencia técnica o funcionales, así como con cualquier otros departamento o cliente.
- Respuesta a Incidentes de Seguridad: Éste área será la encargada de coordinar los incidentes de seguridad que se puedan recibir del SOC o de otras fuentes. En este sentido colaborará en la definición de los procedimientos de respuesta a incidentes de la Organización y de sus diferentes clientes o departamentos si aplicara.
- Herramientas de Monitorización de la Seguridad: Éste área colaborará activamente en la configuración de las herramientas de Monitorización de la Seguridad de las que disponga EJIE. Entre otras, colaborará en la definición de casos de uso para el SIEM.

5.2.1.6 Aspectos comunes al Área de Operación

- Procesos ITIL: Éste área será el encargado de llevar a cabo todos los procesos ITIL asociados a las fases de Diseño, Transición, Operación y Mejora continua de todos los entornos indicados en el Anexo I – Entorno Tecnológico que ya han sido entregados a Operación según la normativa de EJIE.
- Entregas: Éste área será la encargada de llevar a cabo las entregas “estándar” de Servicios ofrecidos por BATERA a través del Soporte Seguridad. Cuando algo no sea estándar o surjan dudas, se colaborará con el área de Estrategia para la realización de la entrega.
- Planes de Continuidad de Negocio: Éste área colaborará en los preparativos y ejecución de los PCN periódicos promulgados por EJIE responsabilizándose de todo lo relativo a los activos bajo la responsabilidad de su Servicio.
- Operación Avanzada: Se consideran labores de “Operación Avanzada” todas aquellas que requieran un nivel de especialización y conocimiento del entorno elevado, como pueden ser procesos de automatización complejos, tratamiento de problemas, configuraciones complejas, atención a incidencias complejas, etc. Se considera “complejo” todo aquello que no pueda ser reflejado en un procedimiento de forma sencilla y lineal, sino que implica tener un nivel de especialización y conocimiento elevado.
  En general estas labores serán realizadas por Técnicos Avanzados de Seguridad a los que se escalarán estas acciones por parte de los Técnicos de Seguridad cuando no las puedan resolver ellos en primera instancia.
- RMA: Éste área será el encargado de la ejecución de RMAs para la sustitución de equipos averiados siguiendo el procedimiento indicado en el contrato de mantenimiento asociado y con la aprobación previa del Responsable de Operación.

5.2.2 Dimensionamiento

Los recursos con los que se dimensione el servicio dependerán de las ofertas presentadas, pero se considera, y por tanto es un requisito mínimo, que para cubrir los roles planteados al menos es necesario que el equipo tenga la capacidad equivalente a 30.600 horas de dedicación en un periodo de un año. Dichas horas se distribuirán de la siguiente manera por cada rol:

- Responsable del Servicio: 1.700 horas.
- Responsable de Procesos: 1.700 horas.
- Responsable de Estrategia: 1.700 horas.
- Responsable de SecOps: 1.700 horas.
- Responsable de Operación: 1.700 horas.
- Arquitecto de Seguridad: mínimo 5.100 horas.
- Técnico Avanzado SecOps: mínimo 1.700 horas.

- Técnico Avanzado de Seguridad: mínimo 6.800 horas.
- Técnico de Seguridad: mínimo 8.500 horas.

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.

5.2.3 Dedicación

Los recursos adscritos al 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 20% (redondeo al alza) de la suma de los recursos con rol Arquitecto de Seguridad, Técnico Avanzado SecOps y Técnico Avanzado de Seguridad pueda tener una dedicación menor, siempre y cuando esta no sea inferior al 50%. En estos casos, el adjudicatario deberá reportar mensualmente la dedicación de los técnicos no dedicados al 100% al servicio según modelo proporcionado por EJIE.

5.2.4 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.

5.3 Carga de trabajo

A continuación, se indica, a modo de referencia y sin implicaciones contractuales de ningún tipo, el número de incidencias y peticiones atendidas en los últimos seis meses de los que se poseen datos a la hora de la redacción del presente pliego. Se debe tener en cuenta que sólo se registran las peticiones de usuarios, no están registradas todas las tareas de coordinación, mantenimiento preventivo, evolución de entornos, migraciones, proyectos, etc. que pueden suponer una parte muy importante del trabajo total.

	Octubre 2020	Noviembre 2020	Diciembre 2020	Enero 2021	Febrero 2021	Marzo 2021
Incidencias	203	215	165	154	163	197
Peticiones	648	774	663	464	700	775

En caso de preverse alguna variación en la carga de trabajo EJIE comunicará al menos con 1 mes de antelación las características de la misma. Las causas de dichas variaciones están contempladas en el apartado 16 del PCP.

5.4 Actualización tecnológica

En el transcurso de la ejecución del contrato el servicio deberá recepcionar las nuevas tecnologías 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 implantada. El incumplimiento de este punto será objeto de penalización.

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 preexistentes. 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.

5.4.1 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 40 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 existentes en el servicio con objeto de detectar posibles lagunas de conocimiento que pudieran tener un impacto pernicioso

en el soporte a la infraestructura. 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.

5.5 Horario del Servicio

El servicio se ofrecerá en régimen de 24x7 (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.

5.5.1 Requerimientos en horario habitual

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.

Este número de teléfono deberá permitir un mínimo de 3 llamadas simultáneas con los técnicos asociados al servicio.

5.5.2 Requerimientos en horario extendido

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

- Soporte de atención telefónica.
- Acceso vía RAS/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.

5.5.2.1 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.
- Se estima un total de 400 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 fuera del "Horario Habitual".
    - 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 se realizarán a demanda de EJIE, y la adjudicataria deberá presentar informe de propuesta y seguimiento de las mismas que deberá ser aprobado por EJIE.
    - Las horas no consumidas anualmente se sumarán a las horas del año siguiente o se podrán detraer del importe de la factura mensual a lo largo de la vigencia del contrato a razón del coste/hora ofertado para la ampliación de la bolsa de horas.
    - Ante necesidades del servicio, EJIE podrá solicitar la incorporación de recursos adicionales al servicio, descontándose las horas efectivas de trabajo de esta bolsa de horas, a razón de 1:0,7 (1 hora de trabajo en "Horario Habitual" computará 0,7 horas a descontar de la bolsa de horas). La solvencia técnica de estos recursos será la solicitada en el presente expediente.
    - Mejora: la ampliación del número de horas incluidas (según lo indicado en el apartado de criterios de adjudicación del PCP).
      Se recuerda que esta información (por ser un dato de carácter objetivo a incluir en el Sobre B) NO se debe INCLUIR dentro de la Propuesta Técnica del Sobre C ya que en caso contrario se procederá a la exclusión de la propuesta presentada
    - 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).

5.5.2.2 Servicio de guardia

La adjudicataria deberá ofrecer un servicio de guardia en "Horario Extendido" para la atención de incidencias graves o incidencias 24x7 relativas a la infraestructura de Seguridad bajo su responsabilidad. Durante dicho servicio se velará por el cumplimiento de los ANS pactados con EJIE relativos al proceso de Gestión de Incidencias.

Por cada llamada recibida en el teléfono de guardia la adjudicataria se compromete a enviar un correo de reporte siguiendo en todo momento las directrices consignadas en el Modelo de Comunicación de EJIE.

La adjudicataria deberá velar también porque los técnicos del Servicio no participen en intervenciones en "Horario Extendido" durante las semanas en las que estén de guardia.

5.5.2.3 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 indicando, al menos, los siguientes aspectos:

- Características del servicio en horario habitual. Planteamiento de turnos y recursos por turno para cobertura de horario habitual.
- Características del servicio de intervenciones fuera de hora habitual ofertado.
- Características del servicio de guardia ofertado.
- Número de recursos con disponibilidad 24x7.
- Roles con disponibilidad 24x7.
- Periodo de rotación de recursos con disponibilidad 24x7.
- Escalados internos en "Horario Extendido".
- Características de los servicios telefónicos para ofrecer el servicio.

5.6 Interconexión con BATERA

La adjudicataria deberá disponer de infraestructura de comunicaciones que le permita establecer VPNs contra los entornos objeto del expediente:

- Acceso a Internet:
  - El caudal lo determinará la empresa adjudicataria.
- Terminador de túneles VPN.

5.7 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:

5.7.1 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. 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 de la nueva adjudicataria hasta el momento en que el proveedor saliente le transfiera efectivamente la responsabilidad del servicio.
2. Durante esta fase el servicio seguirá siendo prestado y las responsabilidades asociadas al mismo ejercidas por el proveedor saliente.
3. 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.
4. 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.
5. El proveedor saliente 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 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.

5.7.2 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.

5.8 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.

5.8.1 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. Se dividirán en requisitos obligatorios y requisitos opcionales:

- Requisitos obligatorios:
  - 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
- Requisitos opcionales:
  - Disponer de una política de continuidad del proveedor que esté alineada con el servicio prestado a EJIE
  - Disponer de un análisis de impacto en el negocio (BIA) que sirva como base para el plan de continuidad del servicio. Este BIA debería contemplar el grado de afección que, sobre el servicio a EJIE, tendría un incidente disruptivo a nivel de la empresa proveedora.

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.).
- Indisponibilidad, planificada o no, de elementos auxiliares habitualmente utilizados para la entrega del servicio (vehículos, maquinaria, herramientas, 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, Responsable de Procesos, Responsable de Estrategia, Responsable SecOps y Responsable de Operación) ante indisposiciones, bajas médicas o laborales, vacaciones…etc.

6 Condiciones de Seguridad/Generales

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 4.1, entre ellas las correspondientes a "seguridad física" (apartado 4.5).
- EJIE, tal como se indica en el apartado 3.3.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 "Anexo IV - *Normativa para empresas proveedoras – Anexo I Infraestructura TIC / Seguridad física y del entorno*" que se encuentra en el Anexo Seguridad de este 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.

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 indicado, 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, desde el momento en que se solicite, 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).
    - A la fecha del presente expediente, Yubikey 5 NFC. Consultar en el futuro.
- El proveedor deberá proporcionar, bajo solicitud de EJIE y en un plazo de 6 meses desde su solicitud, 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).

7 Anexo I – Entorno tecnológico

En este anexo se describe el entorno tecnológico actual a gestionar por la adjudicataria.

La adjudicataria deberá gestionar por completo todos los sistemas especificados a continuación, y cualquier equipamiento relacionado con estos sistemas que haya podido ser añadido y/o modificado hasta la fecha de la adjudicación y/o que se ponga en marcha durante la ejecución del contrato.

Del mismo modo, el servicio deberá recepcionar las nuevas tecnologías que vayan surgiendo a lo largo del contrato.

EJIE dispone de soportes de tercer nivel, de los que la adjudicataria podrá hacer uso en caso de necesidad.

7.1 Sistemas

Los sistemas a mantener se resumen en los siguientes puntos. De cara a los requisitos de solvencia, por norma general, se considerarán Sistemas Estratégicos aquellos que constituyan un Servicio Convergente ofrecido desde BATERA. Existen entorno legacy que también son críticos y hay que mantener, pero no se consideran estratégicos de cara a establecer criterios de solvencia del equipo. Esto significa que, según evolucione BATERA y vaya habiendo cada vez más servicios convergentes, habrá asimismo más Sistemas Estratégicos y, por lo tanto, más requisitos a cumplir por parte de los técnicos:

1. **Navegación web:**
   Navegación de forma segura para los usuarios.
2. **Acceso remoto:**
   Acceso seguro a usuarios ubicados fuera de las redes privadas.
3. **Firewall internos:**
   Segmentación, seguridad y control de acceso entre los diferentes servidores de los CPDs y los clientes.
4. **Firewall externos:**
   Segmentación, seguridad y control de acceso entre Internet, usuarios y los diferentes segmentos DMZ.
5. **Antivirus:**
   Servicios de antimalware para puestos de usuario y servidores.
6. **IDS/IPS:**
   Detección y prevención de intrusiones a nivel externo e interno.
7. **Web Application Firewall (WAF):**
   Acceso seguro a recursos Web.
8. **Radius/TACACS:**
   Servidores Radius y TACACS.
9. **Mobile Device Management (MDM):**
   Gestión de dispositivos móviles.

10. **Correo electrónico seguro:**
    Elementos de securización de correo electrónico.

11. **Análisis Vulnerabilidades:**
    Detección y prevención de vulnerabilidades a nivel externo e interno.

12. **SIEM:**
    Operación y administración de plataforma Security Incident and Event Management (SIEM).

13. **Protección de documentos.**
    Cifrado y control de acceso a documentos.

14. **PKI**:
    Gestión de autoridades de certificación internas.

15. **Seguridad WiFi:**
    Herramientas y configuraciones para securización del entorno WIFI

16. **Monitorización. Gestión de alarmas y rendimiento:**
    Infraestructura para monitorización, gestión de alarmas y rendimiento.

17. **Herramientas de ticketing:**
    Herramientas ITSM de gestión de incidencias, peticiones, problemas, activos, etc.

Queda accesible en el perfil del contratante el libro *Anexo I – Entorno tecnológico* en el que se detallan los fabricantes empleados actualmente en los diferentes sistemas estratégicos enumerados con anterioridad, así como una volumetría aproximada de la planta a administrar. Es conveniente reseñar que en la pestaña “Detalle entorno” de la tabla mencionada aparecen tecnologías que se explotan por parte de la adjudicataria, pero no se administran (marcadas con asterisco), de ahí que no se incluyan en la pestaña “Detalle Equipamiento”.

8 Anexo II – Centros dentro del ámbito

Queda accesible en el perfil del contratante el libro *Anexo II – Centros dentro del ámbito* en el que se detallan las ubicaciones actualmente gestionadas por el Servicio: edificios integrados en la Red Corporativa Administrativa del Gobierno Vasco (RCAGV); hospitales, ambulatorios, centros de salud y consultorios de Osakidetza; Palacios de Justicia de Justizia y centros docentes públicos no universitarios y de apoyo a la docencia de Hezkuntza. En dicho libro no se han incluido las ubicaciones pertenecientes a KZgunea (243 sedes) debido a que la adjudicataria únicamente deberá provisionar equipos para eventuales sedes nuevas y proveer de soporte remoto y reposición ante averías al equipamiento sito en las mismas.

La adjudicataria deberá asumir cualquier centro de nueva apertura que se añada tanto a las infraestructuras de los clientes actuales como futuros a lo largo de la vigencia del contrato.

9 Anexo III – Catálogo de servicio de referencia

Queda accesible en el perfil del contratante el libro *Anexo III – Catálogo de Servicios de Referencia* en el que se detallan los catálogos de las peticiones actualmente atendidas por el Servicio para cada una de las infraestructuras (a excepción de Justizia que carece de catálogo).

Se trata de catálogos vivos que se mantendrán actualizados junto con la evolución de los entornos tecnológicos tendiendo, en la medida de lo posible, a su consolidación en un único catálogo transversal.

La existencia de dichos catálogos no implica que tareas fuera de los mismos no deban atenderse. La adjudicataria deberá gestionar todas las peticiones en las que la tecnología del Anexo I esté implicada.