Eusko Jaurlaritzaren
Informatika Elkartea

Sociedad Informática
del Gobierno Vasco

EXPEDIENTE Nº: EJIE-2026-011

Servicios de auditorías de seguridad de aplicaciones y sistemas de información para BATERA.

Especificaciones de compra / Pliego de condiciones técnicas

Febrero 2026

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	14/01/2026	Versión Inicial	Javier González Tavera	Josu Bagazgoitia Sáez de Vicuña

Índice

1 Introducción 4
1.1 Perfil de la Compañía 4
2 Antecedentes, Situación Actual y Necesidad 5
3 Objeto, Alcance y Lotes del contrato 6
4 Requisitos Globales 7
4.1 Condiciones de Seguridad 7
5 Requisitos Específicos del Servicio 9
5.1 Tipos de Auditorías 9
5.1.1 LOTE 1: Auditorias de Seguridad 9
5.1.2 LOTE 2: Auditorias PCI DSS 11
5.2 Plan de Ejecución 12
5.2.1 Plazo de cancelación 12
5.2.2 Fases de ejecución 13
5.2.3 Esquema 18
5.3 Entregables de auditorías 18
5.3.1 Informes de Auditorías 18
5.3.2 Informes de Retest 19
5.3.3 Memoria final 19
5.3.4 Certificado acreditativo de borrado de información 20
6 Requisitos de Seguimiento 21
6.1 Niveles de Servicio 21
6.2 Indicadores, Informes y Cuadros de Mando 22
6.3 Comités de Seguimiento 22

1 Introducción

1.1 Perfil de la Compañía

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

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

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

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

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

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

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

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

2 Antecedentes, Situación Actual y Necesidad

Desde que la Seguridad IT ha ido adquiriendo relevancia y los ataques de Seguridad han ido representando una amenaza creciente, EJIE ha ido publicando pliegos similares al actual que permiten realizar diferentes tipos de auditorías de seguridad con el objetivo de detectar y corregir posibles brechas que puedan acabar siendo utilizadas para comprometer la seguridad de las organizaciones a las que EJIE da servicio.

Esto ha permitido a EJIE, dentro de su porfolio de Servicios de Seguridad, ofrecer el "Service Offering" denominado Auditoría de Seguridad P3 (Bajo Demanda Especializada) en el marco del "Business Service" Gestión de Vulnerabilidades.

El último de estos pliegos ha sido el denominado EJIE-126-2022, cuya vigencia finalizará en marzo de 2026.

En la actualidad la situación global a nivel de seguridad no ha mejorado, más bien lo contrario, aumentando el número de amenazas y de ataques. Si bien también han evolucionado los mecanismos de vigilancia de la seguridad, tendiendo a soluciones de vigilancia continua sobre todo en lo que a superficies de exposición se refiere, sigue siendo necesaria la realización de diversos tipos de auditorías de seguridad ad-hoc para cubrir diferentes situaciones.

Con el fin de que EJIE pueda continuar ofreciendo este servicio dentro de su porfolio de servicios de seguridad, se hace necesaria la contratación de servicios especializados de seguridad, que contemplen la provisión de **Servicios de auditorías de seguridad de aplicaciones y sistemas de información para BATERA**, de acuerdo al alcance y requerimientos técnicos y de servicio solicitados en la presente contratación.

3 Objeto, Alcance y Lotes del contrato

El objeto del expediente es la **contratación bajo demanda de servicios de auditorías de seguridad** de diversos tipos, con el objetivo de identificar vulnerabilidades ante ataques externos o internos y disponer las medidas adecuadas para mitigar o reducir los riesgos de las mismas, todo ello de acuerdo al alcance y requerimientos técnicos y de servicio solicitados en la presente contratación.

Las metodologías deberán ser acotadas por los auditores para cada servicio de acuerdo a los escenarios que se encuentren en cada momento con el fin de realizar las pruebas más oportunas optimizando los recursos disponibles, siempre con el visto bueno por parte de EJIE.

Como se ha adelantado previamente, la realización de Auditorías de Seguridad forma parte del porfolio de Servicios Convergentes de Seguridad que **se ofrecen a todas las entidades adheridas a BATERA**.

En la actualidad, las principales entidades adheridas son las siguientes:

Red Corporativa Administrativa del Gobierno Vasco (RCAGV), BATERA (Interno), Justizia, Lanbide, ETS, Euskotren, Eustat, Izenpe, Alokabide, Itelazpi, HAZI, EITB y Osakidetza, pudiendo variar estas entidades a lo largo de la duración del contrato.

Se van a dar dos tipos de auditorías claramente diferenciadas, por lo que el expediente se va a dividir en los siguientes lotes:

- Lote 1: Auditorías de Seguridad.

  Este lote es el equivalente a pliegos existentes anteriores, es decir, un contrato que permita solicitar diferentes tipos de auditorías, según el detalle que se proporcionará en apartados posteriores.

- Lote 2: Auditorías PCI DSS.

  Este lote tiene como objeto realizar auditorías específicas de tipo PCI DSS (para entornos de pago: auditorías que verifican si los sistemas cumplen con el estándar de Seguridad de Datos de la Industria de tarjetas de pago y que protegen los datos de los titulares de las tarjetas de filtraciones y fraudes) que requieren un nivel de especialización muy específico y una serie de requisitos de solvencia muy concretos que limitan la concurrencia, razón por la cual se separa el pliego en lotes diferentes.

4 Requisitos Globales

Los siguientes requisitos son comunes al Lote 1 y al Lote 2.

4.1 Condiciones de Seguridad

La empresa adjudicataria está obligada a cumplir todas las reglas de seguridad referidas en el apartado "Reglas de la seguridad" del PCP. En línea con ese apartado, serán de obligado cumplimiento las **"Políticas de Seguridad para personal de empresas proveedoras"** (accesible en la web www.ejie.eus):

- Según dicho documento, serán de aplicación todas las condiciones detalladas en el apartado "Políticas Específicas de Seguridad para Proveedores" en función de la tabla del apartado "Aplicabilidad de las Políticas Específicas de Seguridad para Proveedores".

- El servicio objeto del presente pliego se proporcionará desde las oficinas de la empresa adjudicataria, de modo que, para determinar las opciones que aplican según el apartado "Aplicabilidad de las Políticas Específicas de Seguridad para Proveedores" habrá que considerar:
  - 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".
  - El proveedor "Sí" realiza la "Gestión de tecnologías" de EJIE.

- EJIE, tal como se indica en el apartado "Uso apropiado de los recursos" se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.

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

- La empresa adjudicataria se compromete, según se indica el apartado "Gestión de contingencias" a disponer de un plan que le permita continuar ofreciendo el servicio en situaciones de contingencia.
  Si ante una incidencia o ciber incidente el proveedor no es capaz de activar un plan de contingencia que le permita continuar ofreciendo el servicio, EJIE se reserva el derecho de exigir el desplazamiento físico temporal de los administradores a las ubicaciones que EJIE determine de forma que puedan continuar ofreciendo el servicio con equipamiento "limpio" proporcionado por la propia empresa adjudicataria, hasta el momento en que EJIE valide la recuperación del proveedor según el procedimiento pertinente en cada caso. El plan presentado debe detallar cómo se garantizará que el equipamiento utilizado en estas situaciones está limpio y no ha estado expuesto a la situación de riesgo.

El servicio objeto del presente pliego realizará labores de administración sobre los entornos responsabilidad de EJIE. Por ese motivo, adicionalmente, la empresa adjudicataria deberá implantar las siguientes medidas de seguridad con objeto de reforzar la protección sobre los administradores y aplicar las **medidas estandarizadas a nivel de administradores IT en EJIE**:

- EJIE proporcionará credenciales de "usuarios administradores/privilegiados" a los participantes en el proyecto con objeto de permitirles el acceso a los recursos que requieran. Estas credenciales exigirán un segundo factor de autenticación. La empresa adjudicataria deberá garantizar que los participantes

en el proyecto disponen de hardware que permita la identificación y el acceso a los sistemas con suficientes garantías (MFA). Estos dispositivos podrán ser:

- Teléfono móvil (Android o iOS), con sistema operativo actualizado, capaz de utilizar la APP del servicio de IDaaS implantado.
  - Dispositivos hardware homologados por EJIE: Compatibles FIDO2
- La empresa adjudicataria deberá proporcionar a los administradores equipos securizados con tecnologías EDR y EPP.
- La empresa adjudicataria deberá proporcionar a los administradores equipos compatibles con los sistemas de acceso remoto utilizados en EJIE, es decir, con la solución VPN y/o solución SSE-ZTNA utilizada por EJIE.
- EJIE proporcionará a los administradores acceso a recursos de Office365, utilizando para ello "usuarios invitados" en los que el UPN coincidirá con el email propio de cada administrador en la empresa proveedora (nombre@dominio_adjudicatario). A estos usuarios invitados se les exigirá la utilización de un segundo factor de autenticación (MFA), por lo que la empresa adjudicataria deberá encargarse de proporcionar a sus administradores credenciales compatibles con este requisito.

EJIE se reserva el derecho de exigir a la empresa adjudicataria la implantación de medidas de seguridad específicas que deberá acometer en el plazo de 6 meses, suponiendo el incumplimiento de esa implantación la penalización correspondiente especificada en el PCP.

De acuerdo con las características del servicio objeto de este expediente, la empresa contratista o adjudicataria tiene la obligación de emplear exclusivamente los servidores y los servicios asociados a los mismos que disponga EJIE durante la ejecución del contrato. A tal fin, deberá cumplimentar los siguientes anexos: *Anexo XV: "Declaración Responsable sobre la Previsión o No de Subcontratar los Servidores o los servicios asociados a los mismos" y el Anexo XIV: "Declaración Responsable sobre la Ubicación de los Servidores y Lugar de Prestación de los Servicios Asociados a los mismos"* del PCP, indicando que emplearán exclusivamente los servidores o servicios asociados que EJIE ponga a disposición para este servicio.

5 Requisitos Específicos del Servicio

En este apartado se describen los requisitos técnicos que aplican a cada uno de los lotes:

5.1 Tipos de Auditorías

5.1.1 LOTE 1: Auditorias de Seguridad

El objetivo es la revisión y evaluación de la seguridad desde todos los ámbitos técnicos, tecnológicos y organizativos de la seguridad.

Se describen características y requisitos mínimos que la empresa adjudicataria deberá prestar, pudiendo ésta ampliarlos y mejorarlos, y no siendo el listado que aparece a continuación una relación exhaustiva de las características de los servicios contratados, sino las líneas generales demandadas por EJIE.

Aportará valor el detalle e idoneidad de la propuesta en cada tipo de auditoría, así como los posibles tipos adicionales de auditorías propuestos. No se admitirán únicamente ataques a realizar con herramientas automáticas.

La empresa adjudicataria deberá aportar los conocimientos, metodologías y apoyarse en las herramientas necesarias para asegurar el resultado óptimo del proyecto, teniendo la indicación expresa de no ser admitidos los trabajos que sean realizados únicamente mediante el empleo de técnicas automáticas. El coste asociado a las herramientas, posibles desplazamientos u otros aspectos relacionados al alcance del servicio estará incluido en el Coste por hora que se solicita en el PCP, estos costes serán asumidos en todo caso por el adjudicatario sin repercutir costes a EJIE más allá del número de horas consumido. Esto es independiente del tipo de auditoría a realizar.

EJIE, solicitará bajo demanda, la auditoría de una infraestructura/aplicación/servicio. El alcance de la auditoría puede comprender una o varias de las siguientes tipologías de servicio:

- Auditoría de seguridad de aplicaciones software (nueva o en ejecución): análisis de aplicaciones software para identificar posibles vulnerabilidades de seguridad de las mismas. Se deberán emplear diferentes técnicas de detección y explotación, herramientas de hacking, etc.

Las pruebas y análisis de seguridad a realizar deberán incluir, donde proceda, como mínimo los siguientes: descubrimiento de aplicaciones, identificación de puntos de entrada a la aplicación, posibilidades de inyección de código, gestión de sesiones y análisis del esquema de autenticación, escalada de privilegios, pruebas de autorización y autorización entre aplicaciones, análisis de códigos de error, propagación de vulnerabilidades, ingeniería inversa de protocolos y/o posibles exploits que se pudieran usar, pruebas de denegación de servicio, sistemas de autenticación, posibles suplantaciones, de entrada de datos y de tráfico y comunicaciones.

- Auditoría de seguridad de aplicaciones móviles (nueva o en ejecución): análisis de aplicaciones destinadas a terminales móviles para identificar posibles vulnerabilidades de seguridad de las mismas mediante análisis estáticos y dinámicos, pruebas de intrusión, suplantación de identidades, etc. Se deberán emplear diferentes técnicas de detección y explotación, herramientas de hacking, etc.

Las pruebas y análisis de seguridad a realizar deberán incluir, donde proceda, como mínimo los siguientes: descubrimiento de aplicaciones, identificación de puntos de entrada a la aplicación, posibilidades de inyección de código, gestión de sesiones y análisis del esquema de autenticación, escalada de privilegios, pruebas de autorización y autorización entre aplicaciones, análisis de códigos de error, propagación de vulnerabilidades, ingeniería inversa de protocolos y/o posibles exploits que se

pudieran usar, pruebas de denegación de servicio, sistemas de autenticación, posibles suplantaciones, de entrada de datos y de tráfico y comunicaciones.

- Test de intrusión en la red desde Internet: el objetivo del test de intrusión es evaluar el estado de los sistemas identificando las vulnerabilidades que puedan existir: obteniendo las probabilidades de éxito de un ataque y comprobar la eficacia de las medidas de defensa perimetrales implementadas. El objetivo será cualquier sistema que pudiera estar accesible: routers, IPS/IDS, firewalls, WAF, VPN, servicios web, correo, fichero, etc. En definitiva, cualquier otro servicio accesible desde el exterior.

1. Auditoría de seguridad de red interna: el objetivo es evaluar la seguridad de la red interna: desde DMZ, desde cualquier otra red o plataforma a la que un atacante pudiera obtener acceso. Se deberá determinar si la inseguridad en esas redes y plataformas puede llegar a repercutir en la red interna de la empresa.

2. Auditoría de seguridad de redes WIFI: evaluación de seguridad de las redes WIFI.

3. Auditoría de seguridad de información accesible desde Internet: el objetivo es identificar toda la información que pudiera estar accesible desde internet y que, de algún modo, sirviera a un atacante para sus objetivos: desde pliegos con información técnica, sus redes, sistemas, organización, u otros. Del mismo modo, se deberán obtener una serie de recomendaciones para eliminar o reducir dicha exposición.

4. Auditoría de ingeniería social: con el objeto de obtener información confidencial a través de la manipulación de usuarios legítimos. Es un ataque dirigido a la confianza del usuario con fin de ver qué información sensible puede obtenerse siguiendo una metodología propia desarrollada en base a técnicas de Ingeniería Social, y realizar planes para reducir el riesgo.

5. Auditoría de Seguridad Física: análisis de las posibles amenazas y riesgos de las diferentes ubicaciones físicas donde existan sistemas de IT y/o personal con acceso a la red corporativa, con el objetivo de obtener y mantener un nivel adecuado de seguridad física sobre la infraestructura y los activos, así como la seguridad del edificio analizado.

6. Auditoría forense: análisis forense de las evidencias electrónicas definidas en la norma UNE 71506:2013 o equivalente (“Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas.”)

- Auditorías de dispositivos IoT (Internet of Things): análisis de dispositivos IoT con el objetivo de descubrir cualquier vulnerabilidad que pueda provocar un acceso no autorizado a los sistemas e infraestructuras.

- Simulación APT Ransomware: ejercicio para mostrar el grado de exposición de la organización y el impacto que tendría en caso de materializarse una amenaza de cifrado masivo que permitirían a un atacante potencial bloquear el funcionamiento y/o acceso a una parte o a todos los equipos de la compañía.

- Auditoría de directorio activo: el objetivo es identificar si el directorio activo está debidamente bastionado o no y en el caso de que no sea así, proponer mejoras para un nivel de securización óptimo.

7. Auditoría de configuración de dispositivos de protección (firewall, EDR, etc.): el objetivo es evaluar el nivel de bastionado de diferentes tipos de dispositivos de protección para lo cual se seguirán guías existentes de entidades de referencia y fabricantes.

8. Otros tipos de auditoría y consultoría técnica de ciberseguridad: cualquier otro tipo de auditoría de ciberseguridad que no esté contemplada en los tipos indicados previamente. Adicionalmente, EJIE podrá consultar al contratista aspectos relacionados con la seguridad en sus sistemas de información, con el fin de garantizar una comprensión de los riesgos, identificación de debilidades o mejoras de seguridad en sus sistemas y prevenir vulnerabilidades que puedan surgir en las correspondientes auditorías.

EJIE podrá solicitar al adjudicatario la realización de cualquiera de los tipos de servicios expuestos en cualquier momento durante la vigencia del contrato, siempre y cuando no se haya alcanzado el límite presupuestario.

Ante la importancia del ámbito de uso de las aplicaciones e infraestructura crítica asociada, no se impactará sobre los servicios en producción derivados de posibles pruebas de impacto de la auditoría, que en ningún caso deberán afectar al funcionamiento normal. Se deberán definir previamente los impactos y acordar las horas de actuación sobre plataformas y aplicaciones junto con EJIE.

5.1.2 LOTE 2: Auditorias PCI DSS

El objetivo es la revisión, evaluación y análisis para el cumplimiento del estandar PCI DSS (Payment Card Industry Data Security Standard) mediante el servicio de escaneos de vulnerabilidades externos ASV según los **requerimientos desarrollados por el PCI SSC (PCI Security Standards Council)** para la identificación temprana de vulnerabilidades en dispositivos conectados a redes no confiables, permitiendo aplicar los controles necesarios para la protección del entorno de cumplimiento antes que dichas vulnerabilidades puedan ser aprovechadas por un usuario malintencionado.

Se describen características y requisitos mínimos que la empresa adjudicataria deberá prestar, pudiendo ésta ampliarlos y mejorarlos, y no siendo el listado que aparece a continuación una relación exhaustiva de las características de los servicios contratados, sino las líneas generales demandadas por EJIE. **Los requisitos de los escaneos de vulnerabilidades externos ASV pueden ser variables en función de lo que indique PCI DSS. La empresa adjudicataria se adaptará a los mismos.**

Aportará valor el detalle e idoneidad de la propuesta en cada tipo de auditoría, así como los posibles tipos adicionales de auditorías propuestos, que en este caso deben **seguir en todo momento los requerimientos desarrollados por el PCI SSC y ser escaneos variables en función de lo que indique PCI DSS**, según lo indicado anteriormente.

La empresa adjudicataria deberá aportar los conocimientos, metodologías y apoyarse en las herramientas necesarias para asegurar el resultado óptimo del proyecto, teniendo la indicación expresa de no ser admitidos los trabajos que sean realizados únicamente mediante el empleo de técnicas automáticas. El coste asociado a las herramientas, posibles desplazamientos u otros aspectos relacionados al alcance del servicio estará incluido en el Coste por hora que se solicita en el PCP, estos costes serán asumidos en todo caso por el adjudicatario sin repercutir costes a EJIE más allá del número de horas consumido. Esto es independiente del tipo de auditoría a realizar.

La empresa adjudicataria deberá contar con la certificación ASV (Approved Scanning Vendors) para escaneos PCI DSS y con un equipo de auditores certificados en AVS, que se encargarán de la formación del resto del equipo y de la calidad de los trabajos. Si cambiaran los requisitos de certificación a

lo largo del contrato, la empresa deberá adaptarse a ellos para poder continuar proporcionando un servicio certificado.

EJIE, solicitará bajo demanda, las auditorías. El alcance de la auditoría puede comprender una o varias de las siguientes tipologías de servicio:

1. Análisis de red externos programados ASV PCI DSS (Escaneos ASV): ejecución de herramienta de escaneo automático, análisis y eliminación de falsos positivos, análisis manual y explotación de las vulnerabilidades más importantes detectadas, usando herramientas autorizadas y certificadas para el cumplimiento PCI DSS. El adjudicatario deberá emplear la metodología PCI DSS y las exigencias de escaneo del requerimiento de PCI DSS.

2. Test de Intrusión Externo (requerimiento PCI DSS): se trata de replicar un ataque externo que tenga como objetivo comprometer la infraestructura IT dentro del alcance del contrato. El servicio debe combinar la experiencia de los auditores con el uso de herramientas de escaneo automático. De entre todas las posibles vulnerabilidades detectadas se debe realizar una selección de las incidencias más críticas para posteriormente realizar labores de eliminación de falsos positivos, análisis y explotación de las vulnerabilidades encontradas.

3. Otros tipos de auditoría: se trata de otro tipo de auditorías que puedan ser necesarias en el ámbito de los estándares establecidos por el PCI SSC.

5.2 Plan de Ejecución

Los siguientes aspectos relativos a la ejecución del proyecto y **las fases para la ejecución de auditorías son comunes al Lote 1 y al Lote 2.**

El adjudicatario deberá asegurar la disponibilidad de todos los recursos que se consideren necesarios cuando EJIE realice una petición de auditoría. La no disponibilidad de los recursos o los retrasos en la ejecución serán objeto de penalización según lo especificado en PCP.

5.2.1 Plazo de cancelación

Con objeto de que el PRECIO UNITARIO OFERTADO €/HORA (SIN IVA) propuesto en el modelo económico no se reduzca artificialmente en la oferta con la intención posterior de imputar más horas de las necesarias durante la ejecución del contrato, a la hora de realizar las estimaciones de horas necesarias para la realización de los trabajos (esto es, durante la ejecución de la Fase 2 que se describe en el apartado 5.2.2.2), el licitador deberá proporcionar un desglose detallado de tareas que justifiquen la cantidad de horas propuesta. EJIE, por su parte, tomará como referencia experiencias previas a la hora de evaluar el número de horas propuestas en cada auditoría, pudiendo negociar modificaciones o incluso rescindir el contrato en ciertas situaciones tal y como se indica más adelante.

Cuando para realizar una actividad (auditoría, retest) el adjudicatario haga una reserva de recursos, **EJIE podrá solicitar la cancelación de la actividad (PLAZO DE CANCELACIÓN) un número de días antes sin coste**. La solicitud de cancelación se realizará por email o teléfono, considerándose las 18 horas el horario límite para considerar la fecha efectiva de la solicitud, no contándose el día de la solicitud dentro del plazo de solicitud de la cancelación. En tal sentido, el adjudicatario deberá presentar una propuesta de PLAZO DE CANCELACIÓN. **Este PLAZO DE CANCELACIÓN será evaluable bajo los criterios objetivos del archivo electrónico de fórmulas. Por lo que el licitador debe tener en cuenta que en ningún caso debe incluir información de los PLAZOS DE CANCELACIÓN en el archivo electrónico**

de juicios de valor. **En el caso de que el archivo electrónico de juicios de valor adelante información reservada para el archivo electrónico de valoración de fórmulas, el licitador será excluido del proceso de licitación.**

Si EJIE solicita cancelar la actividad pasado ese plazo, deberá afrontar, si el adjudicatario así lo requiere, como máximo el coste del número de días hábiles en los que se haya superado dicho PLAZO DE CANCELACIÓN tomando como referencia 8 horas de trabajo diarias al PRECIO UNITARIO OFERTADO €/HORA (SIN IVA) propuesto en PCP.

Por ejemplo, si el PLAZO DE CANCELACIÓN son 10 días y la fecha prevista para el comienzo de una actividad es el lunes (L) día 22 del mes (se toma como referencia el mes de junio de 2026 para el ejemplo):

- Si EJIE solicita cancelar la actividad el miércoles (X) día 3 a las 10 horas: Se cancelará sin coste puesto que se ha avisado 12 días hábiles antes (4J, 5V, 8L, 9M, 10X, 11J, 12V, 15L, 16M, 17X, 18J, 19V). El día 3 se ha avisado antes de las 18h, así que se cuenta a partir del día 4.
- Si EJIE solicita cancelar la actividad el martes (M) día 9 a las 20 horas: Se cancelará con un coste de 3 días (3 días x 8 horas/día x Precio €/hora). Al haber avisado a las 20 horas, el miércoles (X) día 10 será la fecha efectiva de la cancelación. Así, el plazo desde esa fecha efectiva hasta el comienzo de la actividad son 7 días hábiles (11J, 12V, 15L, 16M, 17X, 18J, 19V). Como el PLAZO DE CANCELACIÓN son 10 días, 10-7=3 días hábiles.

5.2.2 Fases de ejecución

El adjudicatario deberá presentar una propuesta de fases de trabajo con tiempos máximos para completar cada fase, teniendo en cuenta los SLAs descritos en el PCP, en línea con el apartado 6.1 del presente Pliego de Condiciones Técnicas. Así mismo, la propuesta de fases de trabajo debe incluir los requisitos, metodología, entregables y trazas de cada fase, según se especifica en los apartados que siguen a continuación.

El alcance de la documentación a presentar en cada fase se revisará y acordará en el inicio del proyecto y se podrá adaptar durante la ejecución del mismo en caso de ser necesario. En cualquier caso, será responsabilidad del adjudicatario crear y mantener un documento de Seguimiento del proyecto en formato Excel o equivalente, con todas las trazas que permita saber lo realizado en cada auditoría y el resultado de las mismas. Será responsabilidad del adjudicatario también generar los entregables. El detalle de la documentación a generar y mantener a lo largo de la ejecución se describe en los apartados siguientes.

Las fases de trabajo a presentar por parte del adjudicatario serán relativas a los servicios solicitados, aunque a nivel general, se solicitan como mínimo las siguientes, indicando un mínimo de trazas, entregables y SLAs:

5.2.2.1 FASE 1: Lanzamiento Auditoría

Inicio Fase:

El responsable de EJIE solicitará al adjudicatario la realización de cada servicio. Esta solicitud se realizará mediante correo electrónico a una dirección establecida.

Fin Fase:

Se llevará a cabo una **reunión de lanzamiento** de **auditoría** entre el adjudicatario y EJIE/Cliente en la que el adjudicatario deberá solicitar todo lo necesario para la correcta realización de la auditoría. Dicha reunión deberá llevarse a cabo en un plazo igual o inferior a 5 días hábiles desde la solicitud por parte de EJIE

(salvo que EJIE por el motivo que fuera decidiese posponerla). El incumplimiento de este plazo será objeto de penalización según lo especificado en PCP.

SLAs:

Plazo reunión inicial: Inferior o igual a 5 días hábiles desde la solicitud por parte de EJIE.

Trazas:

ID Auditoría, Fecha solicitud, Petición ITSM (Interno EJIE), Organización, Descripción, Ámbito, Fecha reunión lanzamiento.

Entregables:

Acta de reunión lanzamiento.

5.2.2.2 FASE 2: Propuesta Auditoría

Inicio Fase:

Fin de la reunión de lanzamiento de la Fase 1.

El adjudicatario establecerá el alcance detallado y presentará una **propuesta** que debe incluir una propuesta con los trabajos a realizar, plazos, hitos y el presupuesto en función del precio propuesto en PCP. **Dicha propuesta** deberá proporcionarse a EJIE en un **plazo igual o inferior a 5 días hábiles desde la finalización de la Fase 1** (salvo que EJIE por el motivo que fuera decidiese posponerla). El incumplimiento de este plazo será objeto de penalización según lo especificado en PCP.

EJIE valorará la planificación y solicitará las correcciones o aclaraciones que considere oportunas.

Fin Fase:

El final de esta fase lo determinará la aceptación de la propuesta por parte de EJIE.

EJIE en todo caso aprobará la propuesta de acuerdo a los servicios solicitados. En el caso de que los plazos no se consideren adecuados por EJIE tras analizar los motivos planteados por la adjudicataria y ésta no acepte los mismos, EJIE podrá rescindir el contrato.

SLAs:

***Plazo entrega propuesta de planificación*:** 5 días hábiles desde la finalización de la reunión de lanzamiento.

Trazas:

Fecha entrega de propuesta. Horas estimadas. Presupuesto.

Entregables:

Propuesta.

5.2.2.3 FASE 3: Preparación Auditoría

Inicio Fase:

Aprobación de la propuesta de auditoría.

A partir de la aceptación de la propuesta, el adjudicatario deberá **proponer una Fecha de Inicio** de la auditoría. **Dicha propuesta** deberá producirse en un **plazo igual o inferior a 5 días hábiles desde la desde la finalización de la Fase 2** (salvo que EJIE por el motivo que fuera decidiese posponerla). El incumplimiento de este plazo será objeto de penalización según lo especificado en PCP.

El plazo para el comienzo de ejecución de la auditoría deberá ser igual o inferior a 20 días hábiles desde la aceptación de la propuesta por parte de EJIE, es decir, desde el final de la fase anterior (desde la finalización de la Fase 2).

Adicionalmente, durante esta fase el adjudicatario deberá realizar los preparativos para la ejecución de la auditoría lo que incluirá, al menos:

- Detalle del alcance específico y trabajos a realizar en cada caso.
- Acuerdos de confidencialidad y recopilación de consentimientos necesarios en cada caso.
- Acuerdos relativos a ventanas de trabajo para ejecutar la auditoría.
- Concretar e informar del potencial impacto de los trabajos.
- Prerrequisitos para la ejecución técnica de la auditoría (accesos, usuarios, etc.)

Fin Fase:

El final de esta fase lo marca la fecha de inicio de la ejecución de la auditoría.

EJIE validará la fecha propuesta o negociará una posterior según las necesidades específicas en cada caso.

SLAs:

Plazo para informar de la fecha de inicio de ejecución de auditoría*:* igual o inferior a 5 días hábiles desde la desde la finalización de la Fase 2.

Plazo para el inicio de la ejecución de la auditoría: igual o inferior a 20 días hábiles desde la aceptación de la propuesta por parte de EJIE.

Trazas:

Fecha recepción de la fecha propuesta para iniciar la auditoría.

Fecha de inicio de ejecución de la auditoría.

Entregables:

Documentos asociados a la preparación: Acuerdos de confidencialidad, consentimientos, solicitudes de altas y accesos, detalle de trabajos a realizar, etc…

5.2.2.4 FASE 4: Ejecución Auditoría

Inicio Fase:

El inicio de esta fase lo marca la fecha de comienzo de ejecución de la auditoría.

El adjudicatario realizará la auditoría (en una 1ª iteración) según su propia metodología, que tendrá que ser descrita en la oferta a este pliego y que deberá ir alineada con los estándares existentes.

El adjudicatario podrá apoyarse en el uso de herramientas de seguridad para la realización de las auditorías. Sin embargo, siempre que sea posible, las vulnerabilidades explotables serán reportadas indicando los pasos que se han seguido para su explotación mediante técnicas de hacking, con suficientes evidencias para poder acometer la remediación. Se propondrán las medidas de remediación que se consideren adecuadas, con una estimación del esfuerzo de implementación necesario.

Fin Fase:

La fase finalizará en el momento en que finalice la auditoría.

Trazas:

Fecha inicio real de la auditoría. Fecha fin de la auditoría.

5.2.2.5 FASE 5: Documentación e informes de resultados

Inicio Fase:

Esta fase comienza en el momento en que finaliza la ejecución de la auditoría.

Una vez finalizada la/s auditoría/s, el adjudicatario proporcionará un informe completo al contacto establecido en EJIE. Los informes identificaran en detalle potenciales vulnerabilidades y recomendaciones para la solución técnica de las mismas, incluyendo también una evaluación ejecutiva de los resultados, así como una propuesta de medidas correctoras a corto, medio y largo plazo.

Se deberán presentar los entregables indicados en el apartado 5.3 del presente pliego. En los casos en los que para una misma aplicación se requieran auditorías de diferente tipología, los resultados de ambas auditorías deberán ser cruzados (relación de las vulnerabilidades detectadas en ambas auditorías) y se elaborará un único informe de resultados.

Los entregables deberán proporcionarse en un plazo igual o inferior a 5 días hábiles desde la finalización de la ejecución de la auditoría.

Los informes de auditoría serán revisados por EJIE y, si se considera necesario, se fijará una reunión para la explicación de los mismos.

No se admitirá un informe basado únicamente en la salida de las herramientas que se usen.

EJIE procederá a dar el visto bueno a la auditoría o propondrá los cambios pertinentes que tendrán que ser revisados y realizados por el adjudicatario.

En caso de que EJIE considere que el informe no tiene la calidad necesaria (de acuerdo a lo establecido en el presente pliego) se lo notificará a la adjudicataria y ésta deberá devolverle el informe corregido. En el caso de que el informe no cumpla con los requerimientos mínimos de acuerdo al presente pliego, no se considerará realizado y, por lo tanto, no será facturable. Si esta situación se repite en tres ocasiones (sean o no consecutivas), EJIE podrá rescindir el contrato.

Fin Fase:

El fin de la fase lo determinará la aceptación de los entregables por parte de EJIE.

SLAs:

Plazo entrega informes: Igual o inferior a 5 días hábiles desde la finalización de la ejecución de la auditoría.

Trazas:

Fecha entrega informes.

Entregables:

Informes de auditoría, incluyendo los entregables indicados en el apartado 5.3. Propuesta Retest.

5.2.2.6 FASE 6: Retest

Inicio Fase:

El inicio de esta fase lo constituye la aceptación de los entregables iniciales de la auditoría.

Una vez aceptado el informe por EJIE, se decidirán las acciones a llevar a cabo para la corrección de las vulnerabilidades encontradas, en la medida de lo posible y en función de las criticidades.

Como fase posterior a la realización de la auditoría, y después de que EJIE ejecute las acciones de remediación que considere oportuno, podría ser necesario confirmar que efectivamente se han remediado con éxito las vulnerabilidades.

La propuesta del Retest, suponiendo que se solicitará verificar la corrección de todas las vulnerabilidades y redactar el informe correspondiente, incluyendo la valoración económica, se entregará junto con el informe de la auditoría. Esta propuesta sería negociable en esta fase si no se considera adecuada por parte de EJIE.

En el caso de que se considere necesario realizar esa confirmación o "Retest", el adjudicatario verificará que las correcciones han sido realizadas, y redactará el informe correspondiente.

Para ello, una vez indicado por parte de EJIE que sí es necesario hacer un Retest, el adjudicatario dispondrá de un plazo igual o inferior a 15 días para la realización de ese Retest. Durante ese plazo se llevarán a cabo los preparativos necesarios para la realización del mismo.

Si la solución aplicada por EJIE no cumple con los requisitos para remediar la vulnerabilidad especificada, el adjudicatario, realizará nuevas recomendaciones para la solución correcta de las vulnerabilidades detectadas y, si se considera necesario, se volverá a iniciar esta misma fase con nuevos Retest.

Fin Fase:

El final de esta fase se dará cuando EJIE de por concluido el proceso de Retest o si no se considera necesario realizar un Retest.

SLAs:

Plazo de ejecución de Retest: Menor o igual a 15 días desde la indicación de la necesidad de realizar un Retest por parte de EJIE.

Trazas:

Fecha inicio Retest. Fecha fin Retest.

Entregables:

Informes tras la realización del Retest.

5.2.2.7 FASE 7: Borrado de información y Fin

Inicio Fase:

Esta fase se inicia en el momento en que EJIE da por finalizada la fase anterior.

Al finalizar cada servicio, el adjudicatario deberá borrar de sus sistemas o archivos los códigos fuente, certificados o cualquier otra información propiedad de EJIE que haya recibido para la realización de su trabajo.

Además, deberá realizar una memoria final resumen de todos los trabajos realizados.

Fin Fase:

Esta fase finaliza en el momento en que el adjudicatario realiza el borrado de información de sus sistemas, quedando todas las trazas y entregables únicamente en los sistemas de EJIE. En ese momento se dará por cerrada la auditoría.

SLAs:

Plazo entrega memoria: Menor o igual a 10 días hábiles para la entrega de la memoria final y del certificado de borrado de información desde la finalización de la fase anterior.

Trazas:

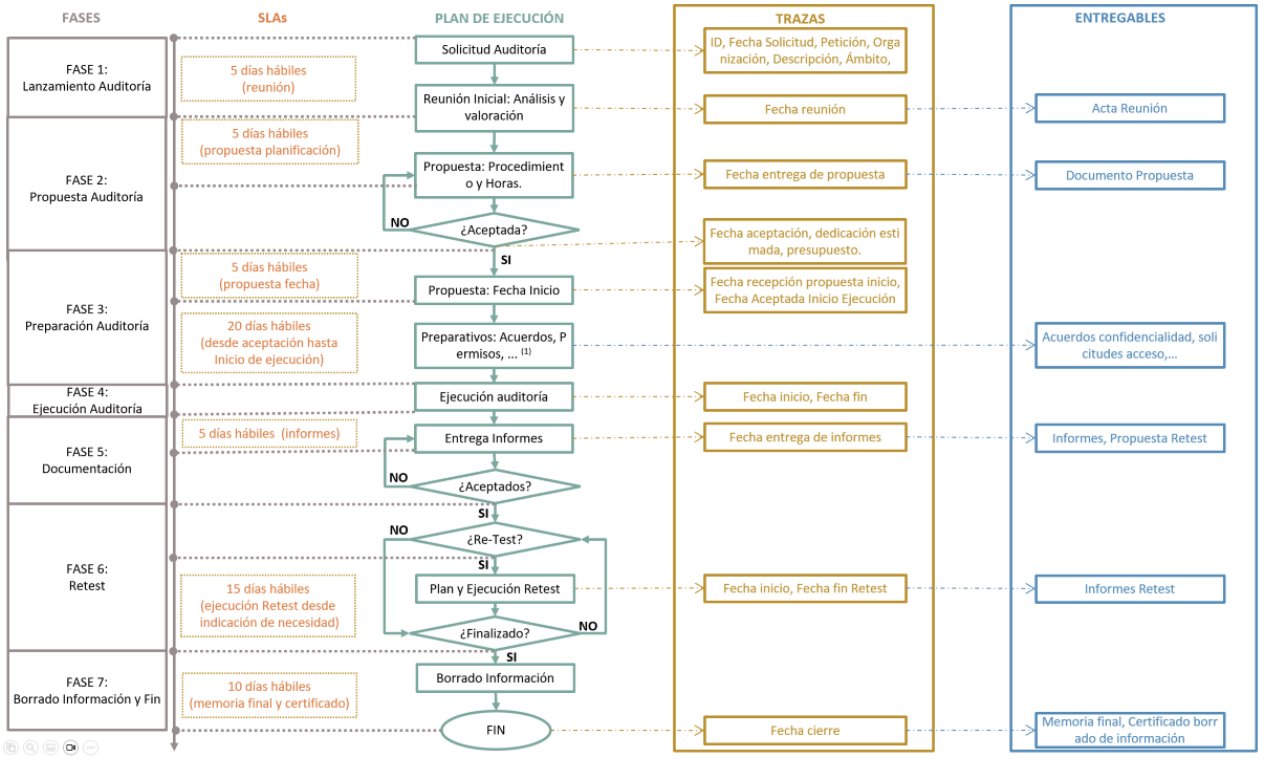
Fecha de cierre.

Entregables:

Memoria final. Certificado de borrado de información.

5.2.3 Esquema

A continuación, se muestra un esquema resumen del plan de ejecución mínimo que debe cubrirse en la oferta, con el mínimo de fases, trazas, entregables y SLAs:



5.3 Entregables de auditorías

Los siguientes aspectos relativos a los entregables relativos al proyecto son comunes al Lote 1 y al Lote 2, aunque puede haber alguna particularidad asociada a los entregables específicos de las auditorías PCI DSS.

5.3.1 Informes de Auditorías

El adjudicatario deberá proporcionar a EJIE informes de auditoría por servicio auditado.

En el caso de las auditorías PCI DSS del LOTE 2, si existe algún requisito particular derivado de los requerimientos desarrollados por el PCI SSC (PCI Security Standards Council), los informes se ajustarán a dichos requisitos particulares.

En general, el objetivo es informar de forma detallada de las vulnerabilidades y vectores de explotación detectados sobre los sistemas auditados, así como de las acciones correctivas que se han de llevar a cabo y aspectos de mejora.

Los informes de auditoría incluirán, como mínimo, los siguientes apartados:

- Elaboración de un informe con un resumen ejecutivo a alto nivel, identificando los principales problemas y procesos afectados, así como las áreas de mejora globales.
    - Objeto y alcance.
    - Resumen ejecutivo.
    - Metodología empleada.
    - Herramientas empleadas.
    - Pruebas realizadas.
    - Hallazgos y debilidades.
    - Vías de explotación exitosas.
    - Riesgos principales e impacto (criticidad, evidencias…).
    - Recomendaciones principales de mejora a alto nivel.
- Informe ligero de cada una de las pruebas:
    - Detalle pruebas realizadas especificando su objetivo.
    - Resultados obtenidos, incluyendo el nivel de vulnerabilidades detectadas.
- Elaboración de un informe técnico en detalle, analizando cada una de las vulnerabilidades y hallazgos detectados a bajo nivel, así como las acciones correctivas concretas:
    - Detalle de cada una de las vulnerabilidades.
    - Valoración del impacto.
    - Descripción y evidencias.
    - Descripción del impacto asociado.
    - Recomendaciones detalladas para su resolución.
- Elaboración de un informe de vulnerabilidad crítica detectada con el detalle técnico:
    - Descripción de la vulnerabilidad.
    - Impacto asociado.
    - Detalle de explotación y prueba de concepto.

En caso de que se encuentren durante las auditorías vulnerabilidades críticas o que impliquen un alto riesgo de fuga de información se emitirá una alerta inmediata (al responsable del servicio auditado a través de EJIE) acompañada de un informe ligero con la información más importante (descripción de la vulnerabilidad, descripción del tipo de impacto y solución o workaround temporal para mitigar la misma en caso de que no hubiese una solución eficiente disponible en el momento).

En todos los tipos de informes indicados, deberá aparecer un apartado final con:

- Plan de acción para mitigar el riesgo.
- En caso de aplicar, se adjuntará un video explicativo de la explotación.
- Propuestas de tratamiento, incluyendo estimación de esfuerzo y priorización.
- Conclusiones: resumen de las principales vulnerabilidades detectadas y recomendaciones de mejora.

5.3.2 Informes de Retest

Como fase posterior a la realización de las auditorías, y después de que EJIE ejecute las acciones de remediación que considere oportuno, podría ser necesario confirmar que efectivamente se han remediado con éxito las vulnerabilidades, y se debería presentar un informe final con la confirmación de dichas remediaciones, tal y como se ha indicado en el plan de ejecución.

5.3.3 Memoria final

Al alcanzar la finalización la auditoría, el adjudicatario deberá presentar una Memoria Final, como informe justificativo del alcance efectivo de todos los trabajos realizados, que debe incluir todos los entregables anteriormente realizados.

Asimismo, la memoria incluirá un capítulo adicional con contenido detallado especificando las herramientas y tácticas empleadas, referencias utilizadas, propuestas de remediación, etc.

5.3.4 Certificado acreditativo de borrado de información

Asimismo, a la finalización de la auditoría el adjudicatario deberá entregar un documento firmado en el que garantiza que todo el código fuente u otra información propietaria de EJIE han sido eliminados de sus sistemas y archivos.

6 Requisitos de Seguimiento

El licitador establecerá en su propuesta un **Plan de Seguimiento y control de Calidad** con las metodologías, procedimientos, indicadores, etc. propuestos para el seguimiento, mejora y optimización de los servicios prestados, todo ello teniendo en cuenta los requisitos establecidos en este pliego. Este apartado se refiere al seguimiento del servicio en general, no de cada auditoría en particular, estas últimas están cubiertas en el apartado 5.

6.1 Niveles de Servicio

El desarrollo del Servicio y su calidad deberá gobernarse de acuerdo a unos Acuerdos de Nivel de Servicio (ANS/SLA) que sirvan para medir el grado de calidad del mismo. La prestación de los servicios objeto del pliego conllevará el cumplimiento, como mínimo, de los ANS indicados a continuación. El licitador podrá ofrecer otros ANS que complementen a los anteriores o mejorar los objetivos solicitados, que serán valorados, durante la fase de adjudicación, de acuerdo con los criterios indicados en el pliego de condiciones particulares.

Indicador	Descripción	Objetivo	Período de Cómputo	Tipo de penalización
Plazo Reunión Inicial	Tiempo transcurrido desde la solicitud de una nueva auditoría hasta la fecha propuesta para la reunión de lanzamiento	<= 5 días hábiles	Por Auditoría	1
Plazo Propuesta Planificación	Tiempo transcurrido desde la finalización de la reunión de lanzamiento hasta la recepción de la propuesta de auditoría	<= 5 días hábiles	Por Auditoría	1
Plazo Entrega Fecha Inicio Auditoría	Tiempo transcurrido desde que se acepta la propuesta de auditoría hasta que se recibe una propuesta de fecha de comienzo de auditoría	<= 5 días hábiles	Por Auditoría	1
Plazo Inicio Auditoría	Tiempo transcurrido desde que se acepta la propuesta de auditoría hasta la fecha propuesta de comienzo de auditoría	<= 20 días hábiles	Por Auditoría	1
Plazo entrega informes	Tiempo transcurrido desde la fecha de finalización de la auditoría hasta que se reciben los informes de la auditoría	<= 5 días hábiles	Por Auditoría	1
Plazo ejecución Retest	Tiempo transcurrido desde que se informa de la necesidad de ejecutar retest hasta la fecha propuesta para la ejecución del mismo.	<= 15 días hábiles	Por Retest	1

Plazo entrega memoria	Tiempo transcurrido desde la finalización de la fase anterior hasta la entrega de la memoria final y del certificado de borrado de la información	<= 10 días hábiles	Por Auditoría	1
Trazas y Seguimiento	Falta de trazas de la auditoría	> 1 trazas incompletas	Por Auditoría	2
Entregables	Falta de entregables	> 1 entregable sin entregar	Por Auditoría	2
Recursos	Nº de Recursos no disponibles para ejecución de auditoría/retest ya planificado	0	Por Auditoría	1

6.2 Indicadores, Informes y Cuadros de Mando

Además de los informes específicos de las auditorías, se deberán generar una serie de indicadores, informes y/o cuadros de mando de seguimiento del servicio.

En cualquier caso, será **responsabilidad del adjudicatario crear y mantener un documento de Seguimiento del proyecto en formato Excel o equivalente, con todas las trazas que permita saber lo realizado en cada auditoría y el resultado de las mismas.**

Además de los informes específicos de las auditorías, se deberán generar una serie de indicadores, informes y cuadros de mando de seguimiento del servicio. La empresa licitadora deberá detallar su propuesta de entregables y cuadros de mando, identificándose, al menos, los siguientes:

- Trazas de Seguimiento de Auditorías
- Informes de Seguimiento para comités de seguimiento.

Los indicadores, informes y cuadros de mando propuestos por la empresa 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 empresa 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.

6.3 Comités de Seguimiento

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

- Ejecutivo/Estratégico: Orientado al seguimiento del estado general del servicio y de la evolución del mismo, así como de los hitos principales del avance del servicio.