Eusko Jaurlaritzaren
Informatika Elkartea

Sociedad Informática
del Gobierno Vasco

Suministros y servicios para la renovación del sistema de Firewalls y plataforma de seguridad asociada en Cyberzaintza

Especificaciones de compra / Pliego de condiciones técnicas

Agosto 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	Agosto 2026	Versión Inicial	Javier Gonzalez Tavera	Aritza Iratzagorria Garay

Índice

1 Introducción 4

1.1 Perfil de la Compañía 4

1.2 Antecedentes 4

2 Objeto del contrato 5

3 Alcance del contrato 6

3.1 Suministros 6

3.2 Servicios 7

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.euskadi.eus

1.2 Antecedentes

En la actualidad, Cyberzaintza dispone de un sistema de seguridad perimetral compuesto, entre otros elementos, por un conjunto de firewalls que dan servicio al tráfico del centro de datos, junto con el licenciamiento de seguridad avanzada asociado y el acceso remoto de aproximadamente 200 usuarios.

Este equipamiento constituye un sistema de importante valor estratégico en materia de ciberseguridad. Por razones de obsolescencia tecnológica y de fin de ciclo de vida de la generación de equipos instalada, y dada su criticidad, se hace necesario iniciar un procedimiento de contratación de suministros que garantice la continuidad de funcionamiento frente a incidencias de cualquier tipo, y que permita disponer de una plataforma con capacidad, rendimiento y capacidades funcionales alineadas con las crecientes necesidades en materia de ciberseguridad, incluyendo la protección del puesto de trabajo remoto y el control del uso de aplicaciones en la nube y de inteligencia artificial generativa.

En virtud de lo expuesto, se plantea la contratación de suministros para la incorporación de una nueva pareja de equipos firewall de nueva generación, la evolución del licenciamiento de seguridad avanzada, de la plataforma de acceso seguro para los usuarios remotos, la consola de gestión unificada en la nube, y los servicios de implantación y migración asociados.

2 Objeto del contrato

El presente expediente tiene por objeto la contratación de los suministros de equipos firewall, suscripción de licencias de seguridad avanzada, plataforma de acceso seguro para usuarios remotos, consola de gestión unificada y el soporte del fabricante, junto con los servicios de implantación y migración de la solución.

En definitiva, el resumen de alcance de este pliego se expone a continuación:

- Suministro de nuevos equipos firewall de nueva generación (Gen5) junto con su garantía y servicios de soporte de fabricante asociados.
- Suministro del licenciamiento de seguridad avanzada perimetral, incluyendo el control de aplicaciones SaaS e IA generativa.
- Suministro de la plataforma de acceso seguro (SASE/ZTNA) para los usuarios remotos, junto con su soporte.
- Suministro de la consola de gestión unificada en la nube para los firewalls y para el entorno de acceso remoto.
- Servicios de implantación y migración de la solución.

No se ha dividido en lotes, dado que el objeto de este expediente es la renovación de una única plataforma de seguridad que constituye una unidad funcional indivisible, cuya división comprometería la coherencia técnica y operativa de la solución.

3 Alcance del contrato

3.1 Suministros

3.1.1 Descripción del suministro

La descripción detallada de los suministros del fabricante Palo Alto Networks incluidos en este contrato se especifica en el documento denominado "*Anexo Reservado PCT*".
A demanda, EJIE proporcionará, **bajo solicitud del licitador**, datos de este escenario tecnológico involucrado cumplimentando el Anexo XVI del Pliego de Condiciones Particulares (PCP) denominado: modelo declaración responsable de confidencialidad, y con el procedimiento de declaración de confidencialidad establecido en la cláusula 20 del PCP.

La empresa adjudicataria deberá suministrar los productos, licencias y servicios indicados a continuación, junto con la garantía y el soporte de fabricante asociado. Todo el equipamiento, las licencias y los soportes de fabricante deberán ser oficiales y estar garantizados por el fabricante, serán a su recepción propiedad de Cyberzaintza y deberán figurar a su nombre.

La empresa adjudicataria deberá incluir, junto con los suministros, la garantía y el soporte del fabricante de acuerdo con las siguientes condiciones:

- Todas las licencias y equipos objeto de suministro deberán disponer de garantía y soporte de fabricante durante el periodo que se establezca en el Pliego de Condiciones Particulares. El adjudicatario deberá poner a disposición de Cyberzaintza las licencias demo necesarias desde la fecha de formalización hasta la fecha de activación de las nuevas licencias.
- Se incluye el software necesario para garantizar las diferentes funcionalidades y tecnologías solicitadas, incluyendo el soporte de fabricante en el periodo indicado.
- El soporte de fabricante debe incluir, sin coste adicional para EJIE ni Cyberzaintza, el acceso a las actualizaciones de parches, alertas de seguridad y nuevas versiones de software durante el periodo de garantía. El suministro de la actualización incluirá tanto las licencias y software como los manuales y la documentación técnica del fabricante asociado.
- Las empresas licitadoras deberán presentar un documento con la descripción de los procedimientos vinculados a la gestión del soporte de fabricante y garantías (gestión RMA) del equipamiento suministrado para el periodo en cuestión.
- Las empresas licitadoras deberán presentar justificación de cumplimiento de las garantías solicitadas mediante la declaración responsable correspondiente, de acuerdo con las condiciones establecidas en el PCP.

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

3.1.2 Justificación de la tecnología

En la actualidad, el sistema de firewalls y de seguridad de Cyberzaintza está formado por equipos y software del fabricante Palo Alto Networks. La incorporación de una tecnología de un fabricante diferente al actual implicaría un impacto significativo en las operaciones y en los siguientes ámbitos.

Afectación en el ámbito técnico:

- La introducción de un nuevo fabricante llevaría implícita la necesidad de disponer de nuevas plataformas de gestión, telemetría y explotación distintas de las actuales (consola unificada, servicio de logging, capacidades AIOps y ADEM), obligando a mantener en paralelo entornos de gestión heterogéneos durante la convivencia.

- La disposición de nuevas tecnologías o fabricantes requeriría maquetas y pilotos previos para confirmar compatibilidades con elementos y dispositivos específicos de la solución (integración con directorio, agente de usuario remoto, interconexión SASE-perímetro, políticas unificadas), compatibilidades ya superadas y validadas en la tecnología instalada.
- La migración de la base de políticas de seguridad, objetos, perfiles de inspección y reglas acumuladas históricamente hacia un fabricante distinto conlleva un riesgo elevado de pérdida de configuración, errores de traducción de reglas y ventanas de exposición durante el corte, en un sistema de criticidad alta.

Afectación en el ámbito organizativo:

- La incorporación de un fabricante adicional incrementaría la complejidad y el esfuerzo de operación y mantenimiento, derivado de la necesidad de gestión paralela sobre tecnologías de fabricantes diferentes contra plataformas distintas.
- Obligaría a definir, con los diferentes grupos de soporte, procedimientos de operación y mantenimiento adicionales para la nueva tecnología, atendiendo a los modelos de relación y de garantías del propio fabricante.
- Requeriría capacitar técnicamente a los recursos actuales de los grupos de soporte en el corto plazo para poder operar la plataforma con los niveles de respuesta exigidos, con el consiguiente riesgo operativo durante el periodo de aprendizaje.

Afectación en el ámbito económico:

- Incorporar un nuevo fabricante supondría un mayor coste en recursos, capacitación y esfuerzo de operación, tanto en la puesta en marcha de la nueva infraestructura como en la operación y mantenimiento posterior.
- Se perdería la inversión ya realizada en la especialización del personal sobre la tecnología instalada.

Continuidad y evolución (salto generacional):

- El presente expediente contempla la adquisición de equipamiento del mismo fabricante que los equipos actuales (Palo Alto Networks), incorporando el salto a la nueva generación tecnológica, con el fin de facilitar la explotación y operación de la solución, preservar la inversión y garantizar los tiempos de respuesta actuales sin costes adicionales de reciclaje tecnológico. Esta continuidad permite además mantener la infraestructura de fibra 10G existente (interfaces SFP+) sin cambios, y evolucionar de forma nativa hacia la gestión unificada (firewall + SASE) bajo una única consola, incorporando nuevas capacidades (control de IA generativa, ZTNA 2.0 y seguridad de datos) sobre una base tecnológica ya conocida y validada por la organización.

En definitiva, el presente expediente de contratación contempla la adquisición de equipamiento del mismo fabricante que los equipos actuales (Palo Alto), con el fin de facilitar la explotación y operación de la solución, garantizando la continuidad de los servicios, manteniendo los tiempos de respuesta actuales, preservando las integraciones y procedimientos ya implantados y evitando los costes y riesgos asociados a un proceso completo de sustitución tecnológica en una infraestructura crítica de ciberseguridad.

3.2 Servicios

En este apartado se describe el alcance de los servicios solicitados.

3.2.1 Proceso de migración

Teniendo en cuenta el escenario tecnológico actual del sistema de cortafuegos de Cyberzaintza descrito en el documento denominado “Anexo Reservado PCT”, con carácter obligatorio, la empresa adjudicataria

deberá incluir en su oferta los servicios de implantación y migración de la solución, garantizando la ejecución completa de las actividades y la entrega de los productos y servicios que se detallan a continuación:

- Instalación física y lógica de los equipos cortafuegos en alta disponibilidad e integración con la infraestructura de fibra 10G (SFP+) existente.
- Migración de la base de políticas, objetos, perfiles de inspección y reglas desde la plataforma actual a los nuevos equipos.
- Alta, configuración y puesta en marcha de la consola de gestión unificada para firewalls y entorno de acceso remoto.
- Despliegue y puesta en producción de la plataforma de acceso seguro para los 200 usuarios remotos.
- Configuración de las capacidades de seguridad avanzada, incluido el control de aplicaciones SaaS e IA generativa.
- Configuración de todos los servicios de la plataforma siguiendo las guías del Centro Criptológico Nacional (CCN) aplicables a cada uno de ellos, aportando evidencia documental del cumplimiento para cada servicio.
- Integración, junto con el equipo de Cyberzaintza, de los logs y la telemetría de la plataforma en el sistema SIEM corporativo.
- Configuración de las copias de seguridad de las configuraciones de todos los elementos de la plataforma y de sus procedimientos de restauración.
- Definición y configuración de los planes de contingencia y recuperación asociados a la plataforma.
- Ajuste y afinado de políticas tras la puesta en producción y acompañamiento durante la estabilización.
- Formación y transferencia de conocimiento al personal técnico de Cyberzaintza sobre la operación de la plataforma.

El plazo máximo para realizar las tareas indicadas en este apartado es de 2 meses desde el inicio del contrato y, en todo caso, se deberán finalizar antes de la fecha de finalización de licencias y soporte de equipos cortafuegos objeto de migración (31/12/2026).

Si, por alguna razón, se superara esta fecha límite (31/12/2026) por razones ajenas a EJIE/Cyberzaintza, el licitador será el responsable de suministrar las licencias y garantías necesarias para los equipos cuyo soporte finaliza en dicha fecha hasta completar la migración.

3.2.2 Servicio de revisión (assessment)

Durante la vigencia del contrato, la empresa adjudicataria realizará revisiones del estado de la plataforma con una periodicidad al menos semestral, orientadas a verificar que la configuración es correcta, que los servicios contratados se están explotando adecuadamente y que se mantienen las buenas prácticas y el cumplimiento de las guías CCN, proponiendo las acciones de mejora que procedan. Cada revisión incluirá, como contenido mínimo:

- Revisión de la configuración de los equipos, consola de gestión y plataforma de acceso remoto frente a las buenas prácticas del fabricante y las guías CCN aplicables.
- Verificación del estado de alta disponibilidad, versiones de software y firmas, y vigencia de licencias y soporte.
- Análisis del grado de aprovechamiento de las suscripciones y capacidades contratadas (seguridad avanzada, control SaaS/IA, ZTNA).
- Revisión de la base de políticas y reglas: reglas obsoletas, solapamientos, permisividad excesiva y oportunidades de optimización.
- Verificación de la integración de logs y telemetría en el SIEM y del funcionamiento de las copias de seguridad de configuraciones.
- Comprobación de la vigencia y validez de los planes de contingencia y recuperación.
- Identificación de hallazgos, clasificación por criticidad y recomendaciones de mejora.

3.2.3 Requisitos para los servicios de puesta en marcha

La empresa adjudicataria deberá considerar, entre los servicios a prestar, el proyecto para el aprovisionamiento y puesta en marcha.

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

- Servicios de construcción y migración al nuevo entorno.
- Configuración y ajuste del servicio.
- Documentación de la solución.
- Transferencia de conocimiento del servicio.
- Servicios de mantenimiento durante la puesta en marcha.

3.2.3.1 Servicios de construcción y migración al nuevo entorno

Con el inicio del contrato, el adjudicatario deberá realizar las tareas necesarias para la construcción y migración de la solución existente a la nueva solución requerida, incluyendo la instalación, configuración y migración de todos los elementos necesarios. Es de destacar, que en caso de que sea necesario activar licencias para acometer tareas de aprovisionamiento de la infraestructura, estas licencias temporales correrán a cargo del adjudicatario.

Se considera, al menos, la ejecución de las siguientes tareas que pasan a describirse posteriormente:

- Consultoría y diseño de la solución para la construcción y migración de los servicios al nuevo entorno.
- Elaboración del conjunto de planes de pruebas y su ejecución necesarios para confirmar que las soluciones quedan convenientemente operativas.
- Vinculado a lo anterior, definición y ejecución del plan de implantación para alcanzar la nueva solución, con la mínima afectación a las personas usuarias actuales.
- Instalación y configuración de los elementos necesarios en el nuevo entorno, atendiendo al diseño validado y plan de implantación.
- Documentación, transferencia de conocimiento y entrega del servicio.
- Soporte y mantenimiento durante el proceso de despliegue y migración de la infraestructura y servicios al nuevo entorno. En este sentido, la empresa adjudicataria desarrollará tareas englobadas en el denominado nivel 2 de soporte de EJIE/Cyberzaintza como son el mantenimiento evolutivo, configuraciones solicitadas y de las incidencias (mantenimiento correctivo) de los servicios en proceso de migración hasta realizar la transferencia de conocimiento y entrega a operación. Tras cada intervención y, en coordinación con EJIE/ Cyberzaintza, el adjudicatario deberá estar disponible, incluso con presencia in-situ si así se requiere, para atender las posibles incidencias que se deriven de cada intervención.

El adjudicatario deberá realizar una propuesta de diseño de detalle (bajo nivel) para la construcción e implantación de la infraestructura y servicios actuales en el nuevo entorno y que será aprobada por EJIE/ Cyberzaintza.

La propuesta de diseño deberá contemplar aspectos tales como:

- Arquitectura de la solución, incluyendo:
- Componentes de la solución, indicando claramente la función de cada uno de ellos.
    - Escalabilidad y flexibilidad de la arquitectura propuesta, en volumen y funcionalidades.
- Funcionamiento lógico de la solución:
    - Funcionamiento de la solución propuesta, cubriendo todas las funcionalidades y requisitos indicados en los puntos previos.

  - Mecanismos de HA (*High Availability*), balanceo de carga y DR (*Disaster Recovery*).
- Gestión de la solución.
- Capacidades de reporting y de gestión de inventario.
- Monitorización y Alertas.
- Valor añadido de la arquitectura y diseño propuesto

El adjudicatario deberá proponer el plan de implantación (plan del proyecto) para la migración de la infraestructura y servicios actuales al nuevo entorno de acuerdo con el diseño validado para garantizar la continuidad del servicio y de ser necesario, la convivencia de la nueva infraestructura con la existente hasta su completa migración, garantizando la mínima afectación a las personas usuarias actuales de los servicios.

El plan deberá identificar diferentes fases para acometer el proceso de cambio y establecer la necesidad de coordinación/ejecución de trabajos por parte de terceros y otros grupos de soporte. Igualmente, el plan deberá contemplar un Plan de Pruebas atendiendo a las fases en las que se defina el Plan de Implantación que verifique la correcta puesta en marcha de los servicios y entorno creado, así como un Plan de Marcha Atrás ante cualquier incidencia acaecida en el proceso de cambio. El Plan de Implantación deberá validarse de forma conjunta con EJIE/Cyberzaintza .

Atendiendo al diseño propuesto y validado por EJIE/Cyberzaintza , y siguiendo el Plan de Implantación acordado, el adjudicatario deberá considerar la ejecución de los siguientes servicios:

- Instalación y configuración de los elementos que componen la solución, de forma que la nueva infraestructura quede preparada para dar soporte a los servicios actuales sobre el nuevo entorno. Se incluye la ejecución de los trabajos necesarios para garantizar la conectividad y comunicación entre los diferentes elementos que constituyen la arquitectura y diseño final del servicio.
- Migración de los servicios que actualmente se prestan según diseño y plan acordado. Asimismo, se acordarán y coordinarán los horarios de los trabajos y ventanas temporales para cada actuación necesaria con EJIE/Cyberzaintza, con el objetivo de reducir la afectación a las diferentes personas usuarias.
- Configuración de backups, monitorización e inventario, colaborando para ello con los grupos correspondientes en EJIE/Cyberzaintza y ajustándose en todo momento a los estándares y procedimientos de EJIE/Cyberzaintza . Integración con las herramientas de operación y gestión, Monitorización, back up, en los casos en que aplique.
- Definición de plantillas de configuración para la puesta en marcha de las soluciones y servicios a migrar, incluyendo las plataformas de gestión e informes.
- Ejecución del Plan de pruebas acordado, que permita validar el funcionamiento correcto de la solución de acuerdo con los requerimientos establecidos en el presente pliego en el nuevo entorno (funcionamiento habitual, monitorización, entre otros). El plan de pruebas incluirá el procedimiento de parada y arranque de la plataforma completa y de elementos por separado, en caso de que aplique.
- Una vez realizadas las pruebas y analizados los diferentes resultados, el adjudicatario deberá, en caso de necesidad:
    - Adecuar el Plan de Migración a adoptar, concretando las diferentes necesidades y servicios a considerar en el despliegue, esfuerzos requeridos, y recursos a disponer.
    - Revisar y adecuar otros procedimientos y metodologías de ejecución, control y seguimiento; adecuación de plantillas de documentación etc.
    - Adecuar aspectos técnicos sobre el diseño de la solución y su parametrización, para garantizar el cumplimiento de los criterios definidos en el presente pliego.
    - Adecuar el Plan global del proyecto a partir de los puntos anteriores.

3.2.3.2 Equipo de trabajo para la ejecución del proyecto

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

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

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

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

Un aspecto clave para el dimensionamiento de recursos y organización es, no solo la ejecución de los trabajos, sino también la necesidad de elaboración de documentación (informes finales, inventarios, documentación de entrega del servicio, actas de servicio…) requerida en las diferentes fases de proyecto.

Asimismo, en el inicio del proyecto, el adjudicatario deberá exponer la relación detallada del equipo de trabajo propuesto y dedicaciones, en base a los medios personales y materiales que adscriba al contrato y con los que haya acreditado el cumplimiento de los requisitos de solvencia que hayan sido exigidos en el pliego de condiciones particulares. EJIE/Cyberzaintza podrá solicitar cambios sobre los recursos propuestos en caso de que, tras el análisis de la propuesta trasladada, determine que los medios propuestos no son suficientes y/o adecuados para el cumplimiento del plan de trabajo.

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

Los componentes del grupo de trabajo desarrollarán su labor con hardware y software propiedad del adjudicatario.

A fin de evitar riesgos de afectación al servicio por la posible indisponibilidad de los equipos que componen la actual infraestructura de seguridad, se considera de suma importancia que el adjudicatario defina las necesidades mínimas, en lo que a disponibilidad y dedicación de los recursos humanos se refiere, para asegurar el cumplimiento de los plazos de migración.

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

- **Jefe/a o Director/a de Proyecto, mencionado previamente,** que será el responsable último del contrato y de la disposición de los medios y su coordinación para cumplimiento de los objetivos del proyecto (plazos, calidad, alcance...), y con los conocimientos y capacidades solicitados en el PCP.
- **Un especialista en tecnología del fabricante de la tecnología ofertada para este expediente** para el diseño y migración, que será el responsable técnico del diseño de la solución, plan de migración y construcción del nuevo entorno, y con los conocimientos y capacidades solicitados en el PCP.

El licitador podrá proponer una misma persona que desempeñe ambos roles siempre y cuando esta persona cumpla los requisitos indicados en los dos roles.

Dichos perfiles y su descripción deberán reflejarse en el Anexo II del PCP (anexo de adscripción de medios), justificando aquellos con requisitos en la fase de solvencia técnica.

Con el inicio del proyecto, el adjudicatario deberá actualizar su plan de trabajo y exponer la relación detallada del equipo propuesto y dedicaciones en cada fase del proyecto. EJIE/Cyberzaintza podrá solicitar cambios sobre los recursos expuestos en caso de que, tras el análisis de la propuesta, determine que los medios expuestos no son suficientes y/o adecuados para el cumplimiento de los planes de trabajo.

3.2.3.3 Documentación del servicio

El adjudicatario deberá documentar la solución desplegada y el servicio configurado, completando la documentación necesaria para el modelado del servicio, incluyendo, al menos:

- Plan de implantación y migración, con fases, ventanas de trabajo y plan de marcha atrás.
- Documento de diseño y configuración final de la solución (equipos, consola, acceso remoto y políticas).
- Evidencias de configuración conforme a las guías CCN para cada servicio.
- Documento de integración de logs y telemetría en el SIEM.
- Procedimientos de copia de seguridad y restauración de configuraciones.
- Planes de contingencia y recuperación.
- Acta de puesta en producción y pruebas de aceptación.
- Documentación de operación y manual para la administración de la plataforma.
- Certificado de formación impartida.
- Informe de cada revisión (assessment), con hallazgos y recomendaciones.
- Documentación técnica (oficial) con las características de las soluciones desplegadas, manuales técnicos y operativos.

3.2.3.4 Transferencia de conocimiento

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

- Descripción técnica y de detalle sobre la solución implantada, así como del conjunto de elementos instalados y que forman parte de la solución.

- Gestión y operación del servicio: monitorización, configuración del servicio, diagnóstico de averías, datos de uso del servicio.

La transferencia de conocimiento deberá garantizar que el equipo de soporte de EJIE/Cyberzaintza adquiera un completo conocimiento, tanto a nivel operativo como de configuración y manejo de la tecnología, que les permita operar el servicio y hacer frente a las incidencias y cambios.

Las sesiones de transferencia de conocimiento deberán ser impartidas, en la modalidad que EJIE/Cyberzaintza consideren oportuna, por personal cualificado que cuente con un amplio conocimiento sobre las tecnologías involucradas en este contrato. La duración de las sesiones deberá ser, como mínimo, de:

- Al menos 4 horas, distribuidas en las sesiones que EJIE/Cyberzaintza estime necesarias para adaptarse a la disponibilidad del personal de EJIE/Cyberzaintza

En base al contenido indicado, EJIE/Cyberzaintza se reservará el derecho de solicitar al adjudicatario dicha formación o parte de ella al inicio del contrato, que permita disponer del conocimiento necesario para hacer frente al mantenimiento del servicio por parte de su equipo de soporte.

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

La transferencia de conocimiento tendrá lugar en remoto o en las instalaciones que EJIE/Cyberzaintza especifique.

3.2.4 Requisitos asociados a los servicios

3.2.4.1 Requisitos generales

Los trabajos a desarrollar por el adjudicatario se consideran "**llave en mano**", por lo que éste deberá aportar todas las prestaciones, suministros y servicios que sean necesarios, excepto aquellos que de forma explícita se hayan establecido como fuera del alcance del contrato. Ello incluye la puesta a disposición del personal técnico adecuado y con la experiencia necesaria para la prestación de los servicios.

Asimismo, el adjudicatario aportará todas las herramientas, aparatos, equipos de medida/pruebas, y cualquier otro material que pueda ser necesario para llevar a cabo las tareas requeridas para la ejecución del contrato.

En el desarrollo de los trabajos objeto del servicio es responsabilidad del adjudicatario atenerse a toda la normativa que sea de obligado cumplimiento y a la buena práctica que en cada momento sea aplicable a la actividad que realiza, tanto en sus aspectos técnicos como administrativos.

Serán por cuenta del adjudicatario los seguros necesarios para la realización de las actividades objeto del presente pliego, así como para cubrir los posibles daños o perjuicios que pudieran ocasionarse.

Como criterio general, durante la ejecución de los trabajos objeto de la contratación, la empresa adjudicataria se compromete a facilitar en todo momento a EJIE/Cyberzaintza y, si es el caso, a las personas designadas por esta, la información y documentación que estas soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan presentarse y de las tecnologías, métodos y herramientas utilizados para resolverlos.

En ningún caso el adjudicatario podrá realizar acciones de comunicación y/o difusión del proyecto sin la debida autorización previa por parte de EJIE/Cyberzaintza.

3.2.4.2 Coordinación con terceros y horarios de actividad (Migración al nuevo entorno).

La empresa adjudicataria deberá considerar la necesidad de coordinación con Soporte EJIE/Cyberzaintza para la ejecución de las tareas de migración de los servicios. En la misma línea y de cara a una entrega a Operación más efectiva, personal del Soporte EJIE/Cyberzaintza podrá participar en la ejecución del proyecto.

El adjudicatario deberá considerar la ejecución de los servicios en horario acordado con EJIE/Cyberzaintza, con el fin de reducir la afectación a las diferentes personas usuarias, según se indique por parte de EJIE/Cyberzaintza en el Plan de Implantación.

3.2.5 Seguimiento y control de ejecución del proyecto

3.2.5.1 Seguimiento por parte de EJIE/Cyberzaintza

EJIE/Cyberzaintza será responsable de la gestión y seguimiento global del proyecto, velando por el cumplimiento de hitos y objetivos establecidos en contrato. Entre las tareas a realizar por parte de EJIE/Cyberzaintza, se incluye:

- Gestión y seguimiento global del proyecto, velando por el cumplimiento de hitos y objetivos establecidos en contrato.
- Establecimiento, en colaboración con el adjudicatario, del conjunto de metodologías y procedimientos necesarios, que garanticen las actuaciones coordinadas y faciliten el cumplimiento de planificación.
- Con relación con la migración de los servicios al nuevo entorno:
    - Validación de la solución final adoptada (nuevo entorno) y participación en la decisión de aspectos técnicos del proyecto.
    - Revisión y validación del Plan de Implantación que se adopte para la migración de los servicios al nuevo entorno.

  - Propuesta en colaboración con adjudicatario, y validación del conjunto de metodologías y procedimientos necesarios para garantizar la coordinación de actividades y cumplimiento de la planificación.
- Coordinación principal de EJIE/Cyberzaintza y adjudicatarias de los soportes y otros agentes que estén involucrados/afectados en/con la ejecución de los trabajos.
  - Verificación de cumplimiento de las condiciones para la entrega del servicio.
- Seguimiento a los servicios de mantenimiento prestados hasta fin de contrato.
- Validación del resto de documentación as-built, para poder establecer el cierre de proyecto.

3.2.5.2 Plataforma de gestión del proyecto

EJIE/Cyberzaintza podrá poner a disposición del proyecto de una plataforma de gestión documental, accesible a todas las personas usuarias autorizadas y donde se mantendrá actualizada con la periodicidad que se establezca la documentación del proyecto. Esta herramienta será de especial relevancia principalmente como herramienta para validación e intercambio de documentación durante la ejecución del contrato.

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

- Datos de partida.
- Actas
- Documentos sobre el diseño de la solución y plan de migración.
- Documentación solicitada por EJIE/Cyberzaintza para la entrega del servicio.
- Criterios y acuerdos relativos a la ejecución de los trabajos.
- Cuadros de mando de carácter ejecutivo para control de avance del despliegue y control sobre las necesidades de materiales.
- Cualquier otra documentación técnica, funcional o de gestión asociada al proyecto.

3.2.5.3 Seguimiento por parte del adjudicatario

Si bien la gestión y dirección global del proyecto será llevada a cabo por parte de EJIE/Cyberzaintza , el adjudicatario será el responsable principal de controlar la ejecución de los trabajos, estableciendo para ello, todos los mecanismos y procedimientos necesarios que garanticen el cumplimiento de la planificación, la correcta operatividad de la solución y la calidad en el servicio final.

Uno de los aspectos más críticos del proceso de implantación y puesta en marcha es la necesidad de coordinación de los trabajos con los siguientes agentes para que la migración de los servicios se realice con éxito y mínimo impacto posible:

- EJIE/Cyberzaintza como operador de la solución.
- Los diferentes Proveedores, que EJIE/Cyberzaintza considere, por ejemplo, empresas que prestan servicios de consultoría, instalación o soporte a EJIE/Cyberzaintza para infraestructuras y servicios relacionados con el objeto de contratación.

Asimismo, el adjudicatario designará una Jefe/a de Proyecto como interlocutor/a principal con EJIE/Cyberzaintza para el control de ejecución del proyecto que tendrá una participación activa en lo relativo a la prestación de los servicios de migración de la infraestructura y servicios desplegados en el nuevo entorno.

La persona designada como Jefe/a de Proyecto se responsabilizará de las siguientes tareas principales:

- Realizará la coordinación y seguimiento continuo de la evolución de los trabajos de migración y velará por mantener el plan de ejecución de trabajos periódicamente actualizado, considerando en todo momento la integración de sus tareas con aquellas que involucren a EJIE/Cyberzaintza (y soportes).

- Será el responsable por parte del adjudicatario de disponer de los medios y organizar los recursos y equipo de trabajo que garanticen los resultados esperados en proyecto en plazos y calidad técnica.
- Podrá tener, a consideración de EJIE/Cyberzaintza , interlocución directa con otros involucrados del proyecto por parte de EJIE/Cyberzaintza como son los grupos de soporte.
- Realizará reportes de avance de proyecto.
- Definirá metodologías para identificación y control de riesgos y definición de propuestas de mitigación de estos.
- Asistirá, junto con los técnicos que se estime conveniente por parte de EJIE/Cyberzaintza, a las reuniones de seguimiento y técnicas que convoque EJIE/Cyberzaintza , y con la periodicidad que se designe.
- Garantizará que toda la información y documentación del proyecto se encuentra en todo momento actualizada en la plataforma de gestión que a tal efecto disponga EJIE/Cyberzaintza .

3.2.6 Retirada y borrado del equipamiento

Una vez finalizada la migración y confirmado el correcto funcionamiento de la nueva plataforma, la empresa adjudicataria será la responsable de la gestión de los equipos obsoletos (equipos afectados por la migración). Este servicio incluirá obligatoriamente las siguientes actuaciones:

- Borrado seguro de datos: Se realizará una sanitización técnica de los soportes de memoria y almacenamiento de los equipos retirados, siguiendo estándares internacionales reconocidos (NIST 800-88 nivel Purge o equivalente) para garantizar la imposibilidad de recuperación de las reglas de seguridad, objetos de red, configuraciones de VPN y credenciales de Cyberzaintza.
- Certificación de borrado: La adjudicataria deberá entregar un certificado detallado por cada número de serie de hardware retirado, acreditando la fecha y el método de borrado utilizado, como condición previa para la recepción definitiva de los servicios de migración.
- Gestión de Residuos de Aparatos Eléctricos y Electrónicos (RAEE): La empresa adjudicataria procederá a la retirada física y transporte de los equipos obsoletos desde su localización actual hacia un centro de tratamiento autorizado, garantizando el cumplimiento de la Ley 7/2022, de 8 de abril, de residuos y suelos contaminados para una economía circular.
- Evidencia de reciclaje: Se deberá aportar el correspondiente certificado de gestión final de residuos (RAEE), que vincule de forma inequívoca los números de serie de los equipos retirados con su correcta eliminación o tratamiento medioambiental.