Eusko Jaurlaritzaren
Informatika Elkartea

Sociedad Informática
del Gobierno Vasco

Servicios para la elaboración de un Plan de Evolución de Ciberseguridad

Especificaciones de compra / Pliego de condiciones técnicas

Junio 2023

Mediterráneo, 14 • 01010 Vitoria-Gasteiz • Tel. 945 01 73 00* • 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	DD/MM/2023	Versión Inicial	Javier González Tavera	Josu Bagazgoitia

Índice

1 Introducción 4
1.1 Perfil de la Compañía 4
1.2 Antecedentes 6
2 Objeto y Alcance del contrato 7
2.1 Objeto de la Contratación 7
2.2 Alcance de la Contratación 7
2.3 Situación Actual 8
3 Requisitos Técnicos 9
3.1 Clientes 9
3.2 Normativa y Referencias 9
3.3 Iniciativas 10
4 Alcance y Requisitos de los servicios del contrato 11
4.1 Servicios de Elaboración del Plan de Evolución de Ciberseguridad 11
4.2 Servicios de Revisión Anual de Estado del Plan de Evolución de Ciberseguridad 11
4.3 Servicios de respuesta a consultas sobre el plan y las revisiones 11
4.4 Entregables 12
4.5 Requisitos asociados a los servicios 12

1 Introducción

1.1 Perfil de la Compañía

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

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

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

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

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

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

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

La actividad objeto de contratación, es necesaria para la prestación de los servicios, competencia de EJIE S.A., y está incluida en los servicios que pueden ser objeto de contratación (según Instrucción Sexta de la

Instrucciones sobre buenas prácticas en la contratación de servicios de Gobierno Vasco). Su prestación no puede ser asumida con los recursos humanos y técnicos de que dispone EJIE S.A., siendo además inviable su reorganización.

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

1.2 Antecedentes

En respuesta al complejo contexto existente en materia de Ciberseguridad, EJIE realizó en el año 2020 un "Plan Director de Seguridad" que pretendía marcar el camino que se debía seguir en la materia en los siguientes cuatro años, es decir, en el periodo 2020-2023 ambos inclusive.

Uno de los principales objetivos de ese Plan era que se incorporara la Seguridad como algo implícito y necesario en todos los ámbitos y entornos, con una implicación y coordinación a nivel general, no únicamente de los grupos especialistas de seguridad. De cara a los clientes, el objetivo era poder ofrecer la Seguridad como servicios o como módulos dentro de sus servicios.



Se tomó como referencia el ENS nivel alto (L5) como objetivo a alcanzar por los servicios ofrecidos por EJIE, al tratarse de un requisito de algunos de los clientes a los que EJIE da servicio. Asimismo, a la hora de clasificar y priorizar las diferentes iniciativas, se trabajó con la referencia NIST 800-137.

Se identificaron 42 iniciativas clasificadas en diferentes ámbitos y con diferentes prioridades que EJIE ha ido trabajando en los últimos 4 años. El resultado ha sido la construcción de un porfolio de **Servicios Convergentes de Seguridad** que ofrecer a sus clientes.

En este punto, con el fin de que EJIE siga evolucionando en su oferta de Servicios de Seguridad para poder responder a los complejos y cambiantes escenarios IT a los que se enfrenta en el día a día, se hace necesaria la contratación de servicios especializados de seguridad, que contemplen la elaboración un Plan de Evolución de Ciberseguridad, de acuerdo al alcance y requerimientos técnicos y de servicio solicitados en la presente contratación.

2 Objeto y Alcance del contrato

2.1 Objeto de la Contratación

El objeto del presente Pliego de Condiciones Técnicas es la contratación de servicios especializados de seguridad, que contemplen la elaboración de un Plan de Evolución de Ciberseguridad, de acuerdo al alcance y requerimientos técnicos y de servicio solicitados en la presente contratación. Ello permitirá evolución los Servicios de Seguridad ofrecidos por EJIE para responder a los complejos y cambiantes escenarios IT a los que se enfrenta en el día a día

2.2 Alcance de la Contratación

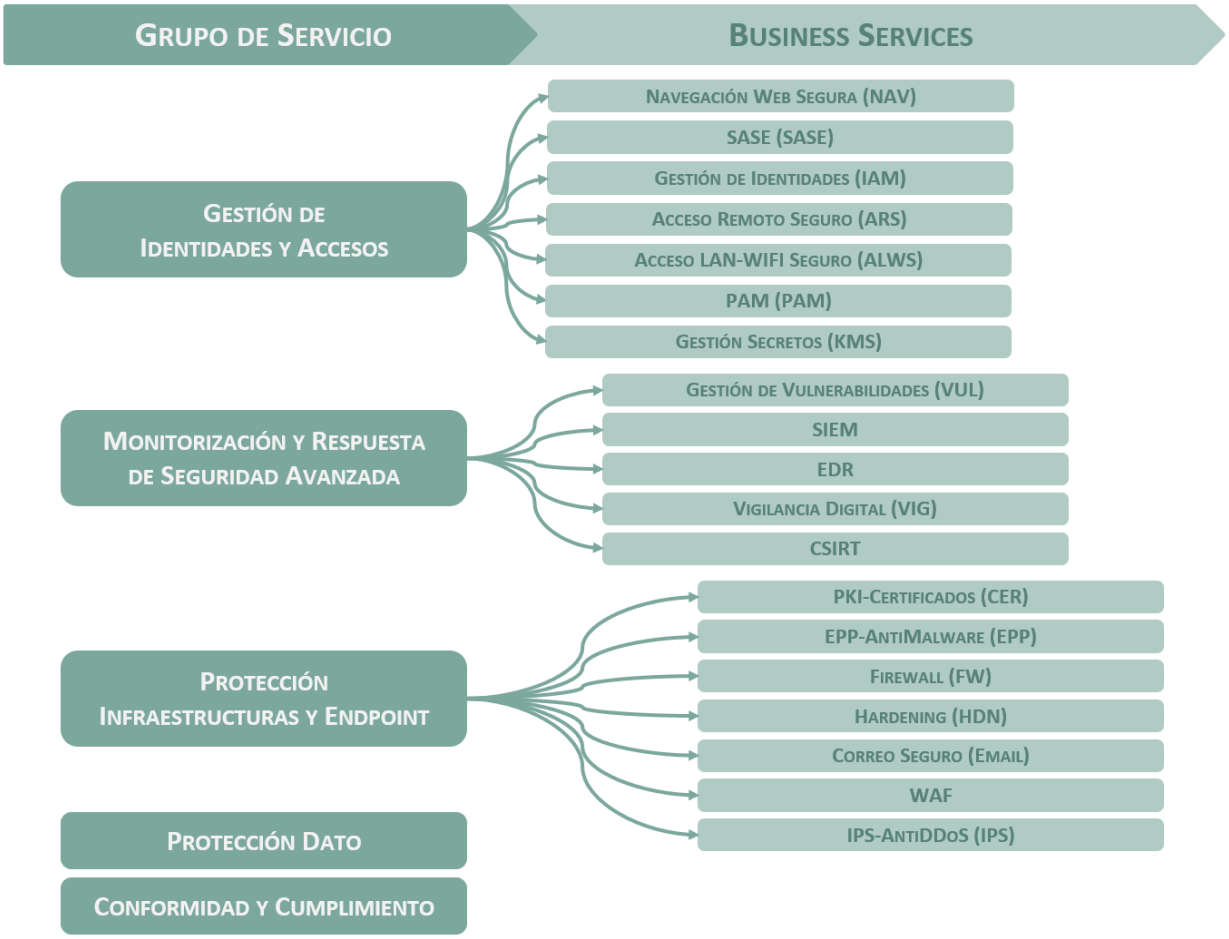
El proyecto deberá considerar el siguiente alcance:

- Servicios necesarios para la elaboración de un Plan de Evolución que permita determinar la estrategia y el camino a seguir en materia de Ciberseguridad en los próximos **3 años (2024-2026)**, permitiendo a EJIE evolucionar el porfolio de Servicios Convergentes de Seguridad que ofrece a las diferentes entidades o clientes a los que da servicio.
- Servicios necesarios para la realización de **una revisión anual (2 en total)** del Plan de Evolución, con objeto de evaluar el progreso y adaptar el plan a posibles nuevas circunstancias.
- Servicios necesarios para la respuesta a consultas sobre el plan y las revisiones realizadas.

2.3 Situación Actual

A continuación, se enumeran los diferentes Servicios Convergentes de Seguridad que EJIE ofrece o tiene previsto ofrecer a sus clientes, con objeto de que el licitador tenga cierto contexto a la hora de elaborar su oferta. Los nombres se consideran suficientemente significativos, por lo que no se proporcionará información adicional al respecto de los servicios en fase de licitación.

Indicar que hay servicios de seguridad que se ofrecen de forma explícita, mientras que otros se ofrecen de forma implícita dentro de otros servicios:



3 Requisitos Técnicos

En este apartado se van a detallar los requisitos técnicos a tener en cuenta a la hora de elaborar el Plan.

3.1 Clientes

EJIE da servicio a múltiples clientes dentro del Sector Público Vasco, por lo que el Plan deberá tener en cuenta no sólo un ámbito y requisitos generales de seguridad, sino también las especificidades de los diferentes clientes. Los ámbitos principales a tener en cuenta son:

- Gobierno Autonómico
- Sanidad
- Justicia
- Seguridad
- Infraestructuras Ferroviarias
- Sector Primario
- Medios audiovisuales
- …

3.2 Normativa y Referencias

Como se ha comentado en el apartado anterior, EJIE da servicio a entidades públicas que, por definición, deben cumplir diferentes normativas. Como referencia, sin que esto signifique que haya que hacer un plan para cumplir todas, las normativas que aplican a EJIE en diferentes niveles son las siguientes:

- Protección de datos personales:
  - REGLAMENTO (UE) 2016/679
  - LO 3/2018, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Infraestructuras Críticas:
  - Ley 8/2011
  - RD 704/2011
- Protección de las redes y sistemas de información:
  - Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información
  - Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

  - Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).
- Administración, identificación y firma electrónicas:
  - Esquema Nacional de Seguridad (RD 311/2022)

Entre todas las normativas referidas, la prioritaria en estos momentos que deben cumplir todas las entidades a las que EJIE da servicio es el ENS en diferentes niveles, por lo que EJIE debe ser capaz de ofrecer servicios al máximo nivel, es decir, ENS nivel ALTO.

Adicionalmente, se requiere que se tengan en cuenta estándares internacionales a la hora de tomar referencias para la elaboración del Plan (NIST, por ejemplo).

3.3 Iniciativas

Se requiere que el plan resultante no sea simplemente una lista de proyectos o de tipos de productos a implantar que se lleven a cabo siempre con nuevos pliegos, inversiones y contrataciones. Tampoco se quiere que sea una revisión contra una norma de las citadas en el apartado anterior y una lista simple de incumplimientos a solucionar.

El objetivo es disponer de un plan que determine la Estrategia global en materia de CiberSeguridad en los próximos tres años. Dicha estrategia se reflejará en una serie de iniciativas de alto nivel que se pretende que sean de diferentes tipos:

- Mejoras/Evolución en Servicios de Seguridad existentes
- Nuevos Servicios de Seguridad
- Otro tipo de iniciativas en el ámbito de la ciberseguridad

4 Alcance y Requisitos de los servicios del contrato

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

4.1 Servicios de Elaboración del Plan de Evolución de Ciberseguridad

La empresa adjudicataria deberá considerar, como servicio principal a prestar, la elaboración de un Plan de Evolución de Ciberseguridad que responda a los requisitos detallados en apartados previos.

Este servicio incluirá todos los trabajos que se consideren necesarios para ello, sin que ninguno de ellos suponga un sobrecoste para EJIE sobre el contrato.

El resultado de este servicio consistirá en uno o varios entregables que detallen el Plan a diferentes niveles (ejecutivo, técnico, etc.).

4.2 Servicios de Revisión Anual de Estado del Plan de Evolución de Ciberseguridad

La empresa adjudicataria deberá considerar los servicios necesarios para realizar una revisión anual del Plan. Es decir, se realizarán 2 revisiones a lo largo de los 3 años de duración del Plan.

El objetivo de las revisiones es, al menos:

- Determinar el estado de cumplimiento de las iniciativas y, por lo tanto, del plan.
- Corregir o añadir iniciativas a lo largo de la vida del Plan. Esto no significa que haya que rehacer el plan cada año, pero sí que haya margen a correcciones sobre el mismo que resulten evidentemente necesarias sin tener que rehacer el Plan desde cero.

El resultado de estas revisiones consistirá en uno o varios entregables que detallen el Estado del Plan a diferentes niveles (ejecutivo, técnico, etc.)

4.3 Servicios de respuesta a consultas sobre el plan y las revisiones

La empresa adjudicataria deberá considerar los servicios necesarios responder a consultas de EJIE durante la duración del contrato relacionadas con la interpretación y aclaración del contenido de la documentación entregada.

La prestación de estos servicios será llevada a cabo por el equipo que ha participado en la preparación de los entregables con un tiempo de respuesta de 5 días laborables.

4.4 Entregables

La empresa adjudicataria deberá elaborar, como mínimo, los siguientes entregables:

Entregable	Descripción	Objetivo	Resultado de la ejecución de
1	Plan Evolución Ciberseguridad	Determinar la estrategia y el camino a seguir en materia de Ciberseguridad en los próximos 3 años	Servicios de Elaboración del plan de evolución
2	Plan Evolución Ciberseguridad (primera revisión)	Evaluar el progreso y adaptar el plan a posibles nuevas circunstancias	Servicios de la primera Revisión Anual de Estado del Plan de Evolución de Ciberseguridad
3	Plan Evolución Ciberseguridad (segunda revisión)	Evaluar el progreso y adaptar el plan a posibles nuevas circunstancias	Servicios de la segunda Revisión Anual de Estado del Plan de Evolución de Ciberseguridad

Se entiende por entregable el documento (o conjunto de documentos) que permitan a EJIE disponer de toda la información necesaria relativa a la estrategia a seguir en materia de ciberseguridad, así como a su seguimiento y evolución.

4.5 Requisitos asociados a los servicios

4.5.1 Plazos Parciales de Ejecución

Servicios de Elaboración del Plan de Evolución de Ciberseguridad: El plazo de ejecución de estos servicios será, como máximo, de 3 meses a ejecutar a partir del inicio del contrato.

Servicios de Revisión Anual del Estado del Plan de Evolución de Ciberseguridad: El plazo para la ejecución de cada una de estas revisiones será de 2 meses. Las revisiones se ejecutarán, respectivamente, 12 meses y 24 meses después de la elaboración del Plan.

Servicios de respuesta a consultas sobre el plan y sus revisiones anuales: durante toda la duración del contrato.

4.5.2 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 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.

4.5.3 Metodología

La empresa adjudicataria deberá presentar el conjunto de técnicas, herramientas y procedimientos para llevar a cabo todas las actividades planteadas en este expediente y cumplir los objetivos marcados por EJIE.

En la propuesta de metodología se deberá tener en cuenta el contexto en el que se desarrollarán los trabajos (Sector Público) y plantear qué datos prevé extraer y contrastar a partir de dicho contexto para conseguir la máxima adaptación a las necesidades de EJIE.

4.5.4 Coordinación con Terceros y Horarios de Actividad.

La empresa adjudicataria deberá considerar la necesidad de coordinación con EJIE para la ejecución de las tareas necesarias para la ejecución de los trabajos.

En general, las tareas a realizar en colaboración con EJIE (reuniones, etc.) se realizarán en el horario laboral de EJIE y siempre teniendo en cuenta las agendas del personal que tenga que participar en los diferentes trabajos.

4.5.5 Seguimiento y Control de Ejecución del Proyecto

4.5.5.1 Seguimiento por parte de EJIE

EJIE 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, 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.
- Validación de la documentación entregada, para poder establecer el cierre de las diferentes fases del proyecto.

4.5.5.2 Seguimiento por Parte del Adjudicatario

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

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

El Jefe/a de Proyecto se responsabilizará de las siguientes tareas principales:

- Realizará la coordinación y seguimiento continuo de la evolución de los trabajos.
- 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.

- Podrá tener, a consideración de EJIE, interlocución directa con otros involucrados del proyecto por parte de EJIE como son los grupos de soporte.
- Realizará reportes de avance de proyecto.
- Definirá metodologías para identificación y control de riesgos y definición de propuestas de mitigación de estos.
- Asistirá, junto con los técnicos que se estime conveniente, a las reuniones de seguimiento y técnicas que se convoquen, 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.

4.5.5.3 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 Jefe/a o Director/a de Proyecto que deberá contar con disponibilidad para atender sin demora los requerimientos de los responsables designados por EJIE. El 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 Delegado será el único interlocutor principal con la Dirección del Proyecto de EJIE. Dispondrá de teléfono móvil, para facilitar su localización, y correo electrónico.

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

Asimismo, en el inicio del proyecto, el adjudicatario deberá exponer la relación detallada del equipo de trabajo propuesto y dedicaciones. EJIE podrá solicitar cambios sobre los recursos propuestos en caso de que, tras el análisis de la propuesta, 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. Si a criterio de la Dirección del Proyecto de EJIE, esto no fuera posible, las dos primeras semanas de trabajo del sustituto/s no serán facturables corriendo a cargo del adjudicatario.

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

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

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

A continuación, se especifican los roles mínimos identificados a los que deberá dar respuesta 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.
- **Equipo de consultoría de Ciberseguridad**, que será el equipo técnico encargado del análisis de los diferentes aspectos necesarios para la elaboración del Plan, así como los encargados de la elaboración del mismo y de las revisiones posteriores, y con los conocimientos y capacidades solicitados en el PCP.

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.

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 establecidos.

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 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.