PLIEGO DE PRESCRIPCIONES TÉCNICAS

Contratación de un servicio de apoyo, seguimiento, control y realización de las iniciativas en materia de ciberseguridad de Osakidetza

NÚMERO DE EXPEDIENTE: 2025/01550

INDICE

1. OBJETO DEL CONTRATO 3
2. ÁMBITO Y ALCANCE DEL CONTRATO 8
3. LOTES 13
4. REQUISITOS NORMATIVOS Y ETIQUETAS O CERTIFICACIONES GENERALES 13
5. REQUISITOS NORMATIVOS Y ETIQUETAS O CERTIFICACIONES POR LOTES 13
6. REQUISITOS TÉCNICOS GENERALES 13
7. REQUISITOS TÉCNICOS POR LOTES 14
8. VARIANTES TÉCNICAS 14
9. MUESTRAS / PRESENTACIÓN DE PRODUCTO / VISITA DE OBRA 14
10. LUGAR Y PLAZOS DE ENTREGA / PLAN DE PUESTA DE MARCHA 15
11. MODELO DE GESTIÓN 18
12. EJECUCIÓN / FACULTAD DE INSPECCIÓN / PLAN DE TRABAJO / PROGRAMA DE TRABAJO 22
13. PROPIEDAD DE LOS PRODUCTOS ENTREGADOS 23
14. CONFIDENCIALIDAD 23
15. CONSULTAS AL PLIEGO 24

1. OBJETO DEL CONTRATO

Osakidetza tiene que hacer frente a los crecientes retos producidos por las amenazas en materia de ciberseguridad. En este contexto, Osakidetza cuenta con el apoyo de una oficina técnica de gestión de Ciberseguridad como apoyo a las necesidades en esta área.

Siendo el objeto del contrato:

> **Oficina técnica de Ciberseguridad (PMO Ciberseguridad):** Contratación de un servicio de apoyo, seguimiento, control y realización de las iniciativas en materia de ciberseguridad de Osakidetza.

Como objetivos generales, el servicio deberá conseguir:

- Actualización en materia de alineamiento estratégico (como son el plan director de ciberseguridad y la organización de la ciberseguridad de Osakidetza).
- Seguimiento de las iniciativas y proyectos de ciberseguridad.
- Realización de cuadros de mando, informes e indicadores.
- Cumplimiento de la legislación aplicable a Osakidetza.
- Soporte a incidentes de ciberseguridad.

Este servicio proporcionará y hará uso de las herramientas, documentación y mecanismos necesarios para una correcta gestión del mismo.

El adjudicatario realizará los servicios requeridos en colaboración con el personal de Osakidetza y con personal externo asignado a los proyectos que Osakidetza determine.

1.1. Justificación de necesidad e idoneidad del contrato

Los retos a los que se enfrenta el sector sanitario en la actualidad son entre otros: el incremento de la atención sanitaria que se debe al envejecimiento de la población o al aumento de enfermos crónicos, las crecientes expectativas y exigencias de los pacientes, cada vez más y mejor formados e informados, o la incorporación de nuevas tecnologías sanitarias en algunos casos muy costosas o dependientes de tecnologías antiguas. Todo esto hace que sean muy relevantes las tecnologías de la información, el equipamiento sanitario y la interoperabilidad del dato, ya que mejoran el cuidado de los enfermos crónicos, optimizan el tiempo y los recursos, almacenan datos de pacientes y facilitan la información de los profesionales para poder ofrecer mejores diagnósticos y soluciones.

Debido al contexto en el que se encuentra el sector, hacen que la ciberseguridad cobre un papel relevante y en constante crecimiento. Cualquier pérdida de información relativa a datos de salud puede acarrear grandes pérdidas económicas y reputacionales para la organización. Asimismo, un incidente de ciberseguridad también podría suponer la pérdida temporal o permanente de servicios esenciales de un hospital teniendo que recurrir a escenarios de contingencia.

En el citado contexto cabe destacar por un lado la iniciativa enmarcada en la "Estrategia de Salud Digital" del Ministerio de Sanidad para avanzar en la coordinación estratégica en ciberseguridad en la que participa Osakidetza. Igualmente es importante destacar el impulso que se está dando desde la Unión Europea a la actualización de la legislación en materia de ciberseguridad con el objetivo de mejorar la capacidad de afrontar los nuevos retos en esta materia.

Con este objetivo, la Subdirección de Informática y Sistemas de Información de Osakidetza, en el marco de sus competencias, se plantea la c**ontratación de un servicio de seguimiento, control y realización de las iniciativas en materia de ciberseguridad de Osakidetza**

1.2. Justificación de insuficiencia de medios en contratos de servicios

El Decreto 106/2008, de 3 de junio, establece el compromiso institucional de Osakidetza de no proceder a la externalización ni privatización de nuevas áreas o servicios. No obstante, dicho compromiso contempla expresamente la **posibilidad de excepciones** en aquellos casos en los que concurran **circunstancias excepcionales**, en cuyo caso se priorizará, siempre que sea posible, la asunción directa del área o servicio por parte del propio Ente Público, sin perjuicio de que, en última instancia, se valore la viabilidad de otras fórmulas de gestión conforme al marco legal vigente.

En coherencia con este principio, **Osakidetza únicamente recurre a la contratación externa cuando resulta estrictamente imprescindible**, garantizando en todo momento el cumplimiento del marco normativo y priorizando la eficiencia en la gestión de los recursos públicos. Esta práctica no responde a una estrategia de externalización sistemática, sino a una **necesidad puntual y justificada** por limitaciones estructurales que impiden la asunción directa de determinadas tareas, garantizando así la sostenibilidad, eficiencia y seguridad del sistema sanitario en el nuevo entorno digital.

Es importante subrayar que esta decisión responde a una necesidad concreta derivada de limitaciones estructurales y funcionales. Desde la constitución de Osakidetza hasta el día de hoy, la función de desarrollo de sistemas de información, así como el apoyo técnico de soluciones tecnológicas y/o infraestructuras complejas ha estado externalizada y las plantillas internas dimensionadas para la gestión de dicha contratación y el aseguramiento diario del servicio a la totalidad de la red. Siendo en la actualidad la totalidad de soluciones corporativas, productos comerciales, desarrollos propios proporcionados por terceros o adquisiciones externas, debido a la limitación de recursos técnicos y organizativos necesarios para abordar internamente este tipo de iniciativas. A ello se suma el hecho de que la misión principal de Osakidetza, como ente

público sanitario, es la provisión de servicios asistenciales a la ciudadanía, no la producción de tecnología. Por ello, **en situaciones excepcionales como la presente, se recurre a servicios tecnológicos externos**, conforme a los principios de eficiencia, legalidad y buena administración.

La Subdirección de Informática no es una factoría de software, sino un órgano de coordinación y supervisión que garantiza la alineación tecnológica con los objetivos sanitarios.

Asimismo, en el contexto actual de transformación digital, el sector de la salud se enfrenta a un nuevo horizonte tecnológico caracterizado por la incorporación de soluciones avanzadas como la inteligencia artificial, la interoperabilidad de sistemas, la medicina personalizada, el análisis masivo de datos clínicos (big data), aplicaciones orientadas a movilidad y la ciberseguridad sanitaria. Este escenario exige capacidades técnicas altamente especializadas y en constante evolución.

Además, la velocidad de cambio tecnológico hace necesaria una continua evolución tanto del marco regulatorio (Reglamento de protección de datos, Esquema Nacional de Seguridad, Espacio Europeo de datos Sanitarios, ...) como de los estándares de interoperabilidad, haciendo inviable la asunción de estas tareas con medios propios. La especialización requerida, junto con la necesidad de actualización constante, supera las capacidades estructurales disponibles.

En este caso y desde el punto de vista técnico, la estrategia de Osakidetza es optar, siempre que sea posible, por los productos comerciales y soluciones de terceros debido a las ventajas que ofrecen:

- Acceso a tecnologías consolidadas y específicas del sector sanitario, desarrolladas por proveedores con experiencia contrastada.
- Reducción de plazos de implementación, evitando los tiempos prolongados del desarrollo interno.
- Actualización tecnológica continua, garantizada por proveedores especializados.
- Escalabilidad y flexibilidad, permitiendo adaptarse a nuevas necesidades sin comprometer la estructura interna.

Esta decisión puntual se enmarca en una evaluación estratégica orientada a la eficiencia y sostenibilidad del sistema, sin que ello implique una modificación del modelo de gestión ni una renuncia al compromiso institucional de no externalización.

Además, permite a Osakidetza:

- Concentrar sus recursos en la provisión de asistencia sanitaria.
- Establecer relaciones contractuales con proveedores líderes en tecnología sanitaria.

- Garantizar la sostenibilidad económica del sistema sanitario vasco mediante una gestión eficiente del gasto tecnológico.

Por otra parte, el artículo 26 de la **Ley 8/1997, de 26 de junio, de Ordenación Sanitaria de Euskadi**, en su apartado 3, determina el número de efectivos de la plantilla de Osakidetza. Textualmente dice: "A los efectos de esta ley, las plantillas de personal del ente público Osakidetza - Servicio Vasco de Salud, que serán aprobadas por su consejo de administración, constituyen el número de efectivos de carácter estructural con que cuentan tanto su organización central de administración como las organizaciones de servicios sanitarios dependientes del mismo. Dichas plantillas deberán ajustarse al número máximo de efectivos, según grupos profesionales, que anualmente aprobará el Consejo de Gobierno a propuesta del Departamento de Sanidad". **De esto se desprende que la facultad de contratar personal no recae de manera discrecional en la Subdirección de Informática y Sistemas de Información, sino que está sujeta a los procedimientos normativos y a la autorización de los órganos competentes.**

Osakidetza se centra en su misión principal: la provisión de servicios sanitarios. El desarrollo, soporte técnico y evolución de soluciones tecnológicas complejas requiere una inversión considerable en recursos humanos, medios tecnológicos y organizativos, así como una estructura interna capaz de asumir tareas complejas de diseño, programación, mantenimiento y evolución tecnológica. Osakidetza hace uso de su capacidad de autoorganización, optando por destinar mayor número de efectivos a la atención y mejora de la asistencia sanitaria proporcionada a la ciudadanía.

El principal valor añadido que aportan los efectivos propios de Osakidetza radica en su profundo conocimiento del negocio y de la estructura organizativa, orientado a garantizar la adecuada prestación del servicio sanitario a la ciudadanía. Este conocimiento, de carácter estratégico y operativo, se materializa en el ejercicio de funciones de gestión, supervisión y coordinación de los distintos equipos de trabajo implicados en el desarrollo y asistencia técnica de los recursos tecnológicos asignados. Así, los efectivos de Osakidetza serán responsables de la gestión estratégica del proyecto, traduciendo las necesidades del negocio al proveedor tecnológico, asegurando el cumplimiento de los objetivos.

Esta licitación responde a la necesidad de reforzar la ciberseguridad operativa en el entorno sanitario, garantizando la protección de los servicios públicos y la adopción de medidas seguras y resilientes. En este contexto, destaca la participación de Osakidetza en la "Estrategia de Salud Digital" impulsada por el Ministerio de Sanidad, orientada a fortalecer la coordinación estratégica en materia de ciberseguridad. Asimismo, resulta relevante el marco normativo europeo, que está siendo objeto de revisión y actualización con el fin de mejorar la capacidad de respuesta ante los nuevos desafíos digitales. En este escenario excepcional, las tareas objeto del contrato se centran en el apoyo técnico y el asesoramiento especializado en soluciones tecnológicas avanzadas de ciberseguridad, cuya complejidad requiere complementar las funciones actualmente desempeñadas por el personal técnico de Osakidetza.

Esta circunstancia singular justifica, de manera puntual y extraordinaria, la necesidad de recurrir a la contratación externa, sin que ello suponga una vulneración del compromiso institucional ni de los acuerdos de negociación colectiva.

El ecosistema digital de Osakidetza está compuesto por más de 31.200 equipos informáticos de usuario final, 14.300 impresoras, 4.300 tablets, 33.000 servidores, 5.200 dispositivos móviles corporativos y más de 300 sistemas de información. Esta infraestructura, por su magnitud y complejidad, representa una superficie de exposición significativa frente a amenazas cibernéticas. Ante este escenario, el personal técnico de Osakidetza requiere refuerzo especializado para la implementación de medidas avanzadas de ciberseguridad, incluyendo protección proactiva, monitorización continua y respuesta eficaz ante incidentes en entornos digitales altamente distribuidos.

La contratación de un servicio técnico especializado permitirá conformar un equipo multidisciplinar que integre tanto recursos propios de Osakidetza como colaboradores externos, aportando por parte de los profesionales internos un conocimiento profundo del entorno organizativo, asistencial y tecnológico del sistema sanitario. Esta combinación garantiza una capacidad operativa eficaz, alineada con los objetivos estratégicos institucionales, y facilita una supervisión pública directa sobre la ejecución de las tareas en materia de ciberseguridad. La colaboración con proveedores especializados se plantea como un complemento técnico bajo dirección y control público, asegurando la calidad, trazabilidad, seguridad y sostenibilidad de las soluciones implementadas. En definitiva, esta actuación responde a una necesidad puntual y extraordinaria, derivada de limitaciones estructurales y funcionales. Osakidetza mantiene su compromiso con la gestión pública directa, centrando sus recursos en su misión principal: la mejora continua de la atención sanitaria a la ciudadanía.

Por último, citar que por todo lo anterior y a la vista de la criticidad e impacto tanto interno como hacia la ciudadanía de las necesidades de la organización, se entiende que queda claramente explicitada la necesidad de disponer de un proveedor especializado en las líneas de negocio requeridas, al disponer éste de la capacidad para proveer un equipo multidisciplinar disponible y capaz de gestionar las necesidades que vayan surgiendo a lo largo de la duración del contrato.

Por ello se concluye:

- Que, dada la complejidad y el nivel de especialización requerida, se hace necesario complementar con medios externos para asumir los trabajos objeto de este expediente de contratación.

- Que la gestión y coordinación del proyecto/servicio la realizarán efectivos de la Subdirección de Informática de la Dirección General de Osakidetza, que alineados con el área usuaria y con amplio conocimiento del negocio interno,

garantizarán el cumplimiento de los requisitos, traduciendo las necesidades del negocio al proveedor de tecnología.

- Que la contratación propuesta se ajusta a la Instrucción sobre Buenas Prácticas en la Contratación del Gobierno Vasco, y responde a criterios de racionalidad económica, eficiencia organizativa y sostenibilidad presupuestaria.

1.3. Procedimiento de adjudicación

Tal y como se menciona en Memoria Justificativa, el procedimiento seleccionado es el procedimiento **ABIERTO.**

2. ÁMBITO Y ALCANCE DEL CONTRATO

2.1. Organizaciones implicadas o lugar de prestación y/o ejecución

Los servicios solicitados se prestarán para toda la red de Osakidetza.

Los servicios solicitados se prestarán, principalmente, en las instalaciones del adjudicatario, aunque también se podrán prestar en las organizaciones de Osakidetza.

2.2. Alcance del contrato

El ámbito de ciberseguridad donde la PMO ciberseguridad prestará el servicio, es el que afecta a la seguridad de los sistemas de información (SSII). Por tanto, los ámbitos de actuación son todos los **relativos a los SSII**.

- Seguridad en la infraestructura.
  - Red.
  - Telefonía IP y Comunicaciones Unificadas.
  - Equipos en movilidad.
  - Almacenamiento.
  - Servidores.
  - Equipamiento de microinformática.
  - Dispositivos de electromedicina (IoMT/IoT).
  - Integración de la Ciberseguridad en la Gestión del Ciclo de Vida de los Datos.
  - …
- Seguridad de identidad de los profesionales.

- Seguridad en las aplicaciones.
- Otros.

No incluye el ámbito seguridad de la información y protección de datos. En todo caso, será necesario establecer una coordinación con el área normativa para tener una gestión global de seguridad.

Los **servicios objeto del presente contrato** se detallan a continuación.

- Alineamiento estratégico, como son el plan director de ciberseguridad y la organización de la ciberseguridad de Osakidetza.
- Seguimiento de iniciativas y proyectos de ciberseguridad.
- Establecimiento de cuadros de mando, informes e indicadores.
- Cumplimiento de la legislación aplicable a Osakidetza.
- Soporte a incidentes de ciberseguridad

2.2.1. Alineamiento estratégico

Alineamiento estratégico, como pueden ser el plan director de ciberseguridad y la organización de la ciberseguridad de Osakidetza.

En coordinación con los responsables de Osakidetza, la PMO ciberseguridad deberá actualizar la estrategia de ciberseguridad.

2.2.2. Seguimiento de iniciativas y proyectos de ciberseguridad

Servicio de apoyo técnico en la realización de iniciativas y proyectos de ciberseguridad, para asegurar el cumplimiento de los parámetros de calidad establecidos por Osakidetza (tiempo, plazo, …). Deberá utilizar las herramientas corporativas de Osakidetza para su realización.

El origen de las iniciativas y proyectos será tanto los identificados por Osakidetza, los propuestos por los grupos de soporte de los proveedores y aprobados por Osakidetza y los identificados por la PMO ciberseguridad dentro de cualquier ámbito del objeto del presente PBT.

Las áreas de trabajo serán:

- Tecnológicas, tal y como se indica en el presente PBT (arquitectura técnica, aplicaciones, gestión de identidad, evaluar herramientas de ciberseguridad, coordinación de campañas de phishing, ejercicios de pentesting, etc.). Incluirán soluciones corporativas, soluciones de OSIs y centros, equipamiento IoT/IoMT, etc.
- Organizativas.
- Otros ámbitos de ciberseguridad que Osakidetza y la PMO ciberseguridad puedan estimar oportuno.

Las iniciativas tecnológicas y proyectos tecnológicos serán realizadas por los proveedores de Osakidetza en una gran parte, siendo en este caso la labor de PMO ciberseguridad la de asesoramiento, gestión y seguimiento. En menor medida, la PMO ciberseguridad realizará los proyectos tecnológicos e iniciativas tecnológicas directamente realizando además la ejecución de las mismas.

La PMO Ciberseguridad realizará como mínimo, las siguientes funciones:

Asesoramiento

- Soporte a la toma de decisión sobre los proyectos e iniciativas planteados.

Gestión

- Consolidar las diferentes iniciativas y proyectos en el área, de forma que permita a Osakidetza la correcta gestión de las mismas.
- Recopilar y mantener la información de los proyectos (dependencias, riesgos, retrasos, …) e iniciativas, en coordinación con Osakidetza y con los proveedores que realizan los proyectos.
- Gestión de capacidad.
- Gestión de costes.
- Informes y cuadros de mando.

Seguimiento

- Realizar reuniones de seguimiento (establecer fechas, agenda a tratar, actas, …).
- Realizar informes de progreso de iniciativas y proyectos.
- Certificaciones de progreso, de aceptación, etc.
- Realizar seguimiento de las tareas coordinando a proveedores, profesionales de Osakidetza, etc.
- Cualquier tarea asociada a la gestión de proyecto y de iniciativas que requiera Osakidetza.

Ejecución

En los casos en los que la PMO ciberseguridad realice directamente el proyecto/iniciativa, deberá realizar las tareas y será gestionado con los mismos parámetros que se establecen para el resto de los proveedores, descritos en este punto del presente PBT.

- Proyectos e iniciativas identificados y en ejecución,
- Proyectos e iniciativas cíclicas
- Proyectos e iniciativas continuas, bajo demanda
- Atención 24x7 de iniciativas y proyectos

2.2.3. Establecimiento de cuadros de mando, informes e indicadores

La PMO de ciberseguridad tendrá entre sus tareas, sobre cualquier ámbito de ciberseguridad en Osakidetza contemplado en el objeto del presente PBT, tomando como punto de partida los cuadros de mando, informes e indicadores existentes, la realización periódica y la realización bajo de demanda de:

- Indicadores
- Informes
- Cuadro de mando

La consecución de este apartado está orientada al soporte a la toma de decisión por parte de Osakidetza.

2.2.4. Concienciación en materia de ciberseguridad

La PMO de ciberseguridad tendrá entre sus tareas, la elaboración de campañas de formación y sensibilización a los profesionales de Osakidetza.

Se realizarán las tareas de:

- Análisis de las necesidades en esta materia.
- Elaboración de soportes (presentaciones, videos demostrativos, …).
- Realización de la propia acción de sensibilización y/o formación, llevando a cabo la tarea de presentador, tanto en directo como grabando videos para su posterior consumo. Será necesario poder utilizar la imagen personal de los componentes de la PMO de ciberseguridad para estas tareas.
- Coordinación con las áreas de Osakidetza para realizar las campañas de formación y sensibilización (Formación, Comunicación, …).

2.2.5. Cumplimiento

Osakidetza, como Ente Público Osakidetza-Servicio vasco de salud tiene como objeto o finalidad la provisión de servicios sanitarios a través de las organizaciones públicas de servicios sanitarios dependientes del mismo. Por este motivo, Osakidetza está obligada a diferentes cumplimientos normativos a los que hay que dar respuesta. En este apartado, Osakidetza solicita asesoría y soporte al cumplimiento en diferentes ámbitos.

Las posibles iniciativas y proyectos surgidos en este apartado, una vez evaluados y aprobados por Osakidetza, pasarán a gestionarse según el punto “2.2.2 Seguimiento de iniciativas y proyectos de ciberseguridad“ del presente PBT.

2.2.5.1. Ley 8/2011 de Infraestructuras críticas

La PMO de ciberseguridad realizará las tareas:

- Revisión de la consideración legal de Osakidetza en relación a la Ley 8/2011 y leyes posteriores que la sustituyan y/o la complementen.
- Revisión de las obligaciones como consecuencia de la consideración legal de Osakidetza.
- Identificación, desarrollo y seguimiento de la puesta en ejecución de las medidas que sea necesario implementar.

2.2.5.2. Revisión de requisitos legales y normativos

La PMO ciberseguridad se encargará de identificar todos aquellos requisitos legales y normativos que, en el ámbito de la ciberseguridad y dentro del objeto descrito en el presente PBT, apliquen a la actividad de Osakidetza. Se analizará la legislación en vigor y la normativa existente en todos ámbitos de la ciberseguridad aplicables a Osakidetza.

Se mantendrá actualizado el informe existente con los requisitos identificados junto a los controles para su cumplimiento e indicadores asociados.

Se prestará especial atención a la actualización que la Unión Europea está realizando en materia de legislación (como la Directiva NIS2).

Asesorará a Osakidetza en la relación de las medidas identificadas.

Se analizará el impacto en Osakidetza y deberán comunicar las medidas a implantar lograr el cumplimiento legal. Se establecerán los controles necesarios para tal cumplimiento, así como sus indicadores de medida.

La tarea de revisión normativo será una labor a realizar de forma continua y permanente, identificando constantemente nuevas necesidades. En todo caso, será necesario establecer las canales de coordinación adecuados y de forma permanente, con el área normativa para tener una gestión global de seguridad.

2.2.6. Soporte a incidentes de ciberseguridad

Los incidentes de ciberseguridad que puedan ocurrir serán gestionados por los proveedores que Osakidetza tiene contratado a estos efectos.

La PMO ciberseguridad deberá:

- Revisar el circuito interno de gestión de incidentes de ciberseguridad y el procedimiento de notificación de brechas (según legislación aplicable) a las autoridades.
- Asesorar y dar soporte a Osakidetza en la interlocución y coordinación cuando ocurra un incidente de ciberseguridad. En caso de un incidente de alto impacto y/o criticidad, será posible que sea necesario una atención 24x7 para lo cual se prestará el servicio tal y como se indica en el apartado “Soporte 24x7 “ del presente PBT.
- Propuestas de mejora en la gestión de los incidentes de ciberseguridad.

3. LOTES

3.1. Lotes: Objeto / Descripción / Códigos.

No hay, un lote

4. REQUISITOS NORMATIVOS Y ETIQUETAS O CERTIFICACIONES GENERALES

Serán referencias metodológicas válidas a la hora de la construcción, presentación y defensa de modelos y propuestas por parte de los ofertantes, las siguientes:

- ITIL (Information Technology Infrastructure Library).
- ISO 27000 (Information Security Management Systems - ISMS).
- ISO 80001 Application of risk management for IT-networks incorporating medical devices.
- ISO 27000 Information technology — Security techniques — Information security management systems.
- ISO 27799 Health informatics — Information security management in health using ISO/IEC 27002.
- ISO 27017 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
- IEC 62304 Medical device software — Software life cycle processes.

La no mención expresa de la totalidad de normativas que sean de aplicación no exime a la empresa adjudicataria de su cumplimiento.

5. REQUISITOS NORMATIVOS Y ETIQUETAS O CERTIFICACIONES POR LOTES

5.1. Requisitos normativos por lote

No hay

6. REQUISITOS TÉCNICOS GENERALES

6.1. Requisitos técnicos generales aplicables a todos los lotes

La plataforma tecnológica utilizada será la de **Osakidetza.** Así se debe contemplar al menos las siguientes herramientas.

6.1.1. Plataforma de gestión de conocimiento y colaboración

La PMO ciberseguridad utilizará las herramientas corporativas ***Microsoft SharePoint y Microsoft Teams*** que Osakidetza tiene implantados en su tenant

propio como repositorio de toda la información generada y como herramienta de colaboración y gobierno de servicio.

6.1.2. Herramienta de gestión del servicio

Osakidetza dispone de la herramienta corporativa **Service Manager** para la operación TIC. La oficina PMO ciberseguridad deberá hacer uso de la herramienta y deberá interactuar mediante tickets, con los grupos técnicos de soporte, proveedores, profesionales de Osakidetza, etc.

6.1.3. Otras herramientas

La PMO ciberseguridad podrá proponer, a iniciativa propia, el uso de otras herramientas con el objetivo de mejorar el servicio.

7. REQUISITOS TÉCNICOS POR LOTES

7.1. Requisitos técnicos excluyentes por lote

Si.

7.2. Requisitos técnicos no excluyentes por lote

No hay.

7.3. Número máximo de lotes a los que licitar

No hay

7.4. Número máximo de adjudicatarios por lotes

No hay

8. VARIANTES TÉCNICAS

No procede.

9. MUESTRAS / PRESENTACIÓN DE PRODUCTO / VISITA DE OBRA

9.1. Muestras

- **Forma de presentación**

No procede

- **Normas para la identificación de las muestras**

  No procede

- **Presentación de las muestras (unidades y destinos)**

  No procede

- **Presentación de producto:**

  No procede.

- **Visita de obra**

  No procede.

10. LUGAR Y PLAZOS DE ENTREGA / PLAN DE PUESTA DE MARCHA

10.1. Ubicación de la prestación del servicio

Sin perjuicio de lo que expresan los siguientes párrafos, **Osakidetza** se reserva el derecho de modificar la política en cuanto a ubicaciones del equipo durante el transcurso del contrato, sin que ello suponga un coste adicional para **Osakidetza**.

Inicialmente los trabajos se realizarán en las instalaciones del adjudicatario.

Es imprescindible que cuando el servicio se proporcione desde las instalaciones del adjudicatario, se cumplan las medidas especificadas sobre seguridad física y de accesos establecidas por Osakidetza para este tipo de servicios.

Se solicitará por parte de la empresa que configure un entorno de trabajo para la realización del trabajo de manera remota, los costes de conexión, infraestructura (hardware y software) que fuesen necesarios, correrán por cuenta del suministrador. Se deberá garantizar la **conectividad bidireccional** desde el proveedor a **Osakidetza**, y viceversa, entre los entornos de ambas organizaciones para facilitar la ejecución d elos trabajos.

El adjudicatario contemplará la necesidad de realizar las tareas asignadas a la PMO ciberseguridad desde las oficinas de Osakidetza en la DG en Vitoria. Esta necesidad se estima en 1 jornada cada trimestre, para la PMO ciberseguridad completa o para parte de la misma. El coste asociado no debe repercutirse a Osakidetza. Puntualmente, se podrá solicitar presencia in situ en alguna de las sedes o edificios (alcance geográfico de País Vasco). El coste asociado no debe repercutirse a Osakidetza

En el caso de factorías de software, el suministrador deberá garantizar la calidad, eficiencia y ahorro en la prestación del servicio. Los niveles de calidad en este formato de prestación deberán ser equivalentes a los de trabajo presencial.

En el caso de factorías de software se exige al suministrador una serie de condiciones para que puedan ser aceptables:

- ✓ Titularidad del Servicio: El suministrador no podrá subcontratar a un tercero la prestación de este tipo de servicios.
- ✓ La factoría deberá de estar ubicada en territorio de la Unión Europea.
- ✓ Infraestructura: **Osakidetza** deberá conocer y aceptar expresamente las medidas de seguridad, equipamiento y comunicaciones de las instalaciones del suministrador desde las que se preste este servicio.
- ✓ La instalación y adecuación de los locales será totalmente por cuenta del suministrador.

10.2. Plazos de entrega

El soporte del servicio, contemplando todas sus fases, se estima de un año contado a partir de la fecha de adjudicación del contrato.

10.3. Plan de Puesta en Marcha

La ejecución del servicio se ajustará a las siguientes fases.

Fase inicial

Osakidetza dispone en la actualidad de una oficina técnica de proyectos en materia de ciberseguridad. El adjudicatario deberá recibir del proveedor saliente toda la información relativa al servicio prestado, que será revisada para establecer el plan de transición:

- La metodología y estrategia de inicio.
- Los recursos (del licitador u otras organizaciones) necesarios para ejecutarlo, responsabilidades y dedicación.
- Los recursos del licitador tendrán la valoración en horas, a modo orientativo que tiene que contemplar en cada objetivo, incluyendo el de los recursos bajo demanda:
  - Alineamiento estratégico.
  - Seguimiento de iniciativas y proyectos de ciberseguridad.
  - Cuadros de mando, informes e indicadores.
  - Cumplimiento de la legislación aplicable a Osakidetza.
  - Soporte a incidentes de ciberseguridad.
- El calendario de hitos propuesto.
- Los entregables del plan.
- Los comités de seguimiento.

En la valoración de las propuestas se tendrá en cuenta el plan inicial, la identificación de riesgos y los mecanismos de mitigación de riesgos que el licitador

establezca para minimizar posibles afecciones de dicho plan en la calidad del servicio.

Fase de prestación normal del servicio

Esta fase se caracteriza por la prestación normal del Servicio según lo requerido en el presente pliego, tanto a nivel operativo como de gobierno.

En el transcurso de la ejecución del contrato aparecerán necesidades dentro del ámbito general del servicio, que requerirán la participación de recursos bajo demanda del licitador. Dichas necesidades de participación serán comunicadas a **Osakidetza** por parte del responsable del servicio, adjuntando la correspondiente valoración de esfuerzo y perfil propuesto y que será contrastado y aprobado en los órganos de gobierno del servicio. La intervención de los técnicos expertos se realizará de la siguiente forma:

- El coordinador de la PMO ciberseguridad indicará al responsable del servicio de Osakidetza la necesidad. La asociará a la iniciativa/proyecto correspondiente y la cuantificará en horas.
- El responsable de servicio de Osakidetza aprobará, solicitará alguna corrección o denegará la propuesta.
- En caso afirmativo, se añadirá al informe de servicio. Se tratará en el comité de seguimiento correspondiente.
- El coordinador de la oficina PMO ciberseguridad comunicará al responsable de servicio de Osakidetza cualquier desviación en la estimación inicial.

Fase de finalización

La fase de devolución del Servicio transcurrirá durante las semanas previas a la finalización del contrato.

El Plan de finalización del servicio puede ejecutarse bajo dos situaciones, entregando el servicio a un nuevo adjudicatario o entregando el servicio a la propia **Osakidetza**. Ambas casuísticas deben contemplarse en esta fase.

En el primer caso, durante este periodo el licitador actual colaborará con el adjudicatario entrante en todas aquellas tareas y responsabilidades para traspasarle el Servicio (conocimiento, documentación, etc.), de acuerdo con el plan de devolución acordado con **Osakidetza**. En concreto el licitador deberá, entre otras:

- Traspasar al nuevo adjudicatario entrante u **Osakidetza** todo el conocimiento asociado con el Servicio de cara a garantizar la prestación futura del servicio:
  - Todos los datos que obren en su poder relativos a la prestación de los Servicios.
  - Cualquier otra información requerida por el Cliente relacionado con los Servicios.

El plazo máximo de ejecución de esta fase será de 1 mes, y los servicios imputarán a la Facturación Base**.** Cualquier modificación a este respecto deberá ser justificada por el proveedor y aprobada por **Osakidetza**.

11. MODELO DE GESTIÓN

11.1. Equipo organizativo

Para la gestión y el desarrollo del servicio, los licitadores deberán detallar lo siguiente aspectos en su propuesta:

- Organigrama del equipo de trabajo, identificando responsables y funciones a desarrollar según considere para la ejecución del servicio de este pliego.
- Detalle del equipo total de trabajo, que los licitadores consideren necesario, identificando la categoría, horas/categoría ofertada y funciones a desarrollar, para la ejecución de las tareas previstas con el alcance definido en este pliego.

El equipo de trabajo **deberá incluir al menos** los siguientes recursos con las horas dedicadas minimas indicadas:

- **Jefe PMO ciberseguridad**
- **Consultor especialista de PMO ciberseguridad**
- **Técnico senior PMO ciberseguridad**
- **Otros Expertos**

Jefe PMO	Consultor Especialista PMO	Técnico senior PMO	Otros Expertos PMO	TOTAL horas (equipo mínimo)
80	1.700	1.550	100	3.430

En la composición del equipo de trabajo se deberán ofertar los perfiles indicados en la tabla anterior y no otros.

Se valorará la inclusión en el equipo de trabajo, de profesionales que acrediten a nivel individual alguna de las siguientes especializaciones:

- Certificaciones gestión proyectos (ITIL)
- CISM-Certified Information security Manager
- CISA-Certified Information Security Auditor de la organización ISACA

Asimismo, deberá garantizar la gestión de un equipo variable que se adecue a las demandas de servicios que vaya solicitando **Osakidetza** en función de las necesidades de cada momento.

El equipo de trabajo propuesto estará formado por personal técnico con categoría profesional y nivel de especialización adecuados a las necesidades planteadas en cada momento, de acuerdo con las actividades que se vayan desarrollando.

El licitador debe comprometerse, en caso de ser adjudicatario, a mantener el equipo, según lo establecido en su oferta, y durante el periodo fijado en cada actividad específica.

Asimismo, el suministrador deberá asegurar la disponibilidad de recursos con los conocimientos requeridos para mantener los niveles de servicio y la planificación acordados que permita hacer frente a sus posibles contingencias imprevistas en su personal.

La modificación de alguno de los componentes del equipo adscrito a la ejecución de los trabajos, sin observar el procedimiento y requisitos exigidos que se señalan a continuación, facultará a **Osakidetza** para calificar dicha modificación como una rotación no planificada. La reiteración en el número de rotaciones no planificadas (mayor o igual al 30 % del Equipo en un año) faculta a **Osakidetza** para instar a la resolución del contrato.

El equipo será configurado y dimensionado por el licitador en base a la información suministrada en el pliego, así como a su experiencia por el tipo de actividades a realizar.

Para la descripción de los recursos humanos, **el licitador deberá incluir en su oferta lo siguiente:**

- Relación nominal de profesionales (incluir solo las iniciales de primer apellido, segundo apellido y nombre, DNI sesgado), incluyendo la categoría a la que se oferta.
- Adicionalmente y como prueba efectiva de que se dispondrá del personal ofertado para la ejecución el contrato, se requiere lo siguiente:
    - En caso de que alguno de los profesionales propuesto no pertenezca a la empresa licitadora, deberá presentarse Carta de compromiso (documento original), de cada uno de estos profesionales, personalizada y firmada o cualquier otra prueba efectiva, que de forma expresa acredite los siguiente:
        - Compromiso del profesional para su incorporación inmediata al equipo de trabajo de la empresa licitadora, para este expediente, en la "Categoría Ofertada" (debe indicarse la categoría), afirmando cumplir los requisitos de titulación, experiencia y conocimientos.

11.2. Constitución inicial del equipo de trabajo

El equipo técnico a incorporar tras la formalización del contrato para la ejecución de los trabajos deberá estar formado por componentes y perfiles relacionados en la oferta adjudicataria y consecuentemente valorados.

Si tras la adjudicación se observará que el equipo de proyecto no se corresponde con el establecido en la oferta técnica y:

- Caso que el adjudicatario presente justificación escrita, detallada y suficiente, explicando el motivo que suscita el cambio, se procederá a:
  - La presentación por el adjudicatario de sustituto/s con un perfil de cualificación técnica igual o superior al de la persona que se pretende sustituir.
  - Aceptación del sustituto/s por parte del responsable del servicio de Osakidetza.
- Caso de que se demostrase que el cambio no se corresponde con causa justificada, Osakidetza se reserva el derecho no solo a la aprobación del sustituto/s sino incluso a la revisión de la adjudicación y en su caso la rescisión del pedido/contrato, si este hecho fuera elemento determinante en la mencionada adjudicación.

11.3. Modificaciones en la composición del equipo de trabajo

El personal adscrito a la ejecución del contrato no tendrá vinculación con OSAKIDETZA y dependerá única y exclusivamente del contratista, el cual asumirá la condición de empresario con todos los derechos y deberes respecto a dicho personal, con arreglo a la legislación vigente y a la que en lo sucesivo se promulgue.

La empresa adjudicataria 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 demandadas para la ejecución del contrato y poder cumplir con los hitos establecidos.

El licitador debe comprometerse, en caso de ser adjudicatario, a mantener el equipo, según lo establecido en su oferta, y durante el periodo fijado en cada actividad específica.

Asimismo, el suministrador deberá asegurar la disponibilidad de recursos con los conocimientos requeridos para mantener los niveles de servicio y la planificación acordados que permita hacer frente a sus posibles contingencias imprevistas en su personal.

La valoración de la calidad de los trabajos objeto del presente pliego corresponde a los responsables de Osakidetza, siendo potestad suya solicitar el cambio de cualquiera de los componentes del equipo de trabajo, con un preaviso de quince días, por otro de igual categoría o superior, si existen razones justificadas que lo aconsejen.

Si el adjudicatario propusiera el cambio de alguna de las personas del equipo de trabajo, se deberá solicitar por escrito con quince días naturales de antelación, y requerirá de las siguientes condiciones:

- Justificación escrita, detallada y suficiente, explicando el motivo que suscita el cambio.

- Presentación de sustituto/s con un perfil de cualificación técnica igual o superior al de la persona que se pretende sustituir.
- Aceptación del sustituto/s por parte del responsable del servicio de Osakidetza.

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 un mínimo de 15 días. Por lo tanto, si a criterio del responsable de Osakidetza, esto no fuera posible, las dos primeras semanas de trabajo del sustituto/s no serán facturables corriendo a cargo del adjudicatario.

11.4. Veracidad de los datos

Osakidetza se reserva la facultad de solicitar, en cualquier momento, antes o después de la adjudicación y durante el curso de los trabajos, de cualquier otro tipo de documento complementario, en orden a la comprobación de cuantos datos haya ofrecido la empresa adjudicataria, tanto respecto a la misma, como a los recursos de que disponga.

La falsedad en los mismos podrá, provocar la resolución del contrato en función de su gravedad, a criterio del responsable de Osakidetza.

11.5. Condicionantes del equipo de trabajo ofertado

La falsedad en el nivel de conocimientos técnicos del personal ofertado, deducida del contraste entre lo reflejado en el currículo y los conocimientos reales demostrados en la ejecución de los trabajos, y en último término, provocar la revisión de la adjudicación y en su caso la rescisión del contrato, en función de la gravedad de las consecuencias provocadas a valorar por el responsable de Osakidetza.

12. EJECUCIÓN / FACULTAD DE INSPECCIÓN / PLAN DE TRABAJO / PROGRAMA DE TRABAJO

12.1. Condiciones de ejecución

Horario

El horario de prestación de servicios será el siguiente:

- **Invierno**: del 01/01 al 30/06 y del 01/09 al 31/12.
    - De lunes a jueves de 08:00 a 17:00 horas.
    - Viernes de 08:00 a 15:00.
- **Verano**: del 01/07 al 31/08.
    - De lunes a viernes de 08:00 a 15:00 horas.

Los festivos serán los aplicables al Territorio Histórico de Álava.

Soporte 24x7

El adjudicatario deberá, tener disponibilidad para acometer actuaciones urgentes o críticas fuera del horario habitual de trabajo, planificados o no, incluyendo noches, fines de semana y festivos a petición de Osakidetza en los ámbitos:

- Asesoramiento y coordinación de incidencias críticas de ciberseguridad que afecten de forma grave al funcionamiento de cualquier servicio y que requieran una solución urgente.
- Coordinación de intervenciones derivadas de iniciativas y/o proyectos que gestiona la PMO ciberseguridad.

Para ello, el adjudicatario deberá disponer de un **teléfono de guardia** del coordinador de la PMO ciberseguridad o de su respaldo.

Estos trabajos fuera del horario habitual no superarán el 2% del total de horas a realizar y se realizarán en remoto.

Osakidetza activará este soporte fuera de horas únicamente desde el responsable de Servicio o desde el director del servicio de Osakidetza.

Condiciones especiales de tipo medioambiental.

La empresa adjudicataria declarará que durante la ejecución del contrato se aplicarán medidas que respeten el medioambiente a través del uso de tecnologías y equipamientos que favorezcan el ahorro energético, el consumo responsable y la promoción del reciclado de materiales.

Idiomas

El adjudicatario incluirá la producción de material tanto en castellano como en euskera, como producto de las tareas que se puedan requerir por parte de Osakidetza.

12.2. Modelo de control y seguimiento

El licitador describirá en su propuesta un Modelo de Gobierno del Servicio, así como los mecanismos de reporte y compartición de información que considere oportuno.

Mínimamente deberá establecer los siguientes comités:

El **Comité de Seguimiento del Contrato:** Con carácter general se reunirá trimestralmente y será el foro donde se analizará y concretarán los servicios base asociados al periodo.

La periodicidad con la que se reunirá este foro podrá variar en función de las necesidades de **Osakidetza**.

El **Comité de Seguimiento del Servicio:** Con carácter general se reunirá una vez al mes y será el foro donde se analizará y concretará:

- Revisión de la actividad llevada a cabo por la PMO ciberseguridad.
- Planificación de la actividad para el siguiente periodo.
- Nuevas necesidades.

Los comités podrán ser presenciales o virtuales, priorizándose los virtuales.

13. PROPIEDAD DE LOS PRODUCTOS ENTREGADOS

Todos los estudios y documentos, así como los productos y subproductos elaborados por el suministrador como consecuencia de la ejecución del contrato **serán propiedad de Osakidetza**, quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el suministrador autor material de los trabajos.

El suministrador **renuncia expresamente** a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del contrato pudieran corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados en base a este pliego de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa de **Osakidetza**.

14. CONFIDENCIALIDAD

En consideración al tipo de información procesada, el adjudicatario está obligado a mantener la más absoluta confidencialidad sobre todos aquellos datos y documentos a que tenga acceso con motivo de la adjudicación. A ellos accederán exclusivamente las personas estrictamente imprescindibles para el desarrollo de las tareas inherentes a la misma. Todas

ellas serán advertidas del carácter confidencial y reservado de la información a la que tendrán acceso.

Todos los ficheros que se pongan a disposición del adjudicatario para la ejecución del contrato son propiedad de Osakidetza y están registrados y sometidos a la salvaguarda que establece la legislación vigente, en especial la relativa a la protección de datos personales. Toda cesión a terceros será perseguida en los tribunales.

Osakidetza se reserva el derecho de establecer cualquier tipo de marcaje de los ficheros que se dejarán al adjudicatario, de manera que sus características puedan constituirse como prueba que posibilite localizar el origen y los responsables de las eventuales cesiones.

Bajo ningún caso ni circunstancia el adjudicatario podrá suministrar a terceros ni utilizar para sí ni para otros los datos facilitados por Osakidetza para fines distintos a los contemplados en el objeto del presente contrato.

El adjudicatario estará obligado a poner en conocimiento de Osakidetza, inmediatamente después de ser detectada, cualquier sospecha de eventuales errores que se puedan producir en el sistema de seguridad de la información.

El adjudicatario faculta a Osakidetza para que al terminar el proyecto pueda responsabilizarlo y/o repercutirle los costes derivados de posibles reclamaciones ocasionadas por negligencia y/o falta de confidencialidad del mismo.

Adicionalmente y como condición general, todos los servicios prestados deberán contar con las medidas de seguridad y de confidencialidad adecuadas al grado de sensibilidad de la información suministrada, de acuerdo con lo descrito en la LOPD.

15. CONSULTAS AL PLIEGO

Durante el periodo de licitación y ante cualquier necesidad de aclaración sobre cuestiones referidas a las especificaciones recogidas en el presente Pliego de Bases Técnicas, los licitadores deberán remitir por correo electrónico las preguntas e información que consideren necesarias para elaborar la Propuesta Técnica.

Los licitadores podrán dirigir sus consultas o aclaraciones a la dirección de correo electrónico de la Subdirección de Informática y Sistemas de Información:

SISI.TECNOLOGIAEXPEDIENTES@osakidetza.eus

Los licitadores deberán identificar, a un único responsable de la oferta, que será durante al periodo de licitación, el interlocutor único con **Osakidetza** para cualquier tipo de consulta o aclaración sobre los términos expuestos en el presente Pliego, no admitiéndose ninguna consulta o aclaración de persona distinta a la señalada.

Así mismo los licitadores para formular sus consultas o aclaraciones deberán cumplimentar la siguiente información:

- Nº. Pregunta
- Capítulo/Apartado
- Página
- Párrafo
- Descripción de la Consulta

Documento firmado por: NICOLAS FRANCISCO GONZALEZ LOPEZ
En la fecha 20.10.2025 08:34:30 CEST