Eusko Jaurlaritzaren
Informatika Elkartea

Sociedad Informática
del Gobierno Vasco

## EXPEDIENTE Nº: EJIE-141-2025

# Suministros y Servicios para la instalación y mantenimiento de la Infraestructura del Servicio Convergente de Protección Avanzada de Correo Electrónico y Entornos Colaborativos.

Especificaciones de compra / Pliego de condiciones técnicas

Diciembre 2025

Mediterráneo, 14 · 01010 Vitoria-Gasteiz · Posta-kutxatila / Apartado: 809 · 01080 Vitoria-Gasteiz · Tel. 945 01 73 00* · Fax. 945 01 73 01 · www.ejie.eus

**Este documento es propiedad de Eusko Jaurlaritzaren Informatika Elkartea – Sociedad Informática del Gobierno Vasco, S.A. (EJIE). Este documento no puede ser reproducido, en su totalidad o parcialmente, ni mostrado a otros, ni utilizado para otros propósitos que los que han originado su entrega, sin el previo permiso escrito de EJIE. En el caso de ser entregado en virtud de un contrato, su utilización estará limitada a lo expresamente autorizado en dicho contrato. EJIE no podrá ser considerada responsable de eventuales errores u omisiones en la edición del documento.**

| Versión | Fecha | Resumen de cambios | Elaborado por: | Aprobado por: |
|---|---|---|---|---|
| 1.0 | 29/11/2025 | 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 Descripción Situación Actual ..... 7
2.4 Modelo de Servicio ..... 8

**3 Requisitos Técnicos y Funcionales ..... 12**

3.1 Arquitectura ..... 12
3.2 Protección de Correo Electrónico frente a Amenazas Básicas ..... 16
3.3 Protección de Correo Electrónico frente a Amenazas Avanzadas ..... 18
3.4 Protección de Entorno Colaborativo ..... 18
3.5 Administración, Reporting y Monitorización ..... 19
3.6 Protección de Entorno Educativo (HEZKUNTZA) ..... 20
3.7 Otras Funcionalidades ..... 21
3.8 Checklist de Requerimientos ..... 21

**4 Alcance y Requisitos de los servicios del contrato ..... 22**

4.1 Servicios de Puesta en Marcha ..... 22
4.2 Servicios de Mantenimiento ..... 28
4.3 Requisitos asociados a los servicios ..... 33
4.4 Otros Requisitos Asociados a la Prestación del Servicio de Mantenimiento ..... 38

**5 Anexos ..... 40**

5.1 Anexo I PCT_Checklist Requisitos Técnicos ..... 40

# 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

El contexto actual en materia de Ciberseguridad resulta cada vez más complejo. En un entorno en el que la movilidad y, en consecuencia, los servicios en cloud y el nivel de exposición de los servicios internos es creciente, el nivel de riesgo aumenta proporcionalmente. Por su parte, las redes criminales son cada vez más especializadas y tienden a dirigir y elaborar cada vez más sus ataques, contando además con la ayuda cada vez más relevante de la inteligencia artificial para perfeccionarlos.

En consecuencia, EJIE, se encuentra en una fase continua de Evolución de los Servicios de Seguridad que ofrece, de cara a mejorar las capacidades ya disponibles y a la incorporación de nuevas capacidades y funcionalidades que permitan hacer frente a la desafiante situación actual.

El Correo Electrónico sigue siendo uno de los principales vectores de entrada que utilizan los criminales en las fases iniciales de ataque para conseguir sus objetivos. Adicionalmente, en un ambiente de colaboración creciente con terceros, los Entornos Colaborativos suponen también un riesgo de seguridad.

En la actualidad, EJIE ya ofrece en su Catálogo de Servicios de Seguridad la protección de los entornos de Colaboración y Comunicación, todo ello en base al pliego EJIE-138-2022, cuya vigencia finalizará en Junio de 2026.

Con el fin de que EJIE pueda continuar ofreciendo servicio a todas las entidades ya adheridas a los Servicios del Catálogo de Seguridad que protegen los Servicios de Colaboración y Comunicación, así como al resto de organismos que así lo deseen, se hace necesaria la contratación de servicios especializados de seguridad, que contemplen la provisión y puesta en marcha de un Servicio de Protección Avanzada de Correo Electrónico y Entornos Colaborativos, 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 provisión y puesta en marcha de un Servicio de Protección Avanzada de Correo Electrónico y Entornos Colaborativos,* de acuerdo al alcance y requerimientos técnicos y de servicio solicitados en la presente contratación. Ello permitirá continuar ofreciendo servicio a todas las entidades ya adheridas a los Servicios del Catálogo de Seguridad que protegen los Servicios de Colaboración y Comunicación, así como al resto de organismos que así lo deseen.

## 2.2 Alcance de la Contratación

El proyecto deberá considerar el siguiente alcance:

- Provisión y puesta en marcha de una solución de Protección Avanzada de Correo Electrónico y Entornos Colaborativos, incluyendo los trabajos de consultoría, diseño y configuración necesarios.
- La incorporación a la nueva solución de los usuarios correspondientes a las entidades adheridas actualmente al servicio.
- La dotación de productos necesarios, junto con su soporte y garantía de fabricante asociados.
- Servicios de seguimiento, gestión, transferencia de conocimiento y documentación del proyecto, incluyendo las tareas de modelado del “Servicio de Protección Avanzada de Correo Electrónico y Entornos Colaborativos”.
- Servicios de mantenimiento (Nivel 3) de la solución implantada.

## 2.3 Descripción Situación Actual

En el anexo denominado **“Anexo I_PCT_Reservado_Situacion Actual”** se incluye la información correspondiente a la situación actual del presente expediente.

*Esta información se considera **confidencial**, por lo cual las empresas licitadoras interesadas en recibir estos datos deberán seguir las instrucciones indicadas en el **Apartado: “20.Confidencialidad” del PCP** del presente expediente y procedimiento de la cláusula 66.5 del PCP.*

## 2.4 Modelo de Servicio

### 2.4.1 Alcance Inicial del Servicio

Como se ha comentado previamente, actualmente EJIE basa su Servicio de Colaboración y Comunicación en Microsoft 365.

Este servicio está protegido actualmente por la solución de TrendMicro descrita previamente, y que resultó contratada a través del pliego EJIE-138-2022. Las licencias asociadas tienen vigencia hasta el 01/06/2026.

Este hecho es el que determina tanto la fecha límite para el arranque productivo (tras la migración correspondiente) como el alcance inicial del servicio, que coincidirá con el alcance actual del servicio.

Por lo tanto, a continuación, se concreta el alcance inicial del servicio y la fecha límite de entrada en producción:

| ALCANCE INICIAL DEL SERVICIO | | |
|---|---|---|
| **ENTIDAD** | **Nº USUARIOS** | **FECHA LÍMITE PRODUCCIÓN** |
| VARIAS | 52.000 | 01/06/2026 (*1) |

(*1) En esta fecha se deberá dejar de hacer uso del servicio actual (EJIE-138-2022), por lo que para esa fecha habrá tenido que concluir la ejecución de los servicios de migración/revisión del servicio actual.

### 2.4.2 Periodo de Prestación del Servicio

El contrato tendrá una duración de 37 meses, de los cuales el primer mes será el tiempo máximo estipulado para el aprovisionamiento y puesta en marcha de la nueva plataforma de Protección Avanzada de Correo Electrónico y el resto de los meses (36) serán de uso en producción de la plataforma.

### 2.4.3 Modelo de Suscripción

La solución de Protección Avanzada de Correo Electrónico se prestará como un servicio en la nube basado en suscripciones al servicio.

A continuación, se describe el modelo de suscripción solicitado al que deberá dar respuesta la empresa adjudicataria durante la vigencia del contrato.

- Existirán dos suscripciones al Servicio de Protección Avanzada de Correo Electrónico y Entornos colaborativos:
    - **Suscripción CONVERGENTE:** Se trata de la suscripción que consumirán todas las entidades a excepción del Entorno Educativo (Hezkuntza).

- **Suscripción HEZKUNTZA:** Se trata de la suscripción que consumirá el Entorno Educativo (Hezkuntza).

- Las suscripciones deberán incluir:
  - Todos los servicios y funcionalidades que la empresa licitadora describa en su solución técnica en respuesta al apartado 3 de Requisitos Técnicos y Funcionales. Existen requisitos diferenciados para cada tipo de suscripción.
  - Los Servicios de Mantenimiento (Nivel 3) solicitados en el apartado 4.2
  - Los Servicios de Puesta en Marcha solicitados en el apartado 4.1

- Se aplicará la misma suscripción CONVERGENTE para proteger cualquier tipo de buzón, independientemente de que esté albergado en SaaS u OnPremise.
  La suscripción HEZKUNTZA protegerá buzones albergados en M365.
- Como se ha indicado previamente, las suscripciones al Servicio de Protección Avanzada de Correo Electrónico y Entornos Colaborativos se realizarán en base a número de USUARIOS.
- En el caso de que las suscripciones de la solución propuesta estén basadas en número de buzones, la empresa adjudicataria tendrá que establecer a nivel interno sus factores de conversión de forma que esa conversión sea transparente para EJIE, que solicitará suscripciones por USUARIO en todo caso.
- La titularidad de las suscripciones será de EJIE desde el momento de adquisición, o en su defecto, se deberá garantizar al inicio mediante documento acreditativo de fabricante, que se trasladará la titularidad de las mismas a EJIE con la finalización del contrato.
- En el contexto de la renovación de licencias vigentes, es imprescindible garantizar que las renovaciones que se produzcan durante la ejecución de este contrato ofrezcan al menos las mismas funcionalidades proporcionadas por el fabricante en la actualidad. Es decir, si el fabricante introduce un nuevo modelo de licenciamiento (incluyendo cambios de nombres de SKUs o separaciones de funciones en SKUs diferentes), la empresa adjudicataria debe adquirir las nuevas licencias necesarias que presten como equivalente al menos las funcionalidades que EJIE tenga adquiridas en cada momento. Asimismo, deberá actualizar el catálogo de suministros, manteniendo los mismos precios.
- La suscripción CONVERGENTE al Servicio de Protección Avanzada de Correo Electrónico y Entornos Colaborativos se realizará en bloques de 1.000 usuarios. Las suscripciones se solicitarán en base a bloques enteros, redondeando al número entero superior con el fin de garantizar la prestación del servicio. Así, por ejemplo, en el caso de la protección de 1.300 usuarios, se contratarían 2.000 suscripciones (2 bloques de 1.000 USUARIOS).
- La suscripción HEZKUNTZA al Servicio de Protección Avanzada de Correo Electrónico y Entornos Colaborativos se realizará en un único bloque de 188.000 usuarios. La entidad Hezkuntza podrá adherirse a esta suscripción únicamente el momento inicial de arranque del proyecto/contrato. Sin embargo, no existe compromiso de realizar esta adscripción inicial y podría no llevarse a cabo si EJIE/Hezkuntza no lo consideran oportuno en el momento del lanzamiento inicial del proyecto.

Es decir, en el momento del lanzamiento inicial del proyecto se decidirá si Hezkuntza se adscribe o no al servicio y, en caso de adscribirse, lo hará en un único bloque de 188.000 usuarios.

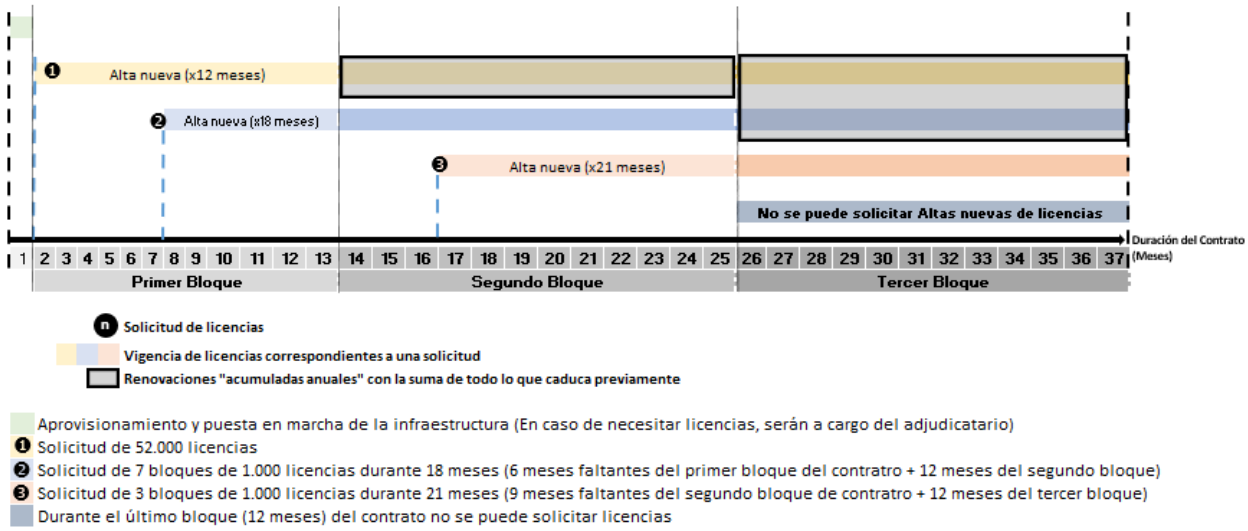
Si se realiza la adscripción inicial y a lo largo de la vida del contrato se requiere ampliar el número de usuarios, se utilizarán bloques de 1.000 usuarios como en el caso de la suscripción CONVERGENTE.

- Durante la fase de aprovisionamiento y puesta en marcha de la infraestructura (máximo 1 mes), de ser necesaria la activación de licencias para acometer esta tarea correrán a cargo de la empresa adjudicataria y no podrán facturarse durante este período máximo de un mes.
- El tratamiento con relación al alta y renovación de suscripciones será el siguiente:
    - En el momento del lanzamiento del proyecto se adquirirán las siguientes licencias:
        - Suscripción CONVERGENTE: Las indicadas en el ALCANCE INICIAL.
        - Suscripción HEZKUNTZA: Como se ha indicado previamente, se decidirá en este momento si se adquiere un bloque de 188.000 usuarios o si, por el contrario, Hezkuntza no se adscribe al servicio. No existe ningún compromiso por parte de EJIE/Hezkuntza para esta adscripción.
    - A lo largo del contrato, la solicitud tanto de nuevas altas como de renovaciones estará sujeta a validación por parte de EJIE.
    - EJIE podrá solicitar altas nuevas durante los primeros 24 meses del contrato del tipo CONVERGENTE. Del tipo HEZKUNTZA sólo podrá adquirirlas si se ha realizado la adscripción inicial.
    - La facturación de las suscripciones será anual, por lo que las fechas de facturación serán el 1 de junio de 2026, 1 de junio de 2027 y 1 de junio de 2028.

      El 1 de junio de 2026 se facturará el pedido inicial (Suscripciones CONVERGENTES y, opcionalmente, suscripciones HEZKUNTZA). El 1 de junio de 2027 se facturará la renovación del pedido inicial (Suscripciones CONVERGENTES y, opcionalmente, suscripciones HEZKUNTZA). El 1 de junio de 2028 se facturará la renovación del pedido inicial ((Suscripciones CONVERGENTES y, opcionalmente, suscripciones HEZKUNTZA) junto con las renovaciones de nuevas altas que puedan haberse dado durante los 12 primeros meses del contrato, tal y como se explica a continuación.
    - Como criterio general, toda alta solicitada tendrá asociada una duración mínima de un año.
        - En caso de altas que tengan lugar a lo largo de cualquiera de los 24 primeros meses de contrato, estas se regularizarán hasta el fin del año siguiente al de adquisición y su coste se calculará como la parte proporcional al precio anual ofertado y se facturará en el momento del suministro. Es decir, si el alta se produce, por ejemplo, el día 1 del mes 10 del contrato, se abonará por la cantidad 1,25 veces el coste anual ofertado.

- La renovación de la suscripción durante la siguiente anualidad se producirá de manera automática, salvo que EJIE indique lo contrario. La empresa adjudicataria deberá realizar un aviso previo antes de la renovación, para conocimiento y toma de decisión de EJIE.

Como ejemplo se muestra el siguiente gráfico:




** Este gráfico es un ejemplo, en ningún momento representa un compromiso de compra de EJIE con la empresa adjudicataria.

- En el momento de realizar la solicitud de altas, deberá confirmarse que, con el volumen de altas solicitadas hasta la fecha y las nuevas, no se superará el importe máximo de licitación con las renovaciones que estas altas implicarían al finalizar el periodo del contrato.

# 3 Requisitos Técnicos y Funcionales

En este apartado se van a detallar los requisitos técnicos y funcionales vinculados a la solución de Protección Avanzada de Correo Electrónico y Entornos Colaborativos.

**Todos los requisitos solicitados serán de obligado cumplimiento**, salvo que se indique lo contrario.

En el Archivo Electrónico De Fórmulas se solicita, entre otros, un **precio unitario por suscripción anual de usuario de cada tipo (CONVERGENTE y HEZKUNTZA)**.

En la propuesta de la empresa licitadora se describirán las funcionalidades de la solución propuesta. **Todas las funcionalidades que se describan para cada tipo de suscripción en la propuesta estarán licenciadas dentro del precio unitario anual por usuario que se solicita en el Archivo Electrónico De Fórmulas (Suscripción CONVERGENTE y Suscripción HEZKUNTZA).**

Es decir, si la solución propuesta por la empresa licitadora dispone de una función o módulo para satisfacer un requisito, pero ese módulo no se va a incluir en la licencia única correspondiente, la empresa licitadora NO describirá esa función o módulo en la propuesta.

No se considerarán válidos los requisitos que se indique que se cumplen haciendo uso de funcionalidades de M365. Los requisitos los debe cumplir la solución del fabricante propuesto, no M365.

Los requisitos deben cumplirse haciendo uso de una misma solución. No será válido proponer un fabricante para unos requisitos y uno diferente para otros.

Como se ha adelantado, se requieren dos tipos de suscripciones (CONVERGENTE y HEZKUNTZA) que corresponden con dos niveles de protección diferenciados. El licitador deberá proponer una solución completa de protección que, para la suscripción CONVERGENTE, cumpla todos los requisitos indicados. Adicionalmente, deberá proponer una solución con menores requisitos obligatorios para la suscripción HEZKUNTZA. Se considera que la solución HEZKUNTZA podrá ser una versión reducida de la solución CONVERGENTE. En el apartado correspondiente a la Protección del entorno Educativo (Hezkuntza) se indicará el subconjunto de funcionalidades obligatorias para esta suscripción. No habrá que duplicar las explicaciones de las diferentes funcionalidades, salvo que realmente sean diferentes.

A continuación, se exponen los requisitos que, al menos, debe cumplir la solución propuesta por la empresa licitadora, debiendo quedar debidamente justificado y detallado su cumplimiento a través de la propuesta presentada, valorándose el detalle a nivel conceptual y específico en configuraciones (pantallazos) y la idoneidad de la solución en cada caso;

## 3.1 Arquitectura

En las descripciones y requisitos no se va a tener en cuenta la existencia de la solución actual de Protección Avanzada de Correo Electrónico de cara a la explicación de la arquitectura y flujos de correo existentes.

La empresa licitadora deberá describir detalladamente la arquitectura propuesta para poder cumplir todos los requisitos que se exponen a continuación, con especial atención a la arquitectura necesaria para proteger el entorno OnPremise y su relación y dependencias con la arquitectura necesaria para proteger el entorno SaaS.

- Tal y como se indica en PCP, la solución propuesta debe permitir el cumplimiento del ENS, formando parte para ello del Catálogo de Productos y Servicios STIC (CPSTIC) del CCN (Centro Criptológico Nacional) y apareciendo, por lo tanto, en la guía CCN-STIC 105.
- La solución de Protección de Correo Electrónico debe ofrecerse en modo servicio (SaaS) en nube mantenida por fabricante. Es decir, todas las labores de instalación, mantenimiento y operación básicas del producto deben ser responsabilidad del fabricante, no de la empresa adjudicataria. Entre ellas, instalación y configuración HW, instalación y configuración de los sistemas operativos correspondientes, instalación y configuración básica del producto hasta el momento en que se ofrece como SaaS, instalación de actualizaciones y parches de sistemas operativos y producto, ampliaciones HW necesarias, monitorización básica de la plataforma para asegurar la alta disponibilidad del servicio.
  Este requisito será obligatorio, excepto para las piezas o elementos necesarios para la protección de Exchange OnPremise cuando aplique.
- La plataforma SaaS se albergará en un DataCenter en la Unión Europea para asegurar el cumplimiento de la legislación vigente.
- Siendo un servicio SaaS, la solución deberá agilizar la puesta en marcha del servicio, independizándolo de infraestructura hardware y su mantenimiento, y facilitando el escalado del mismo en un entorno multitenant.
- Siendo un servicio SaaS, la solución deberá permitir la integración con otros servicios SaaS (Microsoft 365, por ejemplo) sin dependencias de infraestructura onpremise.
    - Este requisito será obligatorio, con excepción de las dependencias que se puedan generar cuando se requiere proteger Exchange OnPremise.
- La empresa adjudicataria deberá garantizar la implantación del servicio de forma que EJIE pueda explotar a través de sus grupos de soporte los servicios, tecnologías y configuraciones adoptadas.
- No se admitirá el despliegue de la solución en nube de la empresa licitadora si ésta no es el fabricante de la solución. Los datos deberán quedar en la nube del fabricante de la solución adjudicataria. El fabricante se encargará de las labores de mantenimiento de la plataforma a todos los niveles, como son, entre otras, mantenimiento HW, instalación y configuración base del producto en HA, escalado HW en caso de crecimiento, instalación de parches y actualizaciones a nivel de sistema operativo y producto, monitorización del estado de la plataforma.
    - Este requisito será obligatorio, excepto para las piezas o elementos necesarios para la protección de Exchange OnPremise cuando aplique. En estos elementos las labores de mantenimiento se realizarán por parte de los grupos de soporte Nivel 2 de EJIE con la ayuda de los servicios de Nivel 3 de la empresa adjudicataria.

- La solución permitirá la integración, al menos, con Microsoft 365. Al estar basado el servicio de Comunicación y Colaboración ofrecido por EJIE en M365, la solución de protección avanzada deberá ser compatible, al menos, con este servicio SaaS.
- La solución permitirá la integración, al menos, con Microsoft Exchange OnPremise 2016 y 2019.
- La solución permitirá la protección del correo electrónico Interno en M365 y en Microsoft Exchange OnPremise:
    - La solución permitirá la protección del correo electrónico Interno dentro, al menos, de un tenant de M365. Es decir, protegerá correos enviados entre dos tenants diferentes de M365 (Un envío entre Osakidetza y Justizia, por ejemplo), así como correos enviados dentro del propio tenant M365 (Un envío entre el usuario1@euskadi.eus y el usuario2@euskadi.eus dentro del tenant M365 de ELKARLAN, por ejemplo).
    - La solución permitirá la protección del correo electrónico Interno dentro de una instalación de Microsoft Exchange OnPremise (Un envío entre el BuzonOnPremise1@osakidetza.eus y el BuzonOnPremise2@osakidetza.eus dentro de la instalación de Microsoft Exchange OnPremise de OSAKIDETZA, por ejemplo).
- La solución permitirá la protección del correo externo, tanto del correo entrante desde Internet hacia las entidades protegidas como del correo saliente desde las entidades protegidas hacia Internet.
  Esta protección de correo externo aplicará a todos los buzones de entidades tanto con todos sus buzones de correo en M365 como con soluciones híbridas en las que tengan buzones en M365 y buzones OnPremise.

  En el escenario en que todos los buzones están en M365, entrada y salida será por M365.

  En el escenario en que parte de los buzones están en M365 y parte están OnPremise, la entrada de correo externo siempre será por M365. Sin embargo, la salida de correos hacia el exterior de los buzones albergados en M365 será por M365, pero la salida de correos de los buzones albergados OnPremise podría ser a través de M365 o a través de Microsoft Exchange OnPremise, según la dirección de destino.

  En todos los casos la solución debería permitir la protección de todo el correo externo (entrante y saliente).
- La empresa licitadora deberá considerar la prestación del servicio en un entorno multitenant, y por tanto deberá presentar un servicio preparado para soportar dicho entorno, en el que las entidades presentan contextos IT diferentes y necesidades en materia de seguridad también diferentes.
  La solución debe ser Multitenant en, al menos, los siguientes aspectos (Recordar la definición de ENTIDAD realizada en apartados previos):
    - *Adscripción al Servicio:* Debe permitir ofrecer el servicio tanto a entidades con tenants de O365 propios como a entidades con tenants de O365 compartidos.

Por ejemplo, dentro del tenant compartido de ELKARLAN, debe permitirse que los usuarios de EJGV estén protegidos mientras que los usuarios de otra entidad dentro de ese tenant de ELKARLAN no estén protegidos.

- *Configuración:* La solución debe permitir establecer configuraciones diferentes para cada una de las entidades si fuera necesario.

  Por ejemplo, debe permitir que en una entidad se haga una excepción específica que a otra entidad no le aplique.

- *Administración:* La solución debe permitir delegar la administración de la configuración de las entidades, al menos, en base a sistemas RBAC (Role Based Access Control).

- *Informes:* La solución debe permitir la generación de informes diferenciados por entidad, de forma que se pueda informar a cada entidad por separado de la situación de su servicio.

- La solución debe proporcionar una cuarentena donde retener el correo malicioso o no deseado, siendo opcional y granular su uso en función de las configuraciones implementadas. La solución debe permitir interactuar con la cuarentena, tanto a los administradores como a los usuarios finales. Al menos en el caso de los usuarios finales debe permitirles trabajar únicamente con correos no maliciosos.
  Teniendo en cuenta que M365 cuenta con su propia cuarentena, la solución debe permitir alcanzar una configuración de cuarentena única.
- La solución proporcionará un mecanismo para que los usuarios puedan reportar de forma autónoma mensajes que consideren que son SPAM, maliciosos o similares para su análisis por parte de la solución de seguridad.
  Este mecanismo, idealmente, será un plugin o un botón que esté disponible en los diferentes clientes de correo (Outlook para Windows, Outlook vía Web, Outlook para sistemas operativos móviles como Android o IOS).

  Teniendo en cuenta que M365 ofrece su propio botón de reporte, la solución deberá permitir alcanzar una configuración con un único botón de reporte.
- Al tratarse de una solución en nube, de cara a la administración del entorno, se debe ofrecer la posibilidad de hacer Single Sign On (SSO) utilizando proveedores de identidad (IDP) de terceros (OKTA al menos) en base a estándares (SAML al menos).
- La solución propuesta deberá ofrecer una API que permita interaccionar con ella y automatizar acciones.

A modo aclaratorio, indicar que la finalidad de algunos de los requisitos indicados es que el servicio SaaS solicitado se preste desde la nube que los fabricantes tienen ya desplegada para dar servicio, creando en ella las instancias que sean necesarias (pudiendo ser esta pública, siempre que sea gestionada y mantenida por el fabricante de la solución ofertada). En caso de que la solución SaaS se aloje en nube pública, la titularidad del alojamiento no podrá ser de la empresa licitadora, salvo que la empresa licitadora sea el propio fabricante.

## 3.2 Protección de Correo Electrónico frente a Amenazas Básicas

Todos los requisitos de protección frente a amenazas básicas deben cumplirse, al menos, en la protección de correo externo, considerándose que aporta valor que se cumplan el mayor número posible de requisitos también para correo interno (En M365 y/o en Microsoft Exchange OnPremise).

- La solución debe permitir filtrar en base, al menos, a los siguientes tipos de filtros básicos:
  - Remitente.
  - Destinatario.
  - Asunto.
  - Contenido Cuerpo del mensaje.
  - Tipos de adjuntos (por extensión, por MIME type, por tipo real de fichero o True File type).

  La configuración de estos filtros básicos debe permitir la configuración de excepciones. Es decir, se debe poder filtrar, por ejemplo, un tipo de fichero excepto si viene de cierto remitente o a cierto destinatario.
- La solución debe permitir el control de, al menos, los siguientes aspectos del envío y la recepción:
  - Control de tamaño de los mensajes y adjuntos.
  - Control del número de destinatarios por mensaje.
- La solución debe permitir, en la recepción, el chequeo/verificación de la implementación de medidas SPF, DKIM y DMARC por parte de los remitentes, siendo configurables y granulares las acciones a realizar en función del chequeo realizado.
- Si la solución incorpora un relay SMTP, debe permitir verificar la existencia de destinatarios antes de la entrega de los mensajes en M365.
- La solución debe permitir el control de los mensajes Bounced, evitando que lleguen a nuestros buzones las respuestas a mensajes enviados por atacantes que intentan suplantar nuestra identidad frente a terceros.
- La solución debe permitir añadir “banners o disclaimers” de forma automática en los mensajes informando al usuario de diversos aspectos relacionados con el mensaje. Estos “banners o disclaimers” podrán personalizarse (texto, idiomas, formato,..).
- La solución debe incluir los siguientes módulos de seguridad básicos:
  - Filtrado en base a listas de reputación de IPs.
  - Filtrado en base a la geolocalización de las IPs que estén remitiendo correo. Esta configuración deberá permitir excepciones, de forma que se pueda denegar la recepción de correo desde un país concreto excepto desde una o varias IPs concretas de dicho país o desde un remitente concreto (dirección/dominio email).
  - Motor AntiSPAM:
    - Debe permitir decidir granularmente qué acciones tomar con el SPAM (Al menos, rechazar; marcar de diferentes modos y dejar pasar).
    - Debe permitir personalizar los parámetros del motor antispam.

- Motor AntiMalware:
  - Debe permitir decidir granularmente qué acciones tomar ante el Malware.

- La solución debe permitir realizar los diversos análisis y filtros asociados a ficheros en adjuntos que lleguen dentro de ficheros comprimidos. Asimismo, la solución debe permitir decidir cómo tratar los ficheros comprimidos en base a diversos aspectos como son la protección por contraseña o el nivel de anidamiento de ficheros comprimidos.
- La solución debe permitir la detección de ficheros adjuntos con contenido activo (macros) y, al menos, debe permitir eliminar esos ficheros del mensaje. Esta configuración debe permitir excepciones para, por ejemplo, sí permitir el envío de ficheros con macros desde ciertos remitentes.

  La detección de contenido activo debe realizarse, al menos, en ficheros de la Suite de Office y en ficheros PDF.

  Idealmente, la solución debe permitir eliminar el contenido activo de los adjuntos, permitiendo entregar una versión “limpia” de los adjuntos.
- La solución debe permitir clasificar el correo electrónico considerado “GrayMail” en diferentes categorías (Marketing, BULK, entre otras) de cara a tomar acciones diferentes granularmente en función de la categoría.
- La solución debe incluir un módulo de filtrado y análisis de URLs que, al menos:
  - Permita detectar, al menos en el contenido de los mensajes, URLs maliciosas y eliminar el mensaje completo o la URL maliciosa.
  - Permita detectar las URLs existentes dentro de un correo electrónico y reescribirlas todas o en base a determinados factores para que, cuando el usuario pinche en la URL, se determine si las URL es maliciosa o no antes de permitir el acceso a la misma.
  - Permita tener trazabilidad de las acciones del usuario sobre las URLs reescritas.
  - Si se determina que una URL no es maliciosa, este módulo permitirá navegar al usuario utilizando el resto de medidas de control de navegación que la organización tenga implementadas, resultando este módulo un complemento, no un sustituto en el control de navegación hacia esas URLs que se reciben por correo electrónico.
  - Permita establecer excepciones de forma que, por ejemplo, no se aplique el módulo a URLs correspondientes a dominios internos.
- La solución deberá permitir aplicar DKIM en los correos salientes hacia Internet, ofreciendo opciones para configurar de forma granular DKIM por cada uno de los dominios.
- Si la solución incorpora un relay SMTP, deberá permitir el envío/recepción de correo SMTP seguro (comunicación a nivel de transporte SMTP entre el relay y el siguiente/anterior servidor de correo), siendo la gestión de los certificados necesarios transparente para los administradores de la plataforma.
- La solución propuesta incorporará una solución de Data Loss Prevention que puede aplicar, al menos, al correo electrónico saliente.

## 3.3 Protección de Correo Electrónico frente a Amenazas Avanzadas

Todos los requisitos de protección frente a amenazas avanzadas deben cumplirse, al menos, en la protección de correo externo, considerándose que aporta valor que se cumplan el mayor número posible de requisitos también para correo interno (En M365 y/o en Microsoft Exchange OnPremise).

- La solución debe incorporar un módulo o funcionalidad específica AntiPhishing que permita hacer frente a los mensajes de phishing más avanzados (BEC, entre otros) gracias a la utilización de tecnologías de Machine Learning e Inteligencia Artificial (IA).
- La solución debe contar con módulos de Análisis de Comportamiento que permitan detectar comportamientos anómalos a diferentes niveles dentro del flujo de correo y tomar diferentes acciones de respuesta.
- La solución debe incorporar la funcionalidad de Sandboxing (sin límite de ejecuciones) con objeto de detectar las amenazas más avanzadas y ataques ZeroDay presentes en:
    - Ficheros: Sandboxing de Ficheros Adjuntos
    - URLs: Sandboxing de URLs detectadas, al menos, en los mensajes.
- La solución debe permitir la limpieza de buzones de usuarios en M365 y en Microsoft Exchange OnPremise después de que los mensajes hayan sido entregados. Es decir, suponiendo que se ha entregado un mensaje en varios buzones y, un tiempo después se determina que ese mensaje era malicioso, la solución debe ser capaz de eliminar ese mensaje de los buzones donde ya había sido entregado.

## 3.4 Protección de Entorno Colaborativo

- La solución permitirá proporcionar medidas de protección en el ámbito colaborativo, al menos, de Microsoft 365. Es decir, la solución, a través de su integración con M365, permitirá ofrecer medidas de protección en, al menos, Teams, SharePoint y OneDrive como herramientas clave dentro del servicio de Colaboración ofrecido por EJIE.
- La solución de protección en el ámbito de colaboración permitirá proteger el intercambio de ficheros y URLs a través de las aplicaciones protegidas.
- La solución de protección en el ámbito de colaboración permitirá, al menos, detectar comportamientos anómalos o situaciones de riesgo en las aplicaciones protegidas. Idealmente permitirá realizar acciones asociadas a esas detecciones.
- La solución de protección en el ámbito de colaboración permitirá, al menos, detectar anomalías en las cuentas con las que los usuarios acceden a estas aplicaciones protegidas. Idealmente permitirá realizar acciones asociadas a esas detecciones.
- Opcionalmente, la solución propuesta incorporará una solución de Data Loss Prevention que puede aplicar a los diferentes entornos colaborativos.

## 3.5 Administración, Reporting y Monitorización

En este apartado es especialmente relevante recordar el concepto de ENTIDAD descrito previamente.

- Como ya se ha indicado previamente, la solución debe ser MULTITENANT a diversos niveles, entre los que se encuentran:
  - *Administración:* Debe permitir, al menos mediante mecanismos RBAC, delegar parte de la configuración de las diferentes entidades a los administradores de las mismas o proporcionarles un acceso de lectura, por ejemplo.
  - *Informes:* Debe permitir, al menos, generar informes diferenciados por entidad donde a cada una de ellas se le muestren datos correspondientes a su propia entidad completa.
- La solución debe proporcionar mecanismos de tracking y troubleshooting avanzados que permitan a los administradores analizar la información y logs recogidos por la herramienta y detectar el origen de los diversos problemas.

  Por ejemplo, deben ser capaces de:
  - Localizar logs de un mensaje pudiendo localizarlo por remitente, destinatario, asunto u otros parámetros del mensaje.
  - Ver el flujo que ha seguido el mensaje dentro de la herramienta, pudiendo determinar qué chequeos se han realizado sobre el mensaje, con qué resultados, qué se ha hecho con el mensaje, por qué se ha bloqueado en un momento dado, dónde ha sido entregado en un momento dado y cualquier otro dato relacionado con el flujo del mensaje.
- La solución debe permitir la integración de sus logs y de sus alertas con herramientas de SIEM. En concreto, debe permitir la integración con el SIEM de EJIE basado en CROWDSTRIKE.
- La solución debe permitir la retención de logs detallados durante, al menos, 30 días, con objeto de poder buscar eventos pasados en caso de necesidad por cuestiones sobre todo de seguridad.
- La solución debe ofrecer dashboards de monitorización a los administradores donde puedan, al menos:
  - Estado del entorno de protección de correo: volumetría, alertas, estado del sistema y otros datos significativos en el contexto del correo electrónico.
  - Métricas y/o Indicadores específicas de seguridad.
- La solución debe permitir programar informes mensuales por cada una de las entidades que, al menos, incorporen los indicadores clave que se determinen para el servicio, como son, volumen de correo tratado, clasificación del correo por categorías (spam, marketing, malware, limpio,…), alertas de seguridad, TOPs en el ámbito de correo, TOPs en el ámbito de colaboración. Todo ello en informes

únicos por entidad completa (no por dominios). Podrían ser informes separados por Correo y Entornos Colaborativos, aunque lo ideal sería un único informe por entidad.

## 3.6 Protección de Entorno Educativo (HEZKUNTZA)

El licitador debe ofrecer una solución para proteger el Entorno Educativo. Esta solución se licenciará a través de la suscripción HEZKUNTZA y no debe cumplir todos los requisitos que se han solicitado previamente.

El licitador deberá detallar en el apartado Checklist de Requerimientos qué nivel de protección ofrece para la protección del Entorno Educativo (Hezkuntza). Se considerará que aporta más valor cuando mayor número de funcionalidades se proporcionen dentro de este entorno.

Sin embargo, como mínimo se deberán cumplir los siguientes requisitos. **Se hará referencia a requisitos ya descritos en apartados previos, por lo que la mención será breve y relativa a dichas descripciones previas**:

- Arquitectura:
  - Mismo fabricante que suscripción CONVERGENTE
  - Producto en CCN-STIC 105
  - Servicio SaaS
  - Integración con M365
  - Protección de correo externo e interno en M365
  - Integración de administración con IDP
- Protección frente a Amenazas Básicas:
  - Filtros básicos
  - AntiSpam
  - AntiMalware
  - Filtros de Adjuntos
  - Clasificación de Graymail
  - Filtrado URL
- Protección frente a Amenazas Avanzadas
  - Sandboxing Ficheros y URLs
  - Análisis de Comportamiento
  - Limpieza de buzones de usuarios en O365
- Protección Entorno Colaborativo
  - Protección entorno Microsoft 365 (Teams, OneDrive).
- Administración, Reporting y Monitorización
  - Administración RBAC

- Informes
- Tracking de mensajes

## 3.7 Otras Funcionalidades

Opcionalmente, la solución podrá proporcionar otras funcionalidades adicionales en el contexto de la securización del correo electrónico y la colaboración que aporten valor añadido sobre las ya requeridas. Únicamente se valorarán funcionalidades que no encajen en los apartados previos y se considere que realmente aportan valor en el ámbito de este pliego.

## 3.8 Checklist de Requerimientos

Ver anexo 5.1

# 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 Puesta en Marcha

La empresa adjudicataria deberá considerar, entre los servicios a prestar, el proyecto para el aprovisionamiento y puesta en marcha de la plataforma a implementar para la protección avanzada de correo electrónico y entornos colaborativos.

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. Tener en cuenta suscripción CONVERGENTE con ALCANCE INICIAL y, potencialmente aunque sin compromiso, suscripción HEZKUNTZA, según lo indicado en el apartado Modelo de Servicio.
- Configuración y ajuste del servicio, tras aprendizaje del entorno.
- Documentación de la solución.
- Transferencia de conocimiento del servicio.
- Servicios de Mantenimiento durante la puesta en marcha.

La empresa adjudicataria deberá tener en cuenta que la implantación puede implicar establecer nuevas políticas de seguridad adaptadas al escenario previamente identificado en la fase de consultoría. Así, el servicio y la plataforma quedará operativa una vez una vez concluido el alcance inicial, documentación y la transferencia de conocimiento.

En caso de que la solución propuesta sea la existente en la actualidad, la empresa adjudicataria deberá responder a este apartado de forma completa como si de una nueva instalación se tratara, aprovechando para revisar por completo el entorno existente y realizar todos los ajustes de configuraciones existentes e incorporaciones de nuevos módulos necesarios que permitan explotar la plataforma según lo solicitado en este pliego, así como actualizar toda la documentación y realizar una nueva transferencia de conocimiento actualizada.

### 4.1.1 Servicios de Construcción y Migración al Nuevo Entorno

Con el inicio del contrato, la empresa adjudicataria deberá realizar las tareas necesarias para la construcción y migración de la solución e infraestructura existente a la nueva solución propuesta, incluyendo la instalación y configuración 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, éstas correrán a cargo de la empresa adjudicataria.

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 afección a los usuarios actuales de los servicios.
- 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 a Operación.
- Soporte y mantenimiento durante el proceso de despliegue y migración de la infraestructura y servicios al nuevo entorno. En este sentido, la empresa adjudicataria se hará responsable de tareas englobadas en el denominado nivel 2 de soporte de EJIE 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.

La empresa adjudicataria 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.

En este punto la empresa adjudicataria deberá considerar el análisis de la arquitectura y servicios actuales, como punto de partida. Adicionalmente, deberá tener en cuenta la implantación de las funcionalidades disponibles en la nueva solución y que son deseables por su mejora significativa en los niveles de seguridad.

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, balanceo de carga y DR.
- Gestión de la solución.
- Capacidades de reporting y de gestión de inventario.
- Monitorización y Alertas.

- Valor añadido de la arquitectura y diseño propuesto

La empresa adjudicataria deberá proponer el plan de implantación 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 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 y entidades afectadas.

Atendiendo al diseño propuesto y validado por EJIE, y siguiendo el Plan de Implantación acordado, la empresa adjudicataria 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 considerarán trabajos fuera del horario normal habitual (de 10 PM a 7 AM) para reducir la afectación a las diferentes personas usuarias.
- Configuración de Backups, Monitorización e Inventario, colaborando para ello con los grupos correspondientes en EJIE y ajustándose en todo momento a los estándares y procedimientos de EJIE. Integración con las herramientas de operación y gestión, Monitorización, SIEM, back up y DR, 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 administración y reporting, así como la elaboración de plantillas para aplicación de políticas de seguridad establecidas por EJIE.
- Colaboración con EJIE en la definición y actualización del catálogo de servicios que pueda ofrecerse a las entidades que hagan uso del servicio objeto del presente expediente (modelado del servicio).
- Ejecución del Plan de pruebas acordado, que permita validar el funcionamiento correcto de la solución de acuerdo a 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.

- Establecimiento de unos usuarios/buzones de correo electrónico como piloto antes de proceder con el despliegue masivo, para la cual la empresa adjudicataria podrá emplear alguno de los equipos alcance de suministro. Las pruebas piloto tienen como objetivo:
    - Validar la solución técnica. Resolver dudas técnicas que puedan surgir con la activación del servicio.
    - Validar la estrategia de migración (Plan de Migración) en la convivencia de infraestructura vieja y nueva y garantizar la continuidad del servicio en estos casos.
    - Confirmar resto de procedimientos de ejecución y metodologías acordadas en inicio y adecuarlos, si se procede con algún cambio.
    - Confirmar los parámetros de configuración de la solución.
    - Validar la relación de entregables esperados. Modificar las plantillas de documentos en caso necesario.

- Una vez realizadas las pruebas y analizados los diferentes resultados, la empresa adjudicataria 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.

El plan global de proyecto que se presente en oferta y posteriormente con el inicio del contrato, deberá reflejar la ejecución de estos usuarios/buzones de correo electrónico piloto, considerando esta una **fase a superar antes del inicio de cualquier despliegue masivo**.

E La empresa adjudicataria contraerá el compromiso formal, que deberá asumir de un modo expreso, de garantizar todos y cada uno de los suministros e instalaciones a realizar contra toda clase de defectos de material empleado.

### 4.1.2 Ajuste y acondicionamiento del servicio

Una vez operativas la plataforma de protección avanzada de correo electrónico y entornos colaborativos, y realizado el testeo de las configuraciones preliminares establecidas, la empresa adjudicataria deberá introducir los ajustes adicionales para un mejor acondicionamiento y personalización de la solución atendiendo a parámetros y políticas corporativas: incorporación nuevas reglas, configuración de cuadros de

mando, inclusión de nuevas alertas, métricas e indicadores de interés, inclusión de nuevas políticas de remediación, definición de informes…

### 4.1.3 Documentación del Servicio

La empresa adjudicataria deberá documentar la solución desplegada y servicio configurado, completando la documentación necesaria para el modelado del Servicio de Protección Avanzada de Correo Electrónico y Entornos Colaborativos, incluyendo, al menos:

- Descripción y diseño de la solución: Se describirá la arquitectura y configuración de la solución desplegada de protección avanzada de correo electrónico, incluyendo:
  - Análisis técnico realizado.
  - Gestión del Servicio.
  - Tipologías: Características Principales y Beneficios.
  - Catálogo de reglas aplicadas.
  - Características de la plataforma.
  - Políticas de telemetría, políticas de remediación y acciones de respuesta acordadas.
  - Configuración de las consolas y cuadros de mando, indicadores, alertas configuradas, informes automáticos definidos...
- Documentación para entrega del servicio a Operación, el cual da respuesta a los siguientes conceptos:
  - Gestión del Conocimiento: Descripción y características generales del entorno, descripción de los distintos elementos que conforman la plataforma con el rol que desempeñan, configuraciones especificas a tener en cuenta, diseño y arquitectura con los diagramas de red o topológicos de la solución incluyendo todos los elementos involucrados en la solución, así como los flujos de comunicaciones necesarios para su funcionamiento.
  - Gestión de Activos: Inventario detallado de activos.
  - Gestión de la Configuración: Detalle de las configuraciones siguiendo las mejores prácticas de fabricante y los estándares de EJIE.
  - Gestión de Backup: Definición de los backups configurados.
  - Gestión de Eventos: Definición de la monitorización necesaria y configurada en los entornos de EJIE, marcándose además la línea base que permita realizar un mantenimiento preventivo efectivo. También se definirán los logs y reporting configurados.
  - Catálogo de Peticiones: Identificación de las peticiones “tipo” que aplican a este entorno de cara a definirlas en las herramientas de ticketing.
  - Gestión de Incidencias: Identificación de las incidencias más relevantes que pueden darse en el entorno, así como la línea de actuación en cada caso.
  - Gestión de la Disponibilidad: Plan de pruebas realizados con resultados obtenidos.
  - Gestión del servicio y reporting.
  - Gestión del Cambio: Identificar los procesos y requisitos involucrados

- Gestión de Despliegues/Onboarding: Se identificarán los aspectos necesarios para la incorporación de una nueva entidad al Servicio.
- Gestión de la Continuidad: Analizar e identificar los riegos sobre la continuidad del servicio para elaborar el plan de continuidad para aplicar las acciones necesarias para mantener la continuidad del servicio.
- Gestión de la Capacidad: Se identificarán los elementos a controlar para mantener la capacidad del servicio.

- Documentación técnica (oficial) con las características de las soluciones desplegadas, manuales técnicos y operativos, etc
- Otros Entregables: Otra documentación que pueda complementar a la anterior (Plan de Calidad, Plan de Recuperación del Servico…).

La documentación deberá mantenerse actualizada con la evolución del servicio (mejoras introducidas, nuevas políticas, nuevas reglas de correlación…)

En el caso de que la solución propuesta sea la existente en la actualidad la empresa adjudicataria deberá actualizar y mejorar la documentación existente.

### 4.1.4 Transferencia de Conocimiento del Servicio

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

- Introducción al Servicio de Protección Avanzada de Correo Electrónico y Entornos Colaborativos.
- Descripción técnica y de detalle sobre la solución implantada, así como del conjunto de elementos instalados y que forman parte de la solución de protección del correo electrónico.
- Presentación de las diferentes consolas, cuadros de mando, informes. Indicadores y alertas, uso de las consolas, búsquedas, generación de reportes...
  - Uso de las consolas. Opciones de configuración. Configuraciones realizadas.
  - Presentación e interpretación de los resultados de la Monitorización.
  - Conocimiento de las métricas e indicadores.
  - Reporting y modelos de informes.
- Onboarding de nuevas entidades. Creación de nuevos tenant.

La transferencia de conocimiento deberá garantizar que el equipo de soporte de EJIE adquiera un completo conocimiento, tanto a nivel operativo como de configuración y manejo de la tecnología, que les permita hacer frente a las incidencias, cambios, incluso al onboarding de nuevas entidades, etc. que puedan adherirse al servicio durante la duración del contrato.

Las sesiones de transferencia de conocimiento deberán ser impartidas, en la modalidad que EJIE 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:

- Sesiones EJIE: Al menos veinte (20) horas, distribuidas en las sesiones que EJIE estime necesarias para adaptarse a la disponibilidad del personal de EJIE

EJIE se reservará el derecho de pedir toda la formación o parte de ella al inicio del contrato que permita disponer del conocimiento necesario para hacer frente al mantenimiento de los equipos por parte de su equipo de soporte (Nivel 2) una vez recepcionados.

La empresa adjudicataria deberá entregar manuales y documentación relativa a los temas tratados en las diferentes sesiones.

La transferencia de conocimiento tendrá lugar en las instalaciones que especifique EJIE.

## 4.2 Servicios de Mantenimiento

En este apartado, se indica el alcance de los servicios de mantenimiento (Nivel 3) solicitados a través del presente expediente.

Estos servicios de mantenimiento se circunscriben a aquellos elementos adquiridos en el marco de este contrato y también se describen los acuerdos de nivel de servicio que deberá de prestar la empresa adjudicataria del expediente y las penalizaciones a aplicar por incumplimiento.

Asimismo, y de acuerdo a lo especificado en capítulos previos, la empresa adjudicataria deberá presentar informes mensuales de servicio con el objetivo de valorar el correcto cumplimiento de los SLAs acordados.

Con el fin de proporcionar correctamente los servicios objeto del contrato, la empresa adjudicataria dispondrá de los acuerdos y contratos de soporte y mantenimiento necesarios con el fabricante.

En caso de modificaciones en la distribución geográfica de los elementos objeto de este contrato, la empresa adjudicataria deberá asumir los cambios que se produzcan en este ámbito (siempre dentro de la CAPV) sin modificar el coste asociado a la prestación del servicio.

Mientras el contrato esté en vigor, la empresa adjudicataria se responsabilizará de la gestión de todas las relaciones con el fabricante: apertura de casos de soporte, incidencias.

EJIE dispone de soportes adicionales denominados de segundo nivel (Nivel 2) que serán los encargados de facilitar el acceso a los elementos incluidos en contrato. Para todas actividades en el marco de este contrato que así lo requieran, dicho acceso será siempre a través de estos soportes de segundo nivel de EJIE no existiendo accesos remotos permanentes.

Así mismo, durante este periodo, EJIE tendrá la posibilidad, si así lo requiere, de realizar la apertura de casos y gestiones directamente con el fabricante a través de sus equipos de soporte Nivel 2, con objeto de reducir los tiempos de respuesta. En este sentido, la empresa adjudicataria deberá habilitar los procedimientos necesarios para esta gestión (cambios de titularidad o cualquier otra modificación necesaria para este fin).

### 4.2.1 Servicio de Mantenimiento Correctivo

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

- Coordinación con los grupos de soporte y resto de proveedores que conforman la solución.
- Administración de los sistemas objeto del contrato y de los servicios ofrecidos a través de estos sistemas.
- Trabajos de reconfiguración de elementos.
- Reparación y/o sustitución de elementos averiados.
- Instalación/desinstalación de elementos, según necesidad.
- Instalación de software por fallo, vulnerabilidades publicadas, necesidad de actualización detectada en el mantenimiento preventivo o por indicación del fabricante.
- Pruebas para verificación de la reposición del servicio.
- Escalado a fabricante.
- Soporte técnico avanzado propio y soporte especializado experto de fabricante en el ámbito de la incidencia.
- Registro, seguimiento y documentación de la incidencia hasta su resolución.
- Elaboración de informes o partes de intervención o averías, a petición de EJIE.

#### 4.2.1.1 Acuerdos de Nivel de Servicio

La empresa adjudicataria proporcionará soporte técnico avanzado con técnicos cualificados y soporte especializado experto de fabricante a través de los canales habituales: correo, web, teléfono y presencial. En este sentido, es necesario cumplimentar el apartado “Medios materiales” del Anexo II: Compromiso de adscripción de medios incluido en el pliego de condiciones particulares con la información relativa al flujo y canales de comunicación.

Durante el periodo objeto de contratación, la empresa adjudicataria se comprometerá a ser el punto de contacto para atender cualquier tipo de incidencia o consulta técnica que pueda surgir en los equipos objeto del contrato y actuar como intermediario en el escalado al soporte técnico especializado experto de fabricante, es decir, asumir labores de gestión, coordinación e interlocución con los soportes adicionales

con los que EJIE cuenta y/o a su vez con el fabricante en el caso de incidencias, actualizaciones de software, consultas y demás circunstancias posibles.

A continuación, se especifican diferentes niveles de servicio requeridos en la prestación del servicio de mantenimiento correctivo:

- Horario de prestación del servicio: 24x7. La empresa adjudicataria deberá disponer tanto de un soporte propio 24x7 como del mantenimiento necesario con el fabricante. Se deberá acreditar la disposición de ambos servicios y que los perfiles profesionales asignados tengan autorización en la apertura de incidentes directamente con el fabricante.

- Se deben cumplir los siguientes tiempos de respuesta y resolución según la siguiente clasificación:
  - Críticas y graves: incidencias en el equipamiento que impidan o degraden el uso del servicio, resultando en incidencias por parte de la persona usuaria final.
  - Leves: incidencias que no impiden el funcionamiento del servicio, pero que degradan su uso de manera leve, sin suponer incidencias de la persona usuaria final.
  - Consultas: consultas técnicas en el ámbito de las tecnologías especificadas.

La siguiente tabla muestra los tiempos máximos a cumplir por la empresa adjudicataria:

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

La notificación de las diferentes averías a la empresa adjudicataria correspondiente se realizará por personal de EJIE o por los soportes con los que EJIE cuenta. Teniendo en cuenta lo anterior, se definen los siguientes conceptos:

- Tiempo de respuesta: tiempo transcurrido desde la comunicación de la avería hasta el inicio de las actividades encaminadas a su resolución.

- Tiempo de resolución: tiempo transcurrido desde la comunicación de la avería hasta el restablecimiento del servicio.

En cualquier caso, deberán entregarse informes mensuales de servicio y cumplimiento de SLAs.

### 4.2.2 Servicio de Mantenimiento Preventivo.

Se realizarán propuestas orientadas a mejorar el rendimiento y/o disponibilidad del Servicio. Se incluye la propuesta de la línea base de monitorización para una detección temprana de problemas, el análisis de las versiones software y estado del servicio buscando el reducir el número de incidencias a futuro en la red, la revisión de obsolescencia tecnológica y fechas de fin de vida, y el health check de la infraestructura para revisar la salud y configuraciones.

Se considerará que aporta valor el tener soporte directo de fabricante para revisiones periódicas de la plataforma, recomendaciones, conocimiento de nuevas funcionalidades y roadmap previsto, así como para otro tipo de tareas de Mantenimiento Preventivo que permitan sacar el máximo partido a la Plataforma a todos los niveles.

#### 4.2.2.1 Acuerdos de nivel de servicio

A continuación, se indican los requisitos relativos a los acuerdos de nivel de servicio en el mantenimiento preventivo que serán de aplicación.

La empresa licitadora a partir de inspecciones y/o mediciones periódicas (como mínimo 2 anuales) debe realizar propuestas orientadas a mejorar el rendimiento y/o disponibilidad de la red, incluyendo:

- Propuesta de la línea base de monitorización para una detección temprana de problemas.
- Análisis de las versiones software y estado del servicio buscando el reducir el número de incidencias a futuro.
- Revisión obsolescencia tecnológica y fechas de fin de vida.
- Health check de la infraestructura para revisar la salud y configuraciones, aplicación de las best practices y las recomendaciones particularizadas a nuestro entorno.

En los informes preventivos, como mínimo dos, uno a final del primer trimestre y otro a final del tercer trimestre, deben de reflejarse las acciones sobre el hardware/software que se consideren necesarias:

- Propuesta.

- Ventajas/inconvenientes de la migración/modificación.
- Inconvenientes de la no migración/modificación.
- Estimación de esfuerzo e impacto sobre el servicio.
- Observaciones si las hubiera.

### 4.2.3 Otros Servicios de Mantenimiento

- Elaboración de informes mensuales de servicio y estadísticas de incidencias. Se realizarán informes mensuales que reflejen el detalle de los servicios prestados en ese periodo, indicándose al menos datos relativos a incidencias ocurridas, causa de las incidencias, tiempos de respuesta, tiempos de resolución, tareas y/o peticiones cursadas como pueden ser la configuración y optimización de los sistemas, revisión de las vulnerabilidades publicadas en ese periodo… con identificación del cumplimiento o incumplimiento de los niveles de servicio comprometidos. Asimismo, si se considera oportuno, se podrán poner a disposición de EJIE herramientas que faciliten el seguimiento de las incidencias y la monitorización de los niveles de servicio vía Web. Los informes deben ser entregados a EJIE los primeros 10 días del mes siguiente en curso, es decir, el informe correspondiente al mes de enero, se deberá entregar los primeros 10 días del mes siguiente en este caso “febrero”.

- Renovación de la suscripción de las licencias. Se renovará la suscripción de las licencias objeto de contrato de acuerdo con los planteamientos indicados en este pliego de condiciones. Todas las renovaciones y mantenimientos deberán ser oficiales y estar garantizadas por el fabricante.

- Asunción de evoluciones sobre la misma plataforma. Si durante la vigencia del contrato, se decidiera actualizar o evolucionar los servicios existentes, la empresa adjudicataria deberá asumir el mantenimiento de esas posibles evoluciones sobre la misma plataforma objeto del presente contrato.

- Intervenciones planificadas. Las operaciones y asistencias que requieran los servicios descritos, por ejemplo, la parada de algún elemento que conforma la plataforma o de alguno de los servicios que presta, se planificarán de acuerdo con el personal técnico de EJIE en un horario convenido y que menos afecte al funcionamiento de dichos servicios.

- Estadísticas de uso de la plataforma. EJIE podrá solicitar a la empresa adjudicataria la elaboración de un informe con toda la información relativa al servicio que la plataforma presta. EJIE validará y podrá a su vez requerir la inclusión de más información en el citado informe.

- Servicio de soporte técnico experto, abierto a las necesidades de EJIE en consultas de soporte y en el ámbito de las tecnologías especificadas y horarios de atención solicitados.

## 4.3 Requisitos asociados a los servicios

### 4.3.1 Plazos Parciales de Ejecución

A continuación, se presentan los hitos y plazos relevantes con relación a la duración y vigencia del contrato:

- Se considera un plazo estimado máximo de 1 mes desde el inicio del contrato para la construcción de la nueva solución y la migración de los servicios actuales al nuevo entorno que se constituirá con los elementos incluidos en la primera solicitud del contrato.
- El plazo de contrato durante el cual se podrán solicitar productos especificados en el apartado 2.4.2 es de 24 meses.
- Los servicios de mantenimiento del integrador según apartado 4.2 se prestarán durante un plazo de 3 años.

### 4.3.2 Requisitos Generales

Los trabajos a desarrollar por la empresa adjudicataria 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, la empresa adjudicataria 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 de la empresa adjudicataria 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 de la empresa adjudicataria 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 la empresa adjudicataria podrá realizar acciones de comunicación y/o difusión del proyecto sin la debida autorización previa por parte de EJIE.

### 4.3.3 Coordinación con Terceros y Horarios de Actividad

Con carácter general, las plataformas actuales de protección de correo electrónico están en producción y está siendo explotada para la prestación de diferentes servicios, por lo que la empresa adjudicataria deberá considerar la necesidad de coordinación con Soporte EJIE para la ejecución de las tareas de migración de los servicios, dependiendo del plan de implantación propuesto y finalmente adoptado por todas las partes. En la misma línea, y de cara a una entrega a Operación más efectiva, personal del Soporte EJIE podrá participar en la ejecución del proyecto.

Asimismo, derivado de que la plataforma en concreto se utiliza para prestar diferentes servicios a las entidades, la empresa adjudicataria deberá considerar la ejecución de los servicios solicitados fuera del horario normal habitual (10pm a 7am), con el fin de reducir la afectación a las diferentes personas usuarias, según se indique por parte de EJIE/entidad en el Plan de Implantación.

### 4.3.4 Seguimiento y Control de Ejecución del Proyecto

#### 4.3.4.1 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 la empresa adjudicataria, del conjunto de metodologías y procedimientos necesarios, que garanticen las actuaciones coordinadas y faciliten el cumplimiento de planificación.
- Con relación a 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 la empresa adjudicataria, y validación del conjunto de metodologías y procedimientos necesarios para garantizar la coordinación de actividades y cumplimiento de la planificación.
    - Coordinación principal de EJIE y adjudicatarias de los soportes y otros agentes (entidad) que estén involucrados/afectados en/con la ejecución de los trabajos.
    - Verificación de cumplimiento de las condiciones para la entrega a Operación.

- Establecimiento de nuevas solicitudes de licencias de servicio (productos).
- 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.

#### 4.3.4.2 Plataforma de Gestión del Proyecto

EJIE pondrá 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.

La empresa adjudicataria y EJIE deberán interactuar directamente contra la Plataforma de gestión indicada, siendo la empresa adjudicataria el responsable último del registro y volcado de la documentación que se vaya generando.

- Datos de partida.
- Documentos sobre el diseño de la solución y plan de migración.
- Plan de Implantación.
- Documentación solicitada por Operación.
- Criterios y acuerdos relativos a la ejecución de los trabajos.
- Planificación del proyecto:
    - Planificación acordada (cerrada) de actuaciones particulares en cada tenant (despliegues, instalaciones, pruebas, etc.).
    - Informe completo de los avances de despliegue de cada tenant (entidad).
- Proyectos finales incluyendo los resultados de las instalaciones realizadas y las pruebas en los diferentes tenants.
- Cuadros de Mando de carácter ejecutivo para control de avance del despliegue y control sobre las necesidades de materiales.
- Etc.

#### 4.3.4.3 Seguimiento por Parte de la Empresa Adjudicataria

Si bien la gestión y dirección global del proyecto será llevada a cabo por parte de EJIE, la empresa adjudicataria 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, 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:

- Entidades en alcance inicial, quienes supervisa el día a día de la operativa,
- EJIE como operador de la solución de correo electrónico actual,

- Los diferentes Proveedores, que EJIE considere.

Asimismo, la empresa adjudicataria designará un Jefe 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 de migración de la infraestructura y servicios desplegados en el nuevo entorno.

El Jefe 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 (y soportes).
- Será el responsable por parte de la empresa adjudicataria 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, 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 convoque EJIE, 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.
- Realizará el seguimiento periódico sobre la calidad de los servicios de mantenimiento solicitados y será el responsable de garantizar el cumplimiento de los acuerdos de nivel de servicio asociados.

#### 4.3.4.4 Equipo de Trabajo para la Ejecución del Proyecto

El equipo de trabajo propuesto por la empresa adjudicataria 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 de la empresa adjudicataria estará dirigido por un Jefe 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 la empresa licitadora, a los tiempos y planificaciones establecidas y a los requerimientos mínimos expuestos en el presente pliego.

En cualquier caso, la empresa adjudicataria 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 a Operación, actas de servicio…) requerida en las diferentes fases de proyecto.

Asimismo, en el inicio del proyecto, la empresa adjudicataria 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 de la empresa adjudicataria.

Los componentes del grupo de trabajo desarrollarán su labor con hardware y software propiedad de la empresa adjudicataria.

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 de la empresa adjudicataria para cumplimiento de los plazos previstos.

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 la empresa adjudicataria 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.

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 requeridas para la ejecución del contrato.

A continuación, se especifican los roles mínimos identificados a los que deberá dar respuesta la empresa adjudicataria 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.
- **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.
- **Equipo para la prestación de los servicios de mantenimiento,** adecuadamente dimensionado para la prestación de los servicios con los SLAs acordados 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.

La empresa adjudicataria 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, la empresa adjudicataria 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.

## 4.4 Otros Requisitos Asociados a la Prestación del Servicio de Mantenimiento

### 4.4.1 Stock de Productos

La empresa adjudicataria podrá disponer de los elementos hardware y software de respaldo que considere necesario para asegurar los niveles de servicio comprometidos.

### 4.4.2 Medios Técnicos y Herramientas de Apoyo al Servicio

Todo el material técnico necesario para posibilitar la prestación del servicio, de acuerdo al alcance y requisitos solicitados, será responsabilidad de la empresa adjudicataria, quedando EJIE exento de cualquier obligación de suministrar dichos elementos.

La empresa adjudicataria deberá disponer de las herramientas adecuadas para el registro de las incidencias y peticiones solicitadas con relación al servicio, documentación de actuaciones para su resolución y medición de los niveles de servicio solicitados.

Asimismo, la empresa adjudicataria debe garantizar la adecuada integración de sus servicios de atención técnica con los servicios de atención técnica establecidos por EJIE, debiendo hacer uso de las plataformas

de gestión y mantenimiento del servicio dispuestas por EJIE y ajustando sus procedimientos, si EJIE así lo solicitara.

# 5 Anexos

## 5.1 Anexo I PCT_Checklist Requisitos Técnicos

Como documentación anexa a la propuesta técnica, y a modo de resumen e índice de la mayoría de los requisitos/funcionalidades de la oferta, la empresa licitadora deberá adjuntar un checklist. Este checklist no exime de detallar cada una de las funcionalidades requeridas en el PCT en la oferta, siendo ese detalle el que se valorará según los criterios indicados en PCP. Destacar que puede haber requisitos o detalles de los mismos que no estén reflejados en el checklist, debiendo responder a ellos según lo solicitado en PCT, no hay que limitarse a responder a lo solicitado en el checklist.

Este anexo (Anexo I PCT_Checklist requisitos tecnicos.xlsx) deberá ser completado por las empresas licitadoras y entregarse junto con la oferta técnica (Archivo Electrónico de Criterios de Juicio y Valor).

Para cada requisito, habrá que indicar si se cumple o no y en qué casos, rellenando para ello las columnas correspondientes a cada caso. Además, habrá que indicar en qué apartado(s) de la oferta se detalla cada requisito/funcionalidad.

Las tres primeras columnas (Correo Externo, Correo Interno y Correo OnPremise) se corresponden con la suscripción CONVERGENTE. La cuarta (Correo HEZKUNTZA) se corresponde con la suscripción HEZKUNTZA.

Eusko Jaurlaritzaren Informatika Elkartea
Sociedad Informática del Gobierno Vasco

**Requisitos Técnicos y Funcionales (Apartado 3 del Pliego de Condiciones Técnicas)**

| Requisito | Cumplimiento para Correo Externo (1) (Si/No/NA) | Cumplimiento para Correo Interno (1) (Si/No/NA) | Cumplimiento para Correo OnPremise (1) (Si/No/NA) | Cumplimiento para Correo HEZKUNTZA (1) (Si/No/NA) | Apartado(s) de la oferta en la que se describe el requisito |
|---|---|---|---|---|---|
| propuesta debe | | | | | |

Este checklist deberá ser cumplimentado por las empresas licitadoras y entregarse junto con la oferta técnica (Archivo Electrónico de Criterios de Juicio y Valor), en el caso de no ser entregado este documento cumplimentado será causa de exclusión por lo que no se procederá a la apertura del archivo electrónico de *Fórmulas* de la propuesta de la empresa licitadora que no lo incluya. Tal como se indica en el PCP del presente pliego.