Eusko Jaurlaritzaren
Informatika Elkartea

Sociedad Informática
del Gobierno Vasco

Servicios de oficina técnica para apoyo en procesos de seguridad y continuidad de EJIE

Pliego de Condiciones Técnicas

Noviembre de 2022

Mediterráneo, 14 • 01010 Vitoria-Gasteiz • Tel. 945 01 73 00* • www.ejie.eus

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

Versión	Fecha	Resumen de cambios	Elaborado por	Aprobado por
1.0	14/11/2022	Versión inicial	Agustín Moyano	Asier Ares

Índice

1 Introducción 4
1.1 Perfil de la compañía 4
2 Objeto y alcance del contrato 5
2.1 Ámbito 5
2.2 Objeto 5
2.2.1 Mantenimiento de procesos de seguridad y continuidad 5
2.2.2 Soporte seguridad a proyectos 6
2.2.3 Plataforma SaaS 6
3 Entregables 8
4 Planificación y organización 9
4.1 Plan de entregas y asignación de recursos 9
4.2 Equipo de trabajo 10
4.2.1 Constitución inicial del equipo de trabajo 10
4.2.2 Modificaciones en la composición del equipo de trabajo 10
4.3 Horario y lugar de realización de los trabajos 11
4.4 Dimensionamiento 11
4.5 Fase salida 11
5 Seguimiento y control 12

1 Introducción

1.1 Perfil de la compañía

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

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

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

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

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

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

2 Objeto y alcance del contrato

2.1 Ámbito

Actualmente se dispone de los siguientes sistemas de gestión en el ámbito de la seguridad y continuidad:

- Gestión y mantenimiento del sistema de gestión de la seguridad de la información (SGSI) (sistema maduro, certificado desde 2008)
- Gestión y mantenimiento de continuidad
- Gestión y mantenimiento del Esquema Nacional de Seguridad (ENS)
- Gestión y mantenimiento de necesidades sobre infraestructuras críticas/esenciales
- Gestión y mantenimiento de aquellos aspectos relacionados con el tratamiento de datos personales que están incluidos en los sistemas de gestión previamente indicados

Se utiliza una plataforma SaaS de apoyo tanto a las tareas como al servicio.

2.2 Objeto

El objeto del expediente es la contratación de servicios de soporte para mantener los procesos de seguridad y continuidad en el ámbito de EJIE/Batera, utilizando una plataforma SaaS como apoyo.

2.2.1 Mantenimiento de procesos de seguridad y continuidad

Gestión del SGSI, incluyendo los aspectos necesarios para el cumplimiento del Esquema Nacional de Seguridad y resto de normativa aplicable en el ámbito de la seguridad.

- Análisis y gestión de riesgos, incluyendo el modelado de activos, catálogo de amenazas, informe de resultados y propuestas de plantes de tratamiento correspondientes.
- Revisión y actualización de la declaración de aplicabilidad.
- Revisión y actualización de los planes de mantenimiento del sistema
- Planificación de auditorías, realización de las auditorías internas necesarias y de auditorías a proveedores, elaborando los informes correspondientes
- Seguimiento de normativa aplicable
- Informes de estado del sistema y revisiones por la dirección
- Gestión de indicadores y cuadros de mando, incluyendo los informes preceptivos en el ámbito del Esquema Nacional de Seguridad
- Soporte y apoyo normativo
- Soporte y apoyo en el ámbito de seguridad y cumplimiento a los responsables de otros procesos
- Apoyo a la concienciación y formación.

Gestión de continuidad:

- Revisión y gestión de la documentación sobre estrategia y política de continuidad
- Soporte y apoyo en el ámbito de continuidad a los responsables de otros procesos y en la definición de servicios
- Seguimiento del sistema: indicadores, cuadros de mando, supervisión
- Apoyo en el seguimiento de los simulacros periódicos
- Elaboración de los informes periódicos de estado de la continuidad.
- Elaboración de posibles nuevos entregables, registros e informes de estado
- Elaboración de posibles nuevos indicadores y cuadros de mando

Infraestructuras esenciales:

- Revisión y mantenimiento del plan del operador
- Elaboración, revisión y mantenimiento de los planes de protección específicos

- Elaboración de posibles nuevos entregables, registros e informes de estado

Colaboración con grupo de interés:

- Apoyo en aquellas iniciativas y proyectos que surjan con los grupos de interés en el ámbito de la seguridad y la continuidad

2.2.2 Soporte seguridad a proyectos

En el ámbito de las iniciativas de convergencia, se considera necesario dedicar recursos de soporte seguridad en los proyectos, para garantizar que la seguridad de la información sea parte integral de los sistemas durante todo el ciclo de vida.

Se debe presentar una propuesta de servicios sobre cómo mantener la seguridad durante todo el ciclo de vida de los sistemas, en especial lo relacionado con el control A14.1.1 de ISO 27001, para proyectos en el ámbito de:

1. Implantación y/o adecuación de infraestructuras para proporcionar nuevos servicios
2. Incorporación de los servicios e infraestructuras de nuevos clientes en Batera: el nivel de transformación ("transformación" o "lift & shift") puede ser variable, la incorporación en las fases que se establecieran en el análisis inicial.
3. Diseño, desarrollo, implantación y mantenimiento de aplicaciones

Se debe presentar una propuesta adecuada a cualquiera de los posibles escenarios.

Cumplimiento normativo: es necesario analizar la normativa aplicable, comprobar los niveles de cumplimiento necesarios, punto de partida del cliente (punto 2, incorporación de nuevos clientes), detectar riesgos y posibles incumplimientos, etc., redactando los correspondientes informes tanto a nivel de proyecto como ejecutivos.

Los recursos dedicados al soporte en seguridad a los proyectos de convergencia no serán inferiores a 1.500 horas/año.

2.2.3 Plataforma SaaS

Este contrato incluye, así mismo, la cesión en uso de las licencias en modo SaaS seguidamente especificadas:

- GlobalSuite módulo ISO 27001
- Delegación adicional para el módulo anterior
- GlobalSuite Data Protection

La plataforma deberá cumplir, al menos, las siguientes condiciones:

- Funcionalidad
  - Gestión de continuidad
  - Gestión de SGSI en base a ISO 27001
  - Gestión de análisis de riesgos, acciones de mejora, no conformidades, indicadores, y demás funcionalidades de gestión necesarias para el SGSI. Debe permitir gestionar la información de una empresa con dos sedes (se utilizará para la gestión del Esquema Nacional de Seguridad en el ámbito del Gobierno Vasco y EJIE).
  - Gestión RGPD

- Garantías del servicio y de seguridad
  - Acuerdos de nivel de servicio (SLAs) del prestador del servicio SaaS para el tratamiento de los datos.
  - Certificación ISO 27001 para el servicio SaaS.
  - Compromiso por parte del prestador del servicio SaaS para la devolución de los datos, configuraciones y registros en herramienta-s SaaS, que siempre serán propiedad de EJIE, en el caso que esta los requiera por cualquier circunstancia.
- Actualmente se está utilizando la plataforma Globalsuite:
  - En el caso de proporcionar otra la funcionalidad debería ser equivalente y el licitante debería asumir todo el proceso de migración, identificando claramente en la oferta todo este proceso, con la dedicación necesaria.
  - En esta plataforma las licencias necesarias son al menos:

Módulo	Alcance	Observaciones
SGSI	1 organización con dos delegaciones	EJIE y Eusko Jaurlaritza
Data Protection	1 organización	EJIE

3 Entregables

Todos los necesarios para mantener los sistemas de gestión objeto del servicio, con las normativas aplicables asociadas.

Se proporcionarán mensualmente informes de seguimiento para cada ámbito, con información sobre la dedicación, tareas y entregables del período.

Se incluyen algunos a modo de ejemplo, pero se espera que en la oferta se prepare un completo plan de entregables para cada uno de los ámbitos de los servicios, indicando su contenido.

No obstante, los entregables aquí detallados se deben considerar como una primera aproximación, es decir, para cada fase del servicio se deberá acordar entre la empresa adjudicataria y la Dirección del Proyecto todos y cada uno de los entregables a generar, así como el "contenido" detallado de cada uno de ellos, convenidos con el objetivo de asegurar la calidad final del servicio realizado.

Ejemplos:

- Declaración de aplicabilidad y alcance
- Cuadro de mando de indicadores
- Formación: propuesta de contenidos y al menos 10 píldoras formativas
- Plan e informe de auditoría interna
- Planes e informes de auditorías a proveedores
- Programa de mantenimiento del SGSI
- Modelado de activos, modelado de amenazas, informe resultado de análisis de riesgos
- Seguimiento cumplimiento ENS, informes periódicos de dicha adecuación e informe INES.
- Informes de estado de seguridad
- Cualesquiera otros que el licitador considere necesarios para la gestión y operación del sistema

4 Planificación y organización

4.1 Plan de entregas y asignación de recursos

Se deben estimar los esfuerzos asociados a su ejecución, tanto por parte del licitador como por parte de EJIE y se debe proponer una planificación temporal de las tareas y actividades en función de las necesidades y requisitos específicos para el mantenimiento de los sistemas de gestión mencionados. Se debe determinar cuáles quedan a su cargo y las que corresponden a EJIE.

Para ejecutar el servicio, el licitador debe tener en cuenta lo siguiente:

- Detallar las tareas y actividades a desarrollar para llevar a cabo el correcto mantenimiento del proceso.
- Llevar a cabo una estimación de los costes asociados por cada participante y perfil a cada una de las tareas y actividades definidas.
- Desarrollar una planificación objetiva de las tareas y actividades definidas, en función de los recursos disponibles previstos.

Se debe preparar una tabla similar a esta propuesta para cada uno de los ámbitos del servicio.

En la misma se debe identificar expresamente en qué tareas participan los roles acreditados en gestión de continuidad y en dirección de seguridad privada.

Descripción Perfil	Fase 1		Fase 2		Fase 3		…		Fase N		Total Horas
	horas	%	horas	%	horas	%	horas	%	horas	%	
Perfil 1											
Perfil 2											
Perfil 3											
…											
TOTAL											

No se considerarán aceptables aquellas propuestas cuyo planteamiento total sea inferior a:

- 1500 horas anuales para el mantenimiento de procesos de seguridad y continuidad.
- 1500 horas anuales para el apoyo a proyectos

4.2 Equipo de trabajo

El licitador se compromete, en caso de ser adjudicatario, a mantener el equipo, según lo establecido en el Documento de Propuesta Técnica, y durante el periodo fijado en cada actividad específica. Los recursos asignados a la ejecución del contrato deberán estar asignados desde el inicio del mismo. En el caso de modificación o sustitución de recursos, deberá comunicarlo previamente a EJIE, con la antelación necesaria en función de la criticidad del servicio, y en cualquier caso al menos 15 días naturales previos a la realización del cambio de recurso, y EJIE aprobará o rechazará dicha modificación o sustitución. En todo caso el sustituto o sustitutos tendrán un perfil igual o superior al ofertado, o recurso a sustituir.

EJIE podrá solicitar el cambio de los recursos asignado a los servicios, por inadecuación de los recursos o por incumplir los requisitos tanto de solvencia como técnicos exigidos, o haber declarado el contratista unas circunstancias que no son veraces, en cuyo caso podrá conllevar la rescisión del contrato y adjudicación al licitador siguiente en las calificaciones.

4.2.1 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 observara 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 EJIE
- Caso de que se demostrase que el cambio no se corresponde con causa justificada, EJIE 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.

4.2.2 Modificaciones en la composición del equipo de trabajo

La valoración de la calidad de los servicios objeto del presente pliego corresponde al responsable del servicio de EJIE, 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 EJIE

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 del responsable del servicio de EJIE, esto no fuera posible, las dos primeras semanas de trabajo del sustituto/s no serán facturables corriendo a cargo del adjudicatario.

4.3 Horario y lugar de realización de los trabajos

Horario de oficina, según horario de EJIE:

- Jornada partida: referencia
  - Lunes a jueves: 8h a 17h.
  - Viernes: 8h a 15h
- Jornada intensiva (junio a septiembre): referencia
  - Lunes a viernes 8h a 14:30h

El servicio se prestará habitualmente en las siguientes ubicaciones:

- Oficinas de EJIE, sitas en Vitoria-Gasteiz, en Avenida del Mediterráneo 14
- En función de las necesidades del servicio podrá ser necesaria presencia puntual en otras ubicaciones (alcance geográfico de País Vasco) como, por ejemplo, auditorías o reuniones en distintos organismos vinculados con EJIE.

Al menos el 75% del servicio asociado al mantenimiento de procesos de seguridad y continuidad se prestará en las ubicaciones establecidas por EJIE. Se considera necesario que gran parte del servicio se proporcione en las mencionadas oficinas dado el nivel de confidencialidad requerido por la información tratada y la necesaria cercanía con los responsables de procesos, servicios y proyectos de la organización así lo requieren.

El adjudicatario asumirá en su propuesta los gastos derivados de los desplazamientos, dietas etc., que tengan lugar, así como aquellos derivados de la disposición de los medios correspondientes para los mismos, y en general para la ejecución del proyecto en las condiciones de presencialidad indicadas.

4.4 Dimensionamiento

Los recursos con los que se dimensione el servicio dependerán de las ofertas presentadas, pero se considera, y por tanto es un requisito mínimo, que para cubrir los roles planteados al menos es necesario que el equipo tenga la capacidad equivalente a:

- Al menos 1.500 horas anuales para el ámbito de EJIE/Batera para mantenimiento de sistemas de gestión
- Al menos 1.500 horas anuales para el ámbito de EJIE/Batera para el soporte a proyectos

4.5 Fase salida

En la oferta se deberá presentar claramente la fase de salida al finalizar el contrato indicando el esfuerzo necesario.

El plazo máximo para la fase de salida no será superior a una semana. Esta fase de salida deberá llevarse a cabo tras la finalización del período del presente contrato o su prórroga sin costo adicional para EJIE.

5 Seguimiento y control

El equipo de trabajo estará dirigido por un Responsable del Servicio con dedicación estable y suficiente, quien coordinará las tareas implicadas en el servicio y será el interlocutor principal con la Dirección del Proyecto.

Deberán establecerse todos los mecanismos de control que permitan verificar de forma continuada el cumplimiento de los objetivos especificados, tanto en plazos como en términos de calidad final. Para ello se contempla:

- Reuniones de seguimiento: periódicamente se celebrarán reuniones destinadas a revisar el grado de cumplimiento de las tareas planificadas, las programaciones de actividades a realizar, etc.
- Informes de situación y progreso: con los que la empresa adjudicataria comunicará a la Dirección del Proyecto el estado puntual de los trabajos, de los objetivos alcanzados, de las incidencias ocurridas, etc. Estos informes deberán quedar adecuadamente registrados y formalizados.
- Documentos de gestión de proyectos/servicios: la empresa adjudicataria cumplimentará los documentos de gestión de proyectos/servicios, según un modelo definido (actas de reuniones, informes de progreso, etc.
- Entregables: puesto que se propone un proceso iterativo de entregas, periódicamente se entregarán los productos obtenidos (documentación, código, etc.) obtenidos con independencia de su calificación de “definitivos” o no.