Eusko Jaurlaritzaren
Informatika Elkartea

Sociedad Informática
del Gobierno Vasco

Servicios para el Diseño e Implantación de Audit Vault

Pliego de condiciones técnicas

Mayo 2022

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

Este documento es propiedad de Eusko Jaurlaritzen 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 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	07/2021	Versión inicial	Iratxe Montoya	Aritza Iratzagorria

Índice

1 Introducción 4
1.1 Perfil de la compañía 4
2 Situación Actual 6
3 Objeto del contrato 7
4 Alcance de la contratación 8
4.1 Diseño de la Solución Audit Vault 8
4.2 Instalación / Configuración y Pasos Post de la Solución Audit Vault 8
4.3 Modelado de Servicio como parte de la oferta de Hosting Avanzado 9
4.4 Migración y Despliegue de Políticas de Auditoría (Primera Fase) 9
4.5 Migración y Despliegue de Políticas de Auditoría (Segunda Fase) 9
5 Requisitos de los lotes de Servicios a contratar 11
5.1 Metodología 11
5.2 Seguimiento 11
5.3 Entregables 11
6 Organización del equipo de trabajo 11
7 Condiciones de Seguridad/Generales 13

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 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.

2 Situación Actual

En la actualidad EJIE alberga en BBDD's Oracle distintas tipologías de aplicaciones, provenientes de distintas entidades/organismos públicos, entre las cuales se encuentran aplicaciones que contienen datos de nivel alto.

El acceso a datos de nivel alto requiere medidas de seguridad para poder garantizar la confidencialidad del dato y poder cumplir la normativa de seguridad establecida.

Hoy en día, cada entidad / organismo público emplea distintos mecanismos para garantizar la confidencialidad y en el caso concreto de las aplicaciones de EJGV existe una solución desarrollada por Oracle Consulting, cuyo nombre es OSA (Oracle Selective Audit) que permite la gestión de las trazas de acceso a los datos de Nivel Alto.

Con el paso del tiempo y debido a distintos motivos: volumen de trazas albergado, número de base de datos auditada, incorporación de nuevas aplicaciones / datos a auditar, incremento del tiempo a mantener las trazas, …
Se han detectado ciertos errores en la solución que es necesario subsanar y que ponen en riesgo la garantía de trazabilidad tal y como requiere la LOPD.

Además,en 2022 se va a abordar un proyecto de evolución de las BBDD's Oracle a una versión Oracle 19c y la versión de OSA actual no es compatible con dicha versión.

Por ello y aunque a corto, se van a tomar algunas medidas que van a poder paliar los problemas, se requiere evolucionar la solución a un producto de mercado, en este caso Audit Vault, que:

- Cubre como mínimo todos los escenarios cubiertos por OSA en la actualidad, tal y como se concluyó en la prueba de concepto elaborada en 2019.
- Cubre los requerimientos de seguridad exigidos por la ley en la actualidad y evoluciona alineado con los nuevos requerimientos que la ley pueda exigir.
- Permite gestionar la trazabilidad en las distintas versiones de BBDD's Oracle prevista en Road Map
- Existe conocimiento en el mercado por parte de distintos proveedores que pueden dar respuesta a nuevos escenarios que pueden surgir, como evolución de las aplicaciones: mayor volumen de trazas, más campos a auditar…
- Existe un soporte de primer nivel con garantías por parte del fabricante a nivel de producto.
- Existe un marco de licencias que nos permite implantar la solución así como proponerla al resto de Entidades / Organismos públicos como una solución de trazabilidad de acceso a datos.

3 Objeto del contrato

El objeto del contrato es la adquisición de servicios para realizar:

- Diseño / Arquitectura de Solución de Oracle Audit Vault.
- Instalación / Configuración y Pasos Post de la Solución.
- Modelado del Servicio como parte de la oferta de Hosting Avanzado: Catálogo de Servicio y Catálogo IT asociado, Configuración en CMDB, Tarifas, … para que la solución se pueda consumir por parte de las distintas Entidades / Organismos Públicos.
  También se deberán concretar la Definición de Roles participantes en la solución y Responsabilidades de los mismos, así como la alineación de la solución con los procesos existentes en EJIE
- En el caso concreto de las aplicaciones de EJGV los servicios contratados deberán acompañar al proyecto de migración a Oracle 19c (fuera del alcance de este pliego), siendo responsabilidad de esta contratación, las tareas de migración de la solución de trazas actual OSA (Oracle Selective Audit) a la nueva solución, Audit Vault en dos fases.
  - Primera Fase: Análisis, Diseño, Migración y Despliegue de Políticas de Auditoría en un número representativo de BBDD's / Aplicaciones
  - Segunda Fase: Análisis, Migración y Despliegue de Políticas de Auditoría en el resto de BBDD's / Aplicaciones

4 Alcance de la contratación

A continuación, se detalla el alcance de las tareas a realizar por parte del servicio.

4.1 PRIMERA FASE

4.1.1 Diseño de la Solución Audit Vault

Se deberá realizar el diseño de la solución de Audit Vault, incluyendo en el mismo:

- Arquitectura (deberá incluir tanto la solución del producto, consolidación de trazas, … como la parte correspondiente a las BBDD's origen en las que se van a generar las trazas)
- La solución deberá disponer de un entorno Auxiliar y uno de Producción (el objetivo del primero será disponer de un entorno en el que se puedan realizar todas las pruebas necesarias, actualización de ciclo de vida, … podría barajarse como alternativa en caso de indisponibilidad del principal)

- Requisitos Hardware
- Requisitos Software
- Requisitos de Comunicaciones / Seguridad
- Requisitos de Integración con terceros
- …

De este modo siguiendo dichas indicaciones, se podrán aprovisionar los requerimientos necesarios junto con los equipos técnicos de Batera.

La solución / arquitectura:

- Deberá ser consumida como servicio por parte de las distintas entidades / organismos públicos
- Estará integrada y alineada con los distintos procesos existentes en Ejie: Seguridad, Servicios de Soporte, Operación, Entregas, Despliegues, Gestión de incidencias, Problemas
- Dispondrá de mecanismos que garanticen la continuidad del servicio (disponibilidad, contingencia)
- Dispondrá de una solución de Backup y Recuperación.
- Deberá disponer de monitorización adecuada y de un número de informes que garantice:
    - La disponibilidad del Producto
    - Los procedimientos de Auditoria se realizan correctamente, tanto en el momento de ser activados, como en el ciclo de vida de la aplicación.

4.1.2 Instalación / Configuración y Pasos Post de la Solución Audit Vault

Como parte de este punto el servicio contratado deberá:

- Descarga y validación del Software de Audit Vault 20C (valorar superior si existiera en el momento de implantación)
- La versión, a descargar e instalar se deberá concretar y consensuar con EJIE en la fase de Diseño de la solución
- Instalación / Despliegue Audit Vault en entorno Auxiliar y entorno Producción
- Configuración de la solución e Integración con terceros: Bases de Datos Origen, Solución de Directorio, ...
- Plan de Pruebas y Aceptación de la solución
- Puesta en Productivo de la solución

4.1.3 Modelado de Servicio como parte de la oferta de Hosting Avanzado

Desde el proyecto se deberá trabajar en que la solución de Auditoría pueda consumirse por parte de los clientes que dispongan soluciones de BBDD's Oracle en el ámbito de Hosting Avanzado.

Para ello se deberá trabajar en:

- Plasmar la solución de CMDB
- Definir e implementar el catálogo IT de la solución
- Definir e implementar el catálogo de Servicio de la solución
- Definir los roles a participar tanto en la construcción como en el ciclo de vida de la solución, concretar las responsabilidades de los mismos, y trabajar en el proyecto para que tras su finalización las tareas y compromisos a asumir por cada uno estén claros y asumidos por parte de EJIE
- Garantizar la alineación del servicio con los distintos procesos existentes en EJIE: gestión de la configuración, gestión de la capacidad, gestión de incidencias, gestión de problemas, gestión de peticiones,

4.1.4 Análisis, Migración y Despliegue de Políticas de Auditoría (Primera Fase)

Como parte de esta fase, se deberán analizar las políticas existentes en un número representativo de las BBDD's / aplicaciones de EJGV, mínimo deberán ser cuatro BBDD's y 8 apliaciones, pero se valorará de forma positiva el incluir un mayor número de BBDD's / aplicaciones en esta fase, para una vez analizadas proceder a su activación / migración en las nuevas BBDD's Oracle 19c

En la actualidad las políticas existentes en las BBDD's origen se corresponden con el modelo de Auditoría Mixta pero tras la migración al activarse en las BBDD's Oracle 19c destino deberán activarse en el modelo de Auditoría Unificada.

Por lo tanto, en dichas BBDD's / aplicaciones se deberá:

- Elaborar y ejecutar el procedimiento de análisis de las auditorías existentes en las BBDD's origen estimadas
- Concretar el modelo de las políticas de auditoría unificada a crear en las BBDD's destino
- Elaborar y ejecutar el procedimiento de migración / activación de las BBDD's destino
- Realizar propuesta y ejecución de pasos a seguir para mantener las trazas consolidadas correspondientes a la auditoria actual
- Elaborar y ejecutar procedimiento de validación que confirme que la migración de las trazas se ha realizado de forma correcta.
- Fijar y concretar monitorizaciones, automatizaciones, … que garanticen la correcta implantación de la solución, así como la correcta evolución de la misma

4.2 SEGUNDA FASE

4.2.1 Análisis, Migración y Despliegue de Políticas de Auditoría (Segunda Fase)

Una vez finalizada la fase Inicial en la que se ha trabajado en los puntos indicados en el 4.1, deberá existir una propuesta de servicio en la que exista mínimo un perfil que colabore con el proyecto de Migración Oracle 19c (fuera del alcance de esta contratación), en la migración del resto de aplicaciones existentes con solución de auditoría activa, siguiendo los pasos establecidos en el punto anterior.

Mínimo uno de los perfiles que participe en este fase deberá haber participado en la fase anterior para poder dar continuidad a lo establecido y trabajado en la primera fase.

5 Requisitos de los lotes de Servicios a contratar

A continuación, se detallan los puntos a tener en cuenta en los servicios a contratar.

5.1 Metodología

El trabajo a realizar se deberá organizar como proyecto de implantación de soluciones software y deberá seguir metodología PMP y mejores prácticas ITILv3 y el marco IT4IT.

En la oferta se deberá presentar una propuesta de la metodología a seguir identificando claramente cómo se organizará el trabajo.

5.2 Seguimiento

A continuación, se detalla una propuesta a modo ejemplo de seguimiento del proyecto. La oferta deberá presentar una propuesta de similares características, explicándola con detalle y pudiendo ofrecer propuestas de mejora sobre la misma

	Objetivo	**Participantes EJIE**	**Entregables**
Comité de Seguimiento (quincenal) *pudiera ser necesario que fuera con mayor frecuencia en fases críticas o ante necesidades puntuales del proyecto	Revisión del Estado del proyecto y tareas asociadas	Responsable tecnológico Responsable Plataformas	Información relevante Acta Informes de Situación y Progreso

5.3 Plan de Trabajo y Entregables

La contratación deberá especificar el plan de trabajo de cada una de las fases e hitos existentes en la mismas, describiendo las tareas a realizar en cada casa, duración, y recursos estimados para las mismas.

La empresa adjudicataria como parte del servicio deberá proporcionar los entregables, correspondientes a cada uno de los puntos expuestos en las distintas fases. Dichos entregables además de dejar plasmado el trabajo realizado deberán permitir el uso de la solución en el día +1.

La propuesta de la empresa proveedora deberá detallar los entregables de cada fase indicando descripción, contenido y objetivo de los mismos.

5.4 Organización del equipo de trabajo

El equipo de trabajo deberá incluir los siguientes roles:

Jefatura de Proyecto por parte del servicio a contratar:

Este rol deberá tener dedicación a tiempo parcial ya que, aunque desde EJIE se asumirá dicha Jefatura de Proyecto bien con personal de EJIE o bien con la colaboración de otros servicios existentes en la actualidad, se requerirá que participe en las reuniones de seguimiento quincenales encargándose tanto de la realización de las actas como de los informes de situación y progreso.

Deberá velar por la correcta evolución del proyecto y será el interlocutor con EJIE para trasladar las distintas problemáticas, … que pudieran surgir

Consultor/a Técnico de la solución:

Este rol deberá participar en las fases de Diseño / Implantación de la Solución y Modelado del Servicio, así como en la primera fase de migración de las políticas.

Técnicos/as:

Este rol deberá acompañar al consultor técnico en la fase de implantación para ser conocedor de la solución, así como participar en la fase I y fase II de migración de las políticas.

El dimensionamiento de los perfiles a cubrir este rol no ha de ser el mismo en ambas fases

La propuesta de equipo, organización, nº de perfiles por cada rol, responsabilidades y funciones de los mismos … en cada una de las fases e hitos presentados en el alcance, deberán ser detalladas por la empresa proveedora en su propuesta y serán valorables como parte de la solución.

6 Condiciones de Seguridad/Generales

EJIE S.A. proporcionará acceso a sus sistemas informáticos y entregará la información, software y documentación necesaria para poder llevar a cabo los Servicios especificados, debiendo la empresa adjudicataria comprometerse a no utilizar para otros fines que los recogidos en el presente Pliego de Condiciones Técnicas, así como a no extraerla, cederla, publicarla o venderla total o parcialmente, ni en soporte informático ni en papel, debiendo proceder a la devolución de los soportes de la información facilitados por EJIE, S.A: , así como a la descarga de la misma de los equipos informáticos (si existieran), una vez se dé por concluido el trabajo. **Queda terminantemente prohibido:**

- El uso de estos recursos para actividades no relacionadas con el propósito del negocio, o bien con la extralimitación en su uso.

Serán también de obligado cumplimiento las "*Políticas de Seguridad para personal de empresas proveedoras*" (accesible en la web www.ejie.eus). El servicio objeto del presente pliego se proporcionará desde las oficinas de la adjudicataria, de modo que:

- Según el apartado "Aplicabilidad de las Políticas Específicas de Seguridad para Proveedores" de dichas políticas:
  - El lugar de ejecución del servicio tendrá la consideración de "remoto".
  - La propiedad de las infraestructuras TIC utilizadas tendrá la consideración "del proveedor".
  - El "nivel de acceso" a los sistemas de EJIE tendrá la consideración de "con acceso privilegiado".
- Serán de aplicación las políticas específicas de seguridad según la tabla del apartado 4.1, entre ellas las correspondientes a "seguridad física" (apartado 4.5).
- EJIE, tal como se indica en el apartado 3.6.c se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.

La adjudicataria además se compromete al cumplimiento y a proporcionar la información solicitada en el documento "Anexo – *Política de Seguridad para empresas proveedoras – Anexo I Infraestructura TIC / Seguridad física y del entorno*" que se encuentra en el Anexo Seguridad de este documento. Esta información será utilizada en las auditorías que se realizarán periódicamente. Será obligación de la adjudicataria proporcionar esta información anualmente y ante cualquier cambio significativo en su contenido.

El servicio objeto del presente pliego realizará labores de administración sobre los entornos responsabilidad de EJIE. EJIE se reserva el derecho de exigir al adjudicatario la implantación de medidas de seguridad específicas que deberá acometer en el plazo indicado, suponiendo el incumplimiento de esa implantación la penalización correspondiente especificada en el PCP.

Como referencia, sin que suponga un compromiso inicial, se especifican los siguientes ejemplos de posibles elementos a exigir:

- El proveedor deberá proporcionar, bajo solicitud de EJIE, desde el momento en que se solicite, dispositivos hardware que permitan la identificación y el acceso a los sistemas con suficientes garantías. Estos dispositivos podrán ser:
  - Teléfono móvil corporativo (Android o iOS), con sistema operativo actualizado, capaz de utilizar la APP del servicio de IDaaS implantado.
  - Dispositivos hardware homologados por EJIE:
    - Compatibles FIDO FIDO Alliance - Open Authentication Standards More Secure than Passwords y Okta https://www.okta.com).
    - A la fecha del presente expediente, Yubikey 5 NFC. Consultar en el futuro.
- El proveedor deberá proporcionar, bajo solicitud de EJIE y en un plazo de 6 meses desde su solicitud, la utilización por parte de los administradores de equipos específicos (físicos o virtuales) securizados utilizados exclusivamente para las labores de administración, debiendo utilizar equipos diferentes para sus labores no administrativas (email, navegación, ofimática, etc.). Como referencia, en algunos ámbitos este tipo de soluciones se denominan Estaciones de Acceso Privilegiado (PAW).