



Eusko Jurlaritzaren  
Informatika Elkarte

Sociedad Informática  
del Gobierno Vasco

# **Solución de anonimización y seudoanonimización y Servicios de soporte y mantenimiento**

Pliego de Condiciones Técnicas

Junio 2026

Este documento es propiedad de Eusko Jauriaritzaren Informatika Elkarte – 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     | 01/06/2026 | Versión inicial    | Leire Rojo<br>Aitor Cabero | Iratxe Montoya |

## Índice

|          |                                                                   |          |
|----------|-------------------------------------------------------------------|----------|
| <b>1</b> | <b>Introducción .....</b>                                         | <b>4</b> |
| <b>2</b> | <b>Situación Actual .....</b>                                     | <b>5</b> |
| <b>3</b> | <b>Objeto del contrato.....</b>                                   | <b>6</b> |
|          | 3.1 Objeto y alcance del producto y servicio.....                 | 6        |
| <b>4</b> | <b>Requisitos de la solución .....</b>                            | <b>8</b> |
|          | 4.1 Requisitos funcionalidades .....                              | 8        |
|          | 4.2 Requisitos técnicos .....                                     | 9        |
|          | 4.3 Requisitos de seguridad, cumplimiento y certificaciones ..... | 11       |
|          | 4.4 Licenciamiento y onboarding .....                             | 12       |

# 1 Introducción

**EJIE**, Eusko Jauriaritzaren Informatika Elkarte – 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>

## 2 Situación Actual

En la actualidad existen distintas iniciativas en el ámbito del dato estructurado y no estructurado, correspondientes tanto a EJGV como a otros organismos / entidades convergentes que hacen uso de información que contiene datos personales u otra tipología de datos que por su sensibilidad requieren ser anonimizados o seudoanonimizados.

Hoy en día, los distintos equipos de trabajo realizan la anonimización o seudoanonimización mediante soluciones no estandarizadas: uso de scripts específicos, transformación de datos o reglas de ETL, uso de algoritmos de cifrado, ...

Es una situación artesanal, distribuida o fragmentada, reactiva y poco coherente en materia de anonimización y seudoanonimización de datos. No porque falten iniciativas o necesidad, si no precisamente por lo contrario: cada ámbito, cada proyecto y, en ocasiones, cada proveedor ha ido resolviendo el problema de forma aislada, utilizando técnicas distintas, herramientas diferentes y criterios no siempre alineados entre sí.

El objeto de contratación del presente pliego se encuadra dentro de la prestación de servicios a contratar mediante encargo, por parte de las entidades integrantes del sector público de la Comunidad Autónoma de Euskadi, a través de sociedades que tengan la condición de medio propio de acuerdo con la legislación vigente. EJIE, como sociedad pública, órgano gestor tecnológico y medio propio, tiene encomendada la gestión centralizada de contratación, de conformidad con el Decreto 36/2020, de 10 de marzo, por el que se regula el Modelo de Gestión de las Tecnologías de la Información y la Comunicación en el Sector Público de la Comunidad Autónoma de Euskadi.

## 3 Objeto del contrato

### 3.1 Objeto y alcance del producto y servicio

El objeto del contrato es dotarse de una solución , en concreto una plataforma SaaS y servicios profesionales que den soporte y mantenimiento sobre la misma, de anonimización y seudonimización de datos, orientada a la protección de información sensible en entornos estructurados y no estructurados, garantizando el cumplimiento normativo, la seguridad de la información y la habilitación en iniciativas de compartición de datos, copias entre entornos, uso analítico, o similares.

La solución deberá permitir la aplicación de técnicas de anonimización y seudonimización sobre conjuntos de datos personales, sensibles o confidenciales, garantizando la irreversibilidad del proceso de anonimización cuando sea exigible, así como la adecuada gestión de claves o información adicional en los procesos de seudonimización, todo ello conforme a lo dispuesto en la normativa vigente en materia de protección de datos personales.

La solución deberá cumplir con los principios y obligaciones establecidos en la normativa aplicable en materia de protección de datos personales y seguridad de la información, asegurando en todo momento la confidencialidad, integridad, disponibilidad y resiliencia de los datos tratados.

Una vez que se configure inicialmente la plataforma serán necesarias horas de servicios para dar soporte y mantenimiento sobre la misma. Por lo tanto, se requieren horas de soporte avanzado y mantenimiento evolutivo y adaptativo por parte del adjudicatario para una vez realizada la configuración inicial de la solución, poder adecuar la misma a necesidades particulares de EJIE o sus clientes que pudieran surgir a lo largo del contrato.

Dichos servicios de soporte y mantenimiento deberán ser suministrados por el propio fabricante de la solución, o por la adjudicataria autorizado por el fabricante.

Una vez configurada la plataforma, será necesario disponer de los servicios de soporte y mantenimiento a contratar:

#### De forma fija:

Los servicios de soporte técnico y mantenimiento correctivo.

|                                |           |
|--------------------------------|-----------|
| Horas de mantenimiento anuales | 150 horas |
|--------------------------------|-----------|

#### De forma variable:

Los servicios de mantenimiento evolutivo y adaptativo.

|                                |           |
|--------------------------------|-----------|
| Horas de mantenimiento anuales | 150 horas |
|--------------------------------|-----------|

En resumen, el alcance del contrato comprenderá:

- La configuración e integración de la solución con los sistemas corporativos de EJIE
- Los servicios de formación a los usuarios designados por EJIE.
- Los servicios de soporte técnico, mantenimiento correctivo, evolutivo y adaptativo durante la vigencia del contrato.
- La actualización de la solución para garantizar su adecuación a cambios normativos o tecnológicos.

## 4 Requisitos de la solución

Los requisitos descritos en este apartado deben estar disponibles en la solución en el momento de la presentación de la oferta.

### 4.1 Requisitos funcionalidades

#### 4.1.1 Capacidades de anonimización y seudonimización

- Anonimización irreversible y seudonimización reversible
- Soporte de múltiples técnicas de sustitución:
  - Enmascaramiento (blacklining, asteriscado).
  - Tokenización basada en clasificación de entidades (persona, localización, fecha, etc.).
  - Generación de datos sintéticos equivalentes en tipología y extensión.
- Mantenimiento de consistencia en la sustitución en procesos de tokenización.
- Posibilidad de reversión segura en procesos de seudonimización mediante mecanismos criptográficos.

#### 4.1.2 Identificación inteligente de datos

- Identificación automática de datos personales mediante tecnologías de procesamiento de lenguaje natural (NLP) y análisis contextual.
- Uso de modelos NER (Named Entity Recognition) propios ya entrenados, sin dependencia de servicios SaaS o LLMs de terceros
- Capacidad de detección en texto libre, documentos complejos y campos no estructurados.
- Capacidad de detección de texto en orientación horizontal y vertical.

#### 4.1.3 Configuración avanzada

- Configuración personalizable por iniciativas o proyectos:
  - Inclusión/exclusión de tipologías de datos.
  - Listas blancas y listas negras.
  - Definición de excepciones positivas y negativas.
- Activación/desactivación de tipologías de datos mediante configuración.

#### 4.1.4 Supervisión y control

- Posibilidad de supervisión manual del resultado de la anonimización.
- Interfaz visual que permita:
  - Revisar entidades detectadas.
  - Incluir/excluir datos del proceso.
  - Aplicar cambios globales en el documento.

#### 4.1.5 Procesamiento

- Procesamiento en tiempo real (online).
- Procesamiento batch (por lotes), incluyendo:
  - Carga de múltiples documentos.
  - Monitorización del estado.
  - Descarga masiva de resultados.
- Procesamiento de bases de datos con selección de tablas y campos.

#### 4.1.6 Tratamiento de firmas, códigos e imágenes

Deberá permitir la anonimización de:

- Firmas digitales
- Firmas manuscritas
- Códigos QR
- Códigos de barras
- Logos e imágenes

#### 4.1.7 Idiomas

La solución deberá permitir anonimizar y seudoanonimizar en al menos en los siguientes idiomas:

- Castellano
- Euskera
- Inglés

### 4.2 Requisitos técnicos

#### 4.2.1 Formatos en datos no estructurados

La solución deberá soportar la anonimización o seudoanonimización de:

- Documentos ofimáticos (.doc, .docx, .xls, .xlsx, .ppt, .pptx)
- Texto plano (.txt)
- PDF
- Imágenes (.jpg, .jpeg, .png, .tiff)
- Emails (.eml / .msg)
- JSON
- Extracción de texto mediante OCR asistido por IA.

#### 4.2.2 Datos estructurados

La solución deberá permitir la conexión al menos a las siguientes bases de datos relacionales:

- Oracle
- SQL Server

- MySQL
- PostgreSQL
- Bases de datos relacionales nativas de cloud pública como pueden ser AWS, Azure o GCP

#### 4.2.3 Tipologías de datos

El sistema deberá incluir, al menos, las siguientes tipologías predefinidas:

- Dirección
- Email
- Fecha
- IBAN
- IP (IPv4 / IPv6)
- NIF/NIE
- Seguridad Social
- Pasaporte
- Teléfonos
- Matrículas
- URLs
- Entidades jurídicas
- Cantidades monetarias
- Normativa (leyes, decretos)

Y debe permitir ampliación/customización de dichas tipologías.

#### 4.2.4 Arquitectura y despliegue

- Acceso mediante:
  - Interfaz gráfica (web).
  - API REST para integración.
- Modalidades de despliegue SaaS con recursos dedicados y posibilidad de segmentar en múltiples clientes
- La solución deberá ofrecer el servicio SaaS desde CPDs ubicados en regiones de la Unión Europea.

#### 4.2.5 Seguridad

La solución deberá cumplir con:

- Cifrado de metadatos mediante AES-256.
- Hashing seguro de credenciales (Argon2 o equivalente).
- Comunicación segura mediante HTTPS (TLS 1.2 o superior).
- No persistencia de documentos tras el procesamiento.
- Protección de metadatos en procesos reversibles.

## 4.3 Requisitos de seguridad, cumplimiento y certificaciones

La solución deberá cumplir con altos estándares en materia de seguridad de la información, privacidad y cumplimiento normativo, acreditables mediante certificaciones oficiales vigente, las cuales se detallan en este apartado.

### 4.3.1 Requisitos de seguridad técnica

La solución deberá garantizar:

- Cifrado de la información en tránsito mediante protocolos seguros (TLS 1.2 o superior).
- Cifrado de información sensible en reposo, incluyendo metadatos asociados a procesos de seudonimización.
- Uso de algoritmos robustos de seguridad (ej. AES-256 para cifrado, Argon2 o equivalente para hashing de credenciales).
- No persistencia de datos procesados tras la anonimización, salvo requerimiento explícito.
- Protección de accesos mediante autenticación segura.
- Registro de actividad (logging) y trazabilidad de procesos.

### 4.3.2 Cumplimiento normativo

La solución deberá facilitar el cumplimiento de:

- A nivel europeo cumplir con el Reglamento General de Protección de Datos (RGPD).
- A nivel nacional cumplir con la LOPDGDD que adapta la europea y detalla aspectos específicos.
- NIS 2 – Normativa marco de ciberseguridad en torno a redes y seguridad de la información

Asimismo, la anonimización o seudonimización deberá garantizar que los datos resultantes no tengan valor explotable en caso de fuga o acceso no autorizado.

### 4.3.3 Arquitectura segura

El sistema deberá:

- Estar desplegado en entornos protegidos (VPC, firewalls, control de puertos).
- Despliegues en entornos cloud
- Garantizar comunicaciones seguras entre componentes propios de la solución, así como con componentes ajenos como, por ejemplo, bases de datos operacionales
- Asegurar que los accesos administrativos se realizan mediante canales seguros (ej. SSH).

## 4.4 Licenciamiento y onboarding

El licenciamiento SaaS basado en suscripción deberá incluir:

- **Procesamiento**, al menos un procesamiento anual mínimo de 1 TB de datos
- **Documentación**, oficial de la solución
- **Nuevas versiones**, actualizaciones y mejoras funcionales
- **Soporte fabricante**, a través de creación de tickets con horario de atención en horario de servicio requerido de 8h a 17h, de lunes a viernes
- **Onboarding a la solución**, donde el fabricante de la solución deberá realizar las siguientes tareas:

### 4.4.1 Configuración e integración con los sistemas corporativos

Configuración de la solución e integración de la misma con los sistemas corporativos de EJIE, los cuales comprenden:

- Configuración via VPN entre la solución en cloud y el cloud híbrido de EJIE, que comprende tanto cloud pública como infraestructura on premise en CPDs propiedad de EJIE
- Configuración de la solución para ofrecer servicio a múltiples clientes con aislamiento a nivel de accesos y permisos, orígenes de datos, plantillas, etc.
- Configuración e integración con solución de identidades corporativas tanto de EJIE, como de cliente. A fecha de elaboración de este documento se contemplan Okta y Microsoft EntraID
- Configuración de conexión contra una base de datos relacional on premise, y otra en cloud pública
- Configuración del API de la solución para que se permita el uso desde desarrollos desplegados tanto en on premise, como en cloud pública

### 4.4.2 Formación en la solución

La formación estará incluida con la suscripción SaaS estará orientada a dos perfiles objetivo:

- Dos sesiones de 4 horas cada sesión orientadas a un perfil funcional o usuario de la solución. Esta formación deberá contemplar al menos formación en:
  - uso de la consola UI de la solución
  - uso de los canales de integración con bases de datos, API, etc.
- Tres sesiones de 4 horas cada sesión orientadas a un perfil administrador de la solución. Esta formación deberá contemplar al menos formación en:
  - configuración de la integración vía API
  - configuración y mantenimiento de conectores a orígenes de datos
  - configuración y mantenimiento de identidades, grupos, permisos y accesos