

Evaluación de impacto (EIPD)

EVALUACIÓN DE IMPACTO EN PROTECCIÓN DE DATOS (EIPD)

Artículo 35 del Reglamento (UE) 2016/679 (RGPD)

Tratamiento: **Generación de documentos administrativos con inteligencia artificial - Módulo Edilia**

DATOS DE LA EVALUACIÓN

Responsable del tratamiento	La entidad cliente, CIF Representado/a por ,
Encargado del tratamiento	Edilia Tech, S.L., CIF B-27552728 Roberto López Miquel, Administrador
Responsable de la EIPD	Edilia Tech, S.L. (Responsable de Seguridad)
DPD consultado	DPD de La entidad cliente (art. 35.2 RGPD - consulta obligatoria)
Fecha de elaboración	11/09/2026
Próxima revisión	11/09/2027, o ante cambio significativo en el tratamiento
Justificación de la EIPD	El tratamiento implica el uso de tecnologías innovadoras (IA generativa) para procesar datos de expedientes administrativos con efectos jurídicos potenciales, lo que puede suponer un alto riesgo según el art. 35.1 RGPD. Asimismo, el tratamiento incluye datos de ciudadanos y funcionarios. Se realiza la EIPD de forma preventiva conforme al principio de responsabilidad proactiva (art. 5.2 RGPD).

1. DESCRIPCIÓN SISTEMÁTICA DEL TRATAMIENTO (art. 35.7.a RGPD)

1.1. Naturaleza y contexto del tratamiento

El módulo **Edilia** es una plataforma SaaS que asiste a La entidad cliente en la generación de documentos administrativos mediante inteligencia artificial. El proceso consiste en:

1. El usuario (funcionario o cargo electo del municipio) inicia un expediente y completa un formulario con los datos del procedimiento.
2. Los datos del expediente, junto con el contexto jurídico (tipo, legislación aplicable), se envían directamente a Google Cloud Vertex AI europe-west1 (UE) para la generación del borrador, con Amazon Bedrock eu-central-1 (Fráncfort, Alemania, UE) como respaldo automático en caso de indisponibilidad. No se realiza anonimización previa. El procesamiento se realiza íntegramente en la UE bajo Acuerdo de Procesamiento de Datos (DPA) con Google y política de Zero Data Retention (ZDR).
3. El borrador generado se devuelve al servidor de Edilia (IONOS, Alemania, UE) para su almacenamiento.
4. El borrador resultante se presenta al usuario para su revisión, modificación y aprobación. **Ningún documento tiene efectos jurídicos hasta que el titular del órgano competente lo aprueba y firma.**

1.2. Datos personales tratados

Categoría de datos	Origen	Interesados	Sensibilidad
Datos identificativos (nombre, DNI/NIF, dirección, email, teléfono)	Introducidos por el usuario en los formularios de expediente	Ciudadanos, empresas, funcionarios	Ordinaria
Credenciales de acceso al sistema	Registro de usuario	Funcionarios y cargos electos	Ordinaria (hash irreversible)
Datos económicos (importes, referencias bancarias en expedientes de contratación/subvención)	Formularios de expediente	Ciudadanos, empresas	Ordinaria

Datos de auditoría de uso del sistema (IP pseudonimizada, acción, timestamp)	Generados automáticamente por el sistema	Funcionarios (usuarios)	Pseudonimizados
--	--	-------------------------	-----------------

Nota importante: El sistema **no trata habitualmente datos de categoría especial** (art. 9 RGPD: salud, ideología, orientación sexual, etc.) en la modalidad estándar. Si un expediente concreto requiriese tratar tales datos, sería necesaria una evaluación específica adicional.

1.3. Tecnología y flujo de datos

Componente	Descripción	Datos que maneja
Formularios Edilia (Laravel/Filament)	Captura de datos del expediente por el funcionario	Datos reales del expediente (sin pseudonimizar)
Google Cloud Vertex AI (europe-west1, Bélgica)	Modelo de lenguaje grande para generación del texto del documento. DPA firmado 26/03/2026. ZDR activo (no retiene datos). Procesamiento íntegro en la UE.	Datos del expediente procesados directamente. Sin retención.
Amazon Bedrock (eu-central-1, Fráncfort, Alemania)	Proveedor de respaldo automático de modelo de lenguaje en caso de indisponibilidad de Vertex AI. Addendum estándar de protección de datos de AWS (art. 28 RGPD). Procesamiento íntegro en la UE.	Datos del expediente procesados directamente en caso de fallback. Sin retención.

Mistral AI (París, Francia)	Embeddings semánticos (codestral-embed) para la búsqueda RAG: vectoriza las consultas del chat y los documentos aportados por el usuario, además del corpus. DPA art. 28. Procesamiento en la UE. No genera documentos.	Texto de la consulta o del documento aportado (puede contener PII antes de pseudonimización). Sin retención para entrenamiento.
PostgreSQL + pgvector (IONOS Alemania)	Base de datos RAG: legislación (161K chunks) + documentos ejemplo anonimizados	Legislación pública + documentos con PII minimizada mediante pseudonimización y verificación de PII residual.
MySQL 8 (IONOS Alemania)	Almacenamiento de expedientes, documentos generados y datos del sistema	Datos reales del expediente (cifrados en reposo)
Redis (IONOS, local)	Cache de sesiones (24h) y cálculos intermedios	Sesiones de usuario (TTL 24h), rate limits (IP pseudonimizada)

2. EVALUACIÓN DE NECESIDAD Y PROPORCIONALIDAD (art. 35.7.b RGPD)

2.1. Finalidad y base jurídica

El tratamiento tiene como finalidad la prestación del servicio de generación de documentos administrativos para La entidad cliente en el ejercicio de sus competencias municipales.

Base jurídica del tratamiento	Art. 6.1.e RGPD - El tratamiento es necesario para el cumplimiento de una misión realizada en interés público encomendada al responsable del tratamiento (La entidad cliente), en el ejercicio de sus competencias municipales (art. 103 CE, LBRL, LPAC).
--------------------------------------	--

Limitación de la finalidad (art. 5.1.b)	Los datos se usan exclusivamente para generar el borrador del documento del expediente concreto. No se usan para perfilado, ni para finalidades comerciales, ni para nada ajeno al expediente.
Minimización de datos (art. 5.1.c)	Solo se capturan los datos estrictamente necesarios para el expediente concreto. La seudonimización garantiza que los modelos de IA nunca reciben más información de la necesaria.
Limitación del plazo de conservación (art. 5.1.e)	Sesiones de generación IA: purga automática a las 24 horas. Logs de auditoría: 90 días. Documentos generados: a decisión del responsable según normativa de archivos.
Exactitud (art. 5.1.d)	Los datos del expediente son introducidos por el funcionario responsable. El sistema no modifica los datos de hechos; únicamente genera el texto jurídico-formal del documento.

2.2. Garantías de los derechos de los interesados

Los interesados cuyos datos figuren en los expedientes tienen garantizados todos sus derechos conforme al RGPD frente al Responsable del Tratamiento (La entidad cliente):

- **Derecho de acceso (art. 15):** Solicitable al Ayuntamiento como responsable.
- **Derecho de rectificación (art. 16):** El funcionario puede modificar los datos del expediente antes de la generación del documento.
- **Derecho de supresión (art. 17):** Implementado técnicamente; la supresión en el sistema se realiza bajo instrucción del responsable.
- **Derecho a la limitación (art. 18):** El municipio puede solicitar la limitación del tratamiento al encargado.
- **Derecho a la portabilidad (art. 20):** Exportación en formatos estándar (ZIP, CSV, JSON, PDF) disponible.
- **Derecho de oposición (art. 21):** Gestionado por el Responsable; puede incluir el bloqueo de datos en el sistema.

3. EVALUACIÓN DE RIESGOS (art. 35.7.c RGPD)

N.º	Riesgo identificado	Probabilidad sin medidas	Impacto	Medidas de mitigación	Riesgo residual	Aceptación
R1	Re-identificación de interesados por el modelo de IA <i>El modelo podría re-identificar a personas a partir de datos pseudonimizados</i>	MEDIA	ALTO	Procesamiento directo en Vertex AI europe-west1 (UE) con DPA y ZDR activo. No se realiza anonimización previa. TLS 1.3. Aislamiento multi-tenant por municipio_id.	BAJO	Aceptado
R2	Acceso no autorizado a datos del expediente <i>Usuario no autorizado accede a datos de un municipio distinto</i>	BAJA	ALTO	Aislamiento multi-tenant: municipio_id en todas las consultas. Políticas Laravel (Form Requests + Políticas). Middleware de autenticación en cada ruta. Audit log con alertas. Bcrypt + sesión única.	BAJO	Aceptado

R3	Fuga de datos personales a proveedores externos <i>Transferencia de PII real a Google, Mistral u otros fuera del EEE</i>	BAJA	ALTO	Procesamiento íntegro en la UE: Google Vertex AI europe-west1 (Bélgica, contratado a Google Cloud EMEA Limited), Mistral AI (Francia, jurisdicción UE plena), IONOS (Alemania, jurisdicción UE plena), Amazon Bedrock eu-central-1 (Fráncfort, contratado a Amazon Web Services EMEA SARL). Todos los proveedores con DPA RGPD firmado y Cláusulas Contractuales Tipo de la Comisión Europea para encargados con matriz extra-EEE. ZDR activo. Fallback Anthropic US eliminado (29/03/2026). Monitoría de endpoints API.	BAJO	Aceptado
----	---	------	------	--	------	----------

R4	Decisiones automatizadas con efectos jurídicos (art. 22 RGPD) <i>El sistema podría aplicarse como si tomara decisiones administrativas autónomas</i>	MUY BAJA	MUY ALTO	Los documentos generados son borradores . Ningún documento tiene efectos jurídicos hasta la firma expresa del titular del órgano competente. Flujo UI: borrador → revisión → aprobación → firma. Intervención humana obligatoria e irrenunciable. Art. 22 RGPD no aplica.	MUY BAJO	Aceptado
R5	Pérdida o destrucción de datos del expediente <i>Fallo de infraestructura o ciberataque que destruye datos</i>	BAJA	ALTO	Backups diarios cifrados, retención 30 días, offsite. VPS IONOS SLA 99.9%. Restauración probada mensualmente. Cifrado AES-256 en reposo. Procedimiento de recuperación documentado.	BAJO	Aceptado

R6	Generación de documentos con errores jurídicos <i>La IA genera un documento con fundamentos de derecho incorrectos o desactualizados</i>	MEDIA	MEDIO	Sistema RAG con legislación actualizada (BOE diario). Actualización de legislación indexada periódica. Revisión obligatoria por funcionario competente antes de firma. Descargo de responsabilidad visible en la UI. El municipio es el único responsable jurídico del acto administrativo.	BAJO	Aceptado
-----------	--	-------	-------	---	-------------	----------

4. MEDIDAS PARA AFRONTAR LOS RIESGOS (art. 35.7.d RGPD)

Medida	Implementación técnica	Riesgos mitigados
Seudonimización (art. 25 RGPD)	Procesamiento en Vertex AI europe-west1 (UE) con DPA firmado y ZDR activo. Cifrado TLS 1.3 en tránsito. Aislamiento multi-tenant. IPs pseudonimizadas con SHA-256 en logs de auditoría.	R1, R3

Cifrado (art. 32 RGPD)	TLS 1.2+ en tránsito, HSTS. AES-256 en reposo (bases de datos y backups). Bcrypt cost-12 para contraseñas. HTTPS con Let's Encrypt en todos los subdominios.	R2, R3, R5
Aislamiento multi-tenant	Todas las consultas a BBDD incluyen WHERE municipio_id = ?. Políticas Laravel que verifican pertenencia al tenant. Middleware de autorización en cada ruta. Audit log que registra cualquier intento de acceso cruzado.	R2
Registro de auditoría pseudonimizado	ed_audit_logs: 25 tipos de acción, IP hasheada SHA-256, retención 90 días, tabla inmutable. Nunca se almacenan nombre completo ni DNI en los logs.	R2, R5
Limitación temporal y purga automática	Sesiones Redis con TTL 24h. Purga automática de sesiones de chat IA. Backups con retención máxima de 30 días. Procedimiento de baja documentado.	R1, R5
Intervención humana obligatoria	Flujo de trabajo en UI: generación → revisión → aprobación → firma. No es posible omitir la revisión. Mensaje legal visible en la interfaz: «Este documento es un borrador. Revise antes de firmar.»	R4, R6

RAG legislativo actualizado	Ingesta diaria del BOE (07:00). 161K chunks de legislación estatal en PostgreSQL+pgvector. Actualización automática ante cambios normativos. Datado de los fragmentos legislativos.	R6
Subencargados exclusivamente EU	Google Cloud Vertex AI europe-west1 (Bélgica), Mistral AI (Francia), IONOS SE (Alemania). DPA firmados. ZDR activo. Sin transferencias a países terceros. Fallback US eliminado, sustituido por Amazon Bedrock eu-central-1 (Fráncfort, Alemania, UE).	R3

5. CONSULTA PREVIA A LA AUTORIDAD DE CONTROL (art. 36 RGPD)

Se concluye que **no es necesario realizar consulta previa a la AEPD** conforme al art. 36.1 RGPD, dado que las medidas de mitigación implementadas reducen los riesgos identificados a un nivel residual BAJO que no es «alto riesgo» en el sentido del art. 35.1 RGPD. En particular:

- La seudonimización efectiva garantiza que los modelos de IA no tratan datos personales reales.
- Ningún documento tiene efectos jurídicos sin revisión y firma humana expresa, eliminando el riesgo del art. 22 RGPD.
- El tratamiento se realiza íntegramente en el Espacio Económico Europeo, sin transferencias internacionales.
- Los datos no son de categoría especial en la modalidad estándar del servicio.

Si en el futuro se incorporasen tratamientos de datos de categoría especial o funcionalidades de decisión automatizada vinculante, se revisará esta conclusión y se realizará consulta previa si el riesgo residual resultante fuera alto.

6. CONCLUSIÓN DE LA EVALUACIÓN

La presente Evaluación de Impacto concluye que el tratamiento de datos personales en el módulo Edilia, tal como se ha descrito y con las medidas de

mitigación implementadas:

- Es **necesario y proporcionado** para los fines de interés público perseguidos por La entidad cliente.
- Los riesgos identificados han sido mitigados a un nivel **residual BAJO** mediante medidas técnicas y organizativas adecuadas.
- **No requiere consulta previa a la AEPD** conforme al art. 36 RGPD.
- El tratamiento puede llevarse a cabo de forma lícita y segura.

7. REVISIÓN

La presente EIPD se revisará anualmente o cuando concurra alguno de los siguientes supuestos (art. 35.11 RGPD):

- Cambio significativo en el sistema de IA utilizado (nuevo modelo, nuevo proveedor).
- Incorporación de nuevos tipos de datos o nuevas categorías de interesados.
- Materialización de alguno de los riesgos identificados (brecha de seguridad).
- Cambio normativo relevante (RGPD, ENS, normativa sectorial).
- Incorporación de funcionalidades de decisión automatizada vinculante.

Y en prueba de conformidad con la presente Evaluación de Impacto en Protección de Datos, ambas partes la suscriben en la fecha indicada en las firmas electrónicas.

EL ENCARGADO DEL TRATAMIENTO Edilia Tech, S.L. CIF: B-27552728 Fdo.: Roberto López Miquel Administrador Fecha: 11/09/2026	EL RESPONSABLE DEL TRATAMIENTO La entidad cliente CIF: Fdo.: Fecha: 11/09/2026
---	---