Procedimiento de brechas de seguridad

PROCEDIMIENTO DE GESTIÓN DE BRECHAS DE SEGURIDAD

Artículos 33 y 34 del Reglamento (UE) 2016/679 (RGPD)

Medida op.exp.8 del Anexo II RD 311/2022 (ENS)

PARTES

Encargado del tratamiento (Prestador): Edilia Tech, S.L., con CIF B-27552728, con domicilio en Calle Mayor 13, 3.º Izquierda, 28013 Madrid (Madrid). Contacto: **contacto@edilia.tech**.

Responsable del tratamiento (Ayuntamiento): La entidad cliente, con CIF , con sede en , (), representado/a por , .

1. DEFINICIÓN Y ALCANCE

De acuerdo con el **artículo 4.12 del RGPD**, una **violación de la seguridad de los datos personales** (en adelante, «brecha») es toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

El presente procedimiento se aplica a **todos los datos personales tratados en el sistema Edilia** en el marco de la prestación de servicios a La entidad cliente, incluyendo:

- Datos de funcionarios y cargos electos del municipio almacenados en el sistema.
- Datos de ciudadanos y terceros que figuren en los expedientes administrativos gestionados.
- Credenciales de acceso y datos de sesión de los usuarios del sistema.
- Documentos administrativos generados con contenido de datos personales.

2. EQUIPO DE RESPUESTA A INCIDENTES

Rol	Titular	Contacto	Responsabilidad principal
Responsable de Seguridad (Prestador)	Edilia Tech, S.L.	contacto@edilia.tech	Detección, contención, análisis técnico, notificación al ayuntamiento en 48h
Responsable del Tratamiento (Ayuntamiento)	- La entidad cliente	A cumplimentar por el ayuntamiento	Toma de decisiones, notificación AEPD en 72h, comunicación a interesados si procede
DPD del Ayuntamiento	El designado por La entidad cliente (art. 37 RGPD - obligatorio para AAPP)	A cumplimentar por el ayuntamiento	Asesoramiento en la evaluación del riesgo, coordinación con la AEPD, supervisión del proceso

3. FASES DEL PROCEDIMIENTO

FASE 1 - DETECCIÓN (Plazo: inmediata)

Una brecha de seguridad puede detectarse a través de los siguientes mecanismos:

- **Sistema de auditoría (ed_audit_logs):** alertas por patrones anómalos (IP_ANOMALIA, accesos fallidos masivos, acceso desde país inusual).
- **fail2ban:** detección automática de ataques de fuerza bruta y bloqueo preventivo de IPs.

- **Monitorización de infraestructura IONOS:** alertas de uso anormal de CPU/RAM/disco, caídas de servicio.
- **Notificación de usuario:** comunicación de un funcionario del ayuntamiento sobre actividad sospechosa en su cuenta.
- **Alerta de proveedor:** notificación de IONOS SE, Google Cloud (Vertex AI), Amazon Web Services (Bedrock) o Mistral AI sobre incidente en sus sistemas que afecte a datos del servicio.
- **Detección manual:** identificación por el equipo técnico durante tareas de mantenimiento o revisión de logs.

Acción inmediata: El detector de la posible brecha la comunica al Responsable de Seguridad en el plazo máximo de **1 hora** desde su conocimiento, mediante correo electrónico a contacto@edilia.tech con asunto: *«[URGENTE] Posible brecha de seguridad - [fecha]»*.

FASE 2 - CONTENCIÓN (Plazo: dentro de las primeras 4 horas)

El Responsable de Seguridad adoptará de forma inmediata las medidas de contención que correspondan según la naturaleza de la brecha:

Tipo de brecha	Medida de contención inmediata
Acceso no autorizado a cuenta de usuario	Bloqueo inmediato de la cuenta afectada. Revocación de todas las sesiones activas. Notificación al titular.
Compromiso de infraestructura	Aislamiento del componente afectado. Cambio de credenciales del sistema. Activación de modo mantenimiento si necesario.
Filtración o exposición de datos	Revocación de tokens/credenciales expuestos. Solicitud de eliminación a terceros si fuera accesible externamente.
Ataque activo (ransomware, intrusión)	Aislamiento total del servidor afectado. Activación de backup más reciente. Contacto con IONOS SE para soporte urgente.

FASE 3 - EVALUACIÓN Y CLASIFICACIÓN (Plazo: dentro de las primeras 12 horas)

El Responsable de Seguridad, con el apoyo del DPD del ayuntamiento, evaluará la brecha aplicando el **test de notificabilidad del art. 33 RGPD**:

Clasificación	Criterios	Obligación de notificación
BAJA	Incidente técnico sin exposición de datos. Datos pseudonimizados y/o cifrados. Impacto prácticamente nulo en derechos de interesados.	Registro interno. **No notificar a AEPD.**
MEDIA	Exposición limitada de datos personales ordinarios. Riesgo bajo para derechos y libertades de los interesados. Datos no especialmente sensibles.	Notificación al ayuntamiento (48h). **Notificar a AEPD** (72h, art. 33). Evaluar comunicación a interesados.
ALTA	Exposición significativa de datos personales. Riesgo elevado para derechos fundamentales. Posible impacto económico, discriminación o daño reputacional a los afectados.	Notificación al ayuntamiento (24h). **Notificar a AEPD** (72h, art. 33). **Comunicar a interesados** (art. 34.1).
CRÍTICA	Brecha masiva o de datos de categoría especial. Riesgo muy alto e irreversible para los interesados. Posible impacto sistemático.	**Notificación inmediata** al ayuntamiento (<6h). **AEPD a la mayor brevedad** (máx. 72h). **Comunicación urgente a todos los interesados afectados** (art. 34.1).

FASE 4 - NOTIFICACIÓN (Plazos regulados en art. 33-34 RGPD)

A) Notificación al ayuntamiento (Responsable del Tratamiento):

El encargado notificará al ayuntamiento **sin dilación indebida y en un máximo de 48 horas** desde el conocimiento de la brecha (art. 33.2 RGPD), usando la plantilla de notificación incluida en el apartado 6 del presente procedimiento.

B) Notificación a la AEPD (obligación del Responsable - ayuntamiento):

La entidad cliente, como Responsable del Tratamiento, deberá notificar la brecha a la **Agencia Española de Protección de Datos (AEPD)** dentro de las **72 horas siguientes** a haber tenido conocimiento de ella (art. 33.1 RGPD), salvo que sea improbable que suponga un riesgo para los derechos y libertades de las personas físicas.

Canal de notificación: **https://sedeagpd.gob.es** (sede electrónica AEPD - formulario de notificación de brechas). Si no es posible notificar en 72 horas, la notificación incluirá los motivos de la dilación (art. 33.1 in fine).

C) Comunicación a los interesados (si procede, art. 34.1 RGPD):

Cuando la brecha suponga un **alto riesgo para los derechos y libertades de las personas físicas**, La entidad cliente comunicará la violación a los interesados afectados sin dilación indebida. La comunicación se realizará en lenguaje claro y sencillo, e incluirá como mínimo la información prevista en el art. 34.2 RGPD (naturaleza de la brecha, datos de contacto DPD, consecuencias probables, medidas adoptadas).

No será necesaria la comunicación a interesados si concurre alguna de las circunstancias del art. 34.3 RGPD (datos cifrados, medidas que impidan riesgo, esfuerzo desproporcionado - en este caso, publicación pública).

FASE 5 - DOCUMENTACIÓN (Obligatoria, art. 33.5 RGPD)

Toda brecha, con independencia de si es notificable o no, debe documentarse en el **Registro Interno de Incidencias de Seguridad**, incluyendo:

- Fecha y hora de detección y de comunicación al equipo de respuesta.
- Descripción técnica detallada de la brecha (causa raíz, vector de ataque).
- Categorías y número aproximado de interesados y registros afectados.
- Clasificación de la brecha (baja/media/alta/crítica) y justificación.
- Medidas de contención adoptadas y plazos.
- Notificaciones realizadas (al ayuntamiento, a la AEPD, a interesados) con fecha y contenido.
- Consecuencias identificadas de la brecha.

- Medidas correctivas implementadas para evitar recurrencia.

Este registro se conservará durante **5 años** y estará disponible para la AEPD si lo requiriese.

FASE 6 - MEJORA CONTINUA (Post-mortem)

Dentro de los **30 días siguientes** a la resolución de cualquier brecha de clasificación MEDIA o superior, el Responsable de Seguridad elaborará un informe post-mortem que incluya:

- Análisis de la causa raíz (root cause analysis).
- Evaluación de si las salvaguardas existentes fueron suficientes.
- Propuesta de medidas correctivas y preventivas con responsable y plazo.
- Actualización del Análisis de Riesgos si la brecha revela nuevas amenazas o cambia la valoración de riesgos existentes.
- Revisión de la presente Política si fuera necesario.

4. CRITERIOS PARA NOTIFICACIÓN A INTERESADOS (art. 34 RGPD)

Se considerará que la brecha supone **alto riesgo para los derechos y libertades** (obligando a comunicar a los interesados) cuando concurra alguna de las siguientes circunstancias:

- Exposición de datos que permitan usurpación de identidad (DNI, datos bancarios, credenciales).
- Exposición de datos de categoría especial (art. 9 RGPD): datos de salud, ideología, religión, orientación sexual, datos penales.
- Exposición de datos de menores de edad.
- Exposición masiva de datos (más de 100 interesados afectados).
- Brecha que pueda dar lugar a discriminación, daños económicos significativos o daño reputacional grave.

5. CONTACTOS DE EMERGENCIA

Entidad / Servicio	Contacto	Disponibilidad

Responsable de Seguridad - Edilia Tech, S.L.	contacto@edilia.tech	L-V 09:00-19:00. Urgencias: respuesta en 4h
AEPD - Agencia Española de Protección de Datos	https://sedeagpd.gob.es Tel.: 901 100 099	Sede electrónica 24/7. Formulario brechas.
IONOS SE - Soporte técnico VPS	Panel IONOS + tel. soporte empresarial	24/7 para incidencias críticas
Google Cloud - Incidencias Vertex AI	https://cloud.google.com/support Cloud Console → Soporte	24/7 para incidencias de seguridad de datos
Amazon Web Services - Incidencias Bedrock	https://aws.amazon.com/support AWS Console → Support Center	24/7 para incidencias de seguridad de datos
INCIBE-CERT - Centro de Respuesta a Incidentes	https://www.incibe-cert.es Tel.: 017	24/7 para incidentes de ciberseguridad

6. PLANTILLA DE NOTIFICACIÓN AL AYUNTAMIENTO (datos mínimos art. 33.3 RGPD)

NOTIFICACIÓN DE VIOLACIÓN DE SEGURIDAD DE DATOS PERSONALES

De: Edilia Tech, S.L. (Encargado del Tratamiento)

Para: La entidad cliente (Responsable del Tratamiento)

Fecha de la notificación: _____

N.º de referencia del incidente: INC-[AÑO]-[NÚMERO]

1. **Naturaleza de la violación (art. 33.3.a):** Descripción de la naturaleza de la brecha, incluyendo, si es posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

   _____

2. **Datos del DPD o punto de contacto (art. 33.3.b):** Nombre y datos de contacto del delegado de protección de datos u otro punto de contacto en el que pueda obtenerse más información.
   Roberto López Miquel - contacto@edilia.tech
3. **Consecuencias probables (art. 33.3.c):** Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

   _____

4. **Medidas adoptadas o propuestas (art. 33.3.d):** Descripción de las medidas adoptadas o propuestas por el encargado del tratamiento para poner remedio a la violación de la seguridad, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

   _____

5. **Clasificación de la brecha:** BAJA / MEDIA / ALTA / CRÍTICA

   _____

6. **Recomendación de notificación a la AEPD:** SÍ / NO - Justificación:

   _____

7. **Recomendación de comunicación a interesados (art. 34):** SÍ / NO - Justificación:

   _____

Y en prueba de conocimiento y aceptación del presente Procedimiento de Gestión de Brechas de Seguridad, ambas partes lo 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