04.00.-Información sobre brechas de seguridad

Serenia Capital, S.A

Índice

1. Objeto y alcance

1.1 Finalidad del documento

El presente documento tiene por objeto establecer el marco de referencia para la identificación, comunicación y documentación de las brechas de seguridad que puedan afectar a los datos personales tratados por Serenia Capital, S.A (en adelante Serenia).

Constituye una guía informativa que recoge las obligaciones legales derivadas del Reglamento General de Protección de Datos (RGPD), la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), así como de las normas internacionales de gestión de seguridad de la información (ISO/IEC 27001, ISO/IEC 27701).

Su finalidad es:

- Sensibilizar a todos los actores implicados sobre la importancia de notificar y gestionar adecuadamente cualquier incidente de seguridad que pueda implicar datos personales.
- Definir los principios básicos que rigen la gestión de brechas, sin entrar en el detalle operativo (que se regula en el Plan de Actuación Interna).
- Garantizar que la organización pueda acreditar en todo momento la responsabilidad proactiva (*accountability*) exigida por el RGPD.

1.2 Ámbito de aplicación

Este documento es de aplicación a todas las actividades de tratamiento de datos personales realizadas por Serenia, independientemente de su soporte o sistema, y afecta a los siguientes colectivos:

- **Organización:** todas las áreas y departamentos que intervienen en el tratamiento de datos personales.
- **Empleados y colaboradores:** cualquier persona que, en el ejercicio de sus funciones, pueda tener conocimiento de una brecha o incidente de seguridad.
- **Encargados del tratamiento:** proveedores que tratan datos personales por cuenta de la organización, quienes deberán notificar sin dilación cualquier incidente que detecten.
- **Subencargados del tratamiento:** terceros autorizados por los encargados, quienes a su vez deberán comunicar las incidencias a través del encargado principal.
- **Delegado de Protección de Datos (DPO):** como figura de supervisión y asesoramiento en la gestión y notificación de brechas

2. Definición de brecha de seguridad

2.1 Concepto según RGPD

De acuerdo con el artículo 4.12 del Reglamento General de Protección de Datos (RGPD), se entiende por brecha de seguridad de los datos personales:

> *"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".*

Una brecha de seguridad afecta por tanto a la **confidencialidad, integridad o disponibilidad de los datos personales**. Debe distinguirse de otros incidentes de seguridad que, aun siendo relevantes, no involucren datos personales y por tanto no constituyan brecha en el sentido del RGPD.

El marco normativo establece:

- **Artículo 32 RGPD y art. 32 LOPDGDD**: obligación de aplicar medidas técnicas y organizativas adecuadas y de documentar todas las brechas, incluso si no son notificables.
- **Artículo 33 RGPD**: notificación a la AEPD en un plazo máximo de 72 horas, salvo que sea improbable que suponga un riesgo.
- **Artículo 34 RGPD**: comunicación a los interesados cuando la brecha entrañe un alto riesgo.

De acuerdo con la **Guía de la AEPD (2018)** y con los estándares **ISO/IEC 27001 (A.16), ISO/IEC 27002 (16) e ISO/IEC 27701 (6.13)** , la

organización debe disponer de un procedimiento documentado para la gestión de brechas, que garantice trazabilidad, notificación adecuada y mejora continua.

2.2 Tipología de brechas

Las brechas de seguridad pueden clasificarse en tres grandes categorías, que se corresponden con los **principios fundamentales de la seguridad de la información**: **confidencialidad, integridad y disponibilidad (CID)**.

- **Brechas de confidencialidad**:
  Acceso o divulgación no autorizada de datos personales o información sensible.
  - *Ejemplos*: envío de información a un destinatario equivocado; pérdida de un dispositivo USB sin cifrar; acceso indebido a ficheros de clientes por parte de un empleado.
  - *Medidas preventivas*: autenticación multifactor, políticas de control de acceso y acuerdos de confidencialidad con empleados y proveedores.
- **Brechas de integridad**:
  Alteración no autorizada o accidental de datos personales, comprometiendo su exactitud o fiabilidad.
  - *Ejemplos*: modificación indebida de expedientes; corrupción de bases de datos; manipulación de información en un sistema por error humano o malware.
  - *Medidas preventivas*: sistemas de detección de intrusiones, registros de auditoría, controles de validación y actualización de software.
- **Brechas de disponibilidad**:
  Pérdida o destrucción de datos personales, accidental o ilícita, que impide el acceso o uso normal de la información.
  - *Ejemplos*: borrado accidental de registros sin copia de seguridad; ataque de ransomware que bloquea el acceso a datos; caída prolongada de un servidor que impide atender a los interesados.
  - *Medidas preventivas*: políticas de backup y recuperación ante desastres, planes de continuidad de negocio y redundancias en sistemas críticos.

Es importante destacar que no todos los incidentes de seguridad informática son considerados "brechas de seguridad" en el sentido del **artículo 4.12 RGPD**. Solo aquellos que afecten a datos personales y puedan comprometer los derechos y libertades de las personas entran en esta categoría.

2.3 Ejemplos prácticos de brechas

Algunos ejemplos típicos de brechas de seguridad son:

- Pérdida o robo de dispositivos con información personal (ordenadores, móviles, discos duros).
- Filtración de datos de clientes a través de ataques externos (phishing, malware, intrusión).
- Envío masivo de correos electrónicos con direcciones visibles (copia abierta) en lugar de ocultas.
- Acceso a historiales médicos o financieros por personal no autorizado.
- Eliminación accidental de registros de nóminas o de facturación sin copia de seguridad disponible.

Además de estos ejemplos, es fundamental entender las **causas frecuentes de brechas**, que pueden ser de naturaleza **organizativa** o **técnica**:

- **Causas organizativas**:
  - Falta de clasificación de la información según nivel de confidencialidad.
  - Deficiente delimitación de accesos (no aplicación del principio de mínimo privilegio).
  - Ausencia de formación y sensibilización del personal en seguridad de la información.
  - Carencia de acuerdos de confidencialidad con empleados y colaboradores.
  - Insuficiente control de proveedores y subencargados.
- **Causas técnicas**:
  - Malware o código malicioso que permanece oculto en sistemas mientras extrae información.
  - Accesos no autorizados derivados de sistemas y aplicaciones desactualizados.
  - Debilidades en la seguridad en la nube por contraseñas débiles o configuración insegura.
  - Uso de dispositivos personales (BYOD) sin políticas de cifrado, autenticación fuerte o VPN.

3. Marco normativo aplicable

3.1 Reglamento General de Protección de Datos (RGPD)

- **Art. 4.12:** define "violación de la seguridad de los datos personales".
- **Art. 33:** obligación de notificar a la autoridad de control en un máximo de 72h, salvo que sea improbable que suponga un riesgo.
- **Art. 34:** obligación de comunicar a los interesados cuando la brecha entrañe alto riesgo.

3.2 Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD)

- **Art. 32:** obligación de aplicar medidas de seguridad en el tratamiento de datos.
- En relación con el RGPD (arts. 5.2 y 24), exige responsabilidad proactiva y la documentación de las incidencias, aunque no sean notificables.
- La AEPD, mediante guías y resoluciones, ha fijado criterios sobre conservación de registros de brechas (mínimo 5 años).

3.3 Normas ISO aplicables

- **ISO/IEC 27001 – Anexo A.16:** gestión de incidentes de seguridad de la información.
- **ISO/IEC 27002 – sección 16:** controles y buenas prácticas para clasificar, notificar y gestionar incidentes.
- **ISO/IEC 27701 – extensión de privacidad:** requisitos para la notificación de violaciones de datos personales en línea con el RGPD.

4. Procedimiento de gestión de brechas

Serenia dispone de un procedimiento sistemático para la detección, análisis, gestión y notificación de las brechas de seguridad de datos personales, siguiendo el ciclo de vida recomendado por la AEPD, el INCIBE y las normas ISO 27001/27701.

4.1 Detección e identificación

Todo empleado, colaborador o proveedor que detecte una posible brecha deberá comunicarla inmediatamente a rgpd@auratechlegal.es . Se considera brecha cualquier incidente que afecte a la confidencialidad, integridad o disponibilidad de datos personales, según el art. 4.12 RGPD. El área de Privacidad abrirá un registro preliminar en el Registro de Incidencias.

4.2 Contención y primera respuesta

El Responsable de Seguridad/IT aplicará medidas de contención inmediatas para evitar una mayor exposición de los datos (ej. desconexión de sistemas comprometidos, bloqueo de accesos, cambio de credenciales). Se generará un informe inicial con: fecha, persona que detecta, sistema afectado y medidas urgentes adoptadas.

4.3 Análisis y evaluación del impacto

El Comité de Seguridad/Privacidad (o el DPO, en su caso) realizará una evaluación preliminar del impacto en los derechos y libertades de los interesados.

La clasificación seguirá tres niveles:

- **Bajo:** sin riesgo para las personas (ej. datos cifrados).
- **Medio:** riesgo moderado (ej. pérdida de datos no críticos).
- **Alto:** riesgo significativo (ej. filtración de datos sensibles).

Esta evaluación determinará la obligación de notificación a la AEPD y/o a los interesados.

4.4 Notificación y comunicación

- **A la AEPD:** si la brecha entraña riesgo, el responsable notificará en un plazo máximo de 72 horas desde la detección, incluyendo la información del art. 33 RGPD.
- **A los interesados:** si la brecha entraña alto riesgo, se comunicará directamente a los afectados, conforme al art. 34 RGPD, en lenguaje claro y sencillo.
- **Cuando la organización actúe como encargado o subencargado:** la notificación se realizará sin dilación al responsable, quien decidirá la comunicación a la AEPD o a los interesados.

4.5 Documentación y registro

Todas las brechas, sean notificables o no, se documentarán en el Registro de Brechas de Seguridad.

Cada registro contendrá:

- Descripción de la brecha.
- Categorías de datos y personas afectadas.
- Medidas técnicas y organizativas adoptadas.
- Evaluación de riesgo y decisión sobre notificación.
- Acciones de mitigación y plan de seguimiento.

Los registros se conservarán durante un plazo mínimo de 5 años desde el cierre del incidente.

4.6 Lecciones aprendidas y mejora continua

Tras el cierre de la brecha, se realizará un análisis post-incidente para identificar fallos, vulnerabilidades y medidas de mejora. Estas lecciones serán incorporadas a los controles de seguridad y a la formación del personal, en cumplimiento del principio de responsabilidad proactiva (art. 5.2 RGPD).

4.7 Formación y concienciación

La organización reconoce que la **ingeniería social** es uno de los vectores de ataque más frecuentes y que el factor humano constituye un riesgo crítico. Para mitigar este riesgo, se establecerán programas periódicos de **formación en ciberseguridad y privacidad**, incluyendo simulacros de phishing y campañas de concienciación adaptadas a los distintos colectivos de la organización.

Estas actividades se consideran parte esencial del sistema de gestión de la seguridad y estarán alineadas con lo dispuesto en la **ISO/IEC 27001 (cláusulas 7.2 y 7.3)** sobre competencias y concienciación.

5. Roles y responsabilidades

5.1 Responsable del tratamiento

- **Responsable (R)** de garantizar el cumplimiento de los arts. 33 y 34 RGPD.
- Decide si la brecha debe notificarse a la AEPD y a los interesados.
- **Aprueba (A)** las comunicaciones externas oficiales.
- Debe asegurarse de que existan procedimientos documentados y de que los encargados/subencargados los cumplan.

5.2 Encargado y subencargados del tratamiento

- **Responsables (R)** de notificar sin dilación indebida al responsable del tratamiento cualquier brecha detectada (art. 28.3.f RGPD).
- No pueden notificar directamente a la AEPD salvo autorización expresa del responsable.
- **Informan (I)** al responsable y coordinan con sus subencargados, cuando existan.

5.3 Empleados y colaboradores

- **Responsables (R)** de detectar y comunicar inmediatamente cualquier incidente o sospecha de brecha al canal interno designado.
- No evalúan ni notifican; su rol se limita a **informar (I)** de forma inmediata.
- Deben seguir la formación y directrices recibidas en materia de seguridad y privacidad.

5.4 Delegado de Protección de Datos (DPO)

- **Consultado (C)** en todo el proceso de análisis y notificación.
- Aporta criterio jurídico y técnico sobre la evaluación de riesgos.
- Puede actuar como punto de contacto con la AEPD, si así se le delega.
- Supervisa la correcta documentación y archivo de cada brecha (*accountability*).

Esquema RACI simplificado

Rol	Detectar	Analizar	Notificar AEPD	Notificar interesados	Documentar	Aprobar
Responsable del tratamiento	I	A	R	R	A	A
Encargado/Subencargado	R	I	I	I	I	-
Empleados/Colaboradores	R	-	-	-	-	-
DPO	C	C	C	C	C	-

6. Registro y conservación

6.1 Registro de todas las brechas (notificables o no)

Serenia llevará un Registro de Brechas de Seguridad, en el que se documentarán todas las incidencias detectadas, incluso aquellas que, tras su análisis, no resulten notificables a la AEPD ni a los interesados.

El registro debe permitir acreditar el cumplimiento del principio de responsabilidad proactiva (art. 5.2 RGPD) y de la obligación de documentación recogida en la Guía AEPD para la gestión de brechas de seguridad.

Cada entrada del registro deberá contener, como mínimo:

- Fecha y hora de detección.
- Descripción de la brecha.
- Sistemas y datos afectados.
- Categorías y volumen de interesados afectados.
- Evaluación preliminar del impacto y nivel de riesgo.
- Medidas adoptadas para su contención y mitigación.
- Decisión sobre notificación (sí/no) y justificación.
- Comunicación efectuada (AEPD, interesados, responsable en caso de encargo).
- Fecha de cierre del incidente.

6.2 Plazos de conservación

Los registros de brechas de seguridad se conservarán durante un mínimo de 5 años desde la fecha de cierre de la incidencia.

Este plazo se fundamenta en:

- El periodo de prescripción de infracciones graves y muy graves en materia de protección de datos (art. 78 LOPDGDD).
- La recomendación de la AEPD en su Guía de brechas de seguridad.

Transcurrido este periodo, los registros podrán ser bloqueados y posteriormente eliminados o anonimizados, salvo que exista un procedimiento judicial, administrativo o contractual que justifique su conservación adicional.

6.3 Medidas de seguridad en la conservación del registro

El registro de brechas deberá conservarse aplicando medidas de seguridad técnicas y organizativas adecuadas, en particular:

- Acceso restringido únicamente al DPO, al Responsable de Seguridad y a la Dirección.
- Almacenamiento cifrado en repositorios seguros con copias de seguridad controladas.
- Registro de accesos (logs) para garantizar la trazabilidad de quién consulta o modifica el registro.
- **Integridad y disponibilidad:** medidas para evitar alteraciones no autorizadas y asegurar su disponibilidad en auditorías o inspecciones de la AEPD.

7. Anexos y formularios

7.1 Formulario interno de notificación de brecha

Serenia dispone de un formulario estándar (documento 04.02) para la comunicación interna de incidentes o sospechas de brechas por parte de empleados, colaboradores o proveedores.

Este formulario servirá para:

- Recoger los datos mínimos de la incidencia (fecha, persona que detecta, descripción, sistemas afectados).
- Facilitar la rápida evaluación por parte del Responsable de Seguridad/Privacidad o del DPO.
- Garantizar trazabilidad en la recepción y primera respuesta.

(El modelo de formulario se encuentra en el documento 4.02 específico de formularios corporativos, versión vigente aprobada por la organización).

7.2 Plantilla de notificación a la AEPD

Se utilizará una plantilla basada en el formulario oficial de la AEPD disponible en su sede electrónica.

La plantilla incluye, de acuerdo con el art. 33 RGPD:

- Naturaleza de la brecha (categorías de datos y personas afectadas, volumen estimado).
- Identidad y datos de contacto del DPO o punto de contacto.
- Consecuencias probables de la brecha.
- Medidas adoptadas o propuestas para mitigar sus efectos.

(La plantilla oficial se mantiene en el documento de formularios corporativos, versión vigente).

7.3 Plantilla de comunicación a los interesados

Cuando proceda la comunicación directa a los afectados (art. 34 RGPD), se empleará una plantilla redactada en lenguaje claro y sencillo, que incluirá:

- Descripción de la brecha en términos comprensibles.
- Posibles consecuencias para el interesado.
- Medidas adoptadas por la organización.
- Instrucciones sobre medidas que el interesado puede adoptar.
- Datos de contacto para solicitar más información o ejercer derechos.

(La plantilla se conserva en el documento de formularios corporativos, versión vigente).

Madrid a 3 de octubre de 2025