Brechas de seguridad: actualización de los criterios para su gestión y notificación

El 25 de mayo de 2021, la Agencia Española de Protección de Datos (**"AEPD"**) publicó una nueva Guía para la notificación de brechas de datos personales (la **"Guía"**), actualizando así la versión de 2018 conforme a la experiencia adquirida en el periodo transcurrido tras la entrada en vigor del Reglamento (UE) 2016/679, de 27 abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (**"RGPD"**). Asimismo, esta Guía plasma los criterios establecidos por el Comité Europeo de Protección de Datos en relación con este tipo de incidentes.

Con motivo de esta publicación, la AEPD ha informado de que durante los cinco primeros meses de 2021 ha gestionado alrededor de 700 brechas de seguridad, destacando que la mayoría de ellas han sido producidas por ataques externos e intencionados, principalmente de tipo *ransomware*.

CRITERIOS PARA VALORAR LA PROCEDENCIA DE SANCIONES

En sus últimas resoluciones, la AEPD ha valorado especialmente:

i. La adopción de medidas de seguridad conforme lo establecido en el art. 32 RGPD[1]. Si bien en este precepto no se establece un listado tasado, tanto responsable como encargado del tratamiento deberán aplicar **medidas técnicas y organizativas que sean adecuadas al riesgo**[2] que conlleve el tratamiento, teniendo en cuenta: el estado de la técnica; los costes de aplicación; la naturaleza, alcance, contexto y finalidades del tratamiento; y los riesgos de probabilidad y gravedad para los derechos y libertades de los interesados. En este sentido, la AEPD tiene en cuenta si las medidas adoptadas están destinadas a minimizar los efectos de una eventual brecha de seguridad así como su utilidad para la **identificación, análisis y clasificación**[3] de este tipo de incidentes.

ii. La **actuación diligente y proporcional** en relación con la normativa de protección de datos del responsable[4] o del encargado[5] del tratamiento. A este respecto, la AEPD valora positivamente una reacción proactiva destinada a **notificar, minimizar el impacto e implementar nuevas medidas razonables** o, en su caso, o **actualizar las existentes** para evitar que se repita el incidente[6].

iii. La **notificación** a la AEPD de conformidad con lo establecido en la **Guía**[7].

PRINCIPALES MODALIDADES DE BRECHAS DE SEGURIDAD NOTIFICADAS A LA AEPD[8]

Atendiendo a los datos publicados por la AEPD en enero de 2021, las brechas de seguridad más habituales son las siguientes:

i. El ***ransomware*** es un tipo de *malware* que impide a los usuarios acceder a los datos alojados en sus sistemas. Las brechas de seguridad tipo ransomware se encuadran dentro de los incidentes de **disponibilidad**.

ii. **Pérdida o robo de dispositivo**. Para minimizar los riesgos de este tipo de brechas, la AEPD recomienda la implementación de las siguientes medidas[9]:

- Cifrado de los datos.
- Mantener copias de seguridad en otros dispositivos.
- Contar con contraseñas de bloqueo de pantalla o autenticación.

iii. **Pérdida o robo de documentación**. Para evitar este tipo de incidentes, las organizaciones deben contar con protocolos relativos a procesos de clasificación, digitalización, destrucción y traslado de documentación entre oficinas.

iv. El ***phishing*** es una modalidad de estafa[10] empleada por ciberdelincuentes que, mediante la suplantación de identidad, engañan a las víctimas para conseguir información confidencial, datos personales, credenciales bancarias, etc.

v. **Eliminación incorrecta de datos**. La alteración no autorizada o accidental de datos personales, incluyendo la eliminación de los mismos, podrá suponer una brecha de seguridad de **integridad**. Para evitar este tipo de incidentes, en la Guía la AEPD recomienda, entre otras, la implementación de medidas de control de acceso a bases de datos y de alerta ante modificaciones de archivos.

vi. Envío de datos personales por equivocación, como, por ejemplo, el envío de un correo electrónico sin copia oculta[11].

1 Resolución de 8 de febrero de 2021, procedimiento núm. PS/00354/2020 [JUR 2021\53275].

2 Resolución de 4 de enero de 2021, procedimiento núm. E/10375/2019 [JUR 2021\76956].

3 Resolución de 12 de marzo de 2021, procedimiento núm. E/09159/2020 [JUR 2021\81351].

4 Resolución de 15 de marzo de 2021, procedimiento núm. PS/00492/2020 [JUR 2021\81333].

5 Resolución de 5 de enero de 2021, procedimiento núm. E/02460/2020 [JUR 2021\76953].

6 Resolución de 12 de febrero de 2021, procedimiento núm. E/06746/2020 [JUR 2021\69598].

7 Resolución de 26 de febrero de 2021, procedimiento núm. PS/00461/2020 [JUR 2021\67722].

8 Informe de la AEPD sobre Notificaciones de Brechas de Seguridad de los Datos Personales durante el mes de enero de 2021.

9 https://www.aepd.es/es/prensa-y-comunicacion/blog/brechas-de-seguridad-protegete-ante-la-perdida-o-robo-de-un-dispositivo

10 ATS (Sala de lo Penal, Sección 1ª), de 18 de marzo de 2021 [JUR 2021\99459].

11 Resolución de 15 de marzo de 2021, procedimiento núm. PS/00288/2020 [JUR 2021\81336].

Novedades y aspectos más relevantes de la Guía

El principal objetivo perseguido por la AEPD con la Guía es permitir a responsables y encargados del tratamiento **cumplir de forma eficaz y eficiente con los artículos 33 y 34 RGPD**, que regulan, respectivamente, el régimen de notificación de una violación de seguridad de datos personales a la autoridad de control y la obligatoriedad de comunicar el incidente a los interesados cuando este haya podido afectar a sus derechos y libertades fundamentales. Para cumplir con dicho objetivo, en la Guía, la AEPD hace especial hincapié en las siguientes cuestiones:

¿Qué SÍ es una brecha de seguridad?
Violaciones que ocasionen:

- Destrucción; pérdida o alteración.
- Accidental o ilícita.
- De datos personales transmitidos, conservados o tratados.
- Comunicación o acceso no autorizado a dichos datos.

¿Qué NO es una brecha de seguridad?
Incidentes que:

- No afecten a datos personales (relativos a personas físicas identificables o identificables).
- No afecte al tratamiento llevado a cabo por el responsable o encargado.
- Vulneración que afecte a una persona física en el ámbito doméstico.

PLAZOS

Detección de la brecha e informar al responsable <72h (en el acuerdo de encargo del tratamiento se deberá especificar el plazo de la notificación al responsable).

Notificación de la brecha a la AEPD y comunicación a interesados <72h desde el incidente NO desde comunicación del encargado.

Ampliación o modificación de la notificación a la AEPD <30. En este plazo la AEPD podrá dirigir requerimientos de información adicionales o imponer la obligación de comunicación a afectados.

¿Quién debe notificar?

- La notificación de una brecha de datos personales a la Autoridad de Control conforme al artículo 33 RGPD **corresponde al responsable del tratamiento**.
- El **encargado sólo** podrá notificar en nombre del responsable si así lo tiene establecido en un contrato.
- Deberá realizar **una notificación por cada responsable** afectado, **salvo si la brecha ha afectado por igual** a los derechos y libertades de los interesados de los diferentes responsables a los que presta servicio.

¿Qué información requiere la autoridad de control?

- Detalles sobre el tratamiento y el responsable.
- Intencionalidad y origen de la brecha.
- Tipología (confidencialidad, disponibilidad o integridad).
- Categorías de datos y perfil de los afectados.
- Consecuencias de la brecha.
- Resumen de la misma.
- Implicaciones transfronterizas.
- Información temporal y medios de detección.
- Medidas de seguridad preventivas.
- Acciones tomadas.
- Comunicación a los afectados doméstico.

¿Cuándo no comunicar a los interesados una brecha?

Cuando el responsable haya tomado medidas técnicas y organizativas adecuadas que:

- **Eviten** los riesgos anteriores.
- **Minimicen** los daños a los derechos y libertades y/o los hacen reversibles.
- **Con posterioridad a la brecha**, mitiguen total o parcialmente el impacto para los afectados y garanticen que no hay riesgo para sus derechos y libertades.

¿Cuándo comunicar a los interesados una brecha?

- Cuando sea probable que el incidente entrañe **alto riesgo para los derechos y libertades** de las personas físicas afectadas.
- Cuando así lo dispongan **otras obligaciones legales y/o contractuales.**
- Cuando los **daños** producidos sean **irreversibles, difíciles de mitigar** o puedan ocasionar perjuicios posteriores.

Andy Ramos | Counsel de Propiedad Intelectual, Industrial y Tecnología | aramos@perezllorca.com | T: +34 91 423 20 72
Alicia Maddio | Abogada de Propiedad Intelectual, Industrial y Tecnología | amaddio@perezllorca.com | T: +34 91 423 47 56