Ha ocurrido una brecha… ¿Y ahora qué? Guía Práctica para las empresas

Las brechas en la seguridad, que comprometen datos personales, son eventos extremadamente delicados que cualquier empresa podría experimentar. La pérdida de información, accesos no autorizados, envíos de correos electrónicos equivocados y ciberataques, todo esto genera una inmediata preocupación y la pregunta que siempre surge es: ¿Debemos notificar la brecha o no? La Agencia Española de Protección de Datos (AEPD) destaca que, aparte de esa duda inicial, lo más crucial es como se maneja el incidente desde el mismo instante en que se detecta.

El Reglamento General de Protección de Datos (RGPD) establece que una brecha debe notificarse a la autoridad de control cuando pueda suponer un riesgo para los derechos y libertades de las personas. Esta notificación debe realizarse sin dilación indebida y, como regla general, **en un plazo máximo de 72 horas desde que la empresa tiene constancia del incidente**. No obstante, si tras una evaluación razonada se concluye que la brecha no entraña riesgos para los afectados, no será necesario notificar, siempre que dicha valoración quede debidamente documentada.

Además, cuando el riesgo para las personas sea elevado, la empresa deberá comunicar la brecha directamente a los afectados, **de forma clara y comprensible, explicando qué ha ocurrido y qué medidas pueden adoptar para protegerse**. Esta obligación no responde a un criterio automático, sino a una evaluación concreta del impacto que el incidente puede tener sobre la privacidad, la seguridad o los derechos de las personas implicadas.

La AEPD insiste en que el verdadero error no está en notificar una brecha, sino en no detectarla, no analizarla o no documentar adecuadamente la decisión adoptada. **Notificar de forma diligente no implica necesariamente la apertura de un procedimiento sancionador.** De hecho, la experiencia demuestra que la Agencia valora positivamente la transparencia, la rapidez de actuación y la adopción de medidas correctoras adecuadas.

Por ello, resulta esencial que las empresas cuenten con procedimientos internos claros para la gestión de incidentes de seguridad, que permitan identificar rápidamente una brecha, evaluar su impacto, adoptar medidas de contención y decidir de forma fundamentada si procede la notificación. Incluso cuando no sea necesario comunicar el incidente a la AEPD o a los afectados, el RGPD exige que todas las brechas queden registradas y documentadas.

En Escura, aconsejamos una gestión preventiva y organizada de las brechas de seguridad, unificando la protección de datos con los protocolos de seguridad de la compañía. Una respuesta apropiada frente a un incidente ayuda a cumplir con los requerimientos legales, y ayuda a minimizar daños, proteger la confianza de los clientes y empleados y, además, disminuye las posibles sanciones a futuro.

Consulta la nota de la AEPD.