LA GESTIÓN DE LAS BRECHAS DE SEGURIDAD: ¿CÓMO AFRONTARLAS?

La plena aplicación del Reglamento General de Protección de Datos 2016/679, de 27 de abril (RGPD), ha comportado que, desde mayo de 2018, las empresas hayan notificado más de 475 brechas de seguridad ante la Agencia Española de Protección de Datos (AEPD), según informó ésta durante unas jornadas de ciberseguridad celebradas el pasado mes de diciembre, a falta de estadísticas oficiales hasta la fecha.

La propia AEPD, en colaboración con el Centro Criptológico Nacional y el Instituto Nacional de Ciberseguridad, ha publicado una "*Guía para la gestión y notificación de brechas de seguridad*" -accesible aquí- con el propósito de acompañar al responsable durante el proceso de gestión del incidente.

De conformidad con dicha Guía, toda empresa que trate datos de carácter personal deberá trazar un plan de actuación, que contemple los recursos materiales y humanos que serán necesarios para mitigar las consecuencias y daños asociados a la brecha de seguridad.

A título meramente identificativo, indicar que toda empresa deberá contar con mecanismos ágiles de prevención y detección de este tipo de incidentes, para lo cual existen servicios de avisos o notificaciones sobre bases de datos, productos web, etc. que sin duda merece la pena tener presentes.

Una vez detectada la brecha de seguridad, la empresa afectada deberá clasificar el tipo de incidente, y por supuesto valorar si el mismo afecta o no a datos de carácter personal. En caso de afectación, dicha evaluación debería determinar la peligrosidad potencial del incidente, aportando una estimación de la magnitud del impacto potencial en los individuos afectados.

Seguidamente, será necesario coordinar un proceso de respuesta ante la autoridad de control competente. Con carácter general, dicha notificación deberá realizarse a más tardar 72 horas después de que se haya tenido constancia del incidente.

No puede obviarse que también será necesario valorar si existe un alto riesgo para los derechos y las libertades de las personas físicas, en cuyo caso deberá cursarse una notificación a los afectados. Sin lugar a dudas, resultará especialmente importante que, en su caso, la comunicación a los afectados incluya la información precisa, pertinente y adecuada.

En caso contrario, los daños y perjuicios asociados a la brecha de seguridad podrían ser muy elevados. El incumplimiento de los requerimientos incluidos en el RGPD podría suponerle al infractor una multa administrativa superior a los 10 millones de euros, o el equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, a lo que habría que añadir un más que probable daño reputacional, en ocasiones irreparable.

Todo el proceso de respuesta al incidente debe quedar documentado con la elaboración de un informe de resolución que podrá ponerse a disposición de la Agencia Española de Protección de Datos.

A modo de conclusión, indicar que, ante el interrogante inicial de qué actuaciones o medidas deberían diseñarse e implantarse por cualquier empresa para gestionar una brecha de seguridad, resultará indispensable formalizar un protocolo de actuación que, en atención al tamaño y complejidad de cada organización, incluya detalles sobre cómo deben escalarse las notificaciones internamente.

Y para ello, el papel del delegado de protección de datos, o en su defecto del especialista en la materia, será crucial a fin de coordinar un procedimiento de respuesta que, según hemos descrito, puede revestir cierta complejidad, tanto por la sensibilidad de los intereses en juego, como por la necesidad de responder de forma casi inmediata ante la autoridad de control y los afectados, en su caso.

Carlos García Berned, abogado
Departamento TMT de Fieldfisher JAUSAS
carlos.garcia@fieldfisher.com

Sigue toda la actualidad del sector en el blog de Fieldfisher JAUSAS