LAS EMPRESAS, RESPONSABLES DE LA CORRECTA AUTOEVALUACIÓN DE SUS RIESGOS

26 de enero de 2018

En estos días, y más con el foco puesto en el día de la protección de datos, no vamos a hablar de las principales novedades que vienen de la mano de la aplicación efectiva a partir del próximo 25 de Mayo, del reglamento general de protección de datos, de 27 de abril de 2016, más conocido como RGPD o GPDR.

La nueva normativa, el reglamento general de protección de datos (RGPD), está generando algún que otro quebradero de cabeza a las empresas que ven cómo el plazo de adecuación previsto normativamente se les echa encima, teniendo aún muchas cuestiones por aclarar y resolver. Y es que, a diferencia de la normativa vigente (LOPD - LO15/1999, y RLOPD - RD1720/2007), el RGPD deja de la mano de las entidades la autoevaluación de sus riesgos para la determinación de las concretas medidas de protección a implantar.

La evaluación de riesgos

En materia de análisis de riesgos, la mayor complejidad con la que se encuentran las entidades es la determinación de los riesgos sobre los derechos y libertades de los ciudadanos, en especial en lo relativo a la privacidad del usuario, pues deben tenerse en cuenta amenazas e impactos específicos.

No obstante, los análisis de riesgos a llevar a cabo para la determinación de las medidas de seguridad a implantar (objeto del presente artículo), y la determinación de catálogos de amenazas e impactos, son aspectos que se encuentran mucho más regulados, desarrollados e implantados, tanto a nivel nacional como internacional, lo que sin duda supone una ventaja para las compañías que pueden adoptar estas metodologías en materia de cumplimiento normativo, y en especial, en materia de protección de datos personales.

Los principios de la seguridad y su aplicación con el RGPD

El RGPD en materia de seguridad, se remite a los principios básicos de la seguridad de la información, estableciendo expresamente en su artículo 32, que la medida de seguridad básica a tener en cuenta por cualquier organización debe ser la pseudoanonimización y el cifrado de los datos personales siempre que sea posible, así como la necesidad de reevaluar y verificar periódicamente los riesgos, las medidas de seguridad implantadas y el nivel de cumplimiento.

Pero además, el RGPD remite claramente a los principios básicos de la seguridad (confidencialidad, integridad, y disponibilidad) y casi de forma expresa a las metodologías y estándares internacionales en materia de seguridad y continuidad de negocio.

Gestión de brechas de seguridad

En línea con los principios de seguridad, y en relación directa con la comunicación y gestión de incidentes de seguridad, el RGPD establece una obligación específica de comunicación de brechas de seguridad para todas las entidades, comunicación que debe incluir a las Autoridades de Control, e incluso a los propios titulares de los datos.

Dada la criticidad de este tipo de comunicación, la elaboración de procedimientos específicos de comunicación y gestión de brechas de seguridad, en el que no sólo estén implicados los departamentos técnicos y jurídicos, sino que además incluyan a las áreas de Comunicación Externa de la compañía, es un aspecto esencial para el cumplimiento de la norma y la protección de la imagen y reputación corporativa de la organización.

Estándares internacionales y sistemas de gestión

Para la gestión de riesgos, las compañías se basan en metodologías y estándares ampliamente implantados como la ISO 31000, o metodologías como Magerit, u otras metodologías de análisis de riesgos que se encuentran implantadas en las organizaciones para el cumplimiento de otras materias, pero que sirven de base para los análisis exigidos por el RGPD.

En materia de seguridad de la información, y sobre la necesidad de garantizar la Confidencialidad, Integridad y Disponibilidad de los datos, el estándar más común y conocido es la ISO 27001, pues son muchas las compañías que ya han optado por certificar todos o alguno de sus procesos, tanto como otras que cuentan con marcos normativos implantados basados en los principios de este estándar aún sin contar con la citada certificación.

En materia de continuidad de negocio, y con el objeto de garantizar no sólo la disponibilidad, sino el rápido acceso a la información en caso de incidente, la ISO 22301 es la que tiene mayor implantación. La utilización de una misma metodología en gestión de riesgos y en el establecimiento de marcos normativos, junto con el establecimiento de pruebas y revisiones periódicas, hace que la integración de los marcos normativos de seguridad y continuidad surja casi como algo natural.

Esta misma línea debería seguir la recientemente publicada ISO 29151 relativa a privacidad en los tratamientos de datos personales, o las posibles certificaciones que en base al artículo 42 del RGPD puedan ser aprobadas en el futuro.

Integración de sistemas de gestión

Se encuentran por tanto las entidades ante una oportunidad real de crear un marco de *risk, governance & compliance*, que a través de la integración de distintos sistemas de gestión (seguridad de la información, continuidad, calidad, privacidad, ...), permitan a las compañías, no sólo garantizar y acreditar el cumplimiento de las normas que les resulten de aplicación, sino aportar un verdadero valor añadido a sus clientes a través del respeto a sus derechos y libertades.

¿Futura certificación?

Y para concluir, cabe referenciar, entre otras iniciativas, EuroPriSe (European Privacy Seal), esquema de certificación diseñado para promover la visibilidad con el cumplimiento y respeto por privacidad, mejorando plataformas web, y productos y servicios TI. Al introducir un procedimiento transparente y revisable, EuroPriSe tiene como objetivo movilizar la competencia en la privacidad y fomentar la confianza de los usuarios.

En esta misma línea, la CNIL francesa está desarrollando su propio sello y certificación, al igual que probablemente lo harán otras autoridades de control, o inclusive la propia Comisión Europea.

Fuentes: www.expansion.com