23 de marzo de 2017

3

LA CODIFICACIÓN CON EL NUEVO REGLAMENTO DE PROTECCIÓN DE DATOS

Reglamento (UE) 2016/679

Con la entrada en vigor del Nuevo Reglamento de Protección de Datos (UE), se amplían las obligaciones de implantación de medidas de seguridad tanto para las empresas, como para el resto de entes u organismos públicos. Entre dichas medidas, se encuentran la implementación de cifrados y sistemas de 2FA incluso cuando estemos tratando datos de nivel básico.

Desde la UE se considera, con buen criterio, que las empresas, hoy más que nunca, necesitan proteger de forma contundente su información frente a posibles ataques o intromisiones en sus sistemas informáticos ante los riesgos que una posible brecha de seguridad acarrearía, tanto para la empresa como para sus clientes o potenciales; de ahí que el cifrado y el sistema de doble factor de autenticación (también conocido como 2FA) sean considerados los pilares básicos de la seguridad en el Nuevo Reglamento de Protección de Datos (Considerando 83).

No obstante, la idea preconcebida de sistemas complejos tanto de manejar como de implantar está en la actualidad obsoleta, para ello hacemos referencia a lo destacado por D. Arturo Ribagorda, Catedrático Informático de la UC3M, el cual afirma lo siguiente: "la idea de la dificultad en la aplicación de las medidas de seguridad en materia de Protección de Datos es una idea errónea y falaz".

IMPORTANCIA DEL CIFRADO

Hoy día ninguna empresa, por pequeña o grande que sea, puede asegurar que no ha sufrido o sufrirá un ataque a sus activos; entendiéndose por estos, los ficheros en soporte informático de los que dispone.

Por ello, la AGPD en su informe nº 494/2009 destaca la importancia de llevar a cabo una protección adecuada de los datos: "*La seguridad en el intercambio de información de carácter personal en la que hay que adoptar medidas de seguridad de nivel alto, en particular los requisitos de cifrado de datos, no es un tema baladí, ni un mero trámite*

RIESTRA ABOGADOS
Marketing Legal
Pº de la Castellana, 135 - 7ª pta.
28046 Madrid

t- (34) 91 790.68.94
f- (34) 91 790.68.69
www.riestra-abogados.com

administrativo ni una cuestión de comodidad. Es el medio técnico por el cual se garantiza la protección de un derecho fundamental y al que hay que dedicar el tiempo y los recursos que sean necesarios para su correcta implementación".

¿DE QUÉ OPCIONES DE CIFRADO DISPONEMOS?

Las opciones de cifrado a aplicar en España, se basan tanto en lo establecido por la normativa europea en dicha materia como en el art. 104 del Reglamento de desarrollo de la Ley Orgánica de Protección de Datos (RDLOPD); por tanto, las empresas que se encuentren obligadas por el volumen de activos, etc a adoptar medidas de cifrado, podrán elegir entre:

- Sistema profesional de cifrado robusto.
- Cualquier otro sistema que garantice que la información no será inteligible ni exista posibilidad de manipulación por personas ajenas a la empresa.

Artículo 104 del Reglamento de la LOPD:

> *"Cuando, conforme al artículo 81.3, deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros".*

Por tanto, las empresas se deben ceñir a dichos sistemas de cifrado y omitir aquellos que no garantizan la seguridad adecuada como por ejemplo son las diferentes herramientas para uso particular o la compresión de archivos. La AGPD se ha pronunciado al respecto diciendo lo siguiente: *"Los productos que generan archivos PDF o el realizado por WinZip tienen vulnerabilidades conocidas y se disponen de herramientas de libre distribución que aprovechan dichas vulnerabilidades. Más concretamente, no sólo se pueden obtener en Internet fácilmente utilidades que rompen las protecciones de los archivos PDF o ZIP, sino que el propio algoritmo en el que descansa la cifra de documentos PDF, el algoritmo RC4, es manifiestamente vulnerable"* (Informe 494/2009).

RIESTRA ABOGADOS
Marketing Legal
Pº de la Castellana, 135 - 7ª pta.
28046 Madrid

t- (34) 91 790.68.94
f- (34) 91 790.68.69
www.riestra-abogados.com

3

NOVEDADES QUE INTRODUCE EL NUEVO REGLAMENTO DE PROTECCIÓN DE DATOS

Con motivo del nuevo Reglamento General de Protección de Datos (UE) existen tres "grados" de cifrado:

- *Cifrado obligatorio:*

  - Viene establecido por imposición estatal; es decir; en España todas aquellas empresas u organismos que traten datos especialmente sensibles (origen étnico o racial, opiniones políticas, convicciones religiosas, …) y por tanto tengan que aplicar medidas de seguridad de nivel alto, se verán obligadas a adoptar sistemas de cifrado para proteger sus archivos.
  - Todas aquellas empresas que se hayan adherido a un código de conducta, deberán adoptar obligatoriamente un sistema de cifrado, en el supuesto de que dicho código así lo establezca.
  - Las empresas que traten datos biométricos u observen de forma sistemática zonas de acceso público, deberán cifrar los datos que recaban.
  - Si existe un riesgo cierto, la empresa u organismo en cuestión deberá adoptar un sistema de cifrado para mitigar el mismo, independientemente de la importancia de los datos manejados.

- *Cifrado recomendado:*

  - Todas las empresas, independientemente del volumen o importancia de los datos personales que traten deberían implementar un sistema de cifrado para salvaguardar los archivos en soporte informático de que dispongan y generar mayor seguridad a sus usuarios.

- *Cifrado voluntario:*

  - El sistema de cifrado será una medida opcional para aquellas empresas que traten datos disociados, puesto que a través de los mismos no sería posible identificar a una persona física.

RIESTRA ABOGADOS
Marketing Legal
Pº de la Castellana, 135 - 7ª pta.
28046 Madrid

t- (34) 91 790.68.94
f- (34) 91 790.68.69
www.riestra-abogados.com

3

OBLIGACIONES PARA EL RESPONSABLE Y EL ENCARGADO DEL TRATAMIENTO

Conforme a lo establecido en el art. 32 del RGPD (UE) tanto el responsable como el encargado del tratamiento deberán aplicar medidas técnicas y organizativas apropiadas como:

- La seudonimización y el cifrado de datos personales;
- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
- Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

¿QUÉ OBLIGACIONES EXISTEN ANTE UNA BRECHA DE SEGURIDAD?

Según el RGPD (UE) **TODAS** las empresas están obligadas a notificar cualquier brecha de seguridad sufrida, por ínfima que sea y, comunicarla a los interesados. Por tanto, inmediatamente al conocimiento por parte de la empresa de dicha vulnerabilidad en el sistema de seguridad, se deberá notificar a la AGPD o a la autoridad de control que sea competente.

Dicha notificación se deberá realizar con la mayor celeridad y, siempre que sea posible, dentro de las 72 horas posteriores al momento en el que se tiene consciencia de dicha brecha de seguridad.

Como se puede dilucidar de todo lo anteriormente expuesto, el sistema de cifrado es una medida de seguridad en cierto modo obligada en determinados casos y, siempre recomendada desde las instituciones europeas y que la AGPD ha tomado como suya puesto que de forma diaria se producen millones de ataques a cualquier tipo de empresa u organización para acceder a datos personales; por tanto; el cifrado tiene como objetivo último proteger los derechos y libertades de las personas físicas.

Por ello, las sanciones podrían versar entre multas administrativas de 10 millones de euros como máximo o, una cuantía equivalente al 2% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la cuantía más elevada (art. 83 RGPD (UE).

RIESTRA ABOGADOS
Marketing Legal
Pº de la Castellana, 135 - 7ª pta.
28046 Madrid

t- (34) 91 790.68.94
f- (34) 91 790.68.69
www.riestra-abogados.com