PLAN DE **PREVENCIÓN** Y **GESTIÓN** DE **BRECHAS** DE **SEGURIDAD**

ecix

1 Introducción: las brechas de seguridad

Según datos publicados por la **Agencia Española de Protección de Datos (AEPD)**, en los cinco primeros meses de 2021 han recibido **más de 700 notificaciones de brechas de seguridad.**

Este dato sigue demostrando que este tipo de incidentes sigue una **tendencia al alza**, como ya adelantaban los datos publicados en la memoria anual de la AEPD de 2020, que muestra un **incremento del 3%** en el número de notificaciones de brechas de seguridad trasladadas a la Subdirección General de Inspección de Datos.

Hay que recordar que el Reglamento General de Protección de Datos **define** las quiebras de seguridad de los datos personales como aquellos **incidentes** que ocasionan:

- La destrucción
- La pérdida
- La alteración accidental o lícita de datos personales

Pero también tiene la consideración legal de brecha de seguridad la comunicación o el acceso no autorizado a datos personales cuya protección esté encomendada a un responsable del tratamiento.

Este tipo de incidentes **afecta a cualquier tipo de empresa**, con independencia de su tamaño o sector de actividad, y **provoca serios daños económicos y reputacionales**. Según datos publicados por el Instituto Nacional de Ciberseguridad (INCIBE), en el año 2020 se gestionaron más de 130.000 incidentes de seguridad en empresas y ciudadanos, muchos de los cuales incluían una fuga de datos personales que desembocó en un **procedimiento sancionador** ante la citada AEPD.

Una de las **causas que provoca este aumento** de actividad es que el **ciberdelito** se ha convertido en la industria criminal más lucrativa, por delante del narcotráfico o la falsificación de productos. A esto hay que añadir que la información de las empresas en general, y **los datos personales** que custodian, **son activos de gran valor** que los cibercriminales tratan de robar o hacer inaccesibles a sus legítimos propietarios con tal de extorsionarles, a través de técnicas tales como el *ransomware*.

En relación con este tipo de ciberataque, en Mayo de 2021, la compañía aseguradora AXA anunciaba que **dejaba de dar cobertura aseguradora** a sus clientes en relación con el pago del ransomware, al que consideraba una "pandemia delictiva de dimensiones mundiales".

A la vista de este escenario, el Gobierno de España ha aprobado un **Plan de Choque en Ciberseguridad**, cuyo objetivo es reforzar de manera inmediata las capacidades de defensa frente a las ciberamenazas sobre las **entidades del sector privado** que suministran tecnologías y servicios al sector público estatal, especialmente a través de una actualización de la Estrategia Nacional de Ciberseguridad y del Esquema Nacional de Seguridad.

Estas actuaciones exigidas por el Gobierno a las empresas deben servir para reforzar de manera eficaz la capacidad de prevención, detección, protección y defensa frente a la materialización de las ciberamenazas.

A la vista de lo anterior, cabe concluir que la **transformación digital** debe ir acompañada de medidas organizativas y técnicas de seguridad **proporcionadas a los riesgos**, lo que favorecerá la **confianza** en el uso de tecnologías digitales por parte de los actores económicos y de la ciudadanía en general.

+ 700 Brechas de Seguridad notificadas en 6 meses del 2021

+130.000 incidentes de seguridad en 2020 según el INCIBE

2 La obligación

Tanto el RGPD como la normativa sectorial de aplicación a sectores esenciales y críticos, recogen la obligación de que las empresas **adopten medidas técnicas y de organización, adecuadas y proporcionadas, para gestionar los riesgos** que se planteen para la seguridad de las redes y sistemas de información utilizados, así como para la información que circula y se almacena en aquellos.

En este mismo sentido, tal obligación se extiende al deber de tomar medidas adecuadas para **prevenir y reducir al mínimo el impacto de los incidentes** que puedan producirse y que les afecten.

La **gestión de este tipo de riesgos**, tanto desde el punto de vista de su **prevención** como de su **reacción**, deben abordarse en todas las fases de su desarrollo, como son:

- Identificación del riesgo
- Valoración de su impacto posible y probable
- Implementación de medidas adecuadas
- Acreditación del nivel de eficacia de dichas medidas
- Cobertura del riesgo
- Minimización de su impacto
- Comunicación a la autoridad de control y a los afectados de la producción del incidente

Las brechas de seguridad son una de las principales amenazas para la continuidad del negocio, y una de las principales causas de pérdida de confianza por parte de clientes y usuarios.

3 El responsable

La empresa que trata datos personales es **legalmente responsable** del cumplimiento de la obligación de que tales datos se custodien garantizando una **seguridad adecuada** mediante la aplicación de medidas técnicas y organizativas apropiadas; y, además, debe ser capaz de demostrarlo en base al principio de lo que se conoce como **responsabilidad proactiva.**

A los efectos de asegurar que las medidas que el responsable aplica son **suficientes y apropiadas** para garantizar un nivel de seguridad adecuado al riesgo, deben elegirse soluciones que garanticen, entre otros:

- 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.

Además de implantarlas, la norma exige que las medidas escogidas **se revisen y actualicen** periódicamente, con tal de poder acreditar la idoneidad de su vigencia.

Asimismo, el citado Reglamento también hace recaer en el responsable del tratamiento la responsabilidad de elegir adecuadamente a los encargados de tratamiento, de manera que es obligación del responsable **elegir únicamente aquellos proveedores que ofrezcan garantías suficientes** de que aplican medidas técnicas y organizativas apropiadas para garantizar la protección de los datos que son objeto de tratamiento. Es lo que se conoce como *"third party compliance"*.

El responsable del tratamiento es responsable de elegir únicamente aquellos proveedores que ofrezcan garantías suficientes garantizando el "third party compliance".

4 La obligación de notificar el incidente

Desde la entrada en vigor del RGPD, todo responsable del tratamiento tiene la **obligación de notificar** a la autoridad de control (en el caso de España la Agencia Española de Protección de Datos), las brechas de seguridad que pudiesen afectar a datos personales de cuya custodia es responsable.

A estos efectos, la propia AEPD publicó una guía de notificación de brechas de seguridad, donde se recogen los criterios que deben seguirse a la hora de proceder a este tipo de comunicación.

La **obligación de notificación a los terceros afectados puede no ser exigible** si el responsable puede demostrar, atendiendo al principio de responsabilidad proactiva, la baja probabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas afectadas, lo que puede conseguirse a través de la implantación de medidas preventivas.

5 El riesgo sancionador

Del análisis de los datos de las sanciones impuestas por infracción del artículo 32 del RGPD, que es el que regula las fugas de datos provocadas por incidentes de seguridad que afectan a los sistemas de la empresa, se puede observar el impacto económico que tiene para las empresas que han sido víctimas de un ciberataque*:

Alcance geográfico	Total sanciones	Sanción máxima impuesta	Media sanciones
Todos los países	66.668.890€	27.800.000€	724.661,85€
España	430.800€	60.000€	26.925€

*Datos extraídos de la herramienta eRadar de Ecix, de análisis de la actividad sancionadora, a 16 de junio de 2021.

A estos eventuales costes derivados de la imposición de sanciones hay que sumarles los derivados de la gestión técnica y jurídica que la entidad afectada pudiera necesitar durante la fase reactiva de gestión del incidente.

Respecto a esta situación, y en los términos exigidos por el RGPD, se considera una **infracción grave** la falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento.

El artículo 83 del RGPD, al tratar las consideraciones generales para la imposición de multas administrativas, establece en su apartado 2.d) que:

> *Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual, se tendrá debidamente en cuenta el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado.*

Las infracciones del RGPD se sancionarán con **multas administrativas** de 10.000.000€ como máximo o, tratándose de una empresa, de una cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por **la de mayor cuantía.**

6 Servicio de prevención de Ciberriesgos

La contratación de este servicio de **prevención de ciberriesgos** es una actuación fundamental en el objetivo de ayudar a la empresa a obtener y, sobretodo, a poder acreditar de forma satisfactoria, **un alto nivel de diligencia** a la hora de enfrentarse a un incidente que, eventualmente, pudiera llevar implícito una brecha de datos personales.

Las actuaciones a diseñar se basan en el profundo conocimiento técnico y en la experiencia de gestión de numerosos incidentes de seguridad gestionados por el equipo de ECIX.

Las acciones concretas de implantación del servicio se pueden estructurar en tres fases:

Fase 1. Prevención del incidente

- Revisión y actualización de políticas y procedimientos existentes
- Desarrollo e implementación de nuevas necesidades
- Diseño e implantación de controles de cumplimiento
- Elaboración de un plan de acción
- Auditoría de cumplimiento de aquellos terceros que componen la cadena de suministro de la Empresa
- Diseño, implantación y ejecución de Plan formativo en ciberseguridad
- Realización de simulacros, ciberejercicios, etc.

Fase 2. Detección y reacción ante una brecha de seguridad

- Elaboración de cronología de hechos sucedidos
- Recopilación de evidencias electrónicas necesarias durante el proceso sancionador
- Interlocución con investigadores y Fuerzas y Cuerpos de Seguridad del Estado
- Preparación e interposición de denuncias y reclamaciones
- Asesoramiento en la estrategia de notificación del incidente

Fase 3. Actuación

- Notificación al organismo de control (AEPD)
- Preparación de alegaciones y presentación de evidencias
- Apoyo en la gestión del procedimiento administrativo
- Ayuda en la gestión del procedimiento penal
- Gestión jurídica y de reclamación con el ciberseguro contratado.
- Valoración de notificación a afectados.

7 Tecnología legaltech para la prevención de brechas de seguridad

Todas las actuaciones que se van a diseñar durante todas las fases del servicio pueden **acompañarse de soluciones tecnológicas propias** que garanticen un alto nivel de cumplimiento de las obligaciones legalmente exigidas y, en consecuencia, reforzar aún más si cabe la **acreditación del nivel de diligencia** aplicado por la Empresa en la prevención y gestión de eventuales incidentes de seguridad. Entre dichas herramientas destacan:

eGRC: herramienta de gestión de riesgos empresariales y ciberseguridad

eTPC: herramienta de control de cumplimiento de terceros y proveedores

ePrivacy: herramienta de gestión de privacidad y tratamiento integral de datos personales ciberseguridad

8 Ecix Group

Como especialistas en Cumplimiento Normativo y Derecho Digital, ECIX Group puede ayudarte a afrontar los retos a los que las funciones de Compliance, Riesgos, Privacidad y Ciberseguridad se van a enfrentar en el nuevo escenario empresarial con nuestros servicios especializados y herramientas pioneras.

ECIX: Asesorando desde hace más de 20 años en las áreas de Cumplimiento y Ciberseguridad a las principales empresas españolas. En ECIX prestamos un servicio de primer nivel mediante un equipo de más de 150 profesionales especializados y una Metodología propia fruto del resultado de la investigación y la aplicación de las matemáticas y el Big Data.

www.ecixgroup.com

ELIX Regtech: Desarrollando herramientas desde 2002 que ayuden a nuestros clientes en la identificación y gestión de riesgos legales y empresariales. Desde soluciones de Protección de Datos, Cookies, Consentimientos, GRC, evaluación de terceras partes (TPC), Formación y Concienciación, etc.

www.elixregtech.com

ECIX GROUP

Expertos en gestión de riesgos empresariales

Madrid
Paseo de la Castellana, 52.
28046 Madrid
(+34) 91 001 67 67

Zaragoza
C/Zurita 10, entresuelo dcha.
50001 Zaragoza
(+34) 976 11 37 57

Barcelona
Avenida Diagonal, 468
08029 Barcelona
(+34) 93 807 48 50