¿ESTÁ PREPARADO PARA EL RGPD?

(REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS)

LO QUE LAS EMPRESAS NECESITAN SABER SOBRE EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS Y SU IMPORTANCIA DE CARA A LA SEGURIDAD CIBERNÉTICA

Made possible

QBE

Contenido

1 El panorama cibernético está cambiando rápidamente

2 ¿Qué es el RGPD?
- Consentimiento: un gran cambio
- Solicitud de acceso del interesado
- Notificación de violaciones de seguridad de los datos
- ¿Necesitan un responsable de protección de datos?
- ¿A qué tipo de datos afecta?
- El RGPD en resumen

3 ¿Qué pueden hacer?
- Mejor en el peor escenario
- Formación del personal. Es una cuestión de cultura corporativa
- Protocolos de almacenamiento. Sepa donde almacena sus datos
- Niveles de cumplimiento y certificación. Anticípese
- Los servicios en la nube no le libran de responsabilidad
- La privacidad por diseño
- Lo que debe implementar para cumplir con el reglamento

4 Caso práctico: QBE
- Cómo abordar una violación de la seguridad
- ¿Qué obligaciones tienen hacia sus clientes?

5 Tras la violación de la seguridad de datos
- Gestionar el impacto reputacional
- Restaurar la situación inicial
- Abordar una violación de seguridad
- Grandes brechas de seguridad: los eventos más conocidos
- ¿Qué debe cubrir una buena póliza de seguridad cibernética?
- ¿Está preparado?

6 La cobertura QBE: protección 24/7 contra el riesgo cibernético

7 ¿Quiénes somos?

El panorama cibernético está cambiando rápidamente

Nos encontramos ante el cambio mas importante en materia regulatoria de Privacidad y Protección de Datos de los últimos 20 años. El día 25 de mayo de 2018, el Reglamento General de Protección de Datos (RGPD) entrará en vigor, reemplazando a la Ley Orgánica 15/1999, de 13 de diciembre Protección de Datos de Carácter Personal y su Reglamento de desarrollo.

El alcance del nuevo reglamento es más amplio y las sanciones derivadas de su incumplimiento más severas, pudiendo alcanzar hasta el 4% del volumen global anual de negocio de la empresa (matriz) o 20M€, la mayor cifra de las anteriores.

Ninguna empresa será inmune. Todas las compañías europeas están reevaluando ya sus medidas de seguridad y almacenamiento de los datos.

Hay buenas razones que justifican el nuevo reglamento. Las recientes violaciones de la seguridad de gran repercusión ilustran la necesidad de que las compañías pongan orden en sus casas en cuanto a la protección de datos. De lo contrario, las compañías estarán expuestas a ataques cibernéticos de diversa índole, lo que puede comprometer la seguridad de sus datos.

Es un mito que las Pymes se encuentran menos expuestas a estos riesgos. De hecho asistimos a la tendencia de atacar aquellas empresas cuyas medidas de seguridad son menos robustas, accediendo través de las mismas a empresas más grandes. En 2016, las compañías europeas tuvieron una pérdida total atribuible a delitos cibernéticos de más de un billón de euros.

Las empresas se están dado cuenta de que la encriptación de los datos no es suficiente por si sola para evitar el fraude o el uso indebido. La seguridad cibernética no engloba solo la piratería y el phishing: lo abarca todo, desde el lanzamiento de e-mails con fines comerciales hasta el almacenamiento de archivos por más tiempo del preceptivo.

¿Qué es el RGPD?

Como resultado de cuatro años de trabajo, el RGPD es un reglamento diseñado para fortalecer y unificar la protección de los datos de todas las personas en la Unión Europea. Establece cómo las empresas deben procesar y almacenar los datos, reduciendo la mala gestión de los mismos y fomentando una mejor cultura corporativa respecto de la privacidad de los datos.

Actualmente, la Ley de Protección de Datos en vigor, permite que la Agencia española de Protección de datos imponga sanciones de hasta 600.000 euros por infracciones muy graves. El RGPD es en general más amplio y las consecuencias por incumplimiento más duras.

Según Jade Kowalski, abogado de DAC Beachcroft y especialista en la protección de datos, dice:

"Esto es un hito histórico en el mundo de la protección de datos. El RGPD es la primera actualización sustancial de la protección de datos en dos décadas. La cuenta atrás para su cumplimiento está en pleno proceso, y toda organización debe prepararse para el impacto que el RGPD tendrá en las prácticas empresariales".

"La mayor parte del RGPD ya recoge las particularidades de cada territorio, complementando y mejorando aquellos derechos y obligaciones que ya se encuentran presentes en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su Reglamento de desarrollo. Sin embargo, el RGPD hace más prescriptivas las obligaciones de las compañías que procesan datos personales y más claros y fáciles de ejercitar los derechos de los interesados. El cumplimiento con el nuevo principio de responsabilidad resultará con toda probabilidad, especialmente gravoso en el cumplimiento del rastro documental, cada vez más crucial".

Añade,

> Cada organización necesitará un mayor control de los datos que almacena, por qué los almacena y por cuánto tiempo lo hace. Esto supondrá un cambio radical de actitud para muchos. Las sanciones, que ahora pueden alcanzar hasta el 4% de su facturación mundial anual, implican que la protección de los datos tendrá que estar en el orden del día de la junta directiva.

Actualmente, se aplica la Ley de Protección de Datos a los responsables del tratamiento de datos, pero no a los encargados de su tratamiento. El responsable de los datos es una persona, empresa u organización que determina cómo y por qué se procesan datos. El encargado es el que actúa en nombre del responsable de los datos. Por ejemplo la empresa de externalización de servicios que gestiona los pagos de las nóminas para una determinada compañía sería el encargado del tratamiento, mientras la compañía para la cual desempeña estos servicios sería el responsable de los datos.

El RGPD establece obligaciones legales específicas para ambos, tales como el requerimiento de mantener registros de los datos personales así como de sus actividades para el tratamiento de los mismos. Por vez primera, el encargado tendrá también responsabilidad legal directa en el caso de una violación de la seguridad. Los interesados afectados tienen el derecho de presentar reclamaciones por una violación de la seguridad contra ambas figuras, el responsable y el encargado, quienes podrán tener responsabilidad solidaria. Los responsables tendrán que asegurar que los contratos firmados con el encargado cumplan con el RGPD, dando adecuada cobertura a sus responsabilidades legales.

Consentimiento: un gran cambio

Una de las diferencias principales entre el RGPD y la LOPD es el consentimiento. Bajo el RGPD, los responsables del tratamiento de los datos tendrán que ir más allá para demostrar la existencia de un consentimiento inequívoco del interesado para hacer uso de los datos. Por ejemplo, no es apto el envío de correos electrónicos publicitarios a un cliente que no haya expresado explícitamente su consentimiento para recibirlos.

Según la LOPD, los individuos tienen el derecho de eliminar sus datos personales si la retención de estos datos deviene en daños o sufrimientos injustificados o sustanciales. Según el RGPD, el umbral es diferente y el consentimiento debe ser inequívoco, lo que significa que se debe mantener un registro de cómo y cuándo se ha dado el consentimiento. Además, los individuos tienen el derecho de retirar su consentimiento en cualquier momento. Las compañías deberán asegurarse de que retirar dicho consentimiento sea tan sencillo como darlo. Si se retira, los datos deben ser eliminados de forma definitiva, no siendo válido eliminarlos únicamente de un documento o lista de distribución de correo electrónico.

El consentimiento ha de ser una indicación afirmativa del acuerdo del interesado a que sus datos sean tratados y en ningún caso inferido por silencio, casillas pre-marcadas o inactividad. Los responsables del tratamiento deben poder demostrar que se ha dado el consentimiento de forma expresa e inequívoca y, por tanto guardar evidencia y registro del tal consentimiento –como formularios escritos de consentimiento – , es clave a los efectos de dar correcto cumplimiento a un proceso de auditoría.

Para más información sobre temas relacionados con el consentimiento, visite https://ico.org.uk/about-the-ico/consultations/gdpr-consent-guidance/

Solicitudes de acceso

La solicitud de acceso permite a los individuos solicitar una copia de cualquier dato que una organización pueda tener sobre ellos, así como los detalles de los motivos por lo que estos datos están siendo procesados y el origen de los mismos.

El RGPD establece distintas normas para gestionar las solicitudes de acceso. En la mayoría de los casos, las empresas no podrán cobrar por tramitar una solicitud de acceso, y sólo tendrán un mes para actuar, en lugar de 40 días. Los motivos de denegación a una solicitud de acceso son variadas; las solicitudes infundadas o excesivas pueden ser denegadas o correr a cargo del interesado.

No obstante, deben existir políticas que demuestren que una petición cumple con estos criterios. También se obliga a los responsables a proporcionar información adicional a cualquier persona que lo solicite, tales como los periodos de retención de datos, así como el derecho de rectificación de datos inexactos.

Notificación de una violación de seguridad

En el caso de una violación de la seguridad de los datos, las compañías deben informar a la autoridad competente local en el país de origen dentro de las 72 horas siguientes a su conocimiento. El RGPD define una violación de datos personales como “La destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos”.

La notificación debe incluir la naturaleza de la violación, las categorías de datos y el número de interesados afectados, información de contacto del responsable de la protección de datos, una descripción de las posibles consecuencias del fallo y si procede, una descripción de las medidas adoptadas por parte del responsable para afrontar dicho fallo, incluyendo cualquier esfuerzo para atenuar la situación. Tales fallos pueden dar lugar a sanciones de hasta el 4% de la facturación global anual, con independencia del país en que se produzca el incidente.

¿Necesitas un Delegado de protección de datos?

Según el RGPD, las organizaciones y empresas están obligadas a nombrar un Delegado de protección de datos (DPD), si son autoridades públicas (salvo los tribunales actuando en el ejercicio de su capacidad) o si tienen entre sus actividades principales operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala o el tratamiento a gran escala de datos sensibles, como por ejemplo datos relacionados con delitos o condenas criminales.

La función del Delegado de protección de datos es supervisar de forma independiente el cumplimento de las exigencias del RGPD y asesorar al personal sobre el correcto manejo de los datos personales. Por lo tanto, los Delegados de protección de datos deben tener un conocimiento experto de la normativa y cumplimiento de protección de datos. La Ley establece que las compañías no podrán impedir o influir en las funciones del Delegado de protección de datos.

¿A qué tipo de datos afecta?

El RGPD es de aplicación a los datos personales. Sin embargo, su definición está más detallada que la de la LOPD e incluye aspectos tales como identificadores on-line y direcciones IP. Es razonable suponer que si los datos que usted maneja entran dentro del ámbito de aplicación de la anterior LOPD, también lo harán bajo el nuevo RGPD.

El ámbito de aplicación se extiende a los datos que, por si sólos, no podrían identificar a un individuo, pero que combinados con cualquier otra información sí podrían identificarle. Habrá situaciones en que los datos que usted maneja permiten identificar a un individuo cuyo nombre usted desconoce y que quizás no necesite conocer. De la misma manera, una combinación de datos sobre la edad, sexo, y remuneración puede facilitar la identificación de un empleado en concreto sin mencionar su nombre o cargo.

El RGPD en resumen

El RGPD será
aplicable a partir de
mayo 2018

Reemplaza la
Ley Orgánica de Protección de Datos de Carácter Personal y su Reglamento de desarrollo

Las compañías domiciliadas
fuera de la UE
que interactúen con ciudadanos europeos estarán
sujetas al RGPD

Los responsables del tratamiento de los datos deben notificar a su autoridad competente local
dentro de 72 horas
del conocimiento de cualquier fallo de seguridad

Sanciones de hasta el
4%
de la facturación mundial anual
o
20M€
la que sea superior, podrán ser aplicadas por incumplimiento del RGPD

¿Qué puede hacer?

Mejor en el peor escenario

Todas las organizaciones deben asumir que serán objeto de una violación de seguridad en un momento dado y comenzar a trabajar retrospectivamente desde esta premisa. La adopción de una mentalidad defensiva implica que se implementarán sólidas medidas de seguridad.

Según el RGPD, las compañías tendrán la obligación de implementar medidas técnicas y organizativas oportunas para garantizar un nivel de seguridad adecuado al riesgo y deben poder demostrar que han considerado e integrado la protección de los datos en todos los procesos relativos al tratamiento de los datos.

Formación del personal. Una cuestión de cultura corporativa

Cambiar la cultura del personal de la empresa debe abarcar desde la base hasta la cúspide de la pirámide organizativa. Tradicionalmente las juntas directivas habían prestado una atención relativa a las cuestiones relacionadas con la tecnología de la información, sin embargo actualmente cuanto más conscientes son de que su reputación como empresa está en juego, más probable será que la junta preste su máximo apoyo a este capítulo. La obligación de los Delegados de protección de datos de reportar a la junta directiva ayudará a cambiar la cultura corporativa. Cuanto antes comience a adaptarse a la normativa del RGPD, mejor será para su empresa. Puede que sea necesario adoptar nuevos procedimientos para afrontar el requisito de transparencia en el tratamiento de los datos así como los nuevos derechos de los interesados (tales como el "derecho de cancelación"). Esto puede tener implicaciones presupuestarias, de personal y de gobernanza.

También es aconsejable establecer protocolos de actuación que describan exactamente cómo proceder tras una violación de seguridad de los datos antes incluso de que esta tenga lugar.

Se deben realizar pruebas de intrusión y ensayar el papel de cada persona en el escenario de una violación de seguridad. Es conveniente tener un registro de las personas asignadas a cada paso del proceso y de la responsabilidad de cada una de ellas, desde la gestión de la comunicación externa hasta la rehabilitación de los procesos operativos.

Protocolos de almacenamiento. Sepa donde almacena sus datos

Almacenar los datos adecuadamente es tan importante como protegerlos de una violación de seguridad. Debe considerar la realización de una auditoría para saber qué información está gestionando, de donde proviene, con quién lo comparte, y quién lo está compartiendo. Y se deberán anotar las conclusiones en un registro de datos.

El procedimiento debe incluir detalles sobre el modo en que se comparten los datos con terceros así como la eliminación de los datos si lo solicita un cliente. Bajo el RGPD, los individuos tendrán el derecho de acceso, de rectificación de errores, de eliminación de la información, y de evitar el marketing directo, la toma de decisiones automatizadas, así como la portabilidad de datos y perfiles (movimiento o copias de datos personales de un entorno informático a otro).

Debe tener un procedimiento de localización y eliminación de los datos y acordar a quién le corresponde la decisión de suprimirlos. También tendrán que explicar los fundamentos legales para procesar datos personales ante cualquier requerimiento (la información que pondrán a disposición de las personas cuyos datos recogen).

Niveles de cumplimiento y certificación. Anticípese

Usted debe mantener un sólido sistema que permita solicitar, obtener y registrar el consentimiento, así como unos procedimientos adecuados para detectar, reportar e investigar cualquier violación de la seguridad.

A modo de ejemplo, desde el año 2014, el Plan Básico de Seguridad Cibernética del gobierno del Reino Unido es obligatorio para proveedores de contratos gubernamentales que gestionan la información personal y suministran algunos productos y servicios TIC (tecnologías de la información y la comunicación). Es un plan respaldado por el gobierno y la industria para ayudar a las organizaciones a protegerse contra los ataques cibernéticos comunes. Todavía el plan es voluntario. Sin embargo, conseguir la certificación de Cyber Essentials es una buena manera de protegerse de las amenazas cibernéticas comunes. Además, conseguir este sello de calidad demuestra a los clientes que la empresa se toma el asunto en serio. Muchos departamentos de compras exigen la certificación antes de aceptar una oferta. Tenerla supone una ventaja competitiva para la empresa y no tenerla le deja en una posición competitivamente desventajosa.

Los servicios en la nube no le libran de responsabilidad

De acuerdo con el RGPD si usted almacena o utiliza datos en la nube, sigue siendo usted y no el proveedor de la nube el responsable de los datos. Esto significa que es usted el que debe notificar a los afectados, dentro de un plazo máximo de 72 horas, una violación de seguridad. Si emplea un encargado para el procesamiento de datos en la nube, tales como un servicio online de pago de nóminas, ambos podrían tener responsabilidad conjunta. Gran parte del contenido del RGPD será testado en los Tribunales y este hecho podría conducir a disputas contractuales entre las partes implicadas.

La privacidad por diseño

La privacidad por diseño exige que las empresas integren un modelo de seguridad y privacidad en sus sistemas por adelantado. Una evaluación de Impacto sobre la Protección de Datos (EPD) es una herramienta útil para identificar y reducir riesgos de intrusión en la privacidad. Tenerla puede ayudar a la hora de diseñar procedimientos más eficientes y efectivos para la gestión de datos personales. Una EPD debe describir los riesgos potenciales para los individuos cuyos datos se están procesando y los riesgos corporativos para las empresas que realizan esta actividad, entre ellos el impacto financiero y reputacional.

Lo que debe implementar para cumplir con el reglamento

- Tener en cuenta la privacidad en el diseño del procesamiento de datos personales.
- Elaborar una Evaluación de Impacto sobre la Protección de los Datos que detallará los riesgos potenciales para todos los implicados en la gestión de los datos.
- Asegurarse que sus empleados sean completamente conscientes de los riesgos y conocedores del reglamento, lo que supone reducir la probabilidad de una violación de la seguridad de los datos.
- Implementar una política de escritorios limpios y retención de datos que reducirá los errores humanos. Lo mismo es aplicable a los datos electrónicos, pero no debe olvidar que tendrá que demostrar la cancelación de datos en algunos casos.
- Una suficiente encriptación o cifrado de los datos ayuda a minimizar el impacto en caso de pérdida o vulneración de dichos datos.
- Revisar regularmente sus infraestructuras de seguridad tiene una importancia crucial.
- Los responsables del tratamiento de datos deben examinar cuidadosamente los contratos y otros acuerdos al compartir datos con organizaciones externas.

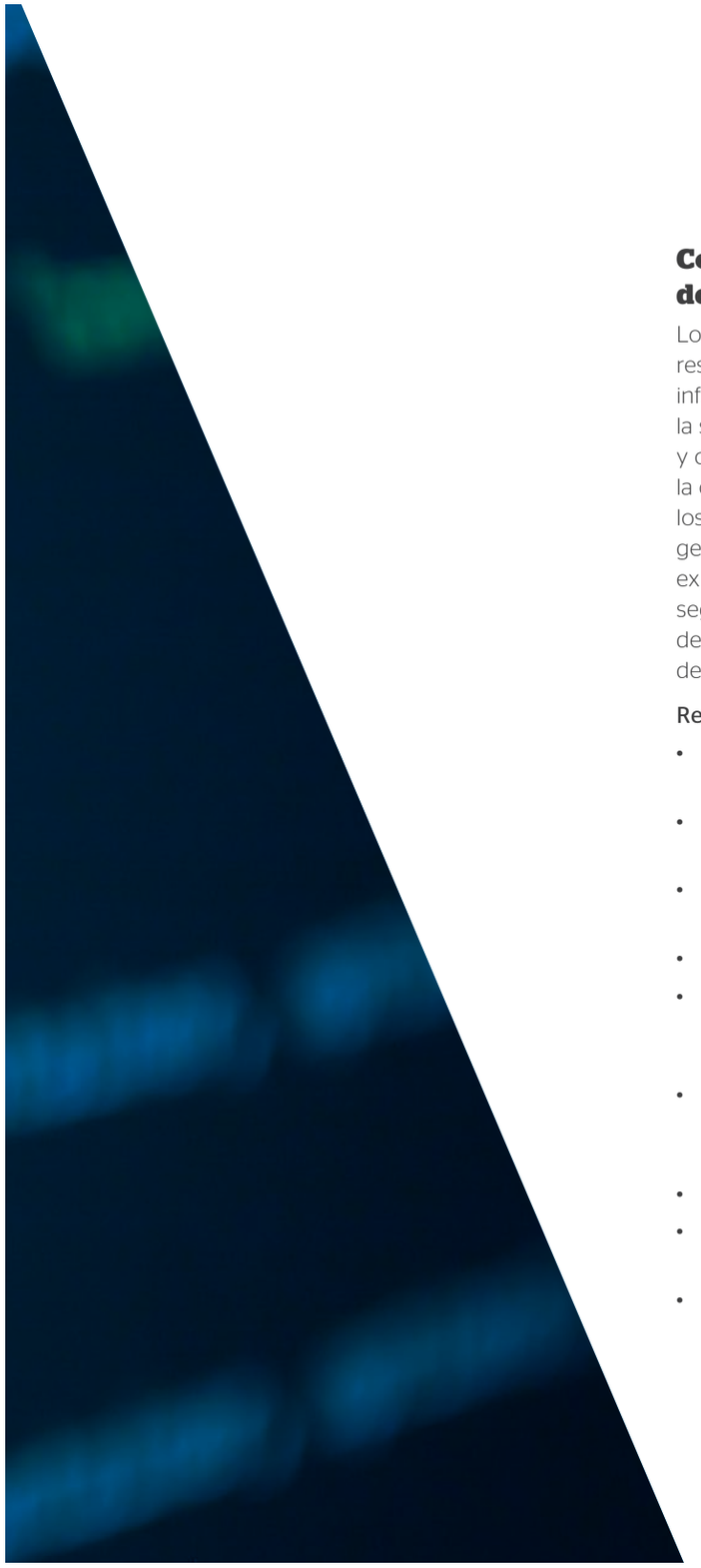
Caso práctico: QBE

En cuanto apareció el RGPD, QBE estableció un grupo de trabajo que incluía expertos en cumplimiento, en legislación aplicable, seguridad de la información, arquitectura de gobernanza de datos y gestión de proyectos.

Este grupo diseñó un modelo que definiera las capacidades de protección de datos de la organización y repasaron la nueva legislación línea por línea para poder determinar lo que exige cada cláusula. El resultado fue una herramienta de análisis.

'Esencialmente'-dice Iain Heron, arquitecto de información corporativa para QBE EO-, nos hemos dado cuenta de que se trata de una cuestión de cambio cultural para la empresa y no un tema de informática. Hay muchos datos personales circulando, y en realidad no son tanto los sistemas informáticos lo que importa en relación a su protección, sino el cambio cultural'.

Heron añade que 'las personas que atienden las llamadas telefónicas de los clientes necesitan concienciarse de que los datos que tratan a diario no sólo tienen un valor, sino que también pueden traer un impacto negativo si no los cuidamos debidamente.' La compañía también realiza simulacros de fallos en la seguridad, 'porque no se sabe si el personal de la empresa reaccionará de manera adecuada a la situación de crisis hasta que no haya sido testado'.



Como abordar una violación de la seguridad

Lo que es más importante, en virtud del RGPD el responsable de los datos tiene hasta 72 horas para informar a la agencia reguladora de una violación de la seguridad de los datos. Actualmente, sólo los bancos y compañías de telecomunicaciones tienen la obligación de hacerlo. Las empresas deben revisar los procedimientos que tienen establecidos para gestionar incidentes antes de decidir si llamar a un experto externo o hacer frente a una violación de seguridad internamente. En adición, los responsables deben mantener un registro interno de las violaciones de seguridad.

Recomendaciones:

- Identificar una violación y tomar medidas para ponerle fin.
- Revisar su póliza de seguros y notificarlo a su compañía de seguros.
- Identificar los datos personales violados, la categoría de los datos y el número de archivos vulnerados.
- Determinar las medidas correctivas.
- Notificarlo sin demora, a la autoridad de protección de datos que corresponda y, en cualquier caso, dentro de las 72 horas.
- Notificar a los afectados si la brecha tiene probabilidad de resultar un alto riesgo para sus derechos y libertades.
- Implementar medidas correctivas y monitorizarlas.
- Revisar las causas que originaron la brecha de seguridad y tomar medidas para que no se repita.
- Dar la necesaria formación adicional al personal.

¿Qué obligaciones tiene hacia sus clientes?

Si una violación de la seguridad de los datos personales tiene la probabilidad de entrañar un alto riesgo para los derechos y libertades de las personas, el responsable de los datos está obligado a notificárselo a los afectados. No obstante, si el responsable ha tomado medidas para mitigar estos riesgos o el proceso de contacto supondría un esfuerzo desproporcionado, puede que el cumplimiento de este requisito no sea necesario.

Si se produce una violación de la seguridad de los datos, debe seguir los procedimientos internos de reporte y las estrategias de respuesta en caso de incidente, compruebe la cobertura de su póliza de seguros aplicable y notifíquelo a su asegurador. Considere la opción de almacenar temporalmente sus datos electrónicos con un proveedor externo si creen que siguen siendo vulnerables a un daño, destrucción, alteración, corrupción, reproducción, robo o uso indebido por parte de un pirata informático.

Los responsables y los encargados del tratamiento de los datos deben aprender del incidente y, por consiguiente, actualizar sus procedimientos internos de reporte y estrategias de respuesta según corresponda.

Tras la violación de la seguridad de datos

Gestionar el impacto reputacional

La violación de la seguridad de datos es carne de cañón para los periodistas y muchos casos de elevada repercusión podrían haberse minimizado con una buena gestión de crisis mediática. Merece la pena contratar, antes de un incidente, los servicios de una empresa de relaciones públicas con experiencia en daños a la reputación para que esté preparada con una respuesta en caso de una violación de seguridad que garantice la comunicación de los mensajes clave. Debe asegurarse que los empleados conozcan el procedimiento a la hora de atender las preguntas de la prensa y que sean plenamente conscientes de cómo cualquier declaración (suya) al respecto podría ser interpretada.

Restaurar la situación inicial

Disponer de un plan de gestión de crisis ayudará a mantener la continuidad de la operación asegurando a sus clientes que su negocio funciona como de costumbre. Es importante mantener una buena comunicación con todos los interesados, tanto externos como internos.

Abordar un violación de la seguridad

Asegúrese de informar a la autoridad competente dentro de las 72 horas siguientes.

- Consulte sus procedimientos de gestión de incidentes; no actúe de forma impulsiva.
- Ponga en cuarentena los datos que han sido vulnerados
- Considere la contratación de una empresa de relaciones públicas con experiencia en gestión de crisis.
- Informe a todas las personas que puedan sufrir un impacto negativo.

Grandes brechas de seguridad: los eventos más conocidos

- En el año 2013, una violación de la seguridad en la multinacional Target Corporation resultó en que los números de tarjetas de crédito e información personal de unos 70 millones de personas pasaron a manos de piratas informáticos.
- Un ataque a JP Morgan Chase en el año 2014 comprometió los datos de 76 millones de hogares americanos y 7 millones de pequeños negocios.
- En el Reino Unido, en el año 2016, Tesco Bank reveló que se habían comprometido 40.000 cuentas de sus clientes y se había sacado dinero de 20.000 de ellas.

¿Qué debe cubrir una buena póliza de seguridad cibernética?

- Gastos de notificación por violaciones de la seguridad de datos.
- Gastos de recuperación de hardware.
- Gastos de defensa y sanciones por procesos regulatorios.
- Gastos de relaciones públicas.
- Gastos de intervención forense y recuperación de activos de información.
- Gastos de monitorización de crédito.
- Pérdida de beneficio.
- Extorsión cibernética.
- Responsabilidad Civil Multimedia.

Comprender las exclusiones

Un buen seguro de riesgos cibernéticos debe dar una protección amplia tanto para los gastos derivados de reclamaciones de terceros como para los gastos propios. Sin embargo, puede haber confusión sobre qué cubre o no cubre una póliza de riesgos cibernéticos, y a este respecto la Asociación de Aseguradoras Británicas ha elaborado una guía muy útil, ***Making sense of cyber insurance***, para aclarar estas dudas.

¿Está preparado?

- ¿Ha realizado una revisión completa de su compañía para determinar qué datos personales gestiona, su origen, para qué se emplean y con quién los comparte?
- ¿Ha revisado los acuerdos contractuales con los terceros con los que comparte datos, incluyendo las organizaciones que procesan datos para la compañía (por ejemplo, proveedores de servicios externos) para garantizar el cumplimiento con la normativa aplicable?
- ¿Ha realizado una revisión de la política de protección de datos y de notificación de privacidad?
- ¿Ha revisado cómo se obtiene y se registra el consentimiento?
- ¿Ha introducido nuevos procedimientos para asegurar que cubren los derechos de los individuos, tales como la eliminación de sus datos y se han actualizado los procesos de solicitud de acceso?
- ¿Tiene un plan de respuesta ante incidentes? ¿Lo ha actualizado de cara al RGPD?
- ¿Necesita un Delegado de protección de datos?

La cobertura QBE: protección 24/7 contra el riesgo cibernético

La responsabilidad y costes asociados derivados del uso de la tecnología de la información pueden afectar a su negocio de muchas maneras.

En el mundo digital y del internet de las cosas, las amenazas pueden surgir desde cualquier ángulo: desde ataques cibernéticos realizados por piratas informáticos criminales o activistas, hasta el uso indebido o la pérdida de datos – accidental o intencional – de los clientes por parte de uno de sus empleados.

En QBE, hemos elaborado una amplia variedad de coberturas de riesgos cibernéticos y servicios especializados para ayudar a mantener su negocio a salvo.

Nuestra cobertura incluye:

- Responsabilidad Cibernética, seguridad de datos y multimedia.
- Gastos de notificación por infracción de privacidad de los datos.
- Gastos de recuperación de hardware.
- Gastos de defensa y sanciones por procesos regulatorios.
- Gastos de relaciones públicas.
- Gastos de intervención forense y recuperación de activos de información.
- Gastos de monitorización crédito.
- Pérdida de beneficio.
- Extorsión cibernética.

¿Por qué QBE?

Por cómo somos

- Nos adaptamos a la estructura y particularidad de cada cliente y a la complejidad de cada riesgo.
- Podemos combinar en un solo condicionado todos los productos ofrecidos por la compañía, lo que facilita su gestión, negociación y diálogo.
- Creemos y apostamos por una gerencia de riesgos integral y profesional en nuestros clientes.
- Compartimos nuestra experiencia y conocimiento con sesiones de formación y divulgación sobre nuestras pólizas y las tendencias en el mercado.
- Buscamos la calidad y la eficiencia en nuestros procesos para facilitar al máximo la gestión de las pólizas.
- Fácil acceso y contacto directo con las personas que tomamos las decisiones.

Por cómo lo hacemos

- Ofrecemos una gestión de siniestros transparente y proactiva, trabajando con especialistas forenses acreditados y despachos de abogados con experiencia internacional.
- Aportamos capacidad en primario y en exceso, pudiendo combinarlas a requerimiento del cliente.
- Preferimos trabajar en directo pero también podemos aportar capacidad en reaseguro.

Made possible

QBE Insurance Europe Ltd

Sucursal en España
Paseo de la Castellana 31- 5ª planta
28046 Madrid

Get in touch

Visítanos en https://QBEespana.com
Tel: +34 91 789 3950

8426GC/¿ESTÁPREPARADOPARAELRGPD?/NOVIEMBRE2017