Mecanismos de seguridad física y de privacidad del RGPD

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea exige que organizaciones de todo el mundo revalúen su manera de acceder, utilizar y mantener los datos personales. Esta documentación técnica describe situaciones de riesgo para los datos que podrían dar lugar a intervenciones administrativas y sanciones económicas en virtud del nuevo reglamento. Asimismo, analiza las mejores prácticas en seguridad física y de privacidad, ya que estas representan un área importarte de la protección de datos que, a menudo, se pasa por alto. La unión de los mecanismos de seguridad administrativa, física y de ciberseguridad puede ayudar a proteger los datos personales confidenciales y demostrar el compromiso de una organización con la privacidad de los datos.

Conclusiones clave:

- Sepa qué es lo que dice el RGPD sobre las medidas de seguridad física y de privacidad para proteger los datos personales.
- Analice el nivel de protección y privacidad de los datos que los expertos del sector consideran razonable.

Viviendo en un mundo basado en los datos
Hoy en día, como parte natural de la actividad empresarial, la mayoría de las organizaciones recopila y utiliza datos personales, tanto sobre el personal como sobre clientes, clientes potenciales o terceros. Por lo general, estos datos se almacenan en formato electrónico, al cual pueden tener acceso la organización[1] y terceros. Asimismo, la función principal de algunas organizaciones consiste en recopilar y analizar volúmenes de datos personales.

Aunque la cantidad y el tipo de datos que reúne cada organización varían, todas están de acuerdo en que encontrar esta información nunca había sido tan fácil. Las personas dejan atrás un amplio reguero de datos cuando crean perfiles en las redes sociales, participan en comunidades online, realizan búsquedas por internet, responden a encuestas y aprovechan las ofertas de códigos promocionales y servicios «gratuitos», como el almacenamiento de fotografías y la transmisión de música.

La tecnología contribuye aún más al proceso de creación de perfiles sólidos de las personas, con avances en inteligencia artificial, etiquetas electrónicas, balizas web, cookies y otras herramientas de control.

La tecnología, junto con actividades de extracción de datos, ha permitido a las organizaciones acumular gran cantidad de datos personales. Estos repositorios podrían desvelar la edad de una persona, su estado civil, fecha de cumpleaños, estudios, aficiones, religión, historial laboral, creencias políticas, preferencias de compra, fuentes de noticias preferidas, ingresos, antecedentes criminales y mucho más.

Aunque la mayor parte de estos datos está centralizada en bases de datos de empresas, a menudo quedan burbujas de datos dispersas en la cadena de suministro en sistemas dispares; además, suele carecerse de mecanismos para transmitir a futuros receptores de los datos cómo o por qué se recopilaron en un principio. Esto deja a los datos personales expuestos a usuarios muy alejados del propósito inicial por el que se obtuvieron.

En un día cualquiera, son muchas las personas de una organización que pueden acceder a los datos almacenados, por ejemplo, para pagar a un empleado, hacer un estudio de mercado, lanzar una campaña de marketing por correo electrónico o realizar un seguimiento del compromiso del cliente. Cada punto de acceso a estos conjuntos de datos representa una oportunidad para que los datos personales se utilicen indebidamente o caigan en malas manos.

Datos básicos

¿Qué es el RGPD?
El Reglamento General de Protección de Datos (RGPD) tiene como objetivo proteger la privacidad de las personas en la Unión Europea (UE).

¿Cuándo entra en vigor?
El 25 de mayo de 2018.

¿A quiénes afecta?
A todas las empresas, independientemente de su ubicación, que controlen o procesen datos personales de personas de la Unión Europea.

¿Qué se consideran datos personales?
Cualquier información relacionada con una persona física o un titular de los datos. Puede ser cualquier cosa, desde un nombre, una fotografía o una dirección de correo electrónico hasta datos bancarios, publicaciones en sitios web de las redes sociales, información médica o la dirección IP de un ordenador.

¿Cuál es su impacto?
Una sanción de 20 millones de euros o hasta un 4 % del volumen de negocios anual global (lo que sea más alto). Esta es la sanción máxima que puede imponerse para las infracciones más graves.

¿Dónde puedo encontrar más información?

- Una visión general del reglamento
- Leer el reglamento
- Soluciones de seguridad física

65 %
de los encuestados dice que los incidentes de violaciones de datos le hicieron dejar de confiar en la organización que los sufre.[5]

Para comprender los riesgos de seguridad física a los que se enfrentan las organizaciones, considere estas tres situaciones:

Un empleado revisa datos confidenciales en su teléfono cuando está en el aeropuerto y no se da cuenta de que alguien cercano está mirando la pantalla.

- Un empleado pierde el ordenador portátil y la información en el disco no está cifrada.
- Un empleado se aleja de su escritorio para ponerse un café dejando la información de contacto de un cliente a la vista en el monitor o en el escritorio cuando entra un observador no autorizado.
- Un empleado descontento hace fotos a documentos que alguien ha dejado en una impresora, a información mostrada en una pantalla y a credenciales de inicio de sesión pegadas en el monitor de un ordenador.
- Se donan a beneficencia ordenadores portátiles y de sobremesa anticuados sin antes borrar por completo los discos duros.
- La consulta de un médico cierra y se tiran los registros de los pacientes a la basura sin destruirlos.

¡En 2016, los piratas informáticos pusieron en peligro
mil millones de registros[2]

Situaciones como estas son cada vez más preocupantes, ya que las violaciones de datos son demasiado habituales en el mundo digitalizado actual. La empresa estadounidense de investigación de mercado Forrester informa que, en 2016, los piratas informáticos pusieron en peligro mil millones de registros en solo 12 meses. En la primera mitad de 2017, se señaló que 918 violaciones de datos pusieron en peligro a 1900 millones de registros de datos en todo el mundo. Esto representa un incremento del 164 % comparado con el primer semestre de 2016.[2]

Con cada nueva violación de datos, aumenta la ansiedad de que la privacidad de los datos se haya perdido por completo. Según un estudio reciente, la gente siente que su privacidad se ve cuestionada por problemas relacionados con la confidencialidad y la seguridad. De hecho, un 91 % teme haber perdido el control sobre cómo se recopilan sus datos personales y cómo son utilizados por las empresas. Una proporción prácticamente equivalente cree que sería muy difícil eliminar información imprecisa sobre ellos online.[3] Las violaciones importantes no son el único motivo de preocupación. Puede que las pequeñas empresas tengan menos información sobre una persona, pero esto no le resta importancia a los ojos de esas personas en caso de robo o uso indebido.

Dichos temores siguen creciendo, aun cuando directivas y reglamentos estrictos sobre privacidad y protección de los datos hayan existido durante más de una década, entre ellos, la Norma de Seguridad de la Ley de Transferibilidad y Responsabilidad del Seguro Sanitario (HIPAA, por sus siglas en inglés) de los EE. UU, la Ley de Informes de Crédito Justos de los EE. UU. y la Directiva de Protección de Datos de la Unión Europea.

La Directiva de Protección de Datos recoge principios como el requisito de que los datos se almacenen de un modo seguro, se procesen con fines limitados y no se mantengan más tiempo del necesario. No obstante, como se trata de una "directiva" y no una ley, la implementación y el cumplimiento en cada país de Europa son variables.

Participe en el RGPD
El RGPD es el reglamento más completo e impactante a nivel mundial introducido para proteger los datos personales. Se creó a partir de la convicción común de que todas las personas tienen un derecho fundamental a la privacidad. Su objetivo es proteger la privacidad de las personas en la UE aplicando una nueva normativa sobre cómo los negocios protegen, procesan y utilizan los datos personales.

El RGPD podría ser el avance más importante en cuanto a normativas sobre seguridad de los datos y privacidad en los últimos 20 años, debido a sus requisitos de rendición de cuentas sobre el mantenimiento de registros y su posible impacto financiero. Impone dos niveles de sanciones: las organizaciones pueden ser penalizadas con el 2 % del volumen de negocios global anual o hasta 10 millones de euros por violaciones como las siguientes:

- No haber notificado una violación de datos a una autoridad de control y a los individuos afectados.
- No haber nombrado a un Responsable de Protección de Datos (RPD) si la organización lo requiere.

Las organizaciones pueden estar sujetas a una sanción del 4 % del volumen de negocios global anual o hasta 20 millones de euros por violaciones como las siguientes:

- No haber respetado los derechos de los titulares de los datos.
- No haber cumplido una orden de una autoridad de control.
- No haber cumplido los requisitos para transferencias internacionales de datos[4].

Estas sanciones se suman a la pérdida de reputación, de valor de marca y de confianza, que puede ser igualmente devastadora para las finanzas de una empresa. De hecho, según informes, los incidentes de violaciones de datos provocan que un 65 % de personas deje de confiar en la organización que los sufre[5].

El cumplimiento del RGPD no es tarea fácil, puesto que responsabiliza a las organizaciones de cómo recopilan, utilizan, mantienen y depuran datos personales, a la vez que preservan su seguridad. Incluso aquellas que disponen de programas

El RGPD es el reglamento más completo e impactante a nivel mundial introducido para proteger los datos personales.[1]

existentes de privacidad y seguridad necesitan revaluar sus procesos. En particular, el RGPD exige a las organizaciones que implementen las medidas técnicas y organizativas apropiadas para prevenir la pérdida de datos personales o el acceso no autorizado a los mismos.

Esto da lugar a muchas preguntas, como las siguientes:

P. ¿Qué se consideran datos personales?
R. Cualquier información relacionada con una persona física identificada o identificable.[6] Podrían incluirse identificadores (como un nombre o un número de identificación) o datos que revelen el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, datos genéticos, información médica, delitos; expectativas de desempeño profesional, situación económica, preferencias personales o intereses, fiabilidad o conducta, ubicación o movimientos, etc.[7]

P. ¿Qué es la seudoanonimización y por qué debería interesarme?
R. En el RGPD se menciona 15 veces el término «seudoanonimización», un procedimiento por el cual los campos de identificación en un registro de datos se sustituyen por uno o más identificadores artificiales o seudónimos. El RGPD recomienda la aplicación de la seudoanonimización a los datos personales para reducir los riesgos a los titulares de los datos y ayudar a responsables y encargados del tratamiento de datos a cumplir sus obligaciones en cuanto a la protección de los datos.[8]

P. ¿Pueden las organizaciones obtener el consentimiento de la gente para recopilar sus datos personales?
R. Sí, pero el consentimiento necesita darse mediante una acción clara y afirmativa que establezca una indicación dada libremente, específica, informada y sin ambigüedades del consentimiento del titular de los datos al tratamiento de sus datos personales. Casillas premarcadas, falta de respuesta o inactividad no se consideran consentimiento.[9] Las organizaciones necesitan mantener un registro de los consentimientos recibidos y asegurarse de que las peticiones de consentimiento se diferencien de otras peticiones, empleando un lenguaje claro y llano.[10] El Artículo 13 recoge amplia información que ha de proporcionarse al titular de los datos en el momento de recopilar los datos personales como, por ejemplo, el fin para el cual se recopila la información, los destinatarios o las categorías de destinatarios de los datos personales y el periodo de tiempo que se almacenarán los datos.

P. ¿En qué consiste una evaluación de impacto en la protección de datos (EIPD)?
R. Una EIPD, que se exige en actividades de alto riesgo, ayuda a las organizaciones a evaluar el origen, la naturaleza, la particularidad y la gravedad de los riesgos, y a implementar las medidas adecuadas para mitigar riesgos, como el cifrado. A la hora de evaluar los riesgos de seguridad de los datos, se deben considerar los riesgos que presente el tratamiento de los 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 que pudiera provocar daños físicos, materiales o no materiales.[11]

P. ¿Es necesario que nombre a un Responsable de Protección de Datos (RPD)?
R. El nombramiento de un RPD es obligatorio siempre que el tratamiento de los datos se lleve a cabo por una autoridad pública (a excepción de un tribunal que actúe en ejercicio de poderes judiciales) o para una empresa cuyas actividades básicas consistan en el procesamiento de operaciones que requieran de un control periódico y sistemático de los titulares de los datos a gran escala. Un RPD es también obligatorio para todas las empresas que procesen datos relacionados con información confidencial, como historiales médicos o creencias religiosas y políticas a gran escala. En particular, el RPD:

- debe nombrarse en base a las cualidades profesionales y, en particular, al conocimiento especializado de la ley y las prácticas de protección de datos.
- puede ser un miembro del equipo o un proveedor de servicios externo.
- debe proporcionar sus datos de contacto al organismo nacional de protección de los datos personales (DPA).
- debe recibir recursos adecuados para realizar sus tareas y mantener sus conocimientos especializados.
- debe depender directamente del nivel más alto de dirección.
- debe rehusarse a realizar otras tareas que pudieran provocar un conflicto de interés.[12]

Seguridad física y requisitos de privacidad
¿Qué deberían hacer las organizaciones para prevenir violaciones de datos? El Artículo 24 del RGPD destaca la responsabilidad de la organización de implementar las «medidas técnicas y organizativas apropiadas» a fin de garantizar y poder demostrar la tramitación correcta de los datos personales. El Artículo 32 va más allá y explica que «al evaluar la adecuación del nivel de seguridad, se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular, como consecuencia de 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».

Un aspecto importante de esta normativa es el énfasis en prevenir el acceso no autorizado. Es aquí donde la seguridad física es esencial. En especial, puede ayudar a salvaguardar datos frente a amenazas humanas internas y externas cuyo fin sea explotar las lagunas existentes dentro de los muros de su organización y a través de sus empleados. Esto incluye limitar qué datos pueden observarse o robarse o a qué datos puede accederse. Revise los requisitos siguientes y evalúe si sus empleados disponen de las medidas técnicas y organizativas apropiadas para cumplir el reglamento.

Implementar la protección de datos desde el diseño y por defecto:
Para proteger los datos por defecto, las organizaciones deben identificar y recopilar de manera proactiva únicamente los datos personales necesarios para sus fines previstos, conservar los datos únicamente durante el tiempo que sea necesario (principio de minimización) y asegurarse de que los datos personales no se harán accesibles a un número indefinido de personas. Es probable que esto conlleve asegurarse de que los riesgos en torno a la privacidad se identifiquen desde un principio y que se diseñen sistemas para mitigar dichos riesgos, seudoanonimizando y anonimizando como corresponda, creando transparencia en las funciones de tratamiento de los datos e identificando a personas o cargos determinados que necesiten acceso a los datos. Pregúntese: ¿Está teniendo en cuenta los riesgos de privacidad que podrían correr las personas antes de elaborar sus sistemas de información, prácticas empresariales y diseño físico? ¿Se ha reunido con su equipo informático para revisar los sistemas y las actividades de tratamiento de datos existentes y para estudiar si se necesitan pasos adicionales para documentar cómo se protegerán los datos personales durante el ciclo de vida completo de la información?

Utilizar mecanismos de seguridad física:
Aunque los controles de ciberseguridad, como el cifrado de los datos y las contraseñas complejas, son esenciales, los controles administrativos y físicos de «baja tecnología» son igualmente importantes. A fin de determinar dónde son necesarias las barreras físicas, hay que identificar dónde se accede a la información confidencial. Por ejemplo, los empleados utilizan normalmente dispositivos móviles para acceder y compartir datos desde cualquier sitio. Una cifra creciente de estos trabajadores accede a información confidencial en lugares públicos, a menudo, bien a la vista de otras personas. Asimismo, también existe un creciente riesgo de exposición de los datos dentro de la oficina. Los diseños habituales de oficinas de planta abierta eliminan las barreras físicas que tradicionalmente ayudaban a salvaguardar las pantallas de ordenadores. Pregúntese: ¿ha colocado las pantallas de ordenador lejos de ventanas, puertas y áreas de acceso público? ¿Equipa los monitores y pantallas de dispositivos móviles con pantallas de privacidad para oscurecer la visión de información a posibles observadores? ¿Están las impresoras, fotocopiadoras y máquinas de fax en áreas protegidas o disponen de cubiertas con cierre? ¿Almacena copias físicas de datos en instalaciones de acceso controlado? ¿Son las trituradoras de papel un elemento esencial en todas las unidades en las instalaciones, en particular, junto a impresoras, fotocopiadoras y máquinas de fax, y un requisito previo para todos los teletrabajadores o aquellos que utilizan conexiones remotas para acceder a activos de información corporativa?

Programar la formación de los empleados:
Los programas de formación deberían cubrir tres aspectos clave: mejores prácticas de observación, acceso físico y prevención de robos. Por ejemplo, debería recordarse a los empleados que sean conscientes de sus alrededores a la hora de acceder y utilizar dispositivos conectados en lugares públicos a través de sus portátiles, tabletas y smartphones. Las pantallas de los dispositivos no deberían estar expuestas a todo el que pasa ni a observadores potenciales, en especial, cuando se introduzca información de inicio de sesión o se visualicen datos de cuenta confidenciales. Cuando se trata del acceso físico, las organizaciones deberían formar a los empleados para borrar la información de pizarras blancas y recoger papeles confidenciales tras reuniones, memorizar contraseñas en lugar de escribirlas en un papel, bloquear con llave archivadores y portátiles, utilizar filtros de privacidad en dispositivos informáticos y mantener una política de escritorio limpio, incluyendo el cierre de sesión de dispositivos sin vigilancia. Pregúntese: ¿abarca su programa de formación el conocimiento del entorno para que sus empleados aprendan a ser conscientes de sus alrededores y puedan identificar y responder a conductas sospechosas? ¿Comprenden los empleados las expectativas de nuestra organización en torno a la política de escritorio limpio? ¿Recuerda frecuentemente a los empleados las buenas prácticas de seguridad que deben seguir?

Elaborar políticas claras:
Para demostrar el compromiso de una organización de implementar medidas adecuadas de seguridad y privacidad, sus políticas deberían señalar qué hacer y qué no hacer con relación a la visualización y el uso de información, y que los empleados y contratistas las pongan en práctica tanto en el lugar de trabajo como cuando trabajan de manera remota. Los contratos de trabajo deberían contener advertencias específicas sobre la responsabilidad de salvaguardar la información sensible y confidencial.[13] Pregúntese: ¿ha comunicado al personal su manual de prácticas de privacidad y de seguridad que explican cómo su organización protege, comparte, elimina y proporciona acceso a los datos personales? ¿Cuenta con una política de BYOD («Lleve su propio dispositivo») que rija la conducta de los empleados y los controles de seguridad requeridos para cuando estos acceden a recursos corporativos desde sus dispositivos personales? ¿Requiere, como parte de su política de seguridad, que los empleados utilicen controles visuales y de ciberseguridad?

Fijar límites de almacenamiento de datos:
Fijar plazos máximos de almacenamiento de los datos personales, de conformidad con la legislación aplicable. Borrar de manera segura todos los datos personales que no sean absolutamente necesarios para apoyar los fines comerciales con los que se recopilaron. Pregúntese: ¿de qué controles técnicos dispone para que los datos se borren en el momento correcto? ¿Cumplen los procesos de destrucción de su organización estrictas directrices de seguridad, como aquellas proporcionadas por las Directrices 800-88 del NIST en los EE. UU. de destruir físicamente los discos duros que han alcanzado el final de su vida útil?

Verificar proveedores independientes:
Utilice únicamente procesadores que ofrezcan suficientes garantías en cuanto a conocimientos especializados, fiabilidad y recursos para implementar medidas técnicas y organizativas, incluidas las que hacen a la seguridad del tratamiento de datos. Pregúntese: ¿dispone de un programa de gestión de proveedores que incluya obligaciones contractuales y establezca actividades de supervisión de la gestión para terceros con acceso a datos personales?

Crear un protocolo para violaciones de datos:
Las organizaciones deben estar preparadas para notificar a la autoridad de control sin dilación indebida cuando tengan conocimiento de que ha ocurrido una violación de datos personales (cuando sea posible, en menos de 72 horas). O bien , ser capaces de demostrar que es poco probable que la violación de datos personales atente contra los derechos y las libertades de personas físicas. Si existe un riesgo alto, también deberá notificarse al titular o los titulares de los datos de la violación de datos sin dilación indebida.[14] Pregúntese: ¿cuándo revisó por última vez las políticas y los planes de respuesta a incidentes y de aviso de violación de datos de su organización? ¿Saben los empleados a quién alertar dentro de la organización si su dispositivo se pone en peligro o si tienen conocimiento de una violación de datos? ¿Dispone de un plan actualizado de respuesta a incidentes y de aviso de violación de datos para determinar cómo y cuándo notificar a las autoridades sobre una violación de datos?

Conocer los derechos de las personas:
Ahora, los residentes de la UE tienen derecho a ver qué datos personales tienen las organizaciones sobre ellos y a solicitar que se borren sus datos en determinadas circunstancias. El derecho de supresión ("el derecho al olvido") exige que la organización suprima cualquier enlace a dichos datos personales, además de copias o reproducciones. Las organizaciones deberán proporcionar un método para que la gente envíe peticiones electrónicamente, en particular, si los datos personales se tratan a través de medios electrónicos.[15] Pregúntese: ¿entiende su organización lo que se consideran «datos personales» y cómo responder a consultas relacionadas con datos personales?

Conclusión:

El RGPD es el cambio más importante en reglamentos sobre políticas de privacidad en los últimos 20 años. Exige que los datos personales se procesen de una manera que ayude a garantizar un nivel adecuado de seguridad y confidencialidad, una tarea que requiere tanto medidas de seguridad técnicas como organizativas. Además, las sanciones por incumplimiento podrían ser abrumadoras. Sin embargo, las mejores prácticas que recoge el reglamento son solo buenas prácticas empresariales. Nadie quiere que sus datos se utilicen de forma indebida y ninguna organización quiere enfrentarse a las repercusiones de una violación de datos. Las organizaciones que consideran la privacidad no como una carga de cumplimiento sino como una responsabilidad corporativa, pueden emplearla como ventaja estratégica para mejorar su reputación y el valor de su marca, atraer mejores empleados y, en última instancia, mantener la confianza del público.

3m.com.es/filtrosdeprivacidad

[1]Forrester, Lessons Learned from the World's Biggest Security Breaches and Data Abuses, 9 de enero de 2017
[2]Índice de Nivel de Filtración de datos 2017 de Gemalto, http://www.gemalto.com/press/Pages/First-Half-2017-Breach-Level-Index-Report-Identity-Theft-and-Poor-Internal-Security-Practices-Take-a-Toll.aspx
[3]Panel sobre privacidad de GfK, Public Perceptions of Privacy and Security in the Post-Snowden Era, 2014.
[4]Artículo 83, el RGPD, 2017
[5]Ponemon Institute, The Impact of Data Breaches on Reputation & Shared Value, patrocinado por Centrify, 2017.
[6]Artículo 4, el RGPD, 2017
[7]Considerando 75 del RGPD, 2017
[8]Considerandos 26 y 28 del RGPD, 2017
[9]Considerando 32 del RGPD, 2017
[10]Artículo 7 del RGPD, 2017
[11]Artículo 35 y considerandos 83-84 del RGPD, 2017
[12]Artículos 37-38 del RGPD, 2017
[13]Considerandos 74, 77-78 del RGPD, 2017
[14]Considerando 81 del RGPD, 2017
[15]Considerandos 59, 63, 65 y 66 del RGPD, 2017

The experts in screen privacy. | 3M