Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 06/11/2026 | Aceptado: 11/11/2026 | Publicación: 16/11/2026

De la conformidad formal a la protección efectiva: privacidad desde el diseño, gestión de terceros y la disociación entre normas y prácticas en la protección de datos personales.

De la conformidad formal a la protección efectiva: la privacidad desde el diseño, la gestión de terceros y la disociación entre la ley y la práctica en la protección de datos personales.

Del cumplimiento formal a la protección efectiva: la privacidad desde el diseño, la gestión de terceros y la disociación entre normas y prácticas en la protección de datos personales.

Cassiano Rodolfo Jung
Estudiante de maestría en Ciberseguridad en la American Global Tech University (AGTU). Especialista en Inteligencia e Investigación de Fuentes Abiertas (OSINT) por WB Educação. Especialista en Informática Forense y Seguridad de la Información por el Instituto de Estudios de Pregrado y Posgrado (IPOG). Especialista en Gestión Estratégica de Tecnologías de la Información por la Universidad Estácio de Sá. Tecnólogo en Seguridad de la Información por la Universidad del Valle de Río dos Sinos (UNISINOS).

RESUMEN

La proliferación de leyes de protección de datos personales, como la Ley General de Protección de Datos (RGPD) en Brasil y el Reglamento General de Protección de Datos (RGPD) en la Unión Europea, no ha ido acompañada de una reducción proporcional de los incidentes que exponen la información de clientes, pacientes y consumidores. Este artículo investiga la brecha entre el cumplimiento formal, expresado en políticas, registros y contratos, y la protección efectiva de datos en el entorno tecnológico de las organizaciones. La investigación, con un enfoque cualitativo y de carácter exploratorio y descriptivo, combina una revisión narrativa de la literatura jurídica, organizativa y de ingeniería de la privacidad con un análisis documental de la legislación, las normas técnicas, los informes sectoriales, las declaraciones oficiales y las decisiones de las autoridades de protección de datos en Brasil, la Unión Europea y Estados Unidos. El análisis indica que el cumplimiento tiende a desvincularse de la práctica cuando se trata como la mera producción de documentos, y que las fallas más recurrentes en los casos examinados involucran controles técnicos básicos, falta de conocimiento de sus propios flujos de datos y supervisión insuficiente por parte de terceros. Las decisiones sancionadoras más recientes han comenzado a examinar la arquitectura de los sistemas, y no solo la existencia de documentos. Se concluye que una protección eficaz depende de traducir las obligaciones legales en requisitos de ingeniería, inventarios actualizados y controles verificables a lo largo de toda la cadena de suministro.

Palabras clave: Protección de datos personales. Cumplimiento normativo. Privacidad desde el diseño. Gestión de riesgos de terceros. LGPD (Ley General de Protección de Datos de Brasil).

ABSTRACTO

La proliferación de leyes de protección de datos personales, como la Ley General de Protección de Datos de Brasil y el Reglamento General de Protección de Datos de la Unión Europea, no se ha visto acompañada por una reducción proporcional de los incidentes que exponen la información de clientes, pacientes y consumidores. Este artículo examina la brecha entre el cumplimiento formal, expresado en políticas, registros y contratos, y la protección efectiva de datos dentro de los entornos tecnológicos de las organizaciones. El estudio sigue un enfoque cualitativo, exploratorio y descriptivo, que combina una revisión narrativa de la literatura jurídica, organizacional y de ingeniería de la privacidad con un análisis documental de la legislación, las normas técnicas, los informes de la industria, los testimonios oficiales y las decisiones emitidas por las autoridades de protección de datos en Brasil, la Unión Europea y Estados Unidos. El análisis indica que el cumplimiento tiende a desvincularse de la práctica cuando se trata como la producción de documentos, y que las fallas más recurrentes en los casos examinados involucran controles técnicos básicos, conocimiento limitado de los flujos de datos propios de la organización y supervisión insuficiente de terceros. Las decisiones de aplicación recientes han comenzado a examinar la arquitectura del sistema en lugar de simplemente la existencia de documentos.

El estudio concluye que la protección efectiva depende de traducir las obligaciones legales en

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 06/11/2026 | Aceptado: 11/11/2026 | Publicación: 16/11/2026

Requisitos de ingeniería, inventarios actualizados y controles verificables en toda la cadena de suministro.

Palabras clave: Protección de datos personales. Cumplimiento normativo. Privacidad desde el diseño. Gestión de riesgos de terceros. LGPD.

1. INTRODUCCIÓN

La última década ha consolidado un ciclo de expansión regulatoria en el ámbito de la protección de datos.
Datos personales. El Reglamento General de Protección de Datos de la Unión Europea ha entrado en vigor.
en mayo de 2018 y sirvió como referencia para varias leyes nacionales, incluida la Ley No.
13.709/2018, la Ley General de Protección de Datos de Brasil (Unión Europea, 2016; Brasil,
2018; Doneda, 2019). La ley brasileña comenzó a exigir, entre otras medidas, la indicación de
Responsable del tratamiento de datos personales, manteniendo un registro de las operaciones de tratamiento.
y la adopción de medidas de seguridad desde el diseño de productos y servicios (Brasil, 2018).
Sin embargo, la ampliación de las obligaciones no fue acompañada de una reducción proporcional de los incidentes.
Un informe de Verizon publicado en 2025 analizó 12.195 filtraciones de datos confirmadas, y el estudio
Un estudio realizado por el Instituto Ponemon para IBM estimó el costo global promedio de una violación de seguridad en US$
4,88 millones en 2024 (Verizon, 2025; IBM, 2024).
La coexistencia de una mayor regulación y una exposición persistente sugiere que el cumplimiento formal y...
La protección efectiva no siempre va de la mano. Waldman (2020) argumenta que las leyes de privacidad
Corren el riesgo de fallar cuando los símbolos de cumplimiento, como la capacitación en protocolo,
Las auditorías y los registros documentales ahora se tratan como si fueran la protección misma.
prometido por ley. La literatura organizacional ha descrito un fenómeno similar durante décadas, mostrando
¿Qué organizaciones pueden adoptar estructuras formales para ganar legitimidad en el entorno?
institucional, sin que estas estructuras alteren realmente sus actividades centrales (Meyer; Rowan, 1977).
La pregunta que guía este trabajo es cómo se manifiesta esta distancia en la protección de
datos personales y qué factores contribuyen a su reducción.
El objetivo de este artículo es analizar los mecanismos mediante los cuales se cumple con las leyes de protección al consumidor...
La protección de datos puede disociarse de la protección efectiva de la información, y la identificación, a partir de la literatura, de que
Las normas técnicas y los estudios de casos documentados describen las condiciones que favorecen la convergencia entre ambos.
El texto explora los fundamentos teóricos de la separación entre normas y práctica, el principio de...
Privacidad desde el diseño y su traducción a la ingeniería, el papel del inventario de datos, la
La seguridad técnica como requisito legal, la gestión de terceros y, finalmente, cuáles son las decisiones de
Las autoridades reguladoras revelan detalles sobre cómo se está evaluando ahora el cumplimiento. Atención.
Se presta especial atención a los sectores sanitario y financiero, que procesan datos sanitarios clasificados bajo la LGPD (Ley General de Protección de Datos de Brasil).
tales como datos personales sensibles y datos financieros, ambos sujetos a una regulación sectorial específica.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 06/11/2026 | Aceptado: 11/11/2026 | Publicación: 16/11/2026

(Brasil, 2018).

2. METODOLOGÍA

Se trata de un estudio de investigación cualitativa con objetivos exploratorios y descriptivos.
Como propone Gil (2008), la investigación exploratoria busca proporcionar una visión general y mayor
familiaridad con un fenómeno que aún está poco sistematizado, mientras que el análisis descriptivo se ocupa de
Caracterización de fenómenos y establecimiento de relaciones entre variables. El tema lo requiere.
combinación, puesto que la distancia entre el cumplimiento y la protección efectiva implica dimensiones legales,
aspectos organizativos y técnicos, y no se identificó ningún indicador estandarizado en la literatura consultada que
permitir su medición directa. Por lo tanto, la elección metodológica prioriza la interpretación articulada.
de fuentes de distinta naturaleza.

El procedimiento bibliográfico tomó la forma de una revisión narrativa, una modalidad que, según Rother
(2007), se presta a la discusión del estado del arte de un tema desde una perspectiva teórica o contextual, sin
La necesidad de protocolos sistemáticos de búsqueda y selección. Se recopilaron tres conjuntos de literatura.
El primero abarca estudios jurídicos y sociojurídicos sobre la aplicación de las leyes de privacidad en
organizaciones como las de Bamberger y Mulligan (2011), Edelman (2016) y Waldman (2020).
El segundo trabajo reúne contribuciones de la teoría organizacional sobre la conformidad simbólica y la auditoría.
La tercera categoría incluye obras de ingeniería de la privacidad, como las de Spiekermann y Cranor.
(2009) y Hoepman (2014). Las obras fueron identificadas a través de Google Scholar, desde los portales
de editoriales y repositorios institucionales.
El análisis documental tuvo en cuenta la legislación y las resoluciones brasileñas y europeas en materia de protección de datos.
Publicaciones de la Autoridad Nacional de Protección de Datos y del Consejo Monetario Nacional
técnicas del Instituto Nacional de Estándares y Tecnología, estándares de la Organización Internacional para
Normalización, directrices del Comité Europeo de Protección de Datos y de la Agencia Europea de Protección de Datos.
Unión Europea para la Ciberseguridad y la propuesta de actualización de la normativa de seguridad de la legislación norteamericana.
El sistema de salud estadounidense. También se analizaron los informes del sector publicados por IBM y Verizon.
una advertencia conjunta de agencias estadounidenses, un informe de la Oficina de Responsabilidad Gubernamental,
un testimonio prestado ante el Senado de los Estados Unidos y decisiones de sanción por parte de la autoridad.
Autoridad irlandesa de protección de datos, la Oficina del Contralor de la Moneda y la ANPD,
complementado con reportajes periodísticos utilizados únicamente para obtener datos fácticos específicos.
El material se organizó en seis ejes analíticos, a saber, los fundamentos del desacoplamiento entre
Norma y práctica, privacidad desde el diseño, inventario y minimización de datos, seguridad
La experiencia técnica como condición para el cumplimiento, la gestión de terceros y la supervisión. Dentro de cada eje, la

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 06/11/2026 | Aceptado: 11/11/2026 | Publicación: 16/11/2026

Los requisitos reglamentarios se enfrentaron con evidencia empírica y casos concretos, de tal manera que...
para identificar convergencias y brechas. La principal limitación del estudio radica en el uso de estudios de caso.
eventos públicos, que tienden a implicar incidentes a gran escala y por lo tanto no reflejan
necesariamente la realidad de las organizaciones más pequeñas. Datos de informes de la industria,
Elaborados con muestras y métodos patentados, se consideran indicadores de tendencias.

3. Conformidad simbólica y el desacoplamiento entre norma y PRÁCTICA

El punto de partida teórico para comprender la brecha entre cumplimiento y protección radica en
en la sociología de las organizaciones. Meyer y Rowan (1977) argumentaron que las organizaciones
Incorporan estructuras formales, como puestos, programas y procedimientos, en gran medida porque
Estas estructuras son reconocidas socialmente como racionales y legítimas, y no necesariamente
Porque aumentan su eficiencia. Cuando los requisitos formales entran en conflicto con la actividad.
En la vida cotidiana, las organizaciones tienden a mantener sus estructuras como una fachada y a desvincularlas de sus prácticas.
eficaz. El concepto de desacoplamiento ofrece una clave de lectura útil para la protección de datos.
un ámbito en el que la adopción de políticas y el nombramiento de funcionarios pueden coexistir con las prácticas.
Las técnicas han cambiado muy poco.
Edelman (2016), al estudiar la aplicación de las leyes antidiscriminación en los Estados Unidos, desarrolló
El concepto de endogeneidad legal para describir el proceso mediante el cual las organizaciones crean
Estructuras simbólicas de conformidad, y con el tiempo, estas estructuras son aceptadas por...
Los propios tribunales sirven como prueba del cumplimiento de la ley. El significado de la regla, en este proceso, es
Conformada progresivamente por las organizaciones que pretendía regular. Su contribución es relevante.
porque cambia el análisis de la simple pregunta de si se está obedeciendo la ley a investigar cómo
En la práctica, las organizaciones definen qué significa el cumplimiento y quién participa en esa definición.
Waldman (2020) transpuso este marco al campo de la privacidad. Basado en entrevistas
con ingenieros, profesionales de la privacidad y ejecutivos de empresas que ofrecen soluciones para
Además de analizar las demostraciones de productos y la literatura del sector, el autor argumenta que, en cumplimiento...
que las leyes de privacidad corren el riesgo de fracasar porque los símbolos de cumplimiento, como
Los programas de capacitación sin efecto práctico, las auditorías y los registros documentales se están confundiendo con...
cumplimiento real de la ley. En un trabajo posterior, Waldman (2021) analizó más a fondo cómo las rutinas
Las prácticas internas de las empresas tecnológicas influyen en la interpretación de las obligaciones de privacidad.
El problema señalado por el autor, por lo tanto, no reside en la existencia de documentos, sino en la posibilidad.
que sean tomadas como sustitutos de la protección real.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 06/11/2026 | Aceptado: 11/11/2026 | Publicación: 16/11/2026

La literatura no es unánime con respecto al alcance de este diagnóstico. Bamberger y Mulligan (2011), en estudio basado en entrevistas con directores de privacidad identificados por sus pares como Expertos del sector constataron que algunas empresas estadounidenses habían cambiado su enfoque. desde un enfoque centrado en el procedimiento, como la advertencia y el consentimiento, hasta una preocupación sustantivo con la prevención de violaciones de las expectativas de privacidad de los consumidores. Entre los Entre los factores asociados a este cambio, los autores señalan las acciones de la Comisión Federal de Comercio, la La presión del mercado y de la prensa, la profesionalización del sector y las leyes estatales de notificación incidentes que han incrementado el coste de la mala gestión de la información personal.

La teoría de la auditoría añade otra capa al problema. Power (1997) describió la expansión de prácticas de verificación en las sociedades contemporáneas y se observó que la auditoría tiende a evaluar la La existencia de sistemas de control, y no necesariamente el desempeño sustantivo de las actividades. que estos sistemas deberían controlar. Aplicado a la protección de datos, este diagnóstico ayuda a explicar por qué una organización podría recibir evaluaciones favorables con respecto a la existencia de políticas y registros y, sin embargo, aún conservan fallas técnicas explotables. En conjunto, los autores discutieron en este Las secciones indican que la efectividad del cumplimiento depende menos de la cantidad de documentos. lo que se produjo, y lo que es más importante, la capacidad de estos documentos para modificar las decisiones técnicas y operativas.

4. PRIVACIDAD DESDE EL DISEÑO: DEL PRINCIPIO LEGAL A LA INGENIERÍA

La idea de que la protección de datos debe incorporarse a los sistemas desde su concepción, y no añadido al final, fue sistematizado por Cavoukian (2009) en siete principios fundamentales, entre ellos Hacen hincapié en la acción proactiva y preventiva, la privacidad como configuración predeterminada y la incorporación de... Privacidad en el diseño, funcionalidad completa, seguridad integral durante todo el ciclo de vida. La esencia de la información, la visibilidad y la transparencia, y el respeto por la privacidad del usuario. La conversión Sin embargo, la aplicación de estos principios a los requisitos concretos del sistema no se deriva automáticamente de su Declaración. Informe preparado para la Agencia Europea de Ciberseguridad por Danezis et al. (2014). El objetivo era precisamente reducir la brecha entre el marco jurídico y las medidas técnicas disponibles. lo cual indica que esta traducción constituye un problema en sí mismo, que requiere un método específico.

El Reglamento General de Protección de Datos ha convertido el principio en una obligación legal en El artículo 25 exige que el responsable del tratamiento de datos adopte medidas técnicas y organizativas. apropiado tanto al momento de definir los medios de tratamiento como durante el tratamiento mismo. tratamiento, además de garantizar que, por defecto, solo se procesen los datos necesarios para cada finalidad. tratados (Unión Europea, 2016). La legislación brasileña siguió una orientación similar. Artículo 46 La LGPD (Ley General de Protección de Datos de Brasil) exige a los agentes de procesamiento de datos que adopten medidas de seguridad, tanto técnicas como...

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 06/11/2026 | Aceptado: 11/11/2026 | Publicación: 16/11/2026

medidas administrativas capaces de proteger los datos personales, y el párrafo 2 de ese artículo estipula que estas medidas debe observarse desde la fase de concepción del producto o servicio hasta su ejecución (Brasil, 2018).

Las directrices del Comité Europeo de Protección de Datos sobre el artículo 25 buscaban reducir la La distancia entre el texto legal y su aplicación. El documento aclara que la obligación está dirigida a Lo que importa es la eficacia de las medidas, y no su mera existencia, y la persona responsable debe ser capaz de... demostrar que las salvaguardias adoptadas producen los efectos previstos en relación con cada principio. protección de datos (EDPB, 2020). Este énfasis en la efectividad acerca la obligación legal a Las preocupaciones de ingeniería y disipan la interpretación de que el cumplimiento del Artículo 25 podría Esto solo puede lograrse mediante el desarrollo de políticas o cláusulas contractuales.

La literatura sobre ingeniería de la privacidad ofrece herramientas para esta traducción. Spiekermann y Cranor (2009) distinguió dos enfoques de diseño, uno basado en políticas, que depende de advertencia, elección y cumplimiento de las reglas por parte de la persona a cargo, y otra basada en la arquitectura, que Su objetivo es reducir la posibilidad de identificar los datos y limitar su recopilación, lo que disminuye la eficacia de la protección. dependiente del comportamiento organizacional. Hoepman (2014) propuso ocho estrategias de diseño. que permiten que la privacidad se aplique desde las primeras etapas del desarrollo, a saber, minimizando, Ocultar, separar, agrupar, informar, controlar, imponer y demostrar. Las estrategias traducen objetivos. protección en las decisiones de diseño de concreto, como recopilar solo los datos necesarios o Separación de bases de datos para dificultar la consulta cruzada de información.

El mismo informe de Danezis et al. (2014) examinó el estado del arte de las tecnologías de refuerzo para privacidad y señaló que, si bien estas tecnologías han demostrado su potencial en Sin embargo, la investigación y los proyectos piloto aún no se habían convertido en un componente estándar y generalizado. utilizado en el diseño de sistemas, con la excepción de la criptografía, y propuso un método para relacionar el Obligaciones legales en materia de estrategias de diseño. En cuanto a las normas técnicas, ISO/IEC 27701, cuya La edición de 2025 comenzó a publicarse como un estándar independiente para sistemas de gestión. Información sobre privacidad, y el Marco de Privacidad del NIST ofrecen estructuras que permiten convertir las obligaciones legales en controles organizativos y técnicos verificables (ISO, 2025; NIST, 2020).

5. COMPRENDER LOS DATOS PARA PROTEGERLOS: INVENTARIO, MINIMIZACIÓN Y DATOS NO ADMINISTRADOS

No se pueden aplicar controles a los datos cuya existencia la organización desconoce. Por esta razón, Las leyes de protección de datos asignan un papel central al registro de las operaciones de procesamiento de datos. El artículo

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 06/11/2026 | Aceptado: 11/11/2026 | Publicación: 16/11/2026

El artículo 37 de la LGPD (Ley General de Protección de Datos de Brasil) estipula que el responsable del tratamiento y el operador deben mantener un registro de las operaciones que realizan.

y el artículo 30 del reglamento europeo establece una obligación equivalente, detallando la
fines, categorías de interesados y interesados, destinatarios y, siempre que sea posible, plazos.
planificado para su eliminación y las medidas de seguridad adoptadas (Brasil, 2018; Unión Europea, 2016).
Desde esta perspectiva, el registro no es simplemente un requisito documental, sino el punto de partida para...
evaluación de riesgos y definición de controles.
El marco de privacidad del NIST le da a este inventario una dimensión operativa. La función
La identificación del modelo incluye inventariar y mapear los sistemas, productos y servicios a los que se refiere.
datos, de los propietarios u operadores de estos sistemas, de las categorías de individuos cuyos datos son
tratado y las acciones de procesamiento realizadas en cada etapa del ciclo de vida de la información (NIST,
(2020). Este mapeo guía las demás funciones del modelo, como gobernar, controlar y comunicar.
y proteger, y explicita la dependencia entre conocer los flujos de datos y ser capaz de gestionarlos.
riesgos que producen. Por lo tanto, un inventario obsoleto compromete todas las decisiones que
Dependen de él.
Los datos empíricos muestran que esta dependencia tiene consecuencias concretas. El estudio de IBM
Un estudio de 2024 registró que el 35% de las violaciones analizadas involucraban datos no gestionados, también
los llamados datos en la sombra, es decir, información almacenada fuera de entornos controlados y
inventariado por la organización (IBM, 2024). Según el mismo informe, las violaciones que
Los estudios que utilizaban este tipo de datos tenían un coste medio un 16 % superior y requerían más tiempo para completarse.
Se identificaron y contuvieron las filtraciones, y aproximadamente el 40% de ellas involucraron datos distribuidos en múltiples redes.
entornos, como nubes públicas, nubes privadas e infraestructura local. La fragmentación de
Estos entornos tienden a aumentar la probabilidad de que las copias de datos escapen al inventario formal.
La minimización de datos es la contraparte del inventario. El artículo 6 de la LGPD establece el principio de...
necesidad, que limita el tratamiento al mínimo necesario para lograr sus fines,
con cobertura de datos relevantes, proporcionales y no excesivos (Brasil, 2018). Desde el punto de vista de
Desde una perspectiva de seguridad, la minimización reduce el área de superficie expuesta, ya que los datos que no estaban
Los activos recaudados o ya eliminados no se pueden restar en un incidente. La estrategia de
La primera de las propuestas de Hoepman (2014), que minimiza el impacto ambiental, se deriva precisamente de este razonamiento.
Las regulaciones europeas aclaran el alcance de esta obligación especificando, en el párrafo 2 del artículo 25,
que la protección predeterminada se aplica a la cantidad de datos recopilados, el alcance del procesamiento y la
Periodo de retención de datos y accesibilidad (Unión Europea, 2016).
En la doctrina brasileña, Bioni (2019) examina la función y los límites del consentimiento como
instrumento de protección, considerando la asimetría entre titulares y organizaciones, y analiza el
La necesidad de mecanismos que no dependan exclusivamente de la elección individual del titular de los datos.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
IRCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 06/11/2026 | Aceptado: 11/11/2026 | Publicación: 16/11/2026

Doneda (2019), al reconstruir la formación de la LGPD, defiende el reconocimiento de la protección de datos.
Analiza los derechos personales como un derecho fundamental y examina la importancia central de los principios en el modelo regulatorio.
adoptado por ley. Leídas junto con la literatura técnica, estas contribuciones refuerzan que la
El inventario y la minimización de datos son obligaciones fundamentales de los responsables del tratamiento de datos, no meras formalidades.
accesorios.

6. LA SEGURIDAD TÉCNICA COMO CONDICIÓN DE CONFORMIDAD

La LGPD (Ley General de Protección de Datos de Brasil) no considera la seguridad de la información como un asunto separado de la protección de datos. Además de...
Además del deber general estipulado en el artículo 46, el artículo 44 considera irregular el trato que no se ajusta a dicho deber.
la seguridad que su titular puede esperar, considerando circunstancias tales como la forma en que se
realizado, el resultado y los riesgos razonablemente esperados, y las técnicas disponibles en ese momento, y el
El único párrafo del mismo artículo asigna responsabilidad por los daños resultantes de la violación de
La seguridad de los datos está en riesgo para el controlador u operador que, al no adoptar las medidas previstas en
Artículo 46, causa el daño (Brasil, 2018). El cumplimiento, en este marco legal, incluye
Depende necesariamente de la calidad de los controles técnicos que se implementen realmente.
El caso de Equifax, una empresa de informes crediticios de EE. UU., ilustra cómo los fallos en
Los controles de seguridad pueden provocar una exposición a gran escala. Según el informe...
Según la Oficina de Responsabilidad Gubernamental en relación con el incidente de 2017, los atacantes obtuvieron acceso a través de...
Internet, un portal de quejas de consumidores, y obtuvo datos personales de al menos
145,5 millones de personas (Estados Unidos, 2018). La investigación, realizada por la propia empresa,
como se informa en el documento, el incidente se atribuyó a fallas en cuatro áreas, la identificación de
vulnerabilidades, detección de intrusiones, segmentación del acceso a bases de datos y gobernanza
datos. Se trata de áreas cubiertas por controles de seguridad que se describen ampliamente en la literatura.
Técnicamente, el problema radica más en la aplicación de estos controles que en la falta de disponibilidad de
soluciones.
En el sector sanitario, el ataque tuvo como objetivo Change Healthcare, una empresa de procesamiento de transacciones sanitarias.
controlada por UnitedHealth Group, ofrece otro ejemplo de esta dinámica. En testimonio de
Comité de Finanzas del Senado de los Estados Unidos, el 1 de mayo de 2024, el director ejecutivo de
El grupo afirmó que los delincuentes accedieron a un portal de la empresa que no estaba protegido por
Utilizando la autenticación multifactor, extrajeron datos e implementaron un ransomware el 21 de febrero de ese año.
y confirmó el pago de un rescate de 22 millones de dólares (Witty, 2024). En enero de 2025, la empresa
Se estima que alrededor de 190 millones de personas se vieron afectadas (Fierce Healthcare, 2025).
La norma de seguridad de la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA) establece requisitos específicos.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 06/11/2026 | Aceptado: 11/11/2026 | Publicación: 16/11/2026

Implementación obligatoria y especificaciones clasificadas como direccionables. Según el propio autor.
Departamento de Salud y Servicios Humanos, ninguno de ellos era opcional, pero la designación permitía
que cada entidad debe evaluar si la medida fue razonable y apropiada en su entorno, con el objetivo
para brindar mayor flexibilidad (Estados Unidos, 2025). En enero de 2025, el departamento publicó
La actualización propuesta a esta regla está motivada, según su preámbulo, entre otros factores, por la fuerte
El aumento de las violaciones de datos de salud reportadas entre 2018 y 2023. La propuesta elimina
Esta distinción hace que el cifrado de los datos de salud en reposo y en tránsito sea obligatorio, y
Ahora se requiere la autenticación multifactor, junto con un inventario escrito de los activos tecnológicos y un mapa de la red.
(Estados Unidos, 2025).
La misma propuesta incluye la obligación de restablecer los sistemas y datos críticos en un plazo de 72 horas tras un fallo.
pérdida, de realizar auditorías de cumplimiento al menos cada doce meses y de obtener, con el mismo
periodicidad, verificación por escrito de que los socios comerciales han implementado las medidas de seguridad.
técnicas requeridas (Estados Unidos, 2025). En el caso de la criptografía, el propio texto de la propuesta lo explica.
que el cambio eximiría a las entidades de evaluar si la medida es razonable y apropiada, lo cual expresa
La sustitución de las evaluaciones caso por caso por requisitos verificables. Este ejemplo es relevante para...
debate brasileño, ya que indica que, incluso en un sistema regulatorio consolidado, el regulador ha pasado
considerar necesario especificar explícitamente los controles básicos, en lugar de confiar únicamente en
Las obligaciones generales de seguridad están sujetas a evaluación por parte de cada entidad.

7. Terceros y la cadena de suministro como vector de exposición

La creciente dependencia de los proveedores de tecnología traslada una parte importante del riesgo fuera de la empresa.
límites organizativos. El informe de Verizon de 2025 señaló la participación de terceros.
El número de infracciones analizadas se duplicó en comparación con el año anterior, alcanzando el 30% de los casos (Verizon,
2025). Estos datos indican que la protección efectiva de los datos de una organización depende, hasta cierto punto...
considerable, por las prácticas de sus proveedores de servicios, y que los enfoques limitados a los controles
Los datos internos tienden a dejar una parte significativa del riesgo sin tratar. Por esta razón, tanto la LGPD como
Las regulaciones europeas rigen expresamente la relación entre quienes deciden sobre el tratamiento y
quién lo ejecuta.
La LGPD establece que el operador debe llevar a cabo el tratamiento de acuerdo con las instrucciones proporcionadas por...
controlador, siendo su responsabilidad verificar el cumplimiento de sus propias instrucciones y las reglas relativas a la
materia, según el artículo 39 (Brasil, 2018). El artículo 42, a su vez, dispone que el operador es responsable.
responsables solidarios por los daños causados al incumplir las obligaciones legales o al no seguir las normas.
instrucciones lícitas del responsable del tratamiento. En el Reglamento europeo, el artículo 28 exige que el responsable del tratamiento recurra a

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 06/11/2026 | Aceptado: 11/11/2026 | Publicación: 16/11/2026

únicamente a subcontratistas que proporcionen garantías suficientes de implementar medidas técnicas y estructura organizativa adecuada y detalles del contenido mínimo del contrato que rige esta relación (Unión). Europeo, 2016).

El caso de MOVEit Transfer demostró la escala que puede alcanzar un solo proveedor. Según una advertencia... Oficina Federal de Investigación conjunta y la Agencia de Seguridad de Infraestructura y Ciberseguridad, A partir del 27 de mayo de 2023, el grupo criminal conocido como CL0P comenzó a explotar una Una vulnerabilidad de inyección SQL previamente desconocida, catalogada como CVE-2023-34362, en este software de transferencia de archivos administrado, instalando un shell web llamado LEMURLOOT en aplicaciones expuestas a Internet y que extraen datos de sus bases de datos (FBI; CISA, 2023). Al permitir la transferencia de archivos entre organizaciones, clientes y socios, la herramienta permitió la explotación de una única vulnerabilidad para exponer simultáneamente datos de múltiples organizaciones.

Las publicaciones técnicas recomiendan que la gestión por parte de terceros se trate como un proceso continuo. y no como una verificación única realizada en el momento de la contratación. La guía del NIST sobre gestión El marco de evaluación de riesgos de ciberseguridad para la cadena de suministro, desarrollado por Boyens et al. (2022), guía la Las organizaciones están integrando estos riesgos en la gestión de riesgos corporativos y definiendo los requisitos de seguridad. en los contratos, para evaluar la importancia de cada proveedor y supervisar su desempeño a lo largo del tiempo. Toda la relación. La propuesta de actualizar la norma de seguridad en la legislación estadounidense de La salud, al exigir una verificación escrita anual de las medidas de seguridad de los socios comerciales, aplica este principio. La misma lógica de supervisión periódica (Estados Unidos, 2025).

En el sistema financiero brasileño, la Resolución CMN No. 4.893/2021 estableció requisitos para... política de ciberseguridad de las instituciones autorizadas para operar por el Banco Central y para la Servicios de contratación para el procesamiento, almacenamiento y computación en la nube de datos. (Consejo Monetario Nacional, 2021). La regla fue enmendada por la Resolución CMN No. 5.274/2025, que Comenzó a requerir, entre otras cosas, la verificación de los controles para los sistemas adquiridos o Desarrollado por proveedores de servicios, autenticación multifactor para el acceso a la red corporativa. comenzando por entornos externos y pruebas de intrusión con una frecuencia anual mínima (Ayuntamiento) Política Monetaria Nacional, 2025). El detalle progresivo de los controles necesarios acerca la regulación. lógica sectorial de requisitos verificables.

8. INSPECCIÓN Y SANCIONES: LO QUE REVELAN LAS DECISIONES SOBRE LA DISTANCIA Entre la norma y la práctica

Las decisiones de las autoridades reguladoras constituyen una fuente privilegiada para observar cómo la

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 06/11/2026 | Aceptado: 11/11/2026 | Publicación: 16/11/2026

El cumplimiento se evalúa en la práctica. En Brasil, la primera sanción monetaria aplicada por la ANPD,
Publicado en julio de 2023, iba dirigido a una microempresa, Telekall Infoservice, con una advertencia y
Se impuso una multa total de R$ 14.400 por violar el artículo 7 de la LGPD (Ley General de Protección de Datos de Brasil), relativo a las hipótesis legales de...
tratamiento, y al artículo 5 del Reglamento de Inspección, que establece las obligaciones de los agentes.
regulado ante la autoridad (Mobile Time, 2023). El proceso se había iniciado en 2022 y el
La lista de hallazgos publicada por la autoridad también mencionaba la ausencia de registros de las operaciones.
y de la persona a cargo, lo que demuestra que, en este primer caso, existen deficiencias básicas en la base legal y de
La documentación ocupaba un lugar central.

El Reglamento sobre la dosificación y aplicación de sanciones administrativas, aprobado por Resolución
La CD/ANPD No. 4/2023 clasifica las infracciones como leves, moderadas y graves, y prevé las circunstancias correspondientes.
Factores atenuantes y agravantes para el cálculo de multas (ANPD, 2023). Entre los factores atenuantes se encuentran...
implementación de una política de buenas prácticas y gobernanza, o la adopción repetida y comprobada de
Mecanismos internos capaces de minimizar el daño a los sujetos de datos y la adopción de medidas para revertir
o mitigar los efectos de la infracción. La segunda hipótesis requiere que los mecanismos internos sean
adoptados repetidamente y de manera demostrable, lo que indica atención a su aplicación efectiva, y no solo
a su pronóstico formal.

En la Unión Europea, las recientes decisiones de la autoridad irlandesa de protección de datos han examinado
directamente a la arquitectura de los sistemas. En noviembre de 2022, la autoridad se aplicó a Meta Platforms.
Irlanda impone multas por un total de 265 millones de euros por infracciones de los párrafos 1 y 2 del artículo 25 de la
regulación, debido al procesamiento realizado a través de herramientas de búsqueda e importación de
Los contactos de Facebook e Instagram se utilizan para la extracción de datos (Protección de datos).
Comisión, 2022). En diciembre de 2024, una nueva decisión impuso multas relacionadas por valor de 251 millones de euros.
de una violación de 2018, de la cual 240 millones correspondieron a violaciones del Artículo 25 y el 11
Millones restantes, debido a fallas en la notificación y documentación de la violación (Protección de datos)
Comisión, 2024).

La decisión de 2024 describe cómo la combinación de funcionalidades de la plataforma permitió la generación
un fallo relacionado con una credencial de acceso, denominada token, que otorga acceso completo al perfil de otro usuario.
explotada entre el 14 y el 28 de septiembre de 2018, y que afectó a aproximadamente 29 millones de cuentas en todo el mundo,
de los cuales aproximadamente 3 millones se encuentran en la Unión Europea y el Espacio Económico Europeo (Datos
Comisión de Protección, 2024). En los Estados Unidos, la Oficina del Contralor de la Moneda
En 2020, impuso una multa de 80 millones de dólares a Capital One por no haber establecido procesos eficaces.
evaluación de riesgos antes de migrar las operaciones tecnológicas relevantes a la nube pública y por
no haber corregido con prontitud las deficiencias identificadas (Oficina del Contralor de la
(Moneda, 2020). La tabla 1 resume estos casos.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 06/11/2026 | Aceptado: 11/11/2026 | Publicación: 16/11/2026

Tabla 1 – Casos seleccionados de sanciones relacionadas con la protección y la seguridad de los datos.
información

Organización	Autoridad y año	Sanción	Principio principal
Servicio de información de Telekall (Brasil)	ANPD, 2023	Advertencia y multa de R$ 14.400	Artículo 7 de la LGPD y artículo 5 del Reglamento de Inspección
Capital One (Estados Unidos)	OCC, 2020	80 millones de dólares estadounidenses	Falta de una evaluación de riesgos eficaz antes de migrar a la nube pública.
Metaplataformas Irlanda (extracción de datos)	DPC, 2022	265 millones de euros	Artículos 25(1) y 25(2) del RGPD, protección desde el diseño y por defecto
Metaplataformas Irlanda (violación de 2018)	DPC, 2024	251 millones de euros	Artículos 25(1) y 25(2) del RGPD (240 millones de euros) y artículos 33(3) y 33(5) (11 millones de euros)

Fuente: compilado por el autor con base en Mobile Time (2023), Oficina del Contralor de la Moneda (2020) y Comisión de Protección de Datos (2022; 2024).

Los casos recopilados en la Tabla 1 difieren en términos de jurisdicciones, tamaño de las empresas y...
fundamentos legales, lo que impide comparaciones cuantitativas directas entre las sanciones.
La contribución analítica, por lo tanto, no reside en la magnitud de las multas, sino en los criterios utilizados por el
autoridades para evaluar el cumplimiento. En las decisiones europeas y norteamericanas, la justificación
Se centra en la ausencia de protección incorporada en el diseño de los sistemas o en la insuficiencia de
Evaluación de riesgos previa a las decisiones tecnológicas. En la decisión de 2024, las infracciones relacionadas con
La notificación y la documentación representaron una parte minoritaria de la multa, reforzando, en este caso, la
La importancia de los fallos en la protección de los materiales. Estos elementos sugieren una orientación supervisora.
centrado en verificar cómo las obligaciones legales se materializan en las decisiones arquitectónicas y
prácticas de gestión. Desde esta perspectiva, las políticas, los registros y los procedimientos no pierden su
Relevancia, pero deben demostrar un vínculo con los controles que realmente se han implementado.
La distinción es fundamental para el debate sobre la conformidad simbólica: la existencia de estructuras formales no implica
Esto, en sí mismo, equivale a proteger a los titulares. Sin embargo, la heterogeneidad y el número limitado de
Estos casos no nos permiten afirmar una trayectoria uniforme de maduración regulatoria; nos permiten...
identificar, en las decisiones examinadas, indicios de una evaluación más sustantiva de la relación entre las normas.
y práctica.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS - Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 06/11/2026 | Aceptado: 11/11/2026 | Publicación: 16/11/2026

9. CONCLUSIÓN

Este artículo examinó la brecha entre el cumplimiento formal de las leyes de protección de datos y la Protección eficaz de la información personal. Se analiza la bibliografía organizativa y sociojurídica al respecto. Esto nos permite entender esta distancia no solo como una desviación individual de organizaciones negligentes, pero también como una tendencia estructural, asociada con la adopción de estructuras formales en busca de legitimidad y la posibilidad de que estas estructuras se desvinculen de las prácticas técnicas. El concepto La endogeneidad legal y su aplicación al campo de la privacidad ofrecen herramientas para identificar cuándo los documentos de cumplimiento dejan de guiar las decisiones y comienzan a reemplazarlos. a ellos.

La literatura también muestra que este resultado no es inevitable. El estudio de Bamberger y Mulligan, A partir de entrevistas con directores de privacidad, se identificaron organizaciones que han cambiado su enfoque. de procedimientos formales para la prevención sustantiva de daños, impulsados por las acciones de Los reguladores, debido a la presión del mercado y la profesionalización del área. Esto indica que el entorno Los factores regulatorios e institucionales influyen en la dirección que toma el cumplimiento normativo dentro de las organizaciones. y que los mecanismos de supervisión orientados a los resultados pueden promover la convergencia entre Estándar y práctica.

Privacidad desde el diseño, tal como se establece en el artículo 25 del Reglamento europeo y en el párrafo 2 de la El artículo 46 de la LGPD constituye un instrumento jurídico central para esta convergencia, siempre que interpretado como una obligación de efectividad. Directrices europeas sobre el tema y la literatura sobre Los enfoques de la ingeniería de la privacidad convergen en el punto de que la protección debe convertirse en requisitos. del sistema, como la minimización de la recopilación de datos, la separación de bases y las configuraciones de protección por Estándar, y que los principios genéricos, por sí solos, no alteran la arquitectura de las aplicaciones.

El inventario de datos demostró ser un requisito previo para cualquier control. La proporción de violaciones que Los datos involucrados información no administrada, registrada en el estudio de IBM de 2024, muestran que el registro de Las operaciones de procesamiento de datos que exige la LGPD solo cumplen su función cuando reflejan el entorno real. incluyendo copias y repositorios creados fuera de los procesos formales. Minimización, mediante la reducción de El volumen de información que se mantiene complementa el inventario y reduce la exposición en caso de... incidente, lo que también lo convierte en una medida de seguridad.

Los casos de Equifax y Change Healthcare demuestran fallos en los controles técnicos. Técnicas ampliamente conocidas, como la identificación de vulnerabilidades y la segmentación del acceso a las bases de datos. Las filtraciones de datos y la autenticación multifactor pueden exponer a decenas o cientos de millones de personas. de personas en grandes organizaciones, sujetas a una amplia regulación sectorial. La propuesta de Una actualización de la normativa estadounidense sobre seguridad en el sector sanitario, que hace obligatorios los controles.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 06/11/2026 | Aceptado: 11/11/2026 | Publicación: 16/11/2026

previamente sujeto a evaluación discrecional por parte de las entidades, indica que el regulador estadounidense de
El sector sanitario ha comenzado a preferir los requisitos explícitos a las obligaciones genéricas de seguridad sujetas a evaluación.
de cada entidad.

La gestión por terceros se ha convertido en una dimensión crucial. La mayor participación de los proveedores
Las violaciones y la explotación masiva de un único software de transferencia de archivos sugieren
que el cumplimiento contractual, limitado a las cláusulas y cuestionarios aplicados durante la contratación, tiende a
no mantenerse al día con la dinámica del riesgo. Las directrices técnicas y los estándares del sector más recientes,
Incluso dentro del sistema financiero brasileño, estos factores apuntan a una supervisión y verificación continuas.
de los controles implementados eficazmente por los proveedores.

Los casos de sanciones examinados sugieren que la supervisión tiende a evolucionar a partir de la verificación.
Información documental para examinar la arquitectura de los sistemas y la calidad de las evaluaciones de riesgos.
En Brasil, las acciones de la ANPD todavía están en la fase de consolidación, pero la regulación de
Las directrices de sentencia ya incluyen, entre los factores atenuantes, la adopción repetida y probada de mecanismos internos de
minimización de daños. Esta directriz, si se mantiene, puede contribuir a reducir el incentivo para
El cumplimiento es meramente simbólico, y deberían fomentarse las inversiones en controles verificables.

Una limitación es que los casos analizados son en su mayoría a gran escala y...
jurisdicciones extranjeras, lo que restringe la generalización de las conclusiones a las organizaciones brasileñas.
a menor escala. Para estudios futuros, se recomienda realizar investigación empírica con
Organizaciones nacionales que comparan la madurez documental de sus programas de privacidad.
con indicadores de protección técnica, así como el análisis sistemático de las decisiones de la ANPD para
a medida que su jurisprudencia administrativa se consolida. Dichos estudios nos permitirían verificar de qué maneras.
El grado en que la desconexión entre norma y práctica se manifiesta en el contexto brasileño.

REFERENCIAS

AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS (ANPD). Resolución CD/ANPD N° 4, de 24 de febrero de 2023. Por la que se aprueba el Reglamento sobre Dosimetría y Aplicación de Sanciones Administrativas. Brasilia, DF: ANPD, 2023.

BAMBERGER, Kenneth A.; MULLIGAN, Deirdre K. La privacidad en los libros y en la práctica.
Revista de Derecho de Stanford, Stanford, vol. 63, núm. 2, pág. 247, 2011.

BIONI, Bruno Ricardo. Protección de datos personales: función y límites del consentimiento. Río de Janeiro: Forense, 2019.

BOYENS, Jon; SMITH, Angela; BARTOL, Nadya; WINKLER, Kris; HOLBROOK, Alexander; FALLON, Matthew. Prácticas de gestión de riesgos de ciberseguridad en la cadena de suministro para sistemas y organizaciones. Gaithersburg: Instituto Nacional de Estándares y Tecnología, 2022. (Publicación especial NIST 800-161, rev. 1). DOI: 10.6028/NIST.SP.800-161r1.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 06/11/2026 | Aceptado: 11/11/2026 | Publicación: 16/11/2026

BRASIL. Ley N° 13.709, de 14 de agosto de 2018. Ley General de Protección de Datos Personales (LGPD). Brasilia, DF: Presidencia de la República, 2018.

CAVOUKIAN, Ann. Privacidad desde el diseño: los 7 principios fundamentales. Toronto: Comisionado de Información y Privacidad de Ontario, 2009.

CONSEJO MONETARIO NACIONAL (Brasil). Resolución CMN n.º 4.893, del 26 de febrero de 2021. Establece la política de ciberseguridad y los requisitos para la contratación de servicios de procesamiento y almacenamiento de datos y computación en la nube. Brasilia, DF: Banco Central de Brasil, 2021.

CONSEJO MONETARIO NACIONAL (Brasil). Resolución CMN n.º 5.274, del 18 de diciembre de 2025. Modifica la Resolución CMN n.º 4.893, del 26 de febrero de 2021. Brasilia, DF: Banco Central de Brasil, 2025.

DANEZIS, George; DOMINGO-FERRER, Josep; HANSEN, Marit; HOEPMAN, Jaap-Henk; LE MÉTAYER, Daniel; TIRTEA, Rodica; SCHIFFNER, Stefan. Privacidad y protección de datos desde el diseño: de la política a la ingeniería. Heraklion: Agencia de la Unión Europea para la Seguridad de las Redes y la Información (ENISA), 2014.

COMISIÓN DE PROTECCIÓN DE DATOS (Irlanda). La Comisión de Protección de Datos anuncia su decisión en la investigación sobre la extracción de datos por parte de Facebook. Dublín: DPC, 28 de noviembre de 2022.

COMISIÓN DE PROTECCIÓN DE DATOS (Irlanda). La Comisión Irlandesa de Protección de Datos multa a Target con 251 millones de euros. Dublín: DPC, 17 de diciembre de 2024.

DONEDA, Danilo. De la privacidad a la protección de datos personales: elementos de la formación del Reglamento General de Protección de Datos. 2.ª ed. São Paulo: Thomson Reuters Brasil, 2019.

EDELMAN, Lauren B. Derecho en la práctica: tribunales, corporaciones y derechos civiles simbólicos. Chicago: University of Chicago Press, 2016.

Comité Europeo de Protección de Datos (CEPD). Directrices 4/2019 sobre el artículo 25: protección de datos desde el diseño y por defecto. Versión 2.0. Bruselas: CEPD, 2020.

OFICINA FEDERAL DE INVESTIGACIÓN (FBI); AGENCIA DE CIBERSEGURIDAD E INFRAESTRUCTURA (CISA). #StopRansomware: La banda de ransomware CL0P explota la vulnerabilidad CVE-2023-34362 de MOVEit. Washington, D.C.: CISA, 2023. (Aviso de Ciberseguridad AA23-158A).

FIERCE HEALTHCARE. UnitedHealth estima que 190 millones de personas se vieron afectadas por el ciberataque a Change Healthcare. Fierce Healthcare, [S. l.], 24 de enero de 2025.

GIL, Antonio Carlos. Métodos y técnicas de investigación social. 6ª edición. São Paulo: Atlas, 2008.

HOEPMAN, Jaap-Henk. Estrategias de diseño de privacidad. En: IFIP INTERNATIONAL INFORMATION SECURITY CONFERENCE, 29.ª, 2014, Marrakech. Seguridad de los sistemas TIC y protección de la privacidad. Berlín: Springer, 2014. págs. 446-459. DOI: 10.1007/978-3-642-55415-5_38.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 06/11/2026 | Aceptado: 11/11/2026 | Publicación: 16/11/2026

IBM. Informe sobre el coste de una filtración de datos 2024. Armonk: IBM Corporation, 2024.

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN (ISO). ISO/IEC 27701: Seguridad de la información, ciberseguridad y protección de la privacidad, sistemas de gestión de la información sobre privacidad, requisitos y directrices. Ginebra: ISO, 2025.

MEYER, John W.; ROWAN, Brian. Organizaciones institucionalizadas: la estructura formal como mito y ceremonia. American Journal of Sociology, Chicago, vol. 83, n.º 2, págs. 340-363, 1977.

MOBILE TIME. La ANPD impone su primera sanción con una multa a Telekall. Mobile Time, São Paulo, 6 de julio de 2023.

INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA (NIST). Marco de privacidad del NIST: una herramienta para mejorar la privacidad mediante la gestión de riesgos empresariales. Versión 1.0.
Gaithersburg: NIST, 2020.

OFICINA DEL CONTRALOR DE LA MONEDA (Estados Unidos). La OCC impone una multa civil de 80 millones de dólares a Capital One. Washington, D.C.: OCC, 6 de agosto de 2020. (Comunicado de prensa 2020-101).

POWER, Michael. La sociedad de auditoría: rituales de verificación. Oxford: Oxford University Press, 1997.

ROTHER, Edna Terezinha. Revisión sistemática versus revisión narrativa. Acta Paulista de Enfermagem, São Paulo, v. 20, n. 2, pág. v-vi, 2007.

SPIEKERMANN, Sarah; CRANOR, Lorrie Faith. Ingeniería de la privacidad. IEEE Transactions on Software Engineering, [Nueva York], vol. 35, n.º 1, págs. 67-82, 2009.

UNIÓN EUROPEA. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Diario Oficial de la Unión Europea, Luxemburgo, L 119, pp. 1-88, 4 de mayo de 2016.

ESTADOS UNIDOS. Oficina de Responsabilidad Gubernamental. Protección de datos: medidas adoptadas por Equifax y las agencias federales en respuesta a la filtración de datos de 2017. Washington, DC: GAO, 2018. (GAO-18-559).

ESTADOS UNIDOS. Departamento de Salud y Servicios Humanos. Norma de seguridad de HIPAA para fortalecer la ciberseguridad de la información sanitaria electrónica protegida: propuesta de norma. Registro Federal, Washington, D.C., vol. 90, n.º 3, págs. 898-1022, 6 de enero de 2025.

VERIZON. Informe de investigaciones de filtraciones de datos de 2025. Basking Ridge: Verizon Business, 2025.

WALDMAN, Ari Ezra. La falsa promesa de la ley de privacidad. Washington University Law Review, St. Louis, vol. 97, núm. 3, pág. 773, 2020.

WALDMAN, Ari Ezra. Industria sin límites: la historia interna de la privacidad, los datos y el poder corporativo. Cambridge: Cambridge University Press, 2021.

WITTY, Andrew. Testimonio ante el Comité de Finanzas del Senado de los Estados Unidos: pirateo del sistema de salud estadounidense, evaluación del ciberataque Changing Healthcare y qué sigue. Washington,

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

RCMOS - Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 06/11/2026 | Aceptado: 11/11/2026 | Publicación: 16/11/2026

DC: Senado de los Estados Unidos, 1 de mayo de 2024.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.