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

Año VII, vol. 2, 2026 | Envío: 14/08/2026 | Aceptación: 10/09/2026 | Publicación: 24/10/2026

La gobernanza de la ciberseguridad como responsabilidad de la alta dirección en las pequeñas y medianas empresas.

La gobernanza de la ciberseguridad como responsabilidad de la alta dirección en las pequeñas y medianas empresas.

Gobernanza de la ciberseguridad como responsabilidad de la alta dirección en pequeñas y medianas empresas.

Eduardo Henrique Bergel Cosenza Junior

Licenciado en Derecho. Máster en Administración de Empresas (MBA) con especialización en Derecho Sanitario y Cumplimiento Normativo Hospitalario. Formación técnica en transacciones inmobiliarias. Abogado colegiado en la Orden de Abogados de Brasil (OAB).

RESUMEN

Este artículo examina los fundamentos teóricos y normativos que sustentan la atribución de la ciberseguridad a la alta dirección, con especial énfasis en las pequeñas y medianas empresas. Parte de la observación de que la creciente dependencia de los proveedores de datos, sistemas y tecnología ha transformado el riesgo cibernético en riesgo empresarial, con repercusiones en la continuidad operativa, la reputación y los resultados financieros. La investigación adopta un enfoque cualitativo, exploratorio y descriptivo, mediante una revisión narrativa de la literatura con elementos de revisión integradora y análisis documental de normas técnicas, marcos de referencia y legislación. El marco articula la literatura sobre gobernanza de la seguridad de la información, teoría de la agencia, teoría de los altos mandos, economía de la seguridad de la información, estudios sobre el comportamiento de cumplimiento, teoría de los accidentes organizacionales y teoría de la organización de alta fiabilidad, en diálogo con la familia ISO/IEC 27000, el Marco de Ciberseguridad 2.0 del NIST, el Reglamento General de Protección de Datos y la normativa de la Autoridad Nacional de Protección de Datos. Los resultados indican que la ciberseguridad forma parte del deber de diligencia debida de los administradores y que su eficacia depende de las decisiones de gobernanza relativas a la inversión, la cultura, la gestión de terceros y la preparación ante incidentes. Se concluye que las pequeñas y medianas empresas pueden ejercer esta responsabilidad mediante medidas proporcionales a su tamaño, siempre que la cuestión sea abordada directamente por su dirección.

Palabras clave: ciberseguridad; gobierno corporativo; alta dirección; gestión de riesgos; protección de datos.

ABSTRACTO

Este artículo examina los fundamentos teóricos y regulatorios para asignar la ciberseguridad a la alta dirección, con énfasis en las pequeñas y medianas empresas. Parte de la observación de que la creciente dependencia de los proveedores de datos, sistemas y tecnología ha transformado el riesgo cibernético en riesgo empresarial, con repercusiones en la continuidad operativa, la reputación y el desempeño financiero. La investigación adopta un enfoque cualitativo, exploratorio y descriptivo, llevado a cabo mediante una revisión narrativa de la literatura con elementos de revisión integradora y mediante el análisis documental de normas técnicas, marcos de referencia y legislación. El marco teórico combina la literatura sobre gobernanza de la seguridad de la información, teoría de la agencia, teoría de los altos niveles, economía de la seguridad de la información, estudios sobre el comportamiento de cumplimiento, la teoría de los accidentes organizacionales y la teoría de las organizaciones de alta fiabilidad, en diálogo con la familia ISO/IEC 27000, el Marco de Ciberseguridad 2.0 del NIST, la Ley General de Protección de Datos de Brasil y la normativa de la Autoridad Nacional de Protección de Datos de Brasil. Los resultados indican que la ciberseguridad forma parte del deber de diligencia de los directivos y que su eficacia depende de las decisiones de gobernanza relativas a la inversión, la cultura, la gestión de terceros y la preparación ante incidentes. El estudio concluye que las pequeñas y medianas empresas pueden cumplir con esta responsabilidad mediante medidas proporcionales a su tamaño, siempre que sus líderes asuman la responsabilidad direc
Palabras clave: ciberseguridad; gobierno corporativo; alta dirección; gestión de riesgos; fecha

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: 14/08/2026 | Aceptación: 10/09/2026 | Publicación: 24/10/2026

protección.

1. INTRODUCCIÓN

Durante gran parte de las últimas décadas, la seguridad de la información ha sido tratada en las organizaciones como
La responsabilidad del sector tecnológico, delegada a los técnicos y medida por la adquisición de equipos y
programas de protección. Esta comprensión se ha vuelto insuficiente a medida que los datos, los sistemas y
Los servicios digitales se han convertido en la base de prácticamente todas las actividades empresariales, desde la generación de ingresos...
a la relación con los clientes. Von Solms y Van Niekerk (2013) observaron que la ciberseguridad
Va más allá de la protección de la información en sentido estricto, ya que implica la protección de personas, bienes y
intereses que pueden ser atacados a través del ciberespacio. Cuando un ataque interrumpe el
Si una operación expone datos de clientes o compromete la reputación de una empresa, el problema deja de existir.
Pasa de ser algo técnico a ser estratégico, impactando directamente en el ámbito de la toma de decisiones de quienes gestionan...
negocio.
El cambio es visible en los marcos normativos más recientes. Versión 2.0 de Ciberseguridad
El marco, publicado por el Instituto Nacional de Estándares y Tecnología en 2024, añadió a
funciones tradicionales de identificar, proteger, detectar, responder y recuperar una nueva función
Denominado gobierno, se centra en establecer la estrategia, las responsabilidades y...
Supervisión del riesgo cibernético por parte del liderazgo (INSTITUTO NACIONAL DE NORMAS Y
TECNOLOGÍA, 2024). En la Unión Europea, la Directiva (UE) 2022/2555 ahora exige que
Los órganos rectores de entidades esenciales e importantes aprueban las medidas de gestión de riesgos de ciberseguridad,
supervisan su implementación y asisten a capacitaciones específicas (SINDICATO).
EUROPEO, 2022). En Brasil, la Ley General de Protección de Datos impuso a los agentes de datos...
gestionar las tareas de seguridad, informar sobre incidentes y la gobernanza, con sanciones que
Pueden representar una parte significativa de los ingresos (BRASIL, 2018).
Las pequeñas y medianas empresas ocupan una posición particular en este escenario. Tienen menos recursos y
Tienen estructuras técnicas más sencillas, pero manejan datos personales y dependen de proveedores de...
La tecnología y están sujetas a las mismas amenazas que afectan a las grandes organizaciones. El objetivo de esta
Este artículo examina, a la luz de la literatura sobre gestión, gobernanza y cumplimiento, el...
Fundamentos teóricos que respaldan la asignación de responsabilidad en ciberseguridad a la alta dirección, con
Se debe prestar especial atención a las empresas más pequeñas. El objetivo es comprender por qué el riesgo cibernético debería...
ser tratado como un riesgo empresarial y qué mecanismos de gobernanza, diligencia debida de terceros y
Los procedimientos de respuesta a incidentes permiten al gerente ejercer esta responsabilidad. Siguiendo la metodología,
Seis secciones desarrollan el tema, seguidas de consideraciones finales.

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: 14/08/2026 | Aceptación: 10/09/2026 | Publicación: 24/10/2026

2. METODOLOGÍA

La investigación tiene un enfoque cualitativo y un carácter teórico-conceptual, con un carácter exploratorio y... descriptivo. Según Gil (2017), la investigación exploratoria permite una mayor familiaridad con un problema y formular proposiciones sobre él, mientras que la investigación descriptiva se ocupa de Caracterización de los fenómenos y las relaciones entre ellos. El fenómeno que se examina aquí es el desplazamiento. Desde la ciberseguridad en el ámbito técnico hasta el ámbito del gobierno corporativo y las relaciones Los análisis abarcan este cambio, las teorías organizativas que lo explican y los instrumentos utilizados. regulaciones que le dan sustancia.

El procedimiento central consistió en una revisión narrativa de la literatura, con elementos de una revisión integradora. Snyder (2019) indica que estas modalidades son apropiadas cuando la intención es monitorear la desarrollar un campo de investigación, articular contribuciones de diferentes disciplinas y proponer Síntesis conceptuales, sin la intención de agregar estadísticamente resultados empíricos. Torraco (2005) agrega que la revisión integradora permite recopilar y criticar literatura representativa sobre un tema. el tema con el fin de generar nuevas perspectivas, una característica pertinente a un objeto situado en la intersección entre sistemas de información, administración, economía y derecho.

La selección del corpus se basó en obras ampliamente reconocidas sobre gobernanza de la seguridad. información, como la de Von Solms y Von Solms (2004) y Posthumus y Von Solms (2004), sobre economía de la seguridad, como las de Anderson (2001) y Gordon y Loeb (2002), y sobre comportamiento de conformidad, como los de Bulgurcu, Cavusoglu y Benbasat (2010) y Siponen y Vance (2010). Con base en estos trabajos, se realizó una búsqueda de estudios publicados relacionados. en revistas revisadas por pares como MIS Quarterly, Information Systems Research, Computers & Seguridad y Revista de Sistemas de Información. Los criterios de inclusión fueron relevancia directa para El tema, su reconocida relevancia en la literatura y la posibilidad de verificar completamente la fuente.

Además, se realizó un análisis documental de las normas técnicas y los marcos de referencia. y legislación. Se examinaron ABNT NBR ISO/IEC 27001:2022 y ABNT NBR ISO/IEC. 27002:2022, ISO/IEC 27014:2020, ABNT NBR ISO 31000:2018, NIST Ciberseguridad Marco 2.0 y las publicaciones NIST SP 800-161 Rev. 1 y NIST SP 800-61 Rev. 3, además de la Ley No. Resolución 13.709/2018 de la Autoridad Nacional de Protección de Datos sobre pequeños agentes de datos. En cuanto a la notificación y comunicación de incidentes, la Ley N° 6.404/1976, el Código Civil y el Decreto N° 11.856/2023 y Directiva (UE) 2022/2555. Para ilustrar la dimensión económica del problema, Se utilizaron datos publicados en los informes anuales de IBM sobre el coste de una filtración de datos y en el propio informe Data Breach. Informe de investigación de Verizon.

El material se organizó mediante categorización temática en seis ejes, correspondientes a las secciones de

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: 14/08/2026 | Aceptación: 10/09/2026 | Publicación: 24/10/2026

desarrollo del artículo. Se reconoce como limitación su naturaleza exclusivamente teórica y
evidencia documental de la investigación, así como el hecho de que los informes sectoriales utilizados se basan en
Nuestras propias muestras, que no necesariamente son representativas de las pequeñas empresas brasileñas.
Por esta razón, los datos cuantitativos se utilizan únicamente para ilustrar la magnitud de
El fenómeno, y las proposiciones formuladas, deben verificarse en futuras investigaciones empíricas.

3. De la seguridad de la información a la cibergobernanza

La literatura sobre seguridad de la información ha seguido un camino que va desde las preocupaciones técnicas hasta...
preocupación organizacional. Dhillon y Backhouse (2001), al revisar las tendencias de investigación
entonces existentes, argumentaron que el enfoque predominante, centrado en los controles técnicos y en
Los modelos de acceso formales fueron insuficientes para abordar los problemas que se originaron en
Estructuras sociales, normas y responsabilidades dentro de las organizaciones. Los autores argumentan
una perspectiva socioorganizacional, en la que la seguridad se entiende como resultado de
interacción entre personas, procesos y tecnología, y no solo como una propiedad de los sistemas.
computacional. Este cambio de enfoque abrió espacio para la gestión y, posteriormente, para la
La gobernanza pasaría entonces a ocupar un lugar central en el debate.
Von Solms y Von Solms (2004) contribuyeron a esta transición al identificar diez errores recurrentes.
en la gestión de la seguridad de la información, entre las cuales se encuentra la percepción de que la seguridad es un problema.
exclusivamente técnico, la ausencia de participación de la alta dirección, la falta de políticas formales
y la falta de mecanismos de monitoreo y cumplimiento. Los autores propusieron que
Estos elementos fueron utilizados por la gerencia como una lista de verificación para evaluar la exhaustividad de
un plan de gobernanza de seguridad. Posthumus y Von Solms (2004), en el mismo año, presentaron
un modelo de gobernanza de la seguridad de la información que sitúa el tema dentro del marco de la gobernanza.
corporativo, bajo la responsabilidad del consejo y la alta dirección, y que incorpora consideraciones
Los requisitos técnicos satisfacen las exigencias comerciales, legales y reglamentarias.
Schneier (2000) resumió el espíritu de esta evolución al afirmar que la seguridad es un proceso, no...
un producto. La adquisición de herramientas tecnológicas, por muy sofisticadas que sean, no sustituye a un producto.
Definir objetivos, asignar responsabilidades, realizar un seguimiento continuo y revisar.
controles periódicos. Soomro, Shah y Ahmed (2016), en una revisión de la literatura sobre el papel de
En el campo de la gestión de la seguridad de la información, concluyeron que la literatura convergía en la necesidad de una
un enfoque holístico, en el que las actividades de gestión, como el desarrollo de políticas, la asignación
En lo que respecta a recursos, concienciación y alineación con la estrategia, reciben la misma atención que...
Los aspectos técnicos ahora se consideran responsabilidad de los gerentes.

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: 14/08/2026 | Aceptación: 10/09/2026 | Publicación: 24/10/2026

Los marcos normativos han seguido esta tendencia. La norma ISO/IEC 27014:2020 aborda esta cuestión.
específicamente en lo que respecta a la gobernanza de la seguridad de la información y la estructuración de las acciones de la agencia.
gobernanza en los procesos de evaluación, dirección, seguimiento y comunicación, distinguiéndolos de
actividades de gestión (ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN;
COMISIÓN ELECTROTÉCNICA INTERNACIONAL, 2020). ABNT NBR ISO/IEC
El Reglamento (CE) 27001:2022, que establece los requisitos para un sistema de gestión de la seguridad de la información, exige
que la alta dirección demuestre liderazgo y compromiso, asegurando que la política y los objetivos
Las medidas de seguridad deben ser compatibles con la dirección estratégica de la organización y deben estar disponibles
los recursos necesarios (Asociación Brasileña de Normas Técnicas, 2022a).
La inclusión de la función de gobernanza en el Marco de Ciberseguridad 2.0 del NIST representa el avance más significativo.
desarrollos recientes en esta trayectoria. El rol abarca el contexto organizacional, la estrategia de gestión de riesgos,
las funciones, responsabilidades y autoridades, la política, la supervisión y la gestión de riesgos de la cadena de suministro.
suministros cibernéticos, y se presenta como un elemento que informa cómo la organización
desempeña otras funciones (INSTITUTO NACIONAL DE NORMAS Y TECNOLOGÍA,
(2024). En Brasil, el Decreto No. 11.856/2023 estableció la Política Nacional de Ciberseguridad y la
Comité Nacional de Ciberseguridad, señalando la incorporación del tema a la agenda pública (BRASIL,
2023). Este conjunto de referencias indica que la ciberseguridad ha llegado a ser comprendida
como una dimensión del gobierno corporativo, cuya dirección recae en aquellos responsables del destino de la empresa.
organización.

4. La responsabilidad de los directores según las teorías de agencia
Y DESDE LOS RANGOS MÁS ALTOS

La teoría de la agencia ofrece una primera base para comprender por qué la seguridad
La cibernética no puede delegarse por completo. Jensen y Meckling (1976) definieron la relación de
Una agencia se define como aquella en la que el principal delega al agente la realización de actividades en su nombre, y
Demostraron que la divergencia de intereses y la asimetría de información entre ellos generan costes.
monitoreo, garantía y pérdida residual. Cuando el propietario o administrador delega la
Para garantizar la seguridad de un equipo interno o de un proveedor externo, este es precisamente el tipo de...
El agente posee información técnica que el principal no tiene, y sus incentivos no son iguales.
Siempre coinciden con los de la organización, ya que el coste de un fallo recae principalmente sobre la empresa.
y sus sujetos de datos.

Eisenhardt (1989) argumentó que la eficiencia de los contratos de agencia depende, entre otros factores,
la existencia de sistemas de información capaces de hacer observable el comportamiento del agente.

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: 14/08/2026 | Aceptado: 10/09/2026 | Publicación: 24/10/2026

En el ámbito de la ciberseguridad, estos sistemas corresponden a indicadores de madurez.
Informes periódicos, auditorías y pruebas de respuesta a incidentes. Sin ellos, el gerente no tiene forma de...
evaluar si la seguridad delegada se está ejerciendo de manera efectiva y la ausencia de incidentes aparentes.
Esto puede confundirse con una protección adecuada. Por lo tanto, la literatura de la agencia sugiere que la
La participación de la alta dirección no sustituye la competencia técnica, pero es un requisito previo para...
La delegación debe controlarse para que los costes de agencia se mantengan en un nivel aceptable.
La teoría de los altos cargos, formulada por Hambrick y Mason (1984), añade un segundo
Esta perspectiva sostiene que los resultados organizacionales reflejan, en parte, las características de la organización.
Las experiencias y valores de los miembros de la alta dirección. Estudios empíricos han aplicado esta teoría.
a la ciberseguridad. Kwon et al. (2013) examinaron la asociación entre la participación de
Los ejecutivos de tecnología en puestos de alta dirección, su estructura de remuneración y la ocurrencia de infracciones.
seguridad de la información. Haislip, Lim y Pinsker (2021), basándose en las violaciones reportadas entre
En 2005 y 2017, se descubrió que los directores ejecutivos con conocimientos en tecnología de la información...
y la presencia del director ejecutivo de tecnología en el equipo directivo superior se asociaron con menores
La ocurrencia de infracciones llevó a la conclusión de que el riesgo es una responsabilidad compartida de la dirección.
El derecho brasileño ofrece un tercer fundamento, de carácter normativo. Ley No.
La Ley 6.404/1976, en su artículo 153, determina que el administrador de la empresa debe emplear, en el ejercicio de
sus deberes, el cuidado y la diligencia que todo hombre activo y honesto suele emplear en
Gestionan sus propios asuntos, y el artículo 158 trata sobre su responsabilidad por daños y perjuicios.
causado cuando se actúa con negligencia o intención o en violación de la ley o estatuto (BRASIL, 1976).
El artículo 1011 del Código Civil reitera el deber de cuidado y diligencia de los administradores de
sociedades en general (BRASIL, 2002). En un entorno donde la dependencia de sistemas y datos es
Dada la intensidad de las amenazas, que son ampliamente conocidas, ignorar los riesgos cibernéticos difícilmente es una opción.
Es compatible con este patrón de conducta.
La LGPD refuerza esta interpretación al exigir que los agentes de procesamiento de datos adopten medidas de seguridad,
medidas técnicas y administrativas capaces de proteger los datos personales del acceso no autorizado y
situaciones accidentales o ilícitas, según se definen en el artículo 46, y al prever, en el artículo 50, la posibilidad de
formulación de reglas de buenas prácticas y gobernanza (BRASIL, 2018). Entre las sanciones
Entre las sanciones administrativas estipuladas en el artículo 52, se encuentra una multa simple de hasta el dos por ciento de los ingresos de la empresa.
entidad jurídica en Brasil en el último año fiscal, limitada a cincuenta millones de reales por infracción, cuya
La aplicación se regió por el reglamento dosimétrico de la Autoridad Nacional de Protección de Datos (AUTORIDADE NACIONAL
DE PROTEÇÃO DE DADOS, 2023). La combinación entre
El deber de diligencia, los requisitos reglamentarios y la evidencia empírica respaldan la conclusión de que el
La ciberseguridad es fundamental entre las responsabilidades de un gerente.

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: 14/08/2026 | Aceptación: 10/09/2026 | Publicación: 24/10/2026

5. La economía de la seguridad y la medición del riesgo cibernético

La economía de la seguridad de la información se ha consolidado como un campo de investigación desde...
el hallazgo de que muchos fallos de seguridad provienen de incentivos desalineados y no de
deficiencias tecnológicas. Anderson (2001) argumentó que los sistemas frecuentemente fallan porque
Quienes podrían protegerlos no son quienes sufren las consecuencias de su fracaso.
Este fenómeno acerca la seguridad a los problemas clásicos de las externalidades y el riesgo moral.
Anderson y Moore (2006), en un artículo publicado en la revista Science, ampliaron este análisis y
Demostraron que conceptos como externalidades de red, asimetría de información y selección adversa...
Explican una parte significativa de las dificultades a las que se enfrentan las organizaciones y los mercados para proteger...
sus sistemas.

Gordon y Loeb (2002) propusieron un modelo económico para definir el nivel óptimo de
Inversión en seguridad de la información. Partiendo de la relación entre vulnerabilidad de la información,
En cuanto a la probabilidad de que se produzcan infracciones y la pérdida potencial, los autores demostraron que, para
Para ciertas clases de funciones de probabilidad, la inversión óptima no supera aproximadamente el 37%.
por ciento, o uno sobre el número de Euler, de la pérdida esperada. Más que el valor numérico, cuyo
Si bien la generalidad del modelo ha sido discutida en estudios posteriores, su contribución radica en demostrar que
La inversión en seguridad debe decidirse en función del valor de la información que se protege y de...
Se ha logrado reducir el riesgo, lo cual, por definición, es una decisión de gestión.
Medir el riesgo cibernético en términos financieros es un requisito previo para tomar esta decisión.
tomado con fundamento. Freund y Jones (2015) presentaron el modelo de análisis factorial de
Riesgo de la información, que desglosa el riesgo en frecuencia de eventos de pérdida y magnitud de las pérdidas,
permitiendo que se exprese en valores monetarios comparables a los demás riesgos de la organización.
Hubbard y Seiersen (2016) criticaron el uso generalizado de matrices cualitativas, que clasifican
Los riesgos se clasificaron como bajos, medios o altos, y abogaron por métodos cuantitativos que permitan la comparación.
alternativas de inversión. Estas propuestas están en línea con ABNT NBR ISO 31000:2018, que
Se recomienda que el análisis de riesgos considere la probabilidad de los eventos y la magnitud de sus consecuencias
(Asociación Brasileña de Normas Técnicas, 2018).
Los efectos económicos de las infracciones han sido documentados mediante estudios de eventos y encuestas.
sectorial. Cavusoglu, Mishra y Raghunathan (2004) encontraron que las empresas que anunciaban
Las brechas de seguridad provocaron una pérdida promedio del 2,1 por ciento de su valor de mercado durante esos dos días.
tras el anuncio. Los informes anuales de IBM, realizados con el Instituto Ponemon, estiman que
El coste medio global de una filtración de datos y le permite realizar un seguimiento de su evolución, según...

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.

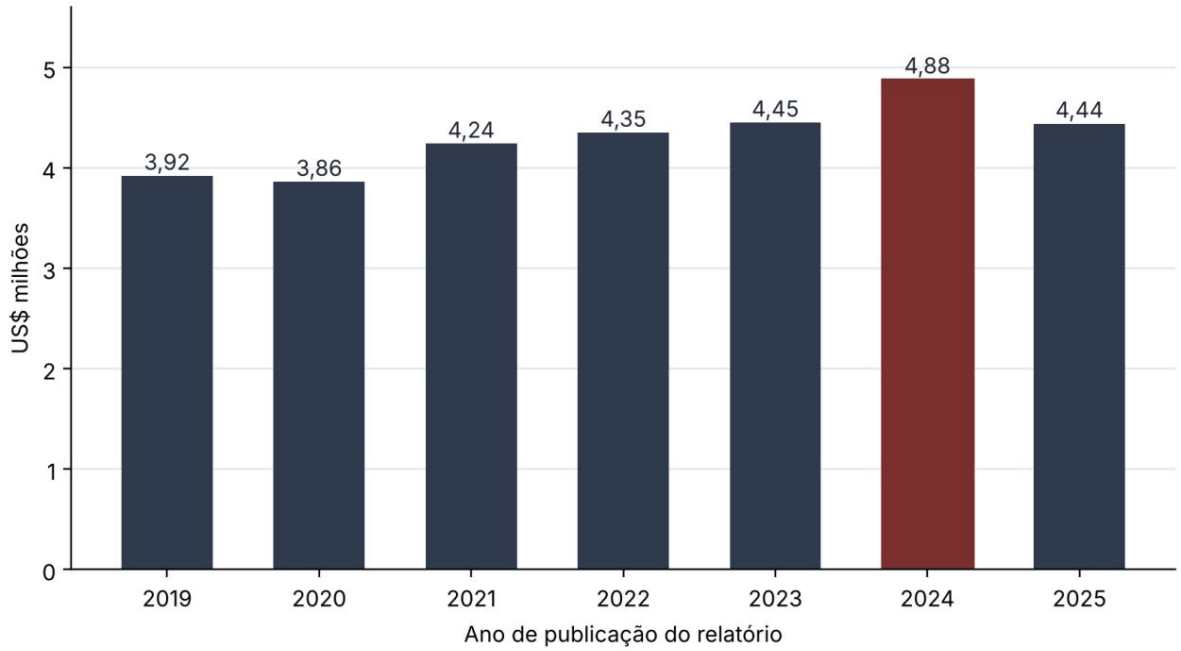
Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 14/08/2026 | Aceptación: 10/09/2026 | Publicación: 24/10/2026

La Figura 1 muestra que el valor promedio aumentó de 3,92 millones de dólares en el informe de 2019 a 4,88 millones de dólares. millones en el informe de 2024, la cifra más alta de la serie, y descendió a 4,44 millones en el informe de 2025. reducción atribuida a la mayor velocidad en la identificación y contención de incidentes (IBM, 2019; 2024; 2025).

Figura 1 – Coste medio global de una filtración de datos por año de publicación del informe.

(Millones de dólares estadounidenses)



Fuente: compilado por el autor con datos de IBM (2019; 2020; 2021; 2022; 2023; 2024; 2025).

En el contexto brasileño, el informe de 2025 estimó el costo promedio de una infracción en 7,19. millones de reales, en comparación con 6,75 millones en el año anterior (IBM, 2025). Estos valores se derivan de muestras. específico para la investigación, compuesto por organizaciones de diferentes tamaños y sectores, y no debería ser Estas cifras se transmiten directamente a las pequeñas empresas, pero dan una idea de la magnitud de las pérdidas. El proceso abarca la detección, la contención, la notificación, la mitigación de pérdidas comerciales y la respuesta posterior. incidente. La reducción observada en 2025, asociada por la propia investigación con la mejora de la capacidad La detección y contención sugieren que las decisiones de gestión relativas a la preparación y la respuesta afectan... Esto repercute directamente en el coste final de los incidentes, lo que refuerza el argumento de que hay que abordar este problema. como una cuestión económica y estratégica, y no solo operativa.

6. El factor humano y la cultura de la conformidad

La dimensión humana ocupa una posición central en la ciberseguridad. Investigaciones de violaciones de 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
RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 14/08/2026 | Aceptado: 10/09/2026 | Publicación: 24/10/2026

Informe de 2024, elaborado por Verizon a partir del análisis de miles de incidentes e infracciones.
Los casos confirmados indicaron que el 68 por ciento de las infracciones involucraron un elemento humano no malicioso.
tales como errores o manipulación a través de ingeniería social, y que el 32 por ciento implicó alguna técnica.
extorsión, incluido el ransomware (VERIZON, 2024). Estos datos refuerzan la percepción de que
Los controles tecnológicos, si bien son indispensables, resultan insuficientes cuando las personas que los operan...
Los sistemas desconocen los riesgos o no se sienten responsables de prevenirlos. Según el gerente, estos datos...
Esto indica que invertir en personas y procesos es tan importante como invertir en...
tecnología, y que la exposición de la empresa depende directamente de las condiciones de trabajo y
información proporcionada a sus empleados.

La investigación en sistemas de información ha dedicado una amplia atención a los factores que explican la
Cumplimiento de las políticas de seguridad por parte de los empleados. Bulgurcu, Cavusoglu y Benbasat (2010)
Demostraron que la intención de cumplir con estas políticas está influenciada por la actitud del empleado.
por creencias normativas y autoeficacia, y esa actitud, a su vez, está moldeada por creencias sobre
los beneficios y costos del cumplimiento y el incumplimiento, sobre los cuales la conciencia en
La seguridad de la información ejerce una influencia significativa. Herath y Rao (2009) encontraron que las presiones
factores sociales, la certeza de la detección y la percepción de que el propio comportamiento contribuye a la
La seguridad se asocia con intenciones más favorables al cumplimiento de las políticas, mientras que
La severidad de los castigos fue contraria a lo que cabría esperar desde un punto de vista puramente ético.
Los elementos disuasorios tienen un efecto negativo sobre estas intenciones.

El enfoque basado en la disuasión ha recibido especial atención. D'Arcy, Hovav y Galletta (2009)
Descubrieron que los usuarios estaban al tanto de la existencia de políticas de seguridad,
Los programas de conocimiento y monitoreo informático están asociados con la percepción de
La severidad de las sanciones y, a través de ellas, la reducción de la intención de hacer mal uso de los sistemas. Siponen
Vance (2010), a su vez, demostró que los empleados recurren a técnicas de neutralización, como
la negación del daño o la invocación de lealtades superiores para justificar violaciones de políticas, y
que estas racionalizaciones pueden reducir el efecto de las sanciones. La combinación de estos resultados indica
Las normas y los castigos tienen un efecto limitado si no van acompañados de una explicación clara.
En cuanto a los motivos de los controles.

La teoría de Reason (1997) sobre los accidentes organizacionales ofrece un marco útil para interpretar
Estos hallazgos. El autor distinguió entre fallas activas, cometidas por quienes están en primera línea, y...
condiciones latentes, creadas por decisiones de diseño, gestión y asignación de recursos, que
Permanecen inactivos en el sistema hasta que se combinan con fallas activas para producir una
accidente. Aplicada a la ciberseguridad, esta distinción sugiere que el clic de un empleado en
Un mensaje fraudulento suele ser simplemente la vulnerabilidad que revela problemas latentes.

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: 14/08/2026 | Aceptación: 10/09/2026 | Publicación: 24/10/2026

Problemas anteriores, como falta de capacitación, permisos excesivos, falta de autenticación multifactor o
Falta de procedimientos para verificar las solicitudes de pago inusuales.
Para la alta dirección, la principal implicación es que la cultura de seguridad es producto de decisiones.
gerencial. ABNT NBR ISO/IEC 27002:2022 incluye, entre los controles relacionados con las personas, el
concienciación, educación y formación en seguridad de la información, términos y condiciones de empleo y el proceso
disciplinario (Asociación Brasileña de Normas Técnicas,
2022b). La Directiva (UE) 2022/2555 va más allá y exige que los miembros de los propios órganos
Los directivos reciben formación, y se debería ofrecer formación similar periódicamente a los empleados (UNIÓN
EUROPEA, 2022). El ejemplo de liderazgo y coherencia
entre el discurso y la asignación de recursos, y la voluntad de escuchar y corregir errores sin buscar a quién culpar.
Los individuos son elementos que la literatura asocia con la formación de una cultura de conformidad eficaz.

7. TERCEROS, CADENA DE SUMINISTRO Y DILIGENCIA DEBIDA EN CIBERSEGURIDAD

La dependencia de los proveedores de tecnología se ha convertido en una característica estructural de las empresas.
empresas contemporáneas, especialmente las más pequeñas, que dependen de servicios y sistemas en la nube
Gestión contratada como servicio, proveedores de pago y proveedores de soporte técnico. Cada uno
Una de estas relaciones amplía la superficie de ataque de la organización. Investigaciones de violación de datos
El informe de 2024 registró que el 15 por ciento de las infracciones analizadas involucraron a un tercero, como
custodios de datos o proveedores de software, lo que representó un aumento del 68 por ciento en
en relación con el período anterior (VERIZON, 2024). La seguridad de la empresa se vuelve dependiente, en mayor medida, de la seguridad de la empresa.
una parte considerable de las prácticas de aquellos que ella contrata, lo que transforma la selección y el seguimiento de
Los proveedores participan en la toma de decisiones sobre la gestión de riesgos.

La economía de los costos de transacción ayuda a comprender por qué esta dependencia requiere gobernanza.
específicamente. Williamson (1985) demostró que las transacciones caracterizadas por activos específicos,
La incertidumbre y la limitada racionalidad de las partes exigen estructuras de gobernanza más elaboradas.
Eso no es simplemente un intercambio de mercado. Los contratos de tecnología exhiben estas características con
intensidad, ya que implica datos de la empresa almacenados en sistemas de terceros e integraciones.
información técnica difícil de reemplazar y que el cliente rara vez llega a evaluar.
En este contexto, la asimetría de la información favorece la selección de proveedores con mejores prácticas.
deficiente, ya que la calidad de la seguridad ofrecida no es directamente observable en el momento de
contratación.
La debida diligencia cibernética de los proveedores es la respuesta organizativa a este problema. (ABNT)
La norma NBR ISO/IEC 27002:2022 dedica un conjunto de controles a las relaciones con los proveedores, que

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: 14/08/2026 | Aceptación: 10/09/2026 | Publicación: 24/10/2026

Engloba la seguridad de la información en estas relaciones, el manejo de la seguridad en los acuerdos con proveedores, gestión de seguridad en la cadena de suministro de tecnología de la información y comunicación, monitoreo y gestión de cambios en los servicios prestados, y seguridad en el uso de servicios en la nube (Asociación Brasileña de Normas Técnicas, 2022b). A

La publicación SP 800-161 Rev. 1 del NIST detalla las prácticas de gestión de riesgos en la cadena de suministro. ciberseguridad y recomienda que la profundidad de las evaluaciones sea proporcional a la criticidad de la proveedor y el servicio prestado (BOYENS et al., 2022).

La LGPD (Ley General de Protección de Datos de Brasil) otorga a esta debida diligencia una dimensión legal directa. El artículo 39 estipula que el operador...

Realice el tratamiento siguiendo las instrucciones proporcionadas por el responsable del tratamiento, quien verificará el cumplimiento. de las propias instrucciones y las reglas sobre la materia, y el artículo 42 establece hipótesis de responsabilidad conjunta entre controladores y operadores por daños causados por procesamiento de datos personales (BRASIL, 2018). En la práctica, la empresa que contrata un sistema de La administración, un servicio de almacenamiento o un proveedor de servicio al cliente sigue siendo responsable de datos de sus clientes, lo que hace esencial conocer las prácticas del proveedor y establecer, El contrato debe incluir obligaciones claras en materia de seguridad, confidencialidad, notificación de incidentes y auditoría. y la devolución o eliminación de los datos al finalizar la relación.

Para las pequeñas y medianas empresas, la aplicación de estos parámetros requiere proporcionalidad. No es Si bien es factible someter a todos los proveedores a evaluaciones exhaustivas, es posible clasificarlos según... su acceso a datos personales y sistemas críticos, y centrar la debida diligencia en los casos más críticos. Riesgo. Cuestionarios estandarizados, verificación de certificaciones reconocidas, cláusulas contractuales de seguridad, previsión de plazos para la notificación de incidentes y reevaluaciones periódicas comprenden un conjunto accesible de medidas. El Marco de Ciberseguridad 2.0 del NIST, al incorporar la gestión de Los riesgos de la cadena de suministro en la función de gobernanza indican que la elección y supervisión de los socios Las decisiones tecnológicas corresponden a la dirección, no solo a los departamentos de compras o tecnología. (INSTITUTO NACIONAL DE NORMAS Y TECNOLOGÍA, 2024).

8. Respuesta ante incidentes, resiliencia organizacional y deberes. REGULADOR

La literatura y las referencias técnicas se basan en la premisa de que ninguna organización es inmune a incidentes, lo que desvía parte de la atención de la prevención a la capacidad de respuesta. La publicación NIST SP 800-61 Rev. 3, 2025, reorganizó las recomendaciones de respuesta a incidentes a la luz de El Marco de Ciberseguridad 2.0 comenzó a considerarse una parte integral de la gestión de riesgos. Ciberseguridad, que vincula las actividades de preparación, detección, respuesta y recuperación con las funciones.

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

Año VII, vol. 2, 2026 | Envío: 14/08/2026 | Aceptación: 10/09/2026 | Publicación: 24/10/2026

Desde este marco, incluyendo la función de gobernar, y no como una actividad aislada del área técnica.
(NELSON et al., 2025). Esta integración implica que las decisiones sobre roles, comunicación, recursos y
Las prioridades de recuperación deben establecerse antes del incidente y con la participación del liderazgo,
será responsable de las consecuencias operativas, financieras y de reputación del evento.
La teoría de las organizaciones de alta fiabilidad proporciona una base para esta preparación. Weick y
Sutcliffe (2007) identificó cinco principios presentes en las organizaciones que operan en entornos
alto riesgo con baja incidencia de fallos graves, preocupación por los fallos, reticencia a
simplificación de las interpretaciones, sensibilidad a las operaciones, compromiso con la resiliencia y...
deferencia a la competencia técnica. Los autores argumentaron que estas organizaciones tratan a las pequeñas
Las desviaciones, vistas como señales de problemas mayores, deben evitarse mediante explicaciones simplistas, y deben hacerse esfuerzos para contenerlas.
y recuperarse de eventos inesperados. Trasladados a la ciberseguridad, estos principios
Sugieren registrar y analizar los incidentes que estuvieron a punto de ocurrir, realizar ejercicios de simulación y definir...
conocimiento previo de quién tiene la autoridad para decidir en una situación de crisis.
Las obligaciones regulatorias otorgan urgencia a esta preparación. El artículo 48 de la LGPD (Ley General de Protección de Datos de Brasil) estipula que...
El responsable del tratamiento deberá notificar a la Autoridad Nacional de Protección de Datos y al interesado la ocurrencia de
Un incidente de seguridad que puede causar un riesgo o daño significativo (BRASIL, 2018). Resolución
La Resolución No. 15/2024 de la Autoridad Nacional de Protección de Datos (ANPD) de Brasil reguló este deber y estableció que la comunicación debe realizarse en
hasta tres días hábiles, contados desde el momento en que el responsable del tratamiento tiene conocimiento de que el incidente ha afectado a los datos.
personal, además de definir criterios para caracterizar el riesgo o daño pertinente, como la participación.
datos sensibles, datos de niños, adolescentes o ancianos, datos financieros, datos de
autenticación o datos a gran escala (AUTORIDAD NACIONAL PARA LA PROTECCIÓN DE
(DATOS, 2024). Cumplir con este plazo es prácticamente imposible sin procedimientos.
previamente definido.
Sin embargo, la normativa brasileña reconoce las particularidades de las empresas más pequeñas.
La Resolución CD/ANPD No. 2/2022 estableció un tratamiento diferenciado y simplificado para los agentes de
Tratamiento a pequeña escala, con flexibilidad en algunas obligaciones y plazos (AUTORIDAD)
LEY NACIONAL DE PROTECCIÓN DE DATOS, 2022), y la Resolución CD/ANPD No. 15/2024 determinaron
que se dupliquen los plazos de notificación de incidentes para estos agentes (AUTORIDAD NACIONAL DE PROTECCIÓN DE
DATOS, 2024). La propia autoridad publicó
Documento de orientación sobre seguridad de la información dirigido a estos agentes, con recomendaciones sobre medidas a adoptar.
aspectos administrativos y técnicos, como la adopción de políticas de seguridad de la información y campañas de sensibilización.
y formación de empleados, gestión de contratos, control de acceso, protección de datos almacenados y gestión de vulnerabilidades
(AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS)
(DATOS, 2021). Sin embargo, esta flexibilidad no elimina el deber de seguridad, solo adapta su

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: 14/08/2026 | Aceptación: 10/09/2026 | Publicación: 24/10/2026

Un método de cumplimiento que se corresponda con el tamaño de la organización.

En este contexto, la resiliencia es tanto una capacidad técnica como un atributo de gobernanza.
La norma ABNT NBR ISO 31000:2018 establece que la gestión de riesgos debe integrarse en todos los...
Actividades organizativas y que la alta dirección es responsable de garantizar esta integración (Asociación Brasileña de Normas
Técnicas, 2018). Recuperación tras un incidente
Depende de las decisiones previas relativas a las copias de seguridad, los contratos con los proveedores y la comunicación.
con clientes y asignación de recursos, todo ello situado dentro del ámbito de la gestión de la empresa. Los datos de
IBM (2025) asoció la reducción del coste medio de las filtraciones con una identificación y contención más precisas.
Las respuestas rápidas confirman que prepararse para responder es una inversión que da sus frutos.
Es cuantificable y refuerza la responsabilidad del liderazgo en su existencia.

CONSIDERACIONES FINALES

Este artículo examinó los fundamentos teóricos y normativos que sustentan la atribución de seguridad.
Ciberseguridad para la alta dirección, con especial atención a las pequeñas y medianas empresas. La revisión demostró
que el tema ha seguido una trayectoria en la literatura y las referencias técnicas que parte del control
Los aspectos técnicos, que abarcan la gestión y llegan hasta la gobernanza, reflejan la creciente dependencia de las organizaciones.
con respecto a los datos y sistemas digitales y el consiguiente aumento del riesgo cibernético al estado de
Riesgo estratégico, con repercusiones en la continuidad, la reputación y los resultados financieros de las empresas.
La evolución del campo ha demostrado que la seguridad de la información ya no se entiende como
propiedad de los sistemas y llegó a ser visto como el resultado de la interacción entre personas, procesos y
tecnología. La inclusión de la función de gobierno en el Marco de Ciberseguridad 2.0 del NIST y los requisitos de
El liderazgo de ISO/IEC 27001 consolida la comprensión de que la dirección estratégica de la seguridad
Corresponde a los gerentes, siendo los equipos técnicos los responsables de implementar los controles definidos a partir de esto.
dirección.
La teoría de la agencia explicaba por qué la delegación de la seguridad, sin mecanismos de información y comunicación...
El control genera costos y expone a la organización a riesgos que el gerente no puede prever. La teoría
desde los altos cargos y los estudios empíricos que lo aplicaron indicaron que la composición y la
El conocimiento de la alta dirección está asociado con la ocurrencia de violaciones, lo que refuerza la
La cumbre defiende la responsabilidad compartida y descarta la idea de que el asunto pueda confiarse a una sola persona.
Un único profesional o un proveedor externo sin supervisión.
En términos legales, el deber de diligencia estipulado en la Ley de Sociedades y el Código Civil,
Además de las obligaciones de seguridad y gobernanza de la LGPD (Ley General de Protección de Datos de Brasil), proporciona una base regulatoria para afirmar...
que la inacción ante el riesgo cibernético es incompatible con el estándar de conducta requerido

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: 14/08/2026 | Aceptación: 10/09/2026 | Publicación: 24/10/2026

administradores. Las sanciones previstas en la legislación y los reglamentos de la autoridad nacional.
Dan forma concreta a este deber, acercando la ciberseguridad a otras obligaciones.
Medidas de cumplimiento que ya forman parte de la rutina de cualquier administrador.
La economía de la seguridad ha demostrado que la inversión en protección debe decidirse en función de...
El valor de la información y la reducción de riesgos lograda son decisiones gerenciales. Los datos sobre la
costo de las violaciones, incluso si se derivan de muestras que no representan específicamente el
Las pequeñas empresas brasileñas resaltan la magnitud de las pérdidas y muestran que la capacidad de
La detección y la contención influyen directamente en el resultado financiero, por lo que la preparación es esencial.
La respuesta a los incidentes debe entenderse como una inversión, no como un gasto secundario.
El análisis del factor humano reveló que la mayoría de las violaciones implican errores, manipulación o
Condiciones organizativas que las favorecen. Concienciación, coherencia entre el discurso y la práctica.
y la corrección de las condiciones latentes creadas por las decisiones de gestión aparecen como elementos centrales.
de una cultura de cumplimiento capaz de reducir la exposición de la organización. Esta cultura no surge
espontáneamente, ya que depende de las decisiones de gestión en cuanto a capacitación, comunicación interna y
Asignación de recursos.
La dependencia de los proveedores de tecnología ha ampliado el perímetro de riesgo para las empresas y las ha hecho...
La debida diligencia cibernética es una parte indispensable de la gobernanza. La responsabilidad del controlador por
El tratamiento de datos por parte de terceros, tal como lo estipula la LGPD (Ley General de Protección de Datos de Brasil), requiere una cuidadosa selección y cláusulas contractuales.
supervisión adecuada y proporcional a la criticidad de cada relación. En empresas más pequeñas, en
¿Qué servicios tecnológicos se contratan con mayor frecuencia? Esta debida diligencia representa una parte...
que expresa la propia gestión de la seguridad.
Como contribución, el estudio propone que las pequeñas y medianas empresas aborden la ciberseguridad.
como un riesgo empresarial, bajo la responsabilidad directa de sus gerentes, respaldado por medidas
proporcional al tamaño de la empresa, como por ejemplo definir responsabilidades, clasificar a los proveedores y proporcionar formación.
Planes de respaldo y respuesta ante incidentes. Se recomienda realizar más investigaciones.
Investigar empíricamente el nivel de participación de los ejecutivos en las pequeñas empresas brasileñas.
La portabilidad está relacionada con el tema y sus efectos en la ocurrencia y el costo de los incidentes.

REFERENCIAS

ANDERSON, R. Por qué la seguridad de la información es difícil: una perspectiva económica. En: CONFERENCIA ANUAL DE APLICACIONES DE SEGURIDAD INFORMÁTICA, 17.ª, 2001, Nueva Orleans. Actas.
[...]. Los Alamitos: IEEE Computer Society, 2001. págs. 358-365.

ANDERSON, R.; MOORE, T. La economía de la seguridad de la información. Science, vol. 314, n.º 5799, págs. 610-613, 2006.

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: 14/08/2026 | Aceptación: 10/09/2026 | Publicación: 24/10/2026

Asociación Brasileña de Normas Técnicas. ABNT NBR ISO 31000: Gestión de riesgos: directrices. Río de Janeiro: ABNT, 2018.

Asociación Brasileña de Normas Técnicas. ABNT NBR ISO/IEC 27001: Seguridad de la información, ciberseguridad y protección de la privacidad: Sistemas de gestión de la seguridad de la información: requisitos. Río de Janeiro: ABNT, 2022a.

Asociación Brasileña de Normas Técnicas. ABNT NBR ISO/IEC 27002: Seguridad de la información, ciberseguridad y protección de la privacidad: Controles de seguridad de la información.
Río de Janeiro: ABNT, 2022b.

AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS. Guía de orientación: seguridad de la información para pequeños agentes de procesamiento de datos. Brasilia, DF: ANPD, 2021.

AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS. Resolución CD/ANPD n.º 2, de 27 de enero de 2022. Se aprueba el Reglamento de aplicación de la Ley n.º 13.709, de 14 de agosto de 2018, Ley General de Protección de Datos Personales (LGPD), para los pequeños procesadores de datos. Boletín Oficial de la Unión, Brasilia, DF, 28 de enero de 2022.

AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS. Resolución CD/ANPD N° 4, de 24 de febrero de 2023. Aprueba el Reglamento sobre Dosimetría y Aplicación de Sanciones Administrativas.
Gaceta Oficial de la Unión, Brasilia, DF, 27 de febrero de 2023.

AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS. Resolución CD/ANPD N° 15, de 24 de abril de 2024. Aprueba el Reglamento de Notificación de Incidentes de Seguridad. Boletín Oficial de la Unión, Brasilia, DF, 26 de abril de 2024.

BOYENS, J. et al. Prácticas de gestión de riesgos de la cadena de suministro de ciberseguridad para sistemas y organizaciones. Gaithersburg: Instituto Nacional de Estándares y Tecnología, 2022. (Publicación especial NIST 800-161 Rev. 1).

BRASIL. Ley N° 6.404, del 15 de diciembre de 1976. Por la que se establecen las sociedades anónimas. Gaceta Oficial de la Unión, Brasilia, DF, 17 de diciembre de 1976.

BRASIL. Ley N° 10.406, del 10 de enero de 2002. Por la que se establece el Código Civil. Gaceta Oficial de la Unión, Brasilia, DF, 11 de enero de 2002.

BRASIL. Ley N° 13.709, de 14 de agosto de 2018. Ley General de Protección de Datos Personales (LGPD).
Gaceta Oficial de la Unión, Brasilia, DF, 15 de agosto de 2018.

BRASIL. Decreto N° 11.856, de 26 de diciembre de 2023. Por el cual se establece la Política Nacional de Ciberseguridad y el Comité Nacional de Ciberseguridad. Boletín Oficial de la Unión, Brasilia, DF, 27 de diciembre de 2023.

BULGURCU, B.; CAVUSOGLU, H.; BENBASAT, I. Cumplimiento de la política de seguridad de la información: un estudio empírico de las creencias basadas en la racionalidad y la concienciación sobre la seguridad de la información. MIS Quarterly, vol. 34, n.º 3, págs. 523-548, 2010.

CAVUSOGLU, H.; MISHRA, B.; RAGHUNATHAN, S. El efecto de una violación de seguridad en Internet

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: 14/08/2026 | Aceptación: 10/09/2026 | Publicación: 24/10/2026

Anuncios sobre el valor de mercado: reacciones del mercado de capitales ante las empresas afectadas por brechas de seguridad y los desarrolladores de seguridad en internet. Revista Internacional de Comercio Electrónico, vol. 9, n.º 1, págs. 69-104, 2004.

D'ARCY, J.; HOVAV, A.; GALLETTA, D. Conocimiento del usuario sobre las contramedidas de seguridad y su impacto en el uso indebido de los sistemas de información: un enfoque disuasorio. Information Systems Research, vol. 20, n.º 1, págs. 79-98, 2009.

DHILLON, G.; BACKHOUSE, J. Direcciones actuales en las perspectivas de investigación sobre seguridad de los sistemas de información: hacia un enfoque socioorganizacional. Information Systems Journal, vol. 11, n.º 2, págs. 127-153, 2001.

EISENHARDT, KM Teoría de la agencia: una evaluación y revisión. Academy of Management Review, vol. 14, n.º 1, págs. 57-74, 1989.

FREUND, J.; JONES, J. Medición y gestión del riesgo de la información: un enfoque FAIR. Oxford: Butterworth-Heinemann, 2015.

GIL, AC Cómo preparar proyectos de investigación. 6ª edición. São Paulo: Atlas, 2017.

GORDON, LA; LOEB, MP La economía de la inversión en seguridad de la información. ACM Transactions on Information and System Security, vol. 5, n.º 4, págs. 438-457, 2002.

HAISLIP, J.; LIM, J.-H.; PINSKER, R. El impacto de la experiencia en TI de los ejecutivos en las violaciones de seguridad de datos reportadas. Information Systems Research, vol. 32, n.° 2, págs. 318-334, 2021.

HAMBRICK, D.C.; MASON, PA. Altos mandos: la organización como reflejo de sus directivos de alto nivel. Academy of Management Review, vol. 9, n.º 2, págs. 193-206, 1984.

HERATH, T.; RAO, HR. Fomento de comportamientos de seguridad de la información en las organizaciones: papel de las sanciones, las presiones y la eficacia percibida. Decision Support Systems, vol. 47, n.º 2, págs. 154-165, 2009.

HUBBARD, DW; SEIERSEN, R. Cómo medir cualquier cosa en el riesgo de ciberseguridad. Hoboken: Wiley, 2016.

IBM. Informe sobre el coste de una filtración de datos 2019. Armonk: IBM Security, 2019.

IBM. Informe sobre el coste de una filtración de datos 2020. Armonk: IBM Security, 2020.

IBM. Informe sobre el coste de una filtración de datos 2021. Armonk: IBM Security, 2021.

IBM. Informe sobre el coste de una filtración de datos 2022. Armonk: IBM Security, 2022.

IBM. Informe sobre el coste de una filtración de datos 2023. Armonk: IBM Security, 2023.

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

IBM. Informe sobre el coste de una filtración de datos en 2025: la brecha en la supervisión de la IA. Armonk: IBM Security, 2025.

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN; COMISIÓN ELECTROTÉCNICA INTERNACIONAL. ISO/IEC 27014: seguridad de la información, ciberseguridad y

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: 14/08/2026 | Aceptación: 10/09/2026 | Publicación: 24/10/2026

Protección de la privacidad: gobernanza de la seguridad de la información. Ginebra: ISO, 2020.

JENSEN, MC; MECKLING, WH Teoría de la empresa: comportamiento gerencial, costos de agencia y estructura de propiedad. Journal of Financial Economics, vol. 3, n.° 4, págs. 305-360, 1976.

KWON, J. et al. La relación entre la participación de la alta dirección y la remuneración y las violaciones de seguridad de la información. Journal of Information Systems, vol. 27, n.º 1, págs. 219-236, 2013.

INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA. Marco de Ciberseguridad (CSF) 2.0 del NIST. Gaithersburg: NIST, 2024. (Documento técnico sobre ciberseguridad del NIST, pág. 29).

NELSON, A. et al. Recomendaciones y consideraciones para la respuesta a incidentes en la gestión de riesgos de ciberseguridad: un perfil de la comunidad CSF 2.0. Gaithersburg: Instituto Nacional de Estándares y Tecnología, 2025. (Publicación especial NIST 800-61 Rev. 3).

POSTHUMUS, S.; VON SOLMS, R. Un marco para la gobernanza de la seguridad de la información. Computers & Security, vol. 23, n.º 8, págs. 638-646, 2004.

REASON, J. Gestión de los riesgos de accidentes organizacionales. Aldershot: Ashgate, 1997.

SCHNEIER, B. Secretos y mentiras: seguridad digital en un mundo interconectado. Nueva York: John Wiley & Sons, 2000.

SIPONEN, M.; VANCE, A. Neutralización: nuevas perspectivas sobre el problema de las violaciones de las políticas de seguridad de los sistemas de información de los empleados. MIS Quarterly, vol. 34, n.º 3, págs. 487-502, 2010.

SNYDER, H. La revisión de la literatura como metodología de investigación: una visión general y directrices. Journal of Business Research, vol. 104, págs. 333-339, 2019.

SOOMRO, ZA; SHAH, MH; AHMED, J. La gestión de la seguridad de la información requiere un enfoque más holístico: una revisión de la literatura. International Journal of Information Management, vol. 36, n.º 2, págs. 215-225, 2016.

TORRACO, RJ. Cómo redactar revisiones bibliográficas integradoras: pautas y ejemplos. Human Resource Development Review, vol. 4, núm. 3, págs. 356-367, 2005.

UNIÓN EUROPEA. Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un alto nivel común de ciberseguridad en la Unión (Directiva SRI 2). Diario Oficial de la Unión Europea, Luxemburgo, L 333, pp. 80-152, 27 de diciembre de 2022.

VERIZON. Informe de investigaciones de filtraciones de datos de 2024. Basking Ridge: Verizon Business, 2024.

VON SOLMS, B.; VON SOLMS, R. Los 10 pecados capitales de la gestión de la seguridad de la información. Computers & Security, vol. 23, n.º 5, págs. 371-376, 2004.

VON SOLMS, R.; VAN NIEKERK, J. De la seguridad de la información a la ciberseguridad. Computers & Security, vol. 38, págs. 97-102, 2013.

WEICK, K.E.; SUTCLIFFE, KM Gestionar lo inesperado: desempeño resiliente en una era de

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: 14/08/2026 | Aceptación: 10/09/2026 | Publicación: 24/10/2026

Incertidumbre. 2ª ed. San Francisco: Jossey-Bass, 2007.

WILLIAMSON, OE Las instituciones económicas del capitalismo: empresas, mercados, contratación relacional. Nueva York: Free Press, 1985.

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.