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

Año VII, vol. 2, 2026 | Envío: 06/05/2026 | Aceptación: 09/06/2026 | Publicación: 11/07/2026

Las primeras horas tras un ciberataque: detección, contención, preservación de pruebas y recuperación como factores determinantes de la resiliencia organizativa.
Las primeras horas después de un ciberataque: detección, contención, preservación de pruebas y recuperación como determinantes de la resiliencia organizacional.
Las primeras horas después de un ciberataque: detección, contención, preservación de pruebas y recuperación como determinantes de la resiliencia organizacional.

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

El intervalo entre el descubrimiento de un incidente cibernético y las primeras decisiones de respuesta implica elecciones difíciles de revertir, como aislar o mantener los sistemas operativos, preservar o descartar rastros volátiles y comunicar o esperar la confirmación de los hechos. Este artículo analiza cómo la detección, la contención, la preservación de la evidencia digital, la comunicación regulatoria y la recuperación operativa, cuando se llevan a cabo en las primeras horas, condicionan la capacidad de una organización para reanudar sus actividades después de un ataque. Se trata de un estudio cualitativo, exploratorio y descriptivo, construido a través de una revisión narrativa de la literatura científica y un análisis documental de estándares técnicos, directrices gubernamentales, informes sectoriales y legislación. Los resultados indican que el tiempo de permanencia del intruso en el entorno, el orden de recopilación de datos volátiles, la disponibilidad de copias de seguridad aisladas y la existencia previa de roles y canales de toma de decisiones definidos explican gran parte de la diferencia entre incidentes contenidos y crisis prolongadas. Se puede concluir que la calidad de la respuesta inicial depende menos de la improvisación técnica y más de la preparación organizacional, lo que requiere tratar la respuesta a incidentes como una capacidad de gestión de riesgos, vinculada a la gobernanza, la experiencia digital y la continuidad del negocio.

Palabras clave: Respuesta a incidentes. Informática forense. Ransomware. Continuidad del negocio. Resiliencia cibernética.

ABSTRACTO

El intervalo entre el descubrimiento de un incidente cibernético y las primeras decisiones de respuesta concentra elecciones difíciles de revertir, como aislar o mantener los sistemas en línea, preservar o descartar rastros volátiles y notificar a las partes interesadas o esperar a que se confirmen los hechos. Este artículo examina cómo la detección, la contención, la preservación de la evidencia digital, la comunicación operativa regulatoria y la recuperación, cuando se llevan a cabo en las primeras horas, determinan la capacidad de una organización para reanudar sus operaciones después de un ataque. Se trata de un estudio cualitativo, exploratorio y descriptivo basado en una revisión narrativa de la literatura científica y en el análisis documental de estándares técnicos, directrices gubernamentales, informes de la industria y legislación. Los hallazgos indican que el tiempo de permanencia del atacante, el orden en que se recopilan los datos volátiles, la disponibilidad de copias de seguridad aisladas y la definición previa de roles y canales de decisión explican gran parte de la diferencia entre incidentes contenidos y crisis prolongadas. El estudio concluye que la calidad de la respuesta inicial depende menos de la improvisación técnica que de la preparación organizacional, lo que requiere tratar la respuesta a incidentes como una capacidad de gestión de riesgos vinculada a la gobernanza, la informática forense y la continuidad del negocio.

Palabras clave: Respuesta a incidentes. Informática forense. Ransomware. Continuidad del negocio. Resiliencia cibernética.

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: 06/05/2026 | Aceptación: 09/06/2026 | Publicación: 11/07/2026

1. INTRODUCCIÓN

Los incidentes de seguridad de la información ya no son eventos raros que se tratan de forma aislada.
Los equipos de tecnología se han integrado en la rutina de gestión de riesgos de organizaciones de todos los tamaños.
Un informe sobre investigaciones de filtraciones de datos publicado por Verizon en 2025 analizó más de
22.000 incidentes, de los cuales 12.195 fueron confirmados como infracciones, y se registró la presencia de
El ransomware estuvo involucrado en el 44% de estos casos (Verizon, 2025). Durante el mismo período, el estudio realizado por
El Instituto Ponemon, en colaboración con IBM, estimó que el coste medio mundial de una filtración de datos asciende a 4,44 millones de dólares estadounidenses.
y el ciclo promedio de identificación y contención es de 241 días (IBM, 2025). Estas cifras revelan que
frecuencia del problema y también la duración de sus efectos, que se extienden mucho más allá de la
El momento en que se percibe el ataque.
Entre el descubrimiento de un ataque y la estabilización del entorno, existe un breve lapso de tiempo en el que se deben tomar decisiones...
Es necesario tomar decisiones de gran trascendencia con información incompleta. Apagar un servidor.
Puede detener la propagación de código malicioso y, al mismo tiempo, borrarlo de la memoria.
rastros volátiles que permitirían reconstruir la intrusión. Restaurar rápidamente los sistemas puede
para reducir las pérdidas operativas, pero también para reintroducir al intruso si falla la ruta de acceso original.
una vez que se ha identificado. Comunicar demasiado pronto puede llevar a información inexacta, mientras que
Comunicarse demasiado tarde puede incumplir plazos legales y minar la confianza de clientes y reguladores. Este trabajo se
centra en este conjunto de tensiones.
El objetivo de este artículo es analizar cómo la detección, contención y preservación de la evidencia digital,
comunicación regulatoria y recuperación operativa, cuando se lleva a cabo en las primeras horas después
El descubrimiento de un incidente influye en la capacidad de recuperación de una organización. Parte-
Si la hipótesis es que la calidad de esta respuesta inicial resulta más de la preparación previa, se expresa
en roles definidos, procedimientos probados e infraestructura de recuperación aislada, en lugar de
Habilidades técnicas movilizadas durante una crisis. Para respaldar esta discusión, el texto articula:
normas técnicas internacionales, estudios académicos sobre equipos de respuesta, informes sectoriales
con datos empíricos recientes y legislación brasileña aplicable, así como casos documentados
en público.

2. METODOLOGÍA

La investigación adopta un enfoque cualitativo, de carácter exploratorio y descriptivo, tal como se propone.
por Gil (2008), para quien los estudios exploratorios buscan brindar mayor familiaridad con
Se identifica un problema, mientras que las variables descriptivas buscan caracterizar los fenómenos y establecer relaciones entre variables.

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: 06/05/2026 | Aceptación: 09/06/2026 | Publicación: 11/07/2026

La elección se justifica por la naturaleza multidisciplinaria del tema, que involucra aspectos técnicos, factores organizativos, legales y de gestión, y la falta de una base de datos única capaz de medir, De igual modo, el efecto de las decisiones tomadas en las primeras horas de un incidente. Por esta razón... Por lo tanto, el estudio prioriza la integración de diversas fuentes en lugar de la medición estadística. a partir de un único conjunto de datos.

En cuanto a los procedimientos, se combinaron la investigación bibliográfica y la investigación documental. La revisión de la literatura siguió el formato de revisión narrativa, que, según Rother (2007), es apropiado. describir y analizar el estado del arte de un tema desde un punto de vista teórico y contextual, sin La intención de agotar todas las fuentes o aplicar criterios sistemáticos de búsqueda y selección. Eran Se consultaron artículos publicados en revistas revisadas por pares, como Computers & Security, Información y Gestión, Revista Internacional de Gestión de la Información, Factores Humanos y Fronteras en Psicología, identificadas a través de búsquedas en Google Académico y en los portales de sus respectivas editoriales, además de obras de referencia en informática forense y gestión organizativa. Alta fiabilidad.

El análisis de documentos incluyó publicaciones técnicas del Instituto Nacional de Estándares y Tecnología. Tecnología (NIST), estándares de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), documento de ingeniería de Internet RFC 3227 Grupo de trabajo, la guía conjunta de agencias estadounidenses sobre ransomware, la Ley General de Protección de Datos. Ley de Protección de Datos Personales, el Código de Procedimiento Penal con las enmiendas introducidas por la Ley No. Se examinaron la Ley 13.964/2019 y la Resolución CD/ANPD N° 15/2024. También se revisaron los informes sectoriales. con datos empíricos ampliamente citados en la literatura, publicados por Mandiant, IBM, Verizon y Sophos y los registros públicos de dos incidentes de alto perfil, el ataque de NotPetya en La empresa AP Møller-Maersk en 2017 y el ataque de ransomware contra Colonial Pipeline en 2021.

El material se organizó en seis áreas temáticas, definidas en función de las fases de respuesta descritas. en las normas de referencia, a saber, modelos de respuesta, detección, contención, preservación de evidencia, comunicación y recuperación. En cada área, el objetivo era comparar los estándares Recomiendan lo que revelan los estudios empíricos y los casos documentados sobre esta práctica.

Se reconoce como limitación que los informes sectoriales sean elaborados por empresas. Privadas, con sus propias muestras y metodologías que no permiten una comparación directa entre ellas. Por Es decir, sus cifras se tratan como indicadores de tendencia, no como medidas exactas de... fenómeno.

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: 06/05/2026 | Aceptación: 09/06/2026 | Publicación: 11/07/2026

3 MODELOS DE REFERENCIA PARA LA RESPUESTA ANTE INCIDENTES Y SU EVOLUCIÓN

Durante más de una década, la principal referencia internacional para organizar la respuesta a
Los incidentes fueron la segunda revisión de la Publicación Especial 800-61 del NIST, preparada por Cichonski et al.
et al. (2012). El documento describe un ciclo compuesto por cuatro fases: preparación, detección y
análisis, contención, erradicación y recuperación, y actividades posteriores al incidente, y enfatiza que la respuesta
No termina con la restauración de los sistemas, ya que las lecciones aprendidas deben volver a la fase de
preparación. La guía también recomienda que las organizaciones formalicen políticas, planes y
procedimientos de respuesta y definen la estructura y las funciones del equipo responsable, lo que permite que
El proceso debe documentarse, comunicarse a los gerentes y verificarse mediante auditorías internas y externas.
En el campo de la normalización internacional, la serie ISO/IEC 27035 desempeña un papel similar. La edición
La primera parte de la norma de 2023 organiza la gestión de incidentes en cinco fases: planificación.
y preparación, detección y notificación, evaluación y decisión, respuestas y lecciones aprendidas (ISO,
2023). La separación entre la detección y la fase de evaluación y decisión es especialmente relevante para la
El tema de este artículo es que reconoce que no todo evento detectado constituye un incidente y que...
Una clasificación correcta, realizada desde el principio, determina la magnitud de los recursos movilizados. Cichonski y
et al. (2012) observan, en este sentido, que para muchas organizaciones la parte más difícil del proceso es
precisamente para detectar y evaluar con precisión los incidentes potenciales, distinguiendo los precursores,
Indicadores y falsos positivos en medio de un gran volumen de alertas.
En abril de 2025, el NIST publicó la tercera revisión de SP 800-61, cuyos autores fueron Nelson et al. (2025).
que reemplaza la versión de 2012 y altera significativamente la perspectiva adoptada. En lugar de una
En su propio ciclo, la respuesta a incidentes se describe ahora como un perfil de ciberseguridad basado en la comunidad.
Marco 2.0, distribuido entre las seis funciones del modelo: gobernar, identificar, proteger, detectar,
Responder y recuperarse (NIST, 2024). Según los autores, se debe incorporar la respuesta a incidentes.
a las actividades de gestión de riesgos de ciberseguridad, de modo que la preparación, reduciendo el número
y el impacto de los incidentes y la mejora de la detección, respuesta y recuperación deben abordarse en
forma integrada (Nelson et al., 2025). Desde esta perspectiva, la respuesta deja de ser una actividad
Se activa únicamente cuando algo sale mal y depende de las decisiones de gobernanza e inventario.
de activos y controles preventivos tomados antes del ataque.
La literatura académica confirma que la brecha entre el modelo normativo y la práctica es real. Tøndel,
Line y Jaatun (2014) realizaron una revisión sistemática sobre la gestión de incidentes de seguridad y
Organizaron las prácticas reportadas de acuerdo con las fases de ISO/IEC 27035, concluyendo que la práctica
En términos generales, el comportamiento observado es coherente con el estándar, pero resulta difícil identificar qué recomendaciones son...
Son más difíciles de seguir en las operaciones diarias de las organizaciones. Baskerville, Spagnoletti y Kim

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: 06/05/2026 | Aceptación: 09/06/2026 | Publicación: 11/07/2026

(2014), basado en un estudio de caso comparativo en tres organizaciones europeas, mostró que la
Las estrategias de seguridad tienden a priorizar la prevención de amenazas predecibles, aunque...
La capacidad de respuesta es esencial para hacer frente a amenazas impredecibles, lo que requiere
un equilibrio deliberado entre los dos paradigmas.
Otro punto recurrente en la literatura es la desconexión entre los equipos de respuesta y la gestión estratégica.
de seguridad. En un estudio de caso sobre la respuesta a incidentes en la práctica, Ahmad, Hadgkiss y
Ruighaver (2012) observó que la organización analizada seguía de cerca las mejores prácticas de la industria.
pero centró sus esfuerzos en los aspectos técnicos y la continuidad del negocio, descuidando la realización de
Actividades de aprendizaje tras incidentes. En un estudio posterior, realizado en una organización
La institución financiera australiana, Ahmad, Maynard y Shanks (2015) identificaron deficiencias sistémicas en
Malas prácticas de respuesta y falta de comunicación entre los responsables de los incidentes y la dirección.
seguridad, que impide que la organización aprenda de sus propios ataques. La Tabla 1 resume
la correspondencia entre los tres modelos analizados en esta sección, mostrando que, a pesar de la
A pesar de las diferencias en la terminología, todas las reservas siguen pasos específicos para la preparación, detección y...
Aprender después del incidente.

Tabla 1 – Correspondencia entre modelos de referencia para la respuesta a incidentes

NIST SP 800-61 Rev. 2 (2012)	ISO/IEC 27035-1 (2023)	NIST SP 800-61 Rev. 3 y CSF 2.0 (2025)
Preparación	Planificación y preparación	Gobernar, identificar y Proteger
Detección y análisis	Detección y notificación, Evaluación y decisión	Detectar
Contención, erradicación y recuperación	Respuestas	Responder y recuperar
Actividades posteriores al incidente	Lecciones aprendidas: Identificar (mejora continua)	

Fuente: preparado por el autor con base en Cichonski et al. (2012), ISO (2023), NIST (2024) y Nelson et al. (2025).

4. Detección de intrusos y tiempo de residencia

La expresión "primeras horas" presupone que el incidente fue notado, pero en la práctica, la respuesta
El condicionamiento comienza mucho antes, por el intervalo durante el cual el invasor permanece en el ambiente sin
para ser notado. Mandiant, la división de respuesta a incidentes de Google Cloud, mide este intervalo mediante
Este indicador se conoce como "tiempo de permanencia", definido como el número de días entre el inicio de la intrusión y
Su identificación. Según el informe M-Trends 2025, la mediana global para este período fue de 11 días.

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.

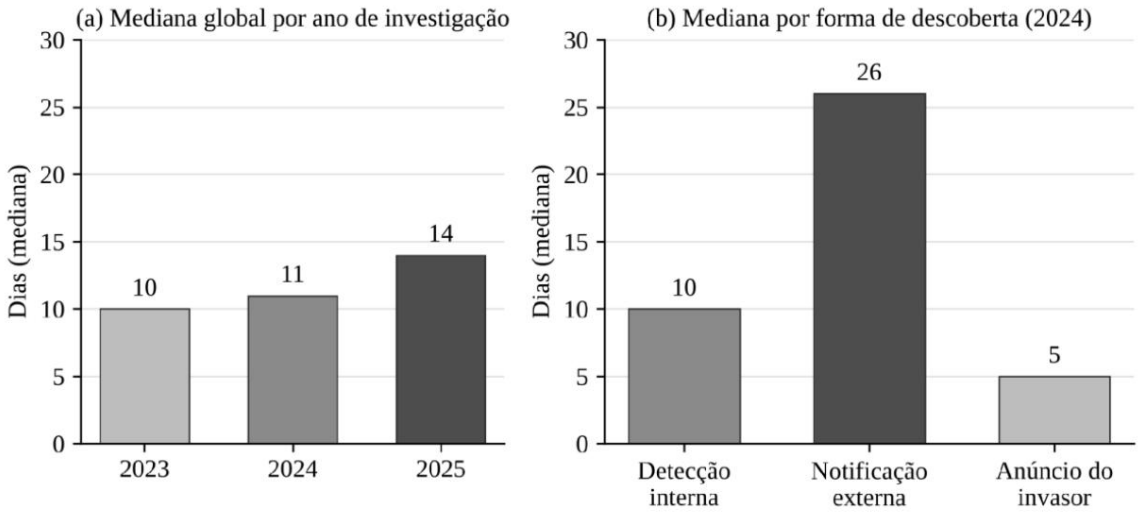
Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 06/05/2026 | Aceptación: 09/06/2026 | Publicación: 11/07/2026

En las investigaciones realizadas en 2024, ligeramente por encima de los 10 días observados en 2023.
(Mandiant, 2025). La siguiente edición registró un nuevo aumento, con una mediana de 14 días en
investigaciones de 2025 (Mandiant, 2026).

Más revelador que la mediana global es el contraste entre los métodos de descubrimiento. En las investigaciones
A partir de 2024, cuando la propia organización identificó la actividad maliciosa, la mediana fue de 10 días.
mientras que en los casos en que el descubrimiento provino de una entidad externa, tardó hasta 26 días. Cuando
El propio atacante anunció su presencia, una situación típica en los ataques de ransomware donde la nota
La primera señal percibida es la de rescate, la mediana se redujo a 5 días (Mandiant, 2025). Figura 1
presenta estos valores. El valor de 5 días no debe interpretarse como un signo de eficiencia defensiva, porque,
En estos casos, el descubrimiento no se produce al vigilar a la víctima, sino más bien por la decisión del atacante de...
Si se revela, esto coloca a la organización en una posición en la que deberá responder bajo la máxima presión.

Figura 1 – Tiempo medio que el invasor permanece en el medio ambiente, en días.



Fuente: compilado por el autor con datos de Mandiant (2025; 2026).

Las cifras de Mandiant y las de IBM miden fenómenos distintos y no deben confundirse.

Mientras Mandiant calcula el tiempo de permanencia medio en las intrusiones que investigó,
Un estudio de IBM estima el número promedio de días necesarios para identificar y contener una filtración de datos.
incluyendo la restauración de servicios, en una muestra de 600 organizaciones. Aun así, ambos
Ambos apuntan en la misma dirección. El ciclo medido por IBM se redujo a 241 días en el estudio de 2025, el más corto.
El nivel se sitúa nueve años y 17 días por debajo del resultado del año anterior, lo que sugiere mejoras en la eficiencia.
lo cual, aunque relevante, deja a las organizaciones expuestas durante meses (IBM, 2025).

La capacidad de detección temprana depende de la visibilidad y el método. El modelo de cadena de
La intrusión propuesta por Hutchins, Cloppert y Amin (2011) describe el ataque como una secuencia 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
RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 06/05/2026 | Aceptación: 09/06/2026 | Publicación: 11/07/2026

Se describe el proceso, desde el reconocimiento hasta la ejecución de los objetivos, y se argumenta que el defensor puede frustrar...
Una operación adversaria puede ser interrumpida al interrumpir cualquiera de ellas. La base de conocimientos MITRE ATT&CK,
Descrita por Strom et al. (2018), desarrolló aún más esta lógica catalogando tácticas y técnicas de manera efectiva.
observado en ataques reales, lo que permite a los equipos de monitoreo formular hipótesis de
Detección basada en el comportamiento, no solo detección basada en firmas de código conocidas.
Datos más recientes muestran por qué esto importa, ya que la explotación de vulnerabilidades ha respondido
El phishing por voz representó el 32% de las intrusiones investigadas en 2025, y alcanzó el 11% (Mandiant, 2026).
La detección no es solo un problema de herramientas, sino también de cognición. Endsley (1995)
Describió la conciencia situacional en tres niveles: percepción de los elementos ambientales,
comprender su significado y proyectar su estado futuro, y demostró que los fallos en cualquier
Uno de ellos compromete la toma de decisiones en sistemas dinámicos. Por analogía, aplicado a un
Centro de operaciones de seguridad, el modelo puede ayudar a explicar por qué una alerta se emite correctamente.
El evento generado puede ignorarse cuando el analista lo percibe pero no comprende su relación con él.
otras señales, o porque una intrusión que se detecta demasiado tarde ya no permite una contención eficaz.
Van der Kleij, Kleinhuis y Young (2017), mientras investigaban los equipos de respuesta en los Países Bajos,
Propusieron un modelo de necesidades que distribuye los factores de rendimiento entre los distintos niveles.
organizacional, de equipo, individual e instrumental, lo que indica que los problemas de desempeño pueden
originándose en cualquiera de estos niveles o en una combinación de ellos.

5. Contención y toma de decisiones bajo presión

La contención es la fase en la que la respuesta al incidente produce sus efectos más inmediatos sobre el
Operación de la organización. Cichonski et al. (2012) recomiendan que la estrategia de contención sea
elegido en función de criterios predefinidos, incluido el potencial de daño y
la sustracción de recursos, la necesidad de preservar la evidencia, la disponibilidad de servicios, la
El tiempo y los recursos necesarios, la eficacia esperada de la medida y la duración de la solución. Los autores
También recomiendan que las organizaciones desarrollen estrategias de contención específicas para cada tipo.
Informe principal del incidente, con criterios claramente documentados, precisamente para facilitar la toma de decisiones.
decisión cuando ocurre el incidente.
El caso del oleoducto Colonial ilustra el alcance que pueden tener estas decisiones. Según el testimonio
desde el entonces presidente de la compañía hasta el Comité de Seguridad Nacional y Asuntos Gubernamentales de
En el Senado de Estados Unidos, un empleado encontró una nota de rescate en un sistema de red.
Tecnología de la información poco antes de las 5:00 AM del 7 de mayo de 2021, y a las 6:10 AM la empresa
confirmó que las aproximadamente 5.500 millas de oleoductos, equivalentes a aproximadamente 8.850

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: 06/05/2026 | Aceptación: 09/06/2026 | Publicación: 11/07/2026

kilómetros habían quedado paralizados (Blount, 2021). La red transportaba casi la mitad de
El combustible se consumió en la costa este de los Estados Unidos, y la operación apenas comenzó a reanudarse.
la noche del 12 de mayo. El mismo testimonio atribuye el acceso inicial a un perfil de red antiguo.
Una red privada virtual (VPN) que no debería estar en uso.
El episodio demuestra que la contención puede requerir la interrupción deliberada de las operaciones antes de...
Averigüe si se vieron afectados. En el mismo testimonio, el ejecutivo afirmó que el cierre buscaba aislar
y contener el ataque para evitar que el código malicioso se propague a la red tecnológica.
operativo, que controla los oleoductos, en caso de que esto no hubiera ocurrido ya, y reconoció que la empresa
En ese momento, desconocía tanto el punto de origen como el alcance del ataque (Blount, 2021).
El intervalo de poco más de una hora entre el descubrimiento y el cierre total indica que se tomó una decisión.
Esta medida de esta magnitud se tomó antes de cualquier diagnóstico completo, lo que refuerza la recomendación.
Cichonski et al. (2012) recomiendan documentar los criterios de contención con antelación.
La guía conjunta sobre ransomware publicada por la agencia de ciberseguridad de EE. UU. y
El departamento de Infraestructura, en colaboración con otros organismos, recomienda determinar qué sistemas se vieron afectados.
y aislarlos inmediatamente, desconectando la red a nivel del conmutador cuando el
compromiso para amplio (CISA, 2023). El mismo documento aconseja que el equipo solo
Deben apagarse cuando no sea posible desconectarlos de la red, advirtiendo que el apagado...
elimina la evidencia almacenada en la memoria volátil. La guía también recomienda el uso de canales para
Se utilizan métodos de comunicación alternativos, como las llamadas telefónicas, para evitar que el intruso...
presentes en los sistemas de correo y mensajería, monitorean la coordinación de la respuesta y anticipan la
medidas de contención.
La bibliografía sobre organizaciones de alta fiabilidad ofrece una perspectiva útil para comprender este fenómeno.
comportamiento. Weick y Sutcliffe (2015) identifican cinco principios que distinguen a las organizaciones
capaz de operar en entornos de alto riesgo con una baja incidencia de fallas graves, la preocupación
con el fracaso, la renuencia a simplificar las interpretaciones, la sensibilidad a las operaciones, la
compromiso con la resiliencia y respeto a la competencia técnica. Este último principio es
particularmente relevante para la contención, ya que propone que, en situaciones críticas, la autoridad de toma de decisiones
Recurre a quien tenga el conocimiento más preciso sobre el problema, independientemente de...
posición jerárquica. Aplicado a un incidente cibernético, el principio sugiere que el analista que
entiende la mecánica del ataque y tiene acceso directo a quién puede autorizar la interrupción de
sistemas.

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: 06/05/2026 | Aceptación: 09/06/2026 | Publicación: 11/07/2026

6. PRESERVACIÓN DE LA EVIDENCIA DIGITAL EN LAS PRIMERAS HORAS

La presión por reanudar las operaciones tiende a relegar la preservación de las pruebas a un segundo plano.
plan, aunque las directrices técnicas son claras en cuanto a la prioridad de la recopilación de datos sobre las intervenciones.
Medidas correctivas. El documento RFC 3227, preparado por Brezinski y Killalea (2002), establece que la recopilación
Debe seguir el orden de volatilidad, comenzando por los registros y la memoria caché, y luego continuando con el resto.
a través de tablas de enrutamiento, la tabla de procesos y la memoria principal, a través de los sistemas de
Archivos temporales y acceso al disco, hasta registros remotos, topología de red y medios de almacenamiento.
archivado. El mismo documento recomienda no apagar el sistema antes de completar la recopilación.
y no confiar en los programas instalados en la máquina comprometida, que pueden haber sido alterados por
invasor.

Kent et al. (2006), en la guía del NIST dedicada a la integración de técnicas forenses en la respuesta a incidentes,
Describen el proceso forense en cuatro etapas: recolección, examen, análisis e informe, y lo llaman...
Tenga en cuenta que muchas de las decisiones tomadas durante la respuesta, como reiniciar un servidor, están sujetas a cambios.
Aplicar una corrección, o hacerlo, altera irreversiblemente el estado de los datos. Por esta razón, los autores
Recomiendan que las organizaciones tengan capacidades forenses, respaldadas por políticas y
Procedimientos que guían, entre otras actividades, la recopilación de datos volátiles antes del cierre.
de los sistemas. Una guía similar aparece en la guía sobre ransomware, que recomienda capturar
imagen y memoria de una muestra del equipo afectado (CISA, 2023).

En el marco regulatorio internacional, la norma ISO/IEC 27037 establece directrices para la identificación,
Recopilación, adquisición y preservación de evidencia digital (ISO, 2012). La norma establece que la
El tratamiento de esta evidencia debe ser auditable, repetible, reproducible y justificable, de modo que
un tercero puede evaluar las acciones tomadas y, cuando corresponda, obtener los mismos resultados de
a partir de los mismos datos. Casey (2011) añade que la integridad de la evidencia digital depende de
Documentación rigurosa de cada acción realizada, utilizando funciones hash para demostrar que la
Los datos no fueron alterados, lo que refleja una comprensión de las limitaciones de las herramientas empleadas, dado que...
Por su propia naturaleza, las pruebas digitales son fáciles de modificar sin dejar rastros evidentes.

En Brasil, la preservación de pruebas adquirió contornos legales más precisos con la Ley No.
Ley 13.964/2019, que insertó los artículos 158-A a 158-F en el Código de Procedimiento Penal y definió la cadena de
custodia como el conjunto de procedimientos utilizados para mantener y documentar el historial
Registro cronológico del rastro, desde su reconocimiento hasta su eliminación (Brasil, 2019). Artículo 158-B
Detalla las etapas de este proceso, que incluyen el reconocimiento, el aislamiento, la fijación, la recolección y...
Embalaje, transporte, recepción, procesamiento, almacenamiento y eliminación.

El texto legal no distingue la naturaleza del rastro, por lo que sus requisitos también se aplican 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: 06/05/2026 | Aceptación: 09/06/2026 | Publicación: 11/07/2026

Los rastros digitales y los errores cometidos en las primeras horas pueden comprometer el uso de...
pruebas en cualquier eventual proceso penal derivado del incidente.
Por lo tanto, la tensión entre preservar y restaurar no se resuelve eligiendo uno de los extremos. La guía
En cuanto al ransomware, propone una solución intermedia recomendando la captura de imágenes y...
memoria de una muestra del equipo afectado, y no de todo, lo que permite recopilar elementos.
para la investigación sin paralizar la recuperación (CISA, 2023). Sin embargo, la aplicación de esta estrategia,
Esto presupone que existen procedimientos definidos de antemano para la recopilación y el almacenamiento seguros de imágenes.
incidente, como recomiendan Kent et al. (2006). Sin esta preparación, la restauración inmediata tiende
borrar los rastros que permitirían identificar la ruta de entrada, el alcance de la intrusión y la
posible pérdida de datos, con el consiguiente riesgo de reinfección, sobre lo cual advierte la propia guía.
al hablar de la fase de recuperación.

7. Comunicación, gobernanza y obligaciones regulatorias

La comunicación durante un incidente involucra a distintos públicos, cada uno con sus propias necesidades y plazos de entrega.
propios, como la alta dirección, los equipos internos, los clientes, los proveedores, las autoridades
organismos reguladores y, en algunos casos, fuerzas de seguridad y la prensa. La introducción de la función de gobierno.
El Marco de Ciberseguridad 2.0 reconoce que definir roles, responsabilidades y
La responsabilidad en materia de ciberseguridad recae en la dirección de la organización, no solo en el departamento técnico.
(NIST, 2024). En respuesta a incidentes, esta definición se traduce en saber, antes de la crisis, quién decide.
En lo que respecta a la comunicación externa, ¿quién habla en nombre de la empresa y qué información se puede compartir?
divulgada sin poner en peligro la investigación ni los esfuerzos de contención.
En el ordenamiento jurídico brasileño, el artículo 48 de la Ley General de Protección de Datos Personales establece 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 a los titulares de los datos (Brasil, 2018).
El plazo fue fijado por la Resolución CD/ANPD No. 15, del 24 de abril de 2024, que establece tres días.
Útil, contado desde el conocimiento de que el incidente afectó datos personales, tanto para fines de comunicación.
a la autoridad con respecto a la comunicación a los titulares, permitiendo una suplementación fundamentada basada en
hasta veinte días hábiles y el doble de tiempo para los agentes de procesamiento de datos pequeños (ANPD, 2024). A
La misma norma exige que el registro del incidente se conserve durante al menos cinco años, ambos inclusive.
cuando no hay comunicación.
La resolución también define criterios objetivos para caracterizar el riesgo o daño relevante, lo que requiere:
que el incidente puede afectar significativamente los intereses y derechos fundamentales de los titulares y que
implican al menos un tipo específico de datos, como datos sensibles, datos de niños, adolescentes

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: 06/05/2026 | Aceptación: 09/06/2026 | Publicación: 11/07/2026

o personas mayores, datos financieros, datos de autenticación, datos protegidos por confidencialidad o datos a gran escala.
escala (ANPD, 2024). Dado que el plazo de comunicación se cuenta en días hábiles a partir de la
Dada la naturaleza del incidente, esta clasificación debe comenzar en las primeras horas, cuando el
El alcance del compromiso aún es incierto. La integración entre el equipo técnico, responsable de
para determinar a qué datos se accedió y quién es el responsable del tratamiento de los datos personales.
La ley exige el diálogo con la autoridad y las partes pertinentes, convirtiéndolo así en un requisito.
Operativo, y no solo una recomendación para una buena gobernanza.
Otras jurisdicciones adoptan plazos igualmente cortos, lo que afecta directamente a las organizaciones con
operaciones internacionales. El Reglamento General de Protección de Datos de la Unión Europea, en
El artículo 33 estipula que cualquier violación de datos personales debe ser comunicada a la autoridad de control.
sin demora indebida y, siempre que sea posible, dentro de las 72 horas siguientes a que la persona responsable haya tenido
conocimiento del hecho (Unión Europea, 2016). En los Estados Unidos, la norma aprobada por la Comisión de Valores
En 2023, la Comisión de Bolsa y Valores exigirá a las empresas que cotizan en bolsa que revelen los incidentes.
medidas de ciberseguridad consideradas importantes dentro de los cuatro días hábiles posteriores a la determinación de
materialidad (Estados Unidos, 2023). La superposición de estos plazos exige que las organizaciones mantengan
Las plantillas de comunicación y los flujos de trabajo de aprobación están listos antes de que ocurra cualquier incidente.
La comunicación con proveedores y socios ha cobrado mayor importancia a medida que los ataques han avanzado.
para explorar las relaciones de confianza entre empresas. El informe de Verizon de 2025 indica que...
La participación de terceros en las infracciones se ha duplicado, alcanzando el 30% de los casos analizados (Verizon, 2025).
Esto significa que, en un número considerable de incidentes, la respuesta requiere coordinación con
Organizaciones externas, cuyos procesos, plazos y prioridades pueden diferir de los de la víctima.
La experiencia reportada por Ahmad, Maynard y Shanks (2015) muestra además que la falta de comunicación
Los conflictos internos entre la gestión de respuesta y la gestión de seguridad dificultan el aprendizaje organizacional, lo que sugiere que
que la comunicación debe ser tratada como parte del propio proceso de respuesta, con registros que
contribuir a la revisión posterior del incidente.

8. RECUPERACIÓN, CONTINUIDAD DEL NEGOCIO Y EL PAPEL DE LAS COPIAS SEGURIDAD

La recuperación suele considerarse la etapa final de la respuesta, pero sus condiciones...
Los factores de éxito se definen mucho antes del incidente. La guía del NIST para la planificación de contingencias,
Desarrollado por Swanson et al. (2010), se recomienda que la organización realice un análisis de impacto.
En el ámbito empresarial, el objetivo es establecer, para cada sistema, el tiempo máximo de inactividad tolerable.
objetivo de tiempo de recuperación y objetivo de punto de recuperación, que expresa la cantidad

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: 06/05/2026 | Aceptación: 09/06/2026 | Publicación: 11/07/2026

La cantidad máxima de datos que se puede permitir perder. La norma ISO 22301 incorpora estas definiciones en un sistema de gestión.
de continuidad del negocio, con requisitos para la planificación, operación, evaluación del desempeño y
Mejora continua (ISO, 2019). Sin estos parámetros, el equipo carece de un criterio objetivo para definir
la orden de restauración, que la propia guía vincula con los resultados del análisis de impacto.

El papel de las copias de seguridad ha cambiado significativamente con la profesionalización de los ataques.
ransomware . En una encuesta de Sophos a 5.000 líderes de tecnología y seguridad en 14 países,
El 94% de las organizaciones afectadas por ransomware informaron que los atacantes intentaron comprometer su seguridad.
sus copias de seguridad durante el ataque, y el 57% de estos intentos tuvieron éxito (Sophos, 2024a).
El mismo estudio estimó el costo promedio de recuperación, excluyendo cualquier posible pago de rescate, en
US$2,73 millones. Los datos más recientes de Mandiant (2026) confirman la tendencia, registrando
Los grupos de ransomware están dirigiendo sus esfuerzos hacia la infraestructura de respaldo, con el fin de
Servicios de identidad y plataformas de gestión de virtualización.

El caso de AP Møller-Maersk, afectado por el ataque de NotPetya el 27 de junio de 2017, se convirtió en un referente.
sobre la fragilidad de las estrategias de recuperación. Según un informe de Greenberg (2018), la
Un código malicioso destruyó los controladores de dominio de la empresa en todo el mundo, y la reconstrucción...
La infraestructura solo fue posible gracias a un único controlador, instalado en una oficina en Ghana,
Se desconectó de la red debido a un corte de energía en el momento del ataque. La empresa
Reconstruyó aproximadamente 4.000 servidores y 45.000 ordenadores; la red se restauró en diez días y...
El presidente estimó que las pérdidas oscilarían entre los 250 y los 300 millones de dólares estadounidenses.
El episodio muestra que la recuperación dependió del azar y no de una copia aislada conservada.
forma planificada.

Las lecciones técnicas aprendidas de estos casos se incorporaron a las recomendaciones oficiales. La guía conjunta sobre
El ransomware ordena que los datos se restauren a partir de copias de seguridad desconectadas y
encriptado, siguiendo un orden de prioridad basado en los servicios críticos, y alertas sobre el riesgo.
de reinfectar sistemas ya limpios durante la restauración (CISA, 2023). Ross et al. (2021), en la guía para
El NIST, en su trabajo sobre ingeniería de sistemas resilientes, propone que la resiliencia cibernética se estructure...
centrado en torno a cuatro objetivos: anticipar, resistir, recuperar y adaptarse, un enfoque que comienza desde
Se parte de la premisa de que la protección puede fallar, y el objetivo es garantizar la continuidad de las funciones esenciales.
incluso en condiciones adversas.

La decisión relativa al pago de un rescate también está vinculada a la disponibilidad de los medios propios de la empresa para...
recuperación. En una encuesta realizada a 2.974 profesionales de organizaciones afectadas por ransomware,
Sophos verificó que las víctimas cuyas copias de seguridad se vieron comprometidas pagaron el rescate.
en el 67% de los casos, en comparación con el 36% entre aquellos que conservaron sus copias intactas, y que solo el 26% de
El primer grupo se recuperó completamente en una semana, en comparación con el 46% de los demás (Sophos, 2024b).

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: 06/05/2026 | Aceptación: 09/06/2026 | Publicación: 11/07/2026

Un estudio de IBM registró que la proporción de víctimas que se negaron a pagar aumentó del 59% al 63%.
en 2025 (IBM, 2025). Sin embargo, la capacidad de recuperación depende de planes probados. Grance et
et al. (2006) argumentan que los planes de tecnología de la información deberían estar sujetos a programas
Pruebas, entrenamientos y ejercicios regulares, que incluyen simulaciones de mesa y ejercicios funcionales.
Precisamente para revelar fallos que solo se harían evidentes durante una crisis real.

9. CONCLUSIÓN

Este artículo partió de la premisa de que las primeras horas después del descubrimiento de un ciberataque
Se centran en decisiones cuyos efectos se extienden durante semanas o meses. El análisis de la literatura, de
Las normas técnicas, los informes sectoriales y los casos documentados confirman esta premisa y permiten
Para matizarlo. Las decisiones iniciales son cruciales, sin duda, pero rara vez se logra la calidad esperada.
en el momento de la crisis, como resultado de las condiciones creadas antes del incidente, como la definición de roles,
la existencia de procedimientos probados y la disponibilidad de infraestructura de recuperación aislada
del entorno de producción.
La evolución de los modelos de referencia expresa esta comprensión. El reemplazo del ciclo propio
La segunda revisión de SP 800-61, a través de un perfil integrado con el Marco de Ciberseguridad 2.0, indica que
La respuesta ante incidentes ya no se concibe como una actividad técnica que se activa únicamente en situaciones específicas.
excepcional y llegó a entenderse como capacidad de gestión de riesgos, vinculada a
gobernanza. La literatura académica refuerza esta interpretación al demostrar la persistente desconexión entre
Equipos de respuesta y gestión estratégica de seguridad, lo que limita la capacidad de las organizaciones para
Aprende de tus propios incidentes.
En términos de detección, los datos muestran que el tiempo de permanencia del intruso se sigue midiendo en
días, y la mediana mundial aumentó de 10 a 14 días entre las encuestas de 2023 y 2025.
contraste entre el descubrimiento interno, la notificación externa y el anuncio realizado por el propio atacante.
Esto demuestra que la forma en que se percibe el incidente determina el margen de maniobra disponible.
Cuando la primera señal es la nota de rescate, la respuesta comienza en desventaja, porque el oponente ya...
Logró sus objetivos. Invirtiendo en visibilidad, detección basada en el comportamiento y en
Por lo tanto, la conciencia situacional del equipo implica invertir en la calidad de las primeras horas.
En lo que respecta a la contención, las fuentes analizadas coinciden en la importancia de los criterios de decisión.
definido de antemano, con autoridad clara para detener operaciones y canales de
Los métodos de comunicación alternativos permiten actuar con rapidez sin actuar a ciegas. El caso de Colonial.
Pipeline demuestra que la interrupción preventiva de las operaciones puede ser necesaria incluso antes de...
Conocer el origen y el alcance del ataque solo es posible cuando la organización sabe quién lo está perpetrando.

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: 06/05/2026 | Aceptación: 09/06/2026 | Publicación: 11/07/2026

legitimidad para tomar esta decisión y qué criterios la sustentan. Los principios de las organizaciones de
La alta fiabilidad proporciona una base teórica sólida para esta práctica.
La preservación de la evidencia digital ha demostrado ser una cuestión crítica, expuesta al riesgo de ser sacrificada.
En nombre de la velocidad. El orden de la volatilidad, los principios de auditabilidad y reproducibilidad y
Los requisitos de cadena de custodia estipulados en el Código de Procedimiento Penal brasileño convergen hacia
Se llega a la misma conclusión de que la recopilación de datos debe realizarse antes de las intervenciones correctivas. La pérdida de estos
Las pruebas socavan la investigación, la responsabilidad de los perpetradores y la propia seguridad de la organización.
Recuperación, ya que impide saber si el acceso del intruso fue efectivamente eliminado. Preparación
El análisis forense debe considerarse parte integral de la respuesta, no una actividad auxiliar.
Las obligaciones regulatorias añaden una dimensión temporal que no se puede ignorar. El plazo
tres días hábiles establecidos por la Autoridad Nacional de Protección de Datos, sumados a los plazos de otros
En algunas jurisdicciones, se requiere que las evaluaciones de riesgo para los asegurados comiencen dentro de las primeras horas, con
Integración efectiva entre el equipo técnico y la persona encargada del tratamiento de datos personales.
La creciente participación de terceros en las infracciones amplifica este requisito, ya que la comunicación se vuelve más...
Involucrar cadenas de suministro cuyos procesos no siempre están alineados con los de la organización.
afectado.

En la sección de recuperación, se incluyen datos sobre ataques dirigidos a copias de seguridad y el caso de...
El caso Maersk demuestra que la existencia de una copia no es suficiente; es necesario que esté aislada.
completo y restaurable dentro del plazo definido por el análisis de impacto empresarial.
Los enlaces de datos comprometieron las copias de seguridad, lo que aumentó la propensión al pago.
Los esfuerzos de rescate y la recuperación más lenta indican que la propia capacidad de recuperación del cuerpo se expande.
El margen de decisión de la organización con respecto a la extorsión. Sin embargo, este margen solo existe cuando la
Los planes de continuidad del negocio se ponen a prueba periódicamente y se ajustan en función de los fallos detectados.
Una limitación es que una parte significativa de los datos empíricos utilizados proviene de informes.
estudios sectoriales desarrollados por empresas privadas, con diferentes muestras y metodologías, lo que impide
No se recomiendan las comparaciones directas y se aconseja precaución al generalizar los resultados. Para futuras investigaciones, se sugiere...
Los planes futuros incluyen realizar estudios empíricos con organizaciones brasileñas para evaluar la relación entre
Madurez en la respuesta a incidentes, tiempo de recuperación y cumplimiento de los plazos reglamentarios.
así como investigaciones sobre la aplicación de la cadena de custodia a los rastros digitales en incidentes
corporativo. Estos estudios nos permitirían verificar, en un contexto nacional, la hipótesis central que se está respaldando.
en este trabajo.

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: 06/05/2026 | Aceptación: 09/06/2026 | Publicación: 11/07/2026

REFERENCIAS

AHMAD, Atif; HADGKISS, Justin; RUIGHAVER, AB Equipos de respuesta a incidentes: desafíos en el apoyo a la función de seguridad organizacional. Computers & Security, [Ámsterdam], vol. 31, n.º 5, págs. 643-652, 2012.

AHMAD, Atif; MAYNARD, Sean B.; SHANKS, Graeme. Análisis de un caso sobre sistemas de información y respuestas a incidentes de seguridad. International Journal of Information Management, [Ámsterdam], vol. 35, n.º 6, págs. 717-723, 2015. DOI: 10.1016/j.ijinfomgt.2015.08.001.

AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS (ANPD). Resolución CD/ANPD N° 15, de 24 de abril de 2024. Aprueba el Reglamento de Notificación de Incidentes de Seguridad. Brasilia, DF: ANPD, 2024.

BASKERVILLE, Richard; SPAGNOLETTI, Paolo; KIM, Jongwoo. Seguridad de la información centrada en incidentes: gestión de un equilibrio estratégico entre prevención y respuesta. Information & Management, [Ámsterdam], vol. 51, n.º 1, págs. 138-151, 2014. DOI: 10.1016/j.im.2013.11.004.

BLOUNT, Joseph A. Testimonio de Joseph A. Blount, Jr., Presidente y Director Ejecutivo de Colonial Pipeline Company, ante el Comité de Seguridad Nacional y Asuntos Gubernamentales del Senado de los Estados Unidos. Washington, D.C.: Senado de los Estados Unidos, 8 de junio de 2021.

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.

BRASIL. Ley N° 13.964, de 24 de diciembre de 2019. Mejora la legislación penal y procesal penal. Brasilia, DF: Presidencia de la República, 2019.

BREZINSKI, Dominique; KILLALEA, Tom. Directrices para la recopilación y el archivo de pruebas. RFC 3227. [S. l.]: Grupo de Trabajo de Ingeniería de Internet, 2002.

CASEY, Eoghan. Pruebas digitales y delitos informáticos: ciencia forense, ordenadores e internet. 3.ª ed. Waltham: Academic Press, 2011.

CICHONSKI, Paul; MILLAR, Tom; GRANCE, Tim; SCARFONE, Karen. Guía para el manejo de incidentes de seguridad informática. Gaithersburg: Instituto Nacional de Estándares y Tecnología, 2012. (Publicación especial NIST 800-61, rev. 2). DOI: 10.6028/NIST.SP.800-61r2.

AGENCIA DE CIBERSEGURIDAD Y SEGURIDAD DE INFRAESTRUCTURAS (CISA) y otros. Guía #StopRansomware. Washington, DC: CISA, 2023.

ENDSLEY, Mica R. Hacia una teoría de la conciencia situacional en sistemas dinámicos. Human Factors, [Thousand Oaks], vol. 37, n.º 1, págs. 32-64, 1995. DOI: 10.1518/001872095779049543.

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

GRANCE, Tim; NOLAN, Tamara; BURKE, Kristin; DUDLEY, Rich; WHITE, Gregory; GOOD, Travis. Guía para programas de pruebas, capacitación y ejercicios para planes y capacidades de TI. Gaithersburg: Instituto Nacional de Estándares y Tecnología, 2006. (Publicación especial NIST 800-84).

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: 06/05/2026 | Aceptación: 09/06/2026 | Publicación: 11/07/2026

GREENBERG, Andy. La historia jamás contada de NotPetya, el ciberataque más devastador de la historia. Wired, San Francisco, 22 de agosto de 2018.

HUTCHINS, Eric M.; CLOPPERT, Michael J.; AMIN, Rohan M. Defensa de redes informáticas basada en inteligencia, informada a partir del análisis de campañas adversarias y cadenas de ataque de intrusión. Bethesda: Lockheed Martin Corporation, 2011.

IBM. Informe sobre el coste de una filtración de datos (2025). Armonk: IBM Corporation, 2025.

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN (ISO). ISO/IEC 27037: Tecnología de la información, técnicas de seguridad, directrices para la identificación, recopilación, adquisición y preservación de pruebas digitales. Ginebra: ISO, 2012.

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN (ISO). ISO 22301: Seguridad y resiliencia, sistemas de gestión de la continuidad del negocio, requisitos. Ginebra: ISO, 2019.

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN (ISO). ISO/IEC 27035-1: Tecnología de la información, gestión de incidentes de seguridad de la información, parte 1, principios y proceso. Ginebra: ISO, 2023.

KENT, Karen; CHEVALIER, Suzanne; GRANCE, Tim; DANG, Hung. Guía para la integración de técnicas forenses en la respuesta a incidentes. Gaithersburg: Instituto Nacional de Estándares y Tecnología, 2006. (Publicación especial NIST 800-86).

MANDIANT. M-Trends 2025. Mountain View: Google Cloud, 2025.

MANDIANT. M-Trends 2026. Mountain View: Google Cloud, 2026.

INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA (NIST). Marco de Ciberseguridad (CSF) 2.0 del NIST. Gaithersburg: NIST, 2024. (Documento técnico sobre ciberseguridad del NIST n.º 29). DOI: 10.6028/NIST.CSWP.29.

NELSON, Alexander; REKHI, Sanjay; SOUPPAYA, Murugiah; SCARFONE, Karen. 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). DOI: 10.6028/NIST.SP.800-61r3.

ROSS, Ron; PILLITTERI, Victoria; GRAUBART, Richard; BODEAU, Deborah; MCQUAID, Rosalie. Desarrollo de sistemas ciberresistentes: un enfoque de ingeniería de seguridad de sistemas. Gaithersburg: Instituto Nacional de Estándares y Tecnología, 2021. (Publicación especial 800- del NIST) 160, vol. 2, rev. 1). DOI: 10.6028/NIST.SP.800-160v2r1.

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

SOPHOS. El estado del ransomware en 2024. Abingdon: Sophos, 2024a.

SOPHOS. El impacto de las copias de seguridad comprometidas en los resultados del ransomware. Abingdon: Sophos, 2024b.

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: 06/05/2026 | Aceptación: 09/06/2026 | Publicación: 11/07/2026

STROM, Blake E.; APPLEBAUM, Andy; MILLER, Doug P.; NICKELS, Kathryn C.; PENNINGTON, Adam G.; THOMAS, Cody B. MITER ATT&CK: diseño y filosofía.
McLean: The MITER Corporation, 2018.

SWANSON, Marianne; BOWEN, Pauline; PHILLIPS, Amy Wohl; GALLUP, Dean; LYNES, David.
Guía de planificación de contingencias para sistemas de información federales. Gaithersburg: Instituto Nacional de Estándares y Tecnología, 2010. (Publicación especial NIST 800-34, rev. 1). DOI: 10.6028/NIST.SP.800-34r1.

TØNDEL, Inger Anne; LINE, Maria B.; JAATUN, Martin Gilje. Gestión de incidentes de seguridad de la información: práctica actual según lo reportado en la literatura. Computers & Security, [Ámsterdam], vol. 45, págs. 42-57, 2014.

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. Comisión de Bolsa y Valores (SEC). Gestión de riesgos, estrategia, gobernanza y divulgación de incidentes de ciberseguridad. Comunicado n.º 33-11216. Washington, D.C.: SEC, 2023.

VAN DER KLEIJ, Rick; KLEINHUIS, Geert; JOVEN, Heather. Efectividad del equipo de respuesta a incidentes de seguridad informática: una evaluación de necesidades. Fronteras de la Psicología, Lausana, v. 8, art. 2179, 2017. DOI: 10.3389/fpsyg.2017.02179.

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

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.