¿Qué es la ciberseguridad?

La ciberseguridad se refiere a todas las tecnologías, prácticas y políticas para prevenir los [ciberataques](https://www.ibm.com/es-es/topics/cyber-attack) o mitigar su impacto. La ciberseguridad tiene como objetivo proteger los sistemas informáticos, las aplicaciones, los dispositivos, los datos, los activos financieros y las personas contra el [ransomware](https://www.ibm.com/es-es/topics/ransomware" \t "_self) y otros [malware](https://www.ibm.com/es-es/topics/malware), las estafas de [phishing](https://www.ibm.com/es-es/topics/phishing), el robo de datos y otras ciberamenazas.

A nivel empresarial, la ciberseguridad es un componente clave de la estrategia general de [gestión de riesgos](https://www.ibm.com/es-es/topics/risk-management) de una organización. Según Cybersecurity Ventures, el gasto mundial en productos y servicios de ciberseguridad superará los 1,75 billones de dólares en total entre 2021 y 2025.1

El crecimiento del empleo en ciberseguridad también es sólido. La Oficina de Estadísticas Laborales de EE. UU. prevé que "el empleo de analistas de seguridad de la información crecerá un 32 % de 2022 a 2032, más rápido que la media de todas las ocupaciones"2.

[Informe](https://www.ibm.com/account/reg/signup?formid=urx-52913" \t "_blank)

[Informe sobre el coste de la vulneración de datos](https://www.ibm.com/account/reg/signup?formid=urx-52913" \t "_blank)

[Obtenga información esencial para ayudar a sus equipos de seguridad y TI a gestionar mejor el riesgo y limitar las posibles pérdidas.](https://www.ibm.com/account/reg/signup?formid=urx-52913" \t "_blank)

[Descargue el informe](https://www.ibm.com/account/reg/signup?formid=urx-52913)

Por qué es importante la ciberseguridad

La ciberseguridad es importante porque los ciberataques y la ciberdelincuencia tienen el poder de interrumpir, dañar o destruir empresas, comunidades y vidas. Los ciberataques que tienen éxito conducen a robo de identidades, extorsión personal y corporativa, pérdida de información confidencial y datos cruciales para la empresa, interrupciones temporales de la actividad, pérdida de negocios y clientes y, en algunos casos, cierres de empresas.

Los ciberataques tienen un impacto enorme y creciente en las empresas y la economía. Según una estimación, la ciberdelincuencia costará a la economía mundial 10,5 billones de dólares al año de aquí a 20253.El coste de los ciberataques sigue aumentando a medida que los ciberdelincuentes se vuelven más sofisticados.

Según el último [*informe "Cost of a Data Breach"*](https://www.ibm.com/es-es/reports/data-breach) de IBM:

* El coste medio de una vulneración de datos pasó de 4,45 millones de dólares a 4,88 millones de dólares en 2023, lo que supone un aumento del 10 % y el mayor incremento desde la pandemia.
* Las pérdidas comerciales (pérdida de ingresos debido al tiempo de inactividad del sistema, pérdida de clientes y daño a la reputación) y los costes de respuesta posteriores a la vulneración (costes para configurar call centers y servicios de monitorización de crédito para los clientes afectados o para pagar multas reglamentarias), aumentaron casi un 11 % con respecto al año anterior.
* El número de organizaciones que pagaron más de 50 000 dólares en multas reglamentarias como resultado de una vulneración de datos aumentó un 22,7 % con respecto al año anterior; las que pagaron más de 100 000 dólares aumentaron un 19,5 %.

Retos en materia de ciberseguridad

Aparte del gran volumen de ciberataques, uno de los mayores desafíos para los profesionales de la ciberseguridad es la naturaleza en constante evolución del panorama de la tecnología de la información (TI) y la forma en que las amenazas evolucionan con él. Muchas tecnologías emergentes que ofrecen nuevas y enormes ventajas para las empresas y las personas también presentan nuevas oportunidades para que los actores de amenazas y los ciberdelincuentes lancen ataques cada vez más sofisticados. Por ejemplo:

* **La adopción generalizada del cloud computing** puede aumentar la complejidad de la gestión de redes y elevar el riesgo de errores de configuración en la nube, de API mal protegidas y de otras vías que los piratas informáticos pueden explotar.
* **Más teletrabajo, trabajo híbrido y**[**políticas de**](https://www.ibm.com/es-es/topics/byod)**"bring your own device" (BYOD)**significan más conexiones, dispositivos, aplicaciones y datos que los equipos de seguridad deben proteger.
* **La proliferación**[**del Internet de las cosas (IoT)**](https://www.ibm.com/es-es/topics/internet-of-things)**y los dispositivos conectados,** muchos de los cuales no son seguros o están mal protegidos por defecto, pueden facilitar el secuestro por parte por malos actores.
* **El auge de la**[**inteligencia artificial (IA),**](https://www.ibm.com/es-es/topics/artificial-intelligence)**y de la**[**IA generativa**](https://www.ibm.com/es-es/topics/generative-ai)en particular, presenta un panorama de amenazas completamente nuevo que los piratas informáticos ya están explotando mediante la inyección de prompts y otras técnicas. Según una investigación reciente del IBM Institute for Business Value, [solo el 24 % de las iniciativas de IA generativa están protegidas](https://www.ibm.com/thought-leadership/institute-business-value/report/securing-generative-ai).

A medida que la superficie de ataque mundial se amplía, el personal de ciberseguridad se esfuerza por seguir el ritmo. Un estudio del Foro Económico Mundial descubrió que la brecha global de trabajadores en ciberseguridad (la diferencia entre los trabajadores de ciberseguridad y los puestos de trabajo que necesitan cubrirse) podría alcanzar los 85 millones de trabajadores en 20304.

La eliminación de este déficit de competencias puede tener un impacto. Según el *informe "Cost of a Data Breach" de 2024*, las organizaciones que sufren una escasez de habilidades de seguridad de alto nivel tuvieron un coste medio por infracción de 5,74 millones de dólares, frente a los 3,98 millones de dólares de las organizaciones con escasez de competencias de menor nivel.

Los equipos de seguridad, con recursos limitados, recurrirán cada vez más a tecnologías de seguridad que incluyan análisis avanzados, inteligencia artificial (IA) y automatización para reforzar sus ciberdefensas y minimizar el impacto de los ataques que tengan éxito.

Tipos de ciberseguridad

Las estrategias integrales de ciberseguridad protegen todas las capas de la infraestructura de TI de una organización contra las ciberamenazas y el cibercrimen. Algunos de los ámbitos más importantes de la ciberseguridad son:

* **Seguridad de la IA**
* **Seguridad de infraestructura crítica**
* **Seguridad de red**
* **Seguridad de punto final**
* **Seguridad de aplicaciones**
* **Seguridad en la nube**
* **Seguridad de la información**
* **Seguridad móvil**

Seguridad de la IA

[La seguridad de la IA](https://www.ibm.com/es-es/think/topics/ai-security) hace referencia a las medidas y la tecnología destinadas a prevenir o mitigar las ciberamenazas y los ciberataques dirigidos contra aplicaciones o sistemas de IA o que utilizan la IA de forma maliciosa.

La IA generativa ofrece a los actores de amenazas nuevos vectores de ataque para explotar. Los piratas informáticos pueden usar prompts maliciosos para manipular aplicaciones de IA, envenenar las fuentes de datos para distorsionar los resultados de la IA e incluso engañar a las herramientas de IA para que compartan información confidencial. También pueden utilizar (y ya han utilizado) la IA generativa para crear código malicioso y correos electrónicos de phishing.

La seguridad de la IA utiliza [marcos de gestión de riesgos](https://www.ibm.com/es-es/blog/ai-risk-management/) especializados (y, cada vez más, herramientas de ciberseguridad habilitadas para la IA) para proteger la superficie de ataque de la misma. Según el *informe "Cost of a Data Breach" de 2024*, las organizaciones que implementaron ampliamente herramientas de seguridad y automatización habilitadas para la IA para la prevención de ciberamenazas registraron un coste medio por infracción 2,2 millones de dólares inferior al de las organizaciones que no implementaron IA.

Seguridad de las infraestructuras críticas

La seguridad crítica de la infraestructura protege los sistemas informáticos, las aplicaciones, las redes, los datos y los activos digitales que una sociedad depende de la seguridad nacional, la salud económica y la seguridad pública.

En Estados Unidos, el Instituto Nacional de Estándares y Tecnología (NIST) ofrece un marco de ciberseguridad para ayudar a los proveedores de TI y a las partes interesadas a proteger las infraestructuras cruciales5. La Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) del Departamento de Seguridad Nacional de los Estados Unidos también proporciona orientación6.

Seguridad de la red

La [seguridad de la red](https://www.ibm.com/es-es/topics/network-security) se centra en impedir el acceso no autorizado a las redes y los recursos de la red. También ayuda a garantizar que los usuarios autorizados tengan un acceso seguro y fiable a los recursos y activos que necesitan para realizar su trabajo.

Seguridad de las aplicaciones

La seguridad de las aplicaciones ayuda a evitar el acceso y el uso no autorizados de las aplicaciones y los datos relacionados. También ayuda a identificar y mitigar fallos o vulnerabilidades en el diseño de aplicaciones. Los métodos modernos de desarrollo de aplicaciones, como [DevOps](https://www.ibm.com/es-es/topics/devops) y [DevSecOps](https://www.ibm.com/es-es/topics/devsecops), incorporan pruebas de seguridad y seguridad en el proceso de desarrollo.

Seguridad en la nube

La [seguridad en la nube](https://www.ibm.com/es-es/topics/cloud-security) protege los servicios y activos basados en la nube de una organización, incluidos aplicaciones, datos, servidores virtuales y otras infraestructuras.

En términos generales, la seguridad en la nube funciona según el modelo de responsabilidad compartida. El proveedor de servicios en la nube es responsable de proteger los servicios que ofrece y la infraestructura que los suministra. El cliente es responsable de proteger sus datos, código y otros activos que almacena o ejecuta en la nube.

Seguridad de la información y seguridad de datos

La [seguridad de la información (InfoSec)](https://www.ibm.com/es-es/topics/information-security) protege la información importante de una organización (archivos y datos digitales, documentos en papel, medios físicos) contra el acceso, el uso o la alteración no autorizados.

La [seguridad de datos](https://www.ibm.com/es-es/topics/data-security), la protección de la información digital, es un subconjunto de la seguridad de la información y el enfoque de la mayoría de las medidas de InfoSec relacionadas con la ciberseguridad.

Seguridad móvil

La [seguridad móvil](https://www.ibm.com/es-es/topics/mobile-security) abarca herramientas y prácticas de ciberseguridad específicas de los smartphones y otros dispositivos móviles, incluida la gestión de aplicaciones móviles (MAM) y la gestión de movilidad empresarial (EMM).

Más recientemente, las organizaciones están adoptando soluciones de [gestión unificada de endopoints (UEM)](https://www.ibm.com/es-es/topics/uem) que les permiten proteger, configurar y gestionar todos los dispositivos de endpoints, incluidos los dispositivos móviles, desde una única consola.

Amenazas comunes de ciberseguridad

Algunos de los tipos más comunes de ciberamenazas incluyen

* **Malware**
* **Ransomware**
* **Phishing**
* **Robo y abuso de credenciales**
* **Amenazas internas**
* **Ataques de IA**
* **Cryptojacking**
* **Denegación de servicio distribuido (DDoS)**

Malware

El malware, abreviatura de "software malicioso", es cualquier código de software o programa informático que se escribe de manera intencionada para dañar un sistema informático o a sus usuarios. Casi todos los [ciberataques](https://www.ibm.com/es-es/topics/cyber-attack) modernos implican algún tipo de malware.

Los piratas informáticos y los ciberdelincuentes crean y utilizan malware para obtener acceso no autorizado a sistemas informáticos y datos confidenciales, secuestrar sistemas informáticos y operarlos de forma remota, interrumpir o dañar sistemas informáticos o tomar como rehenes datos o sistemas a cambio de grandes sumas de dinero (consulte "Ransomware").

[Más información sobre malware](https://www.ibm.com/es-es/topics/malware)

Ransomware

El ransomware es un tipo de malware que encripta los datos o el dispositivo de una víctima y amenaza con mantenerlos encriptados, o algo peor, a menos que la víctima pague un rescate al atacante.

Los primeros ataques de ransomware exigían un rescate a cambio de la clave de cifrado necesaria para desbloquear los datos de la víctima. A partir de 2019, casi todos los ataques de ransomware fueron ataques de *doble extorsión* que también amenazaban con compartir públicamente los datos de las víctimas; algunos ataques de *triple extorsión* añadieron la amenaza de un ataque de denegación de servicio distribuido (DDoS).

Más recientemente, los ataques de ransomware están disminuyendo. Según el [*IBM X-Force Threat Intelligence Index de 2024*](https://www.ibm.com/es-es/reports/threat-intelligence), los ataques de ransomware representaron el 20 % de todos los ataques en 2023, un 11,5 % menos que en 2022. Es probable que el descenso sea el resultado de una mejor prevención del ransomware, una intervención más eficaz de las fuerzas del orden y unas prácticas de copia de seguridad y protección de datos que permiten a las empresas recuperarse sin pagar el rescate.

Mientras tanto, los atacantes de ransomware han reutilizado sus recursos para poner en marcha otros tipos de ciberamenazas, como el malware *infostealer*, que permite a los atacantes robar datos y mantenerlos como rehenes sin bloquear los sistemas de la víctima, y los ataques de *destrucción de datos*, que destruyen o amenazan con destruir datos con fines específicos.

[Más información sobre ransomware](https://www.ibm.com/es-es/topics/ransomware)

Phishing

Los ataques de phishing son mensajes de correo electrónico, texto o voz que engañan a los usuarios para que descarguen malware, compartan información confidencial o envíen fondos a las personas equivocadas.

La mayoría de los usuarios están familiarizados con las estafas de phishing masivo: mensajes fraudulentos enviados en masa por correo electrónico que parecen proceder de una marca importante y de confianza, en los que se pide a los destinatarios que restablezcan sus contraseñas o vuelvan a introducir los datos de sus tarjetas de crédito. Las estafas de phishing más sofisticadas, como el [spear phishing](https://www.ibm.com/es-es/topics/spear-phishing) y el [correo electrónico empresarial comprometido (BEC)](https://www.ibm.com/es-es/topics/business-email-compromise), se dirigen a personas o grupos específicos para robar datos especialmente valiosos o grandes sumas de dinero.

El phishing es solo un tipo de [ingeniería social](https://www.ibm.com/es-es/topics/social-engineering), una clase de tácticas y ataques de "hacking humano" que utilizan la manipulación psicológica para presionar a las personas para que realicen acciones imprudentes.

[Más información sobre el phishing](https://www.ibm.com/es-es/topics/phishing)

Robo de credenciales y abuso de cuentas

El *X-Force Threat Intelligence Index*descubrió que los ataques basados en la identidad, que secuestran cuentas de usuario legítimas y abusan de sus privilegios, representan el 30 % de los ataques. Esto convierte a los ataques basados en la identidad en el punto de entrada más común a las redes corporativas.

Los piratas informáticos tienen muchas técnicas para robar credenciales y apoderarse de las cuentas. Por ejemplo, los ataques de kerberoasting manipulan el protocolo de autenticación Kerberos que se usa habitualmente en Microsoft Active Directory para apoderarse de cuentas de servicio con privilegios. En 2023, el [equipo de IBM X-Force experimentó](https://www.ibm.com/es-es/reports/threat-intelligence) un aumento del 100 % en los incidentes de kerberoasting.

Del mismo modo, el equipo de X-Force observó un aumento del 266 % en el uso de malware infostealer, que registra en secreto las credenciales de los usuarios y otros datos confidenciales.

[Leer más sobre kerberoasting](https://www.ibm.com/es-es/topics/kerberoasting)

Amenazas internas

Las amenazas internas se originan con usuarios autorizados (empleados, contratistas, business partners) que, de forma intencionada o accidental, hacen un uso indebido de su acceso legítimo o cuyas cuentas son secuestradas por ciberdelincuentes.

Las amenazas internas pueden ser más difíciles de detectar que las amenazas externas porque tienen las características de una actividad autorizada y son invisibles para el software antivirus, los firewalls y otras soluciones de seguridad que bloquean ataques externos.

[Más información sobre las amenazas internas](https://www.ibm.com/es-es/topics/insider-threats)

Ataques de IA

Al igual que los profesionales de la ciberseguridad utilizan la IA para reforzar sus defensas, los ciberdelincuentes la utilizan para llevar a cabo ataques avanzados.

En el fraude con [IA generativa](https://www.ibm.com/es-es/topics/generative-ai), los estafadores utilizan ésta para producir correos electrónicos, aplicaciones y otros documentos comerciales falsos para engañar a las personas para que compartan datos confidenciales o envíen dinero.

El *X-Force Threat Intelligence Index*informa que los estafadores pueden utilizar herramientas de IA generativa de código abierto para crear correos electrónicos de suplantación de identidad convincentes en tan solo cinco minutos. A modo de comparación, los estafadores tardan 16 horas en idear el mismo mensaje de forma manual.

Los piratas informáticos también están utilizando las herramientas de IA de las organizaciones como vectores de ataque. Por ejemplo, en los ataques de inyección de prompts, los actores de amenazas utilizan entradas maliciosas para manipular los sistemas de IA generativa y filtrar datos confidenciales, difundir información errónea o algo peor.

[Leer más sobre la inyección de prompts](https://www.ibm.com/es-es/topics/prompt-injection)

Criptojacking

El criptojacking se produce cuando los piratas informáticos acceden a un dispositivo de endpoint y utilizan en secreto sus recursos informáticos para minar criptomonedas como bitcoin, ether o monero.

Los analistas de seguridad identificaron el criptojacking como una ciberamenaza alrededor de 2011, poco después de la introducción de las criptomonedas. Según el *IBM X-Force Threat Intelligence Index*, el criptojacking se encuentra ahora entre las tres principales áreas de operaciones de los ciberdelincuentes.

Denegación de servicio distribuido (DDoS)

Un ataque DDoS intenta colapsar un servidor, un sitio web o una red sobrecargándolos de tráfico, normalmente procedente de una botnet, una red de sistemas distribuidos que secuestra mediante el uso de malware y operaciones remotas controladas.

El volumen global de ataques DDoS se disparó durante la pandemia de COVID-19. Cada vez más, los atacantes combinan ataques DDoS con ataques de ransomware, o simplemente amenazan para lanzar ataques DDoS a menos que el objetivo pague un rescate.

[Más información sobre los ataques DDoS](https://www.ibm.com/es-es/topics/ddos)

Mitos sobre la ciberseguridad

A pesar del volumen cada vez mayor de incidentes de ciberseguridad en todo el mundo y de los conocimientos obtenidos al resolver estos incidentes, persisten algunas ideas erróneas. Algunas de las más peligrosas incluyen:

Las contraseñas seguras son una protección adecuada

Las contraseñas seguras marcan la diferencia; por ejemplo, una contraseña de 12 caracteres tarda 62 billones de veces más en descifrarse que una de 6 caracteres. Pero las contraseñas son relativamente fáciles de adquirir de otras formas, como a través de la ingeniería social, el malware de keylogging, comprándolas en la dark web o pagando a personas internas descontentas para que las roben.

La mayoría de los riesgos de ciberseguridad son bien conocidos

De hecho, el panorama de las ciberamenazas está en constante cambio. Cada año se notifican miles de nuevas vulnerabilidades en aplicaciones y dispositivos nuevos y antiguos. Las oportunidades de cometer errores humanos (específicamente por parte de empleados o contratistas negligentes que, sin querer, provocan una vulneración de datos) siguen aumentando.

Todos los vectores de ciberataque están contenidos

Los ciberdelincuentes encuentran continuamente nuevos vectores de ataque. El auge de las tecnologías de IA, la tecnología operativa (OT), los dispositivos de Internet de las cosas (IoT) y los entornos de nube brindan a los piratas informáticos nuevas oportunidades de causar problemas.

Mi sector es seguro

Cada sector tiene su parte de riesgos de ciberseguridad. Por ejemplo, los ataques de ransomware se dirigen a más sectores que nunca, incluidos los gobiernos locales, las organizaciones sin fines de lucro y los proveedores sanitarios. También han aumentado los ataques contra las cadenas de suministro, los sitios web ".gov" y las infraestructuras críticas.

Los ciberdelincuentes no atacan a las pequeñas empresas

Sí lo hacen. El*Hiscox Cyber Readiness Report* reveló que casi la mitad (41 %) de las pequeñas empresas estadounidenses sufrieron un ciberataque el año pasado7.

Buenas prácticas y tecnologías clave de ciberseguridad

Aunque la estrategia de ciberseguridad de cada organización difiere, muchas utilizan estas herramientas y tácticas para reducir vulnerabilidades, prevenir ataques e interceptar ataques en curso:

* **Formación sobre concienciación sobre seguridad**
* **Herramientas de seguridad de datos**
* **Gestión de identidad y acceso**
* **Detección y respuesta a amenazas**
* **Recuperación ante desastres**

Formación sobre concienciación en materia de seguridad

La formación sobre concienciación en materia de seguridad ayuda a los usuarios a comprender cómo las acciones aparentemente inofensivas (desde el uso de la misma contraseña simple para varios inicios de sesión hasta compartir en exceso en redes sociales) aumentan su propio riesgo de ataque o el de su organización.

En combinación con políticas de [seguridad de datos](https://www.ibm.com/es-es/topics/data-security) bien pensadas, la formación sobre concienciación en materia de seguridad puede ayudar a los empleados a proteger los datos confidenciales personales y de la organización. También puede ayudarles a reconocer y evitar ataques de phishing y malware.

Herramientas de seguridad de datos

Las herramientas de seguridad de datos, como las soluciones de [cifrado](https://www.ibm.com/es-es/topics/encryption) y [prevención de pérdida de datos](https://www.ibm.com/es-es/topics/data-loss-prevention) (DLP), pueden ayudar a detener las amenazas de seguridad en curso o mitigar sus efectos. Por ejemplo, las herramientas DLP pueden detectar y bloquear los intentos de robo de datos, mientras que el cifrado puede hacer que cualquier dato que los piratas informáticos roben sea inútil para ellos.

Gestión de identidades y accesos

La [gestión de identidades y accesos (IAM)](https://www.ibm.com/es-es/topics/identity-access-management) hace referencia a las herramientas y estrategias que controlan cómo acceden los usuarios a los recursos y qué pueden hacer con esos recursos.

Las tecnologías de IAM pueden ayudar a protegerse contra el robo de cuentas. Por ejemplo, la [autenticación multifactor](https://www.ibm.com/es-es/topics/multi-factor-authentication) requiere que los usuarios proporcionen varias credenciales para iniciar sesión, lo que significa que los actores de amenazas necesitan algo más que una contraseña para acceder a una cuenta.

Del mismo modo, los sistemas de autenticación adaptativa detectan cuándo los usuarios tienen un comportamiento de riesgo y les plantean retos de autenticación adicionales antes de permitirles continuar. La autenticación adaptativa puede ayudar a limitar el [movimiento lateral](https://www.ibm.com/es-es/think/topics/lateral-movement) de los piratas informáticos que consiguen entrar en el sistema.

Una arquitectura [zero trust](https://www.ibm.com/es-es/topics/zero-trust) es una forma de aplicar controles de acceso estrictos mediante la verificación de todas las solicitudes de conexión entre usuarios y dispositivos, aplicaciones y datos.

Gestión de la superficie de ataque

La [gestión de la superficie de ataque (ASM)](https://www.ibm.com/es-es/topics/attack-surface-management) es el descubrimiento, el análisis, la corrección y la monitorización continuos de las vulnerabilidades de ciberseguridad y posibles vectores de ataque que conforman la [superficie de ataque](https://www.ibm.com/es-es/topics/attack-surface) de una organización.

A diferencia de otras disciplinas de ciberdefensa, la ASM se lleva a cabo completamente desde la perspectiva de un pirata informático en lugar de desde la perspectiva del defensor. Identifica objetivos y evalúa los riesgos en función de las oportunidades que presentan a un atacante malicioso.

Detección y respuesta a amenazas

Las tecnologías basadas en el análisis y la IA pueden ayudar a identificar ataques en curso y responder a ellos. Estas tecnologías pueden incluir [gestión de eventos e información de seguridad (SIEM)](https://www.ibm.com/es-es/topics/siem), [orquestación, automatización y respuesta de seguridad (SOAR)](https://www.ibm.com/es-es/topics/security-orchestration-automation-response) y [detección y respuesta de endpoints (EDR)](https://www.ibm.com/es-es/topics/edr). Normalmente, las organizaciones utilizan estas tecnologías como parte de un plan formal [de respuesta a incidentes](https://www.ibm.com/es-es/topics/incident-response).

Recuperación ante desastres

Las capacidades de [recuperación ante desastres](https://www.ibm.com/es-es/topics/disaster-recovery) pueden desempeñar un papel clave en el mantenimiento de la continuidad del negocio y la corrección de amenazas en caso de un ciberataque. Por ejemplo, la posibilidad de conmutar por error a una copia de seguridad alojada en una ubicación remota puede ayudar a una empresa a reanudar sus operaciones tras un ataque de ransomware (a veces sin tener que pagar un rescate)

Soluciones relacionadas

Servicios de ciberseguridad

Transforme su negocio y gestione el riesgo con servicios de consultoría de ciberseguridad, nube y seguridad gestionada.

[Explore los servicios de ciberseguridad](https://www.ibm.com/es-es/services/security)

Soluciones de seguridad y protección de datos

Proteja los datos en nubes híbridas, simplifique el cumplimiento normativo y aplique políticas de seguridad y controles de acceso en tiempo real.

[Explore las soluciones de seguridad y protección de datos](https://www.ibm.com/es-es/data-security)

Ciberseguridad de la inteligencia artificial (IA)

Mejore la velocidad, la precisión y la productividad de los equipos de seguridad con soluciones impulsadas por IA.

[Explore la ciberseguridad de la inteligencia artificial (IA)](https://www.ibm.com/es-es/ai-cybersecurity)

Servicios de detección y respuesta a amenazas

Su aliado contra las ciberamenazas, con el nuevo IBM Consulting Cybersecurity Assistant con IA y diseñado para acelerar y mejorar la identificación, investigación y respuesta a amenazas de seguridad críticas.