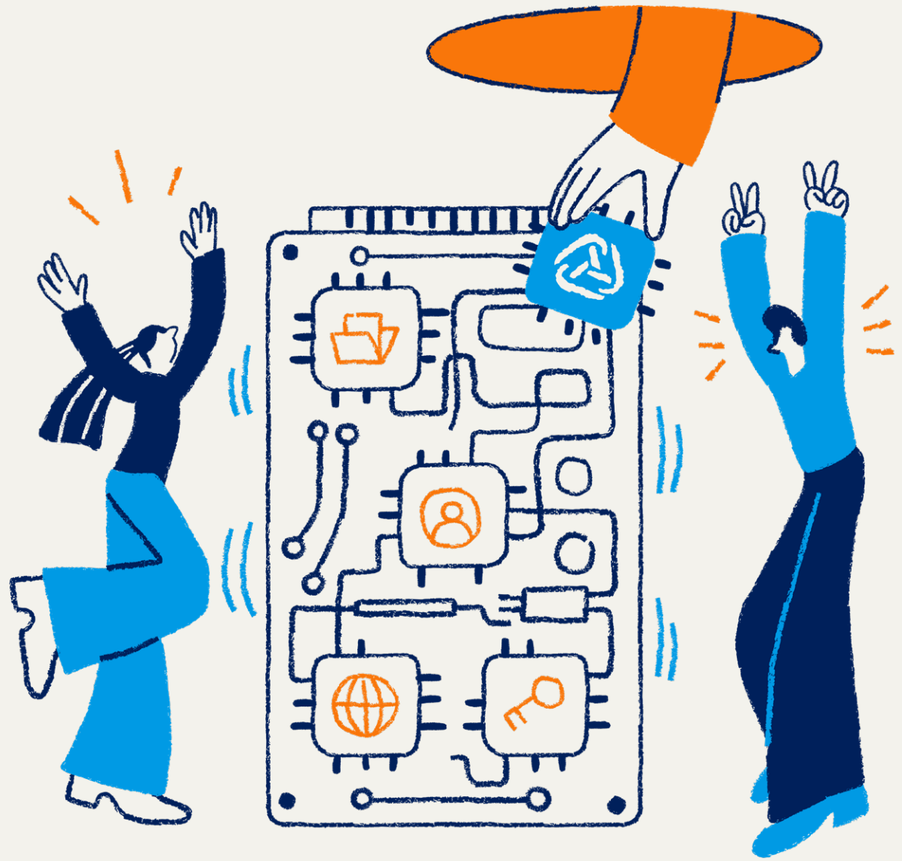
QBE Insurance

La nueva anatomía de las crisis cibernéticas



At the heart of it

Cómo los fallos en las dependencias, la concentración y los controles pueden convertir un incidente cibernético en una interrupción operativa

Tres conclusiones clave

1. La resiliencia cibernética depende de gestionar las dependencias críticas del negocio con el mismo rigor que los controles de ciberseguridad.

2. Vulnerabilidades ya conocidas están haciendo que los incidentes cibernéticos provoquen interrupciones cada vez más prolongadas de la actividad.

3. La capacidad de recuperación es, por sí misma, un factor clave para la resiliencia.

Principales conclusiones

La resiliencia cibernética ya no depende únicamente de la propia organización, sino también de todo el ecosistema tecnológico del que depende para operar. La creciente dependencia de proveedores de software, servicios en la nube y otras infraestructuras digitales críticas hace que buena parte de este riesgo quede fuera de su control directo. Por ello, la capacidad de una organización para resistir una interrupción y recuperar su actividad depende cada vez más de cómo gestiona los riesgos asociados a su red de proveedores y servicios.

Tres cambios que están redefiniendo el riesgo cibernético

1. **Rapidez:** Los atacantes pueden pasar del acceso inicial a la explotación en cuestión de minutos, en lugar de días. Esto deja a las organizaciones cada vez menos margen para detectar un incidente y responder a tiempo.
2. **Concentración:** Los sectores críticos dependen cada vez más de un número reducido de proveedores de servicios en la nube, plataformas de software y otros proveedores tecnológicos. Esto hace que una interrupción en uno de los principales proveedores pueda tener repercusiones en múltiples sectores y países.
3. **Convergencia:** La creciente integración entre las tecnologías de la información (IT), las tecnologías operativas (OT) y los dispositivos conectados amplía el posible impacto de los incidentes cibernéticos, que pueden llegar a afectar a operaciones físicas y servicios esenciales.

La tensión geopolítica intensifica la amenaza cibernética

Los conflictos en Europa y Oriente Medio han ido acompañados de un incremento de los ciberataques contra infraestructuras críticas, servicios públicos y grandes organizaciones, con el objetivo de alterar o interrumpir su actividad.

Al mismo tiempo, la guerra híbrida hace que la línea que separa el conflicto geopolítico de la actividad delictiva sea cada vez más difusa. Sectores estratégicos como la sanidad, el transporte, la logística y la tecnología se encuentran entre los principales objetivos. Un ejemplo se produjo a finales de 2025, cuando Rusia lanzó un ataque a gran escala contra el sector energético de Polonia en pleno invierno.

No todas las interrupciones tienen su origen en un ciberataque

Las interrupciones de Amazon Web Services en octubre de 2025 y de Cloudflare en noviembre de ese mismo año afectaron simultáneamente a plataformas bancarias, comercios, transportes y servicios públicos en distintos mercados. En ambos casos, un fallo en una infraestructura de la que dependían numerosos servicios terminó afectando a todos ellos. Por eso, la resiliencia debe abordarse de forma integral, independientemente de que una interrupción tenga su origen en un ciberataque o en un fallo de infraestructura.

Los gobiernos refuerzan su respuesta ante estas amenazas

Gobiernos y organismos reguladores están adoptando medidas para reforzar la seguridad de las cadenas de suministro, la resiliencia operativa, la notificación de incidentes y los planes de recuperación. La Unión Europea, Reino Unido y Canadá, por ejemplo, han aprobado recientemente legislación para reforzar los requisitos de supervisión de proveedores, las pruebas de los planes de recuperación y la notificación de incidentes.

Al mismo tiempo, la preocupación por la soberanía digital, la dependencia tecnológica y la competencia estratégica está dando lugar a nuevas restricciones en torno a la tecnología, los datos y la actividad digital transfronteriza.



Pymes: reforzar la resiliencia con menos recursos

Las grandes organizaciones se enfrentan a una creciente presión regulatoria y comercial para demostrar su resiliencia cibernética. Las pymes, sin embargo, suelen disponer de menos recursos para hacerlo, aunque dependen de muchas de las mismas tecnologías y cadenas de suministro.

Aumentar la concienciación y facilitar soluciones prácticas resulta clave. La resiliencia cibernética no siempre requiere grandes inversiones tecnológicas: medidas como la autenticación multifactor y unas copias de seguridad eficaces pueden ayudar considerablemente a reducir el impacto de un incidente.

Esta cuestión también afecta a las grandes organizaciones. Reforzar la resiliencia de los pequeños proveedores ayuda a proteger la continuidad de toda la cadena de suministro.

Cinco recomendaciones para reforzar la resiliencia

1. **Seguridad proactiva:** Implantar la autenticación multifactor (MFA) y corregir las vulnerabilidades.
2. **Gobernanza y responsabilidad:** Acordar el nivel de riesgo asumible con la alta dirección y designar a un único responsable.
3. **Análisis de dependencias:** Identificar de qué proveedores dependen los servicios críticos y establecer mecanismos de recuperación.
4. **Pruebas y ejercicios:** Poner a prueba los planes de recuperación y realizar simulacros con la participación de la alta dirección.
5. **Preparación y respuesta:** Contar de antemano con los recursos necesarios en materia forense, legal y de comunicación, y practicar la toma de decisiones ante posibles incidentes.

El valor del seguro de ciberriesgos va más allá de la cobertura

Las empresas no deberían considerar el seguro de ciberriesgos únicamente como un mecanismo de protección financiera que actúa después de un siniestro. También permite acceder a asesoramiento especializado antes, durante y después de un incidente.

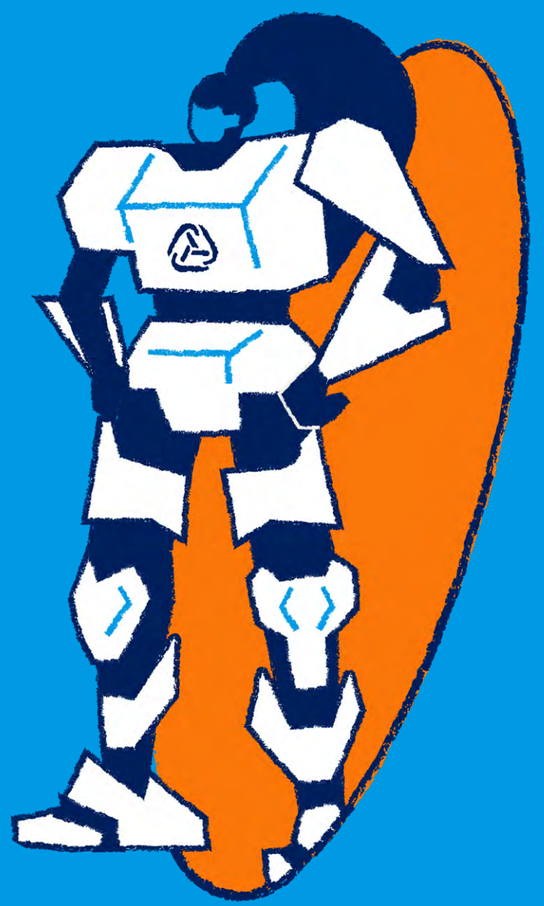
Corredores y aseguradoras pueden ayudar a las organizaciones a comprender mejor su exposición al riesgo, identificar aquellos ámbitos en los que conviene reforzar la resiliencia y aprovechar mejor los servicios especializados que tienen a su disposición.

Introducción: cuando la dependencia supera al control

A medida que aumenta el número de posibles puntos de acceso, la resiliencia cibernética se entrelaza cada vez más con la resiliencia de la empresa en general. Dado que las organizaciones dependen cada vez más de sistemas digitales interconectados, una ciberseguridad eficaz debe ir más allá de la prevención de ataques y abarcar la comprensión de cómo las interrupciones pueden propagarse por toda la empresa y con qué rapidez pueden recuperarse las operaciones críticas.

La mayoría de las organizaciones entienden que los ciberdelincuentes pueden causar una interrupción significativa de las actividades de la empresa. Lo que no se comprende tan bien es por qué esas mismas categorías de ataques tienen ahora un mayor impacto en las organizaciones afectadas que hace tres años. Una encuesta reciente del sector sugiere que el ransomware supone actualmente para la organización afectada media un coste de 24 días de inactividad operativa como consecuencia directa del ataque,[1] mientras que otra estimación señala que el tiempo de recuperación total en caso de incidentes graves alcanza, de media, entre tres y seis meses.[2 3]

La respuesta no está solo en la creciente capacidad de los atacantes, sino también en los cambios que se están produciendo en el entorno de las organizaciones, que debilitan sus defensas y amplían su superficie de ataque.
La amenaza cibernética para la continuidad del negocio está cada vez más ligada a la dependencia de sistemas digitales que las organizaciones no controlan por completo, pero sin los que no pueden operar. También depende de si estas dependencias se han identificado correctamente y de si existe una planificación adecuada para hacer frente a posibles interrupciones.



1 https://www.totalassure.com/blog/cost-of-downtime-after-a-cyber-attack-in-2026
2 https://www.accenture.com/en/insights/security/redefining-cyber-resilience
3 El tiempo de inactividad se refiere a las interrupciones del sistema, de la red o de las aplicaciones cuya causa es un incidente cibernético. La recuperación se refiere al proceso de restaurar los sistemas afectados a un estado seguro y operativo después de un incidente.

Tres cambios han contribuido a aumentar el impacto de las interrupciones y a ampliar la brecha entre la creciente dependencia de la tecnología y el control que las organizaciones ejercen sobre ella:

Rapidez

En los últimos años, los plazos de los ataques se han reducido considerablemente, lo que ha acortado el margen de tiempo de que disponen los defensores para detectar y contener los ataques. Es probable que este

> "Los atacantes pueden aprovechar una vulnerabilidad en tan solo 30 minutos"

cambio sea, en gran medida, resultado de la creciente disponibilidad de herramientas y plataformas de IA de vanguardia. Por ejemplo, una investigación reciente descubrió que una campaña basada en IA llevó a cabo un ataque coordinado y a escala, que a un operador humano le habría llevado unas dos semanas preparar, en menos de diez horas,[4] y otros informes indican que los ciberdelincuentes pueden pasar ahora del acceso inicial a la explotación en solo 30 minutos, en comparación con los aproximadamente 100 minutos de 2021.[5]

Concentración

En todos los sectores y lugares, las iniciativas de digitalización han fomentado la concentración de sistemas y funciones en infraestructuras conjuntas, con el objetivo de racionalizar y simplificar los activos digitales de la empresa. Por ejemplo, AWS, Azure y Google Cloud representaron casi dos tercios del gasto empresarial en redes en la nube en 2025.[6] A medida que se prioriza la velocidad de digitalización y la interoperabilidad sobre los controles, los servicios críticos dependen cada vez más de un pequeño número de proveedores de servicios en la nube, suites de software como servicio (SaaS), plataformas de identidad y proveedores de servicios gestionados (MSP), lo que aumenta la posibilidad de que una interrupción en un nodo crítico se propague por empresas y sectores.

> "La digitalización ha impulsado la concentración de los sistemas"

Convergencia

Los entornos de tecnologías de la información (IT), tecnologías operativas (OT) e Internet de las Cosas (IoT) están cada vez más interconectados, mientras que la gestión de identidades tiende a concentrarse en un único proveedor. Como consecuencia, una brecha de seguridad puede propagarse ahora entre entornos que antes funcionaban de forma independiente.

Esto hace que fallos de seguridad habituales, como la ausencia de autenticación multifactor (MFA), un servidor antiguo sin actualizar o una red sin segmentar, puedan extenderse con mayor rapidez y tener un impacto mucho mayor en toda la organización. De hecho, el 90 % de las brechas analizadas en investigaciones recientes se atribuyen a fallos evitables, como una visibilidad limitada de los sistemas, controles aplicados de forma inconsistente o un exceso de confianza en la gestión de identidades.[7]

La resiliencia falla cuando la dependencia ha superado al control; la concentración y la convergencia agravan la magnitud y la gravedad de la perturbación que se produce en consecuencia. Para desarrollar la resiliencia cibernética es necesario que las organizaciones tengan en cuenta ambos aspectos.

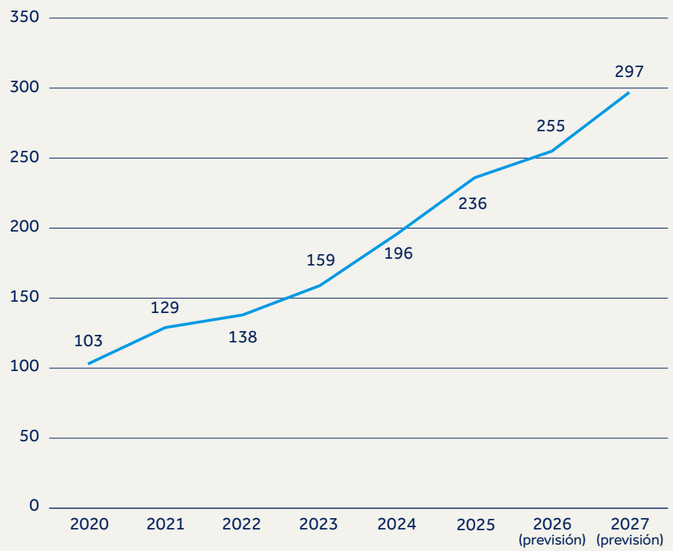
4 https://unit42.paloaltonetworks.com/ai-assisted-cyber-attack-inside-a-unit-42-investigation/
5 https://www.crowdstrike.com/en-us/press-releases/2026-crowdstrike-global-threat-report/
6 Synergy Research Group: AWS, Microsoft Azure y Google Cloud representaron el 63 % del gasto empresarial en servicios de infraestructura en la nube en el tercer trimestre de 2025. https://www.srgresearch.com/articles/cloud-market-share-trends-big-three-together-hold-63-while-oracle-and-the-neoclouds-inch-higher
7 https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report

Retos paralelos: intención de causar disrupción e impacto operativo

En los 14 mercados de QBE analizados (véase Alcance y notas), los incidentes han aumentado cada año desde 2023 y se prevé que vuelvan a aumentar en 2027.[9] Lo que ha cambiado no es solo el volumen, sino el impacto medio de los ataques que tienen éxito: mientras que hace tres años los incidentes solían causar unos días de interrupción, hoy en día es más probable que la interrupción sea prolongada porque hay una parte mucho mayor de la empresa que depende de los sistemas afectados.

Hay tres factores que explican esta evolución: un ecosistema delictivo consolidado que ha profesionalizado el acceso, las herramientas y la negociación; la fragmentación geopolítica y la actividad híbrida que difuminan la línea divisoria entre la acción estatal y la delictiva; y la industrialización de la inteligencia artificial, que probablemente está contribuyendo a acortar los plazos de los atacantes y facilitando que los ciberdelincuentes lleven a cabo ataques de ingeniería social convincentes. Por ejemplo, los investigadores han señalado que los correos electrónicos de phishing personalizados, automatizados y generados por IA tienen una tasa de clic del 54 %. Esto está a la par con el phishing personalizado generado por humanos (que requiere más tiempo y esfuerzo por parte del atacante), pero es significativamente inferior a los intentos genéricos elaborados por humanos, que lograron una tasa de clic del 12 %.[10]

Figura 1: Número de ciberincidentes con impacto significativo a nivel estratégico (2020-27)[11]



Fuente: Control Risks. Véase en Alcance y notas las regiones, metodología de datos y limitaciones

> "Los ciberataques no solo comprometen la información; paralizan las operaciones de las organizaciones y cuestan millones de media.[8] En casi todos los casos a los que respondemos, el factor decisivo no es lo sofisticada que fue la intrusión, sino cuánto dependía la empresa del sistema que dejó de funcionar y lo bien que la empresa había previsto y preparado la interrupción de dicho sistema"
>
> **Responsable de inteligencia de amenazas cibernéticas,** riesgos digitales, Control Risks

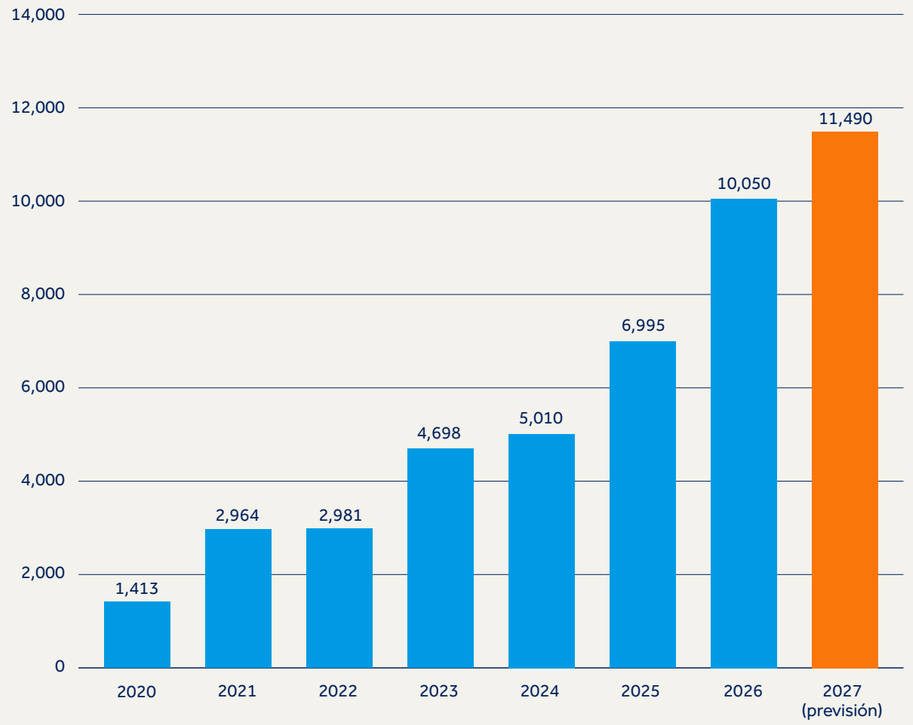
8 Por ejemplo, el informe Cost of Data Breach 2026 de IBM indica que el coste medio de una brecha de seguridad para las víctimas es de 4,99 millones de dólares, https://www.ibm.com/reports/data-breach
9 La cifra total en los 14 mercados
10 https://www.researchgate.net/publication/386374220_Evaluating_Large_Language_Models'_Capability_to_Launch_Fully_Automated_Spear_Phishing_Campaigns_Validated_on_Human_Subjects
11 Estos datos se basan en un conjunto seleccionado de incidentes que cumplen al menos uno de varios criterios, incluidos el tipo de organización atacada, el autor de la amenaza, la naturaleza y objetivos del ataque, y su impacto.

La extorsión criminal sigue predominando

El ransomware y la extorsión por filtración de datos siguen figurando entre las amenazas cibernéticas más costosas desde el punto de vista económico y con mayor potencial de causar trastornos a las que se enfrentan las organizaciones. Con el fin de maximizar el impacto, los autores de los actos de extorsión dan cada vez más prioridad a los proveedores externos conocidos, ya que la interrupción del servicio puede repercutir en múltiples clientes e intensificar la presión durante las negociaciones de extorsión. Las grandes empresas de los sectores de la fabricación, el comercio minorista, los servicios profesionales y las tecnologías de la información son objetivos habituales de operaciones ciberdelictivas disruptivas, en las que los autores se aprovechan de las cadenas de suministro interconectadas. Por ejemplo, se estima que el ataque de ransomware y extorsión por filtración de datos de 2024 contra Change Healthcare, un importante procesador de pagos sanitarios en EE. UU., ha causado más de 2000 millones de dólares en costes directos y daños indirectos.[12]

Según la investigación de Control Risks, el número de organizaciones afectadas que aparecen en webs de filtración de datos por ransomware aumentó un 611 % entre 2020 y 2026 y se prevé que aumente un 14 % en 2027.

Figura 2: Número de organizaciones afectadas que aparecen en webs de filtración de datos por ransomware a nivel mundial (2020-27)



Fuente: Datos de inteligencia e incidentes de Control Risks. Véase en Alcance y notas las regiones, metodología de datos y limitaciones

12 https://hyperproof.io/resource/understanding-the-change-healthcare-breach/

Pero las fricciones geopolíticas agravan el problema

La escalada de las tensiones geopolíticas en Europa y Oriente Medio ha coincidido con un aumento de las operaciones híbridas, incluidas las operaciones cibernéticas destinadas a interrumpir la actividad. Las actividades observadas en 2025 y 2026 han incluido ataques a infraestructuras críticas y marcas de gran repercusión, perpetrados por actores estatales como Rusia e Irán. En los 14 mercados de QBE incluidos en el análisis, es probable que dichos factores geopolíticos se mantengan a medio y largo plazo. Es probable que esto vaya acompañado de picos de actividad a corto plazo relacionados con acontecimientos programados, como las elecciones de mitad de legislatura de Estados Unidos en noviembre de 2026 y las elecciones francesas de 2027, en consonancia con los patrones de injerencia electoral que se han observado desde hace al menos una década. Como resultado, las empresas que tienen actividad en estas jurisdicciones seguirán enfrentándose a amenazas.

> "A finales de 2025, Rusia llevó a cabo un ataque a gran escala contra el sector energético polaco en pleno invierno."

Aunque ha aumentado su intención de interrumpir la actividad, los Estados siguen tratando de evitar que se les atribuyan directamente este tipo de acciones. Para ello, recurren cada vez más a grupos ciberdelincuentes y ciberactivistas como una vía indirecta para causar interrupciones en países adversarios. Aunque la mayoría de estos grupos no están bajo el control directo de los Estados, estos pueden alentarlos, incentivarlos o encargarles directamente operaciones alineadas con sus intereses. Por ejemplo, las reiteradas advertencias y medidas adoptadas por varios países europeos en 2026 muestran que Rusia ha incrementado considerablemente el uso de grupos ciberdelincuentes con base en el país como intermediarios para interrumpir la actividad de organizaciones públicas y privadas en sectores críticos como la sanidad, el transporte y la logística, así como entre proveedores de tecnologías de la información. información.[13] Aunque estos grupos siguen moviéndose principalmente por motivos económicos, el impacto de sus acciones y las interrupciones que provocan pueden contribuir a objetivos estratégicos más amplios en el marco de campañas de guerra híbrida.

Aunque es posible que las empresas en sí mismas no sean los objetivos principales de los ataques motivados por razones geopolíticas, es probable que los incidentes que afecten a proveedores clave de infraestructuras – como el sector energético o los proveedores de sistemas informáticos esenciales – tengan repercusiones en las fases posteriores de la cadena. Por ejemplo, a finales de 2025, Rusia llevó a cabo un ataque a gran escala contra el sector energético polaco en pleno invierno, lo que puso de manifiesto su intención de utilizar operaciones cibernéticas para afectar directamente a la vida de la población civil. Este tipo de incidentes de gran repercusión han sido, históricamente, poco habituales, pero es probable que sean cada vez más frecuentes, motivados tanto por la intención de causar trastornos como por la naturaleza interconectada de los sistemas afectados. Seguirán surgiendo amenazas similares por parte de ciberdelincuentes y ciberactivistas, cuyas capacidades están aumentando gracias al apoyo de actores estatales y al desarrollo de sistemas de inteligencia artificial cada vez más avanzados.

13 https://www.consilium.europa.eu/en/press/press-releases/2026/07/13/cyber-russia-statement-by-the-high-representative-on-behalf-of-the-european-union-denouncing-russia-s-malicious-cyber-ecosystem-targeting-the-eu-its-member-states-and-international-partners/; https://www.gov.uk/government/news/uk-and-eu-strike-russian-cyber-networks-with-new-sanctions; https://www.lovguiden.dk/en/det-offentlige/eu-udenrigstjenesten/2026-07-21-eu-advarer-fn-om-ruslands-cyberproxyer-og-ransomware-mod-sundhedssektoren; https://www.rbb24.de/politik/beitrag/2026/02/krankenhaeuser-berlin-hybride-bedrohungen-russland-cyberangriffe.html; https://therecord.media/ransomware-gangs-advancing-moscow-geopolitical-interests-warns-romania

La fragmentación geopolítica, un factor clave para planificar la resiliencia

La fricción geopolítica también ha favorecido cambios regulatorios, y los responsables políticos se centran en la soberanía digital, las restricciones tecnológicas y las limitaciones comerciales. Aquí se incluye el sector de la IA, donde Estados Unidos y China mantienen su pugna por el liderazgo tecnológico y del mercado global. A medida que los cambios normativos siguen afectando a los acuerdos de protección de datos, a los requisitos de localización y a la disponibilidad tecnológica, las empresas se ven cada vez más obligadas a incorporar las limitaciones normativas y los cambios en las políticas en su planificación de la resiliencia; por ejemplo, a la hora de evaluar proveedores alternativos para la redundancia y los retos de cumplimiento normativo más amplios que podrían surgir en un escenario de crisis.

Dado que es probable que las amenazas sistémicas disruptivas persistan, la resiliencia operativa dependerá de una combinación de la preparación de las empresas, los riesgos asociados a terceros y los marcos normativos nacionales.

Figura 3: Amenazas y nivel de preparación en los 14 mercados analizados

Mercados	Factores geopolíticos de las amenazas[14]	Nivel de preparación[15]
Países nórdicos, Alemania, Países Bajos, Francia, Reino Unido	Ataques de actores vinculados a Estados y grupos ciberactivistas asociados a las tensiones entre Rusia y la OTAN, incluidas las infraestructuras críticas	Contextos nacionales maduros, pero la exposición de la tecnología operativa y de las infraestructuras críticas está concentrada en unos pocos operadores
EE. UU. y Canadá	Gran volumen de ataques s de represalia vinculados a Irán relacionados con la intervención de EE. UU. en Oriente Medio	Mercado de respuesta y recuperación amplio, pero la capacidad es compartida
Australia, Nueva Zelanda, Singapur, Hong Kong	Aumento de la actividad vinculada al Estado y la presión para alinearse entre Washington y Pekín	Las expectativas normativas crecen más rápido que la capacidad de respuesta interna en varios mercados
España e Italia	La actividad de los ciberactivistas prorrusos se centra en el seguimiento de las posiciones políticas europeas, siendo Italia un objetivo habitual de ciberataques de baja intensidad	Grandes bases de proveedores de empresas más pequeñas con una madurez de seguridad desigual

Fuente: Análisis de inteligencia de Control Risks. Véase Alcance y notas para conocer las metodología de los datos y las limitaciones

14 Este resumen se basa en los datos, las pruebas y la evaluación de Control Risks sobre los principales factores geopolíticos de las ciberamenazas disruptivas en estas ubicaciones.
15 Este resumen se basa en la evaluación de Control Risks y en información de terceros sobre las consideraciones clave sobre la preparación en estas ubicaciones, tales como los marcos de resiliencia y preparación a nivel nacional, la madurez del mercado de ciberseguridad y la concentración/disponibilidad de proveedores, entre otros factores.

Fallos de infraestructura sin un atacante

No todas las interrupciones son malintencionadas. La interrupción del servicio de Amazon Web Services (AWS) en octubre de 2025[16] y la de Cloudflare en noviembre de 2025[17] provocaron un deterioro en el funcionamiento de las plataformas bancarias, minoristas, de transporte y de servicios públicos en múltiples mercados al mismo tiempo; en todos los casos debido a que un fallo en una dependencia compartida se propagó a todos los sistemas que se ejecutaban sobre ella. En ninguno de los dos casos intervino un adversario, y eso es precisamente lo que los hace tan reveladores: demuestran que el riesgo de concentración se materializa por sí solo, sin que nadie elija un objetivo. Incluso en el caso de una organización que no tuviera ningún contrato directo con ninguno de los dos proveedores, la consecuencia práctica podría ser la misma: sus proveedores se vieron afectados y el plazo de recuperación lo fijó otra entidad.



16 Análisis de Ookla/Downdetector sobre la interrupción de AWS US-EAST-1 del 20 de octubre de 2025: más de 17 millones de informes de usuarios en más de 60 países y más de 3500 empresas, con un impacto principal que duró aproximadamente 15 horas. https://www.ookla.com/articles/aws-outage-q4-2025
17 Interrupción de Cloudflare del 18 de noviembre de 2025: un fallo de configuración interna degradó los servicios de proxy y CDN a nivel mundial durante aproximadamente 3,5 horas, afectando a una parte sustancial del tráfico global de Internet. https://blog.cloudflare.com/18-november-2025-outage/

Los riesgos de concentración y las limitaciones de los proveedores elevan el riesgo

Figura 4: Dependencias tecnológicas

Dependencia tecnológica	Situación actual	Por qué es importante
Nube	AWS, Azure y Google Cloud representan casi dos tercios del gasto empresarial en infraestructura en la nube.[18]	El fallo de un proveedor genera una exposición correlacionada, no aislada, en todos los sectores y mercados.
Terceros	El porcentaje de brechas de seguridad que afectaron a un tercero se duplicó interanualmente en 2025, pasando del 15 % al 30 %.[19]	El proveedor, y no el perímetro, es ahora la vía de mayor crecimiento en.
Identidad	El acceso se consolida en proveedores únicos que abarcan entornos de sistemas informáticos, tecnología operativa y SaaS.	Una vulneración ahora traspasa dominios que anteriormente estaban separados.
IA	La implantación se ha centrado en un número reducido de modelos, a menudo sin controles de acceso básicos; según los datos, el 77 % de las empresas afirma que la implantación de la IA está avanzando más rápido que los controles.[20]	Se está integrando una nueva dependencia más rápido de lo que se está regulando.

Fuente: Análisis de Control Risks y datos de terceros

Los riesgos analizados en esta sección escapan al control directo de una única organización, pero determinan hasta dónde puede extenderse un incidente y cuánto tiempo puede llevar la recuperación. La creciente dependencia de proveedores comunes de servicios cloud, SaaS, gestión de identidades y servicios gestionados (MSP) hace que un fallo o una brecha de seguridad en un solo proveedor pueda afectar simultáneamente a todas las organizaciones que dependen de él, así como a aquellas cuyos propios proveedores utilizan sus servicios. Por tanto, una interrupción grave de la actividad ya no requiere que una organización sea el objetivo directo de un ataque. Y, cuando se trata de una caída de infraestructuras, ni siquiera es necesario que exista un objetivo concreto. Para muchas organizaciones, esta sigue siendo una de las áreas de riesgo menos identificadas y analizadas, ya que se encuentra a caballo entre la ciberseguridad, la gestión de proveedores y la continuidad del negocio, sin que exista una única función responsable de gestionarla.

Esto plantea retos estructurales que no pueden mitigarse por completo mediante garantías contractuales o redundancia técnica. La dependencia de un grupo reducido de proveedores de tecnología y plataformas genera interdependencias que van más allá del riesgo convencional asociado a los proveedores.

Los ecosistemas modernos en la nube pueden depender en gran medida de un único proveedor para sustentar toda una variedad de servicios esenciales, lo que crea unas condiciones en las que un único punto de fallo puede provocar una interrupción de múltiples servicios en toda la organización. Este riesgo de concentración se ve amplificado por la implantación de la IA, ya que la concentración de la IA refleja y amplía las dependencias tecnológicas y en la nube existentes, dado que muchas de las mismas empresas están presentes en todos estos servicios. Al mismo tiempo, estos riesgos de concentración no pueden mitigarse por completo sin que ello suponga sacrificios, ya sea en materia de capacidad, interoperabilidad o seguridad.

A menudo se da por hecho que los proveedores de tecnología crítica son demasiado importantes como para fallar, lo que lleva a muchas organizaciones a pasar por alto su capacidad de resiliencia. Sin embargo, incidentes como las caídas de AWS y Cloudflare en 2025 demuestran que ninguna tecnología es infalible. Como consecuencia, las empresas, y algunas de sus funciones más críticas, quedan expuestas a riesgos cuando no cuentan con medidas de respaldo ni con planes de continuidad adecuados para responder ante la indisponibilidad de sistemas esenciales gestionados por terceros.

18 Synergy Research Group: AWS, Microsoft Azure y Google Cloud representaron el 63 % del gasto empresarial en servicios de infraestructura en la nube en el tercer trimestre de 2025. https://www.srgresearch.com/articles/cloud-market-share-trends-big-three-together-hold-63-while-oracle-and-the-neoclouds-inch-higher
19 https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf
20 https://newsroom.ibm.com/2026-06-08-new-ibm-study-finds-cios-and-ctos-face-growing-ai-control-gap-as-enterprise-deployment-scales

Caso de estudio: cuando el tiempo de inactividad se convierte en una pérdida

El ataque de ransomware de 2025 contra un minorista con sede en el Reino Unido supuso un impacto estimado de 300 millones de libras esterlinas en el beneficio operativo y provocó la suspensión de los pedidos online durante 46 días, prolongándose la recuperación total hasta 2026.[21] Se estima que la brecha de seguridad en 2023 del fabricante de bienes de consumo Clorox, con sede en EE. UU., causó a la empresa unos 380 millones de dólares en daños, con alrededor de 50 millones de dólares en costes de remediación y el resto vinculado a la imposibilidad de enviar productos a los clientes.[22] En ambos casos, el vector inicial procedía de la cadena de suministro, pero provocó un importante tiempo de inactividad operativa tras la brecha de seguridad, lo que pone de manifiesto el impacto potencial de una dependencia excesiva de la cadena de suministro.

Control Risks también ha intervenido en casos ocurridos en los últimos dos años en los que las empresas afectadas fueron disueltas o vendidas por cantidades simbólicas tras sufrir un ataque. Esto también queda respaldado por estadísticas externas, que muestran que el 60 % de las pequeñas empresas víctimas de ciberataques se ven obligadas a cesar su actividad en los seis meses siguientes al incidente.[23] El factor determinante no fue la complejidad de la intrusión, sino el tiempo durante el cual la empresa no pudo desarrollar su actividad, ya que el tiempo de inactividad en 2026 supondrá para las organizaciones un coste medio de 15 000 dólares por minuto.[24]



21 Divulgaciones e informes contemporáneos de Marks and Spencer Group plc, 2025-26: un impacto estimado de 300 millones de libras esterlinas en el beneficio operativo del ejercicio fiscal 2025/26; pedidos online suspendidos del 22 de abril al 10 de junio de 2025. https://www.bbc.com/news/articles/c0el31nqnpvo

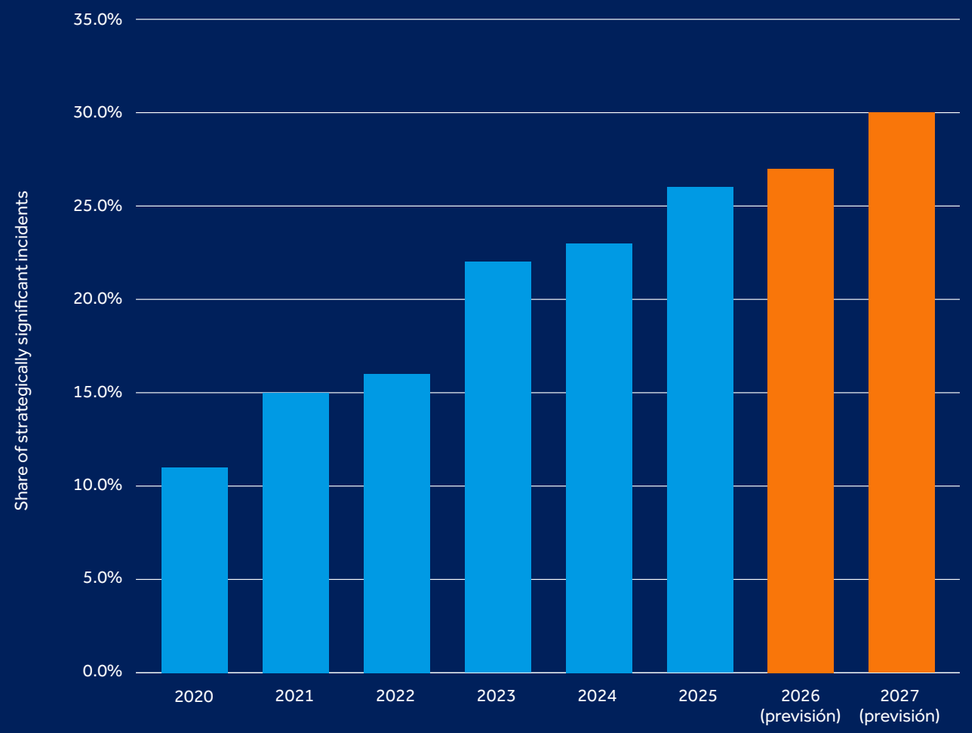
21 The Clorox Company contra Cognizant Technology Solutions, Tribunal Superior del Condado de Alameda, julio de 2025: Se reclaman 380 millones de dólares, que comprenden aproximadamente 49 millones de dólares en costes de remediación y pérdidas por interrupción de la actividad empresarial derivadas del ataque de agosto de 2023. https://www.reuters.com/legal/government/clorox-accuses-it-provider-lawsuit-giving-hackers-employee-passwords-2025-07-22/

21 https://www.totalassure.com/blog/cost-of-downtime-after-a-cyber-attack-in-2026

21 https://www.totalassure.com/blog/cost-of-downtime-after-a-cyber-attack-in-2026

La crisis de los proveedores: el problema va más allá del contrato

Figura 5: Porcentaje de incidentes de importancia estratégica en los que las empresas de TI han sido el objetivo (previsión para 2020-2027)



Source: Control Risks analysis and third-party market data. See Scope and notes for regions, data methodology and limitations

La concentración en determinadas plataformas es, al menos, un riesgo visible. Lo que no resulta tan evidente son las dependencias que existen detrás de ellas. La exposición al riesgo va más allá de los proveedores directos y se extiende a sus subcontratistas y a componentes de software compartidos que pocas organizaciones tienen identificados y, mucho menos, supervisados. Estas dependencias condicionan tanto el impacto de un incidente como la capacidad de recuperación:

- **Puntos únicos de fallo:** Los servicios críticos pueden depender de una región en la nube, una plataforma SaaS o un MSP, a menudo sin una alternativa probada o un derecho contractual a la prioridad de recuperación.
- **Dependencia extendida de la cadena de suministro:** Rara vez se incluye en el análisis a los proveedores de los proveedores, por lo que la organización no puede responder a una pregunta tan sencilla: ¿quién más tiene que estar funcionando para que nosotros podamos seguir trabajando?
- **Dependencia de recuperación:** Los plazos de restauración a menudo dependen de factores ajenos a la organización, como la aplicación de parches por parte del proveedor, el propio plazo de recuperación del proveedor o una plataforma de copia de seguridad de terceros.
- **Naturaleza de las copias de seguridad:** Las pruebas periódicas de las copias de seguridad pueden reducir el tiempo de inactividad en una media de 15 días.[25] Sin embargo, estudios del sector indican que el 94 % de las víctimas de ransomware mantienen sus copias de seguridad en entornos que también pueden verse afectados por el ataque. Esto puede dificultar considerablemente la recuperación de la actividad precisamente cuando más se necesita.[26]

25 https://www.totalassure.com/blog/cost-of-downtime-after-a-cyber-attack-in-2026
26 https://fenix24.com/2026-state-of-recoverability-report/

Un fallo en un proveedor puede afectar a todo un sector

Cada vez más empresas de un mismo sector dependen de las mismas plataformas especializadas, ya sea una solución SaaS dominante, un proveedor común de tecnología operativa (OT) o un mismo proveedor de servicios gestionados (MSP). Esto se debe, en muchos casos, a que los requisitos de certificación, la regulación o las expectativas de los clientes reducen el número de proveedores que cumplen los criterios necesarios. Como consecuencia, un fallo en un único proveedor puede afectar al mismo tiempo a varias empresas de un mismo sector, incluso aunque sean competidoras. Y si la interrupción afecta a todo el sector, también se reduce la posibilidad de recurrir a otras empresas para obtener capacidad o apoyo.

> “Los organismos reguladores han comenzado a tratar esto como un problema sistémico.”

Los organismos reguladores han comenzado a tratar esto como un problema sistémico y no de contratación: Tanto la Directiva sobre seguridad de las redes y la información 2 (NIS2) de la UE como la Ley de Resiliencia Operativa Digital (DORA)[27] la próxima actualización del proyecto de ley británico sobre ciberseguridad y resiliencia (redes y sistemas de información) y la Ley de Protección de los Sistemas Cibernéticos Críticos de Canadá establecen requisitos en materia de supervisión de proveedores, continuidad probada y notificación de incidentes a lo largo de las cadenas de suministro. Las organizaciones afectadas, así como el número mucho mayor de aquellas que les suministran, deben contar con que la concentración y la dependencia de la recuperación pasen a ser una cuestión de cumplimiento demostrable, en lugar de una cuestión de criterio interno.



27 En julio de 2026, Francia, España y los Países Bajos (tres de los 14 mercados de QBE) aún no habían notificado la transposición íntegra, por lo que la Comisión Europea los remitió (junto con Irlanda) al Tribunal de Justicia. https://digital-strategy.ec.europa.eu/es/news/commission-refers-ireland-spain-france-and-netherlands-court-justice-failing-transpose-rules Posteriormente, la Cyberbeveiligingswet de los Países Bajos entró en vigor el 15 de agosto de 2026, con lo que se transpuso la Directiva NIS2. https://www.nldigitalgovernment.nl/dossiers/nis2-directive-cyberbeveiligingswet-cbw/

Cuando los incidentes se convierten en crisis

Los fallos de seguridad que provocan interrupciones de la actividad coinciden de forma recurrente en los casos analizados por Control Risks, tanto a partir de fuentes abiertas como de su experiencia en respuesta a incidentes. Muchos de estos fallos se ven agravados por una superficie de ataque cada vez mayor y por el aumento de las capacidades de los atacantes, incluidas aquellas potenciadas por la inteligencia artificial.

Cinco vulnerabilidades recurrentes pueden convertir un incidente en una crisis



Identidad, acceso y personas: La ausencia de autenticación multifactorial o la posibilidad de eludirla, la reutilización de credenciales y las cuentas con privilegios excesivos amplían la superficie de ataque. La ingeniería social basada en la inteligencia artificial está facilitando la creación y la ampliación de señuelos convincentes, incluidos aquellos dirigidos a personal de alta dirección, personal técnico y personal de áreas clave de la empresa (Recursos Humanos, departamento jurídico y departamento financiero).



Sistemas sin parches y heredados: La mayoría de las vulnerabilidades aprovechadas en 2025 eran problemas conocidos para los que ya existían soluciones.[28] En 2026, la aparición de sistemas de detección de vulnerabilidades basados en IA ha incrementado considerablemente el volumen de notificación de debilidades, lo que ha complicado a las organizaciones la tarea de establecer prioridades en sus prácticas de aplicación de parches.[29]



Segmentación deficiente: Las redes informáticas o de tecnología operativa sin segmentar permiten intrínsecamente que los atacantes se muevan desde un punto de apoyo corporativo directamente a los sistemas de operación, o a través de sistemas críticos de tecnología de la información en una organización. En la actualidad, se está utilizando la IA para encadenar vulnerabilidades de seguridad que, en el pasado, habrían limitado la capacidad de los atacantes para desplazarse por las redes, lo que hace que una verdadera segmentación de los datos resulte aún más crucial.



Exposición a terceros: Los proveedores, los proveedores de servicios gestionados y las plataformas de software constituyen una vía de acceso inicial muy importante, y los ciberdelincuentes llegan incluso a centrar sus ataques en terceros de los proveedores para obtener acceso a entornos objetivo de gran interés.



Brechas de detección y respuesta: Un seguimiento limitado de los incidentes anómalos y/o una capacidad limitada para bloquear rápidamente dichos incidentes, así como planes de continuidad del negocio y de respuesta que no se han probado o que no se han adaptado a los servicios críticos de la organización. A medida que la IA permite a los ciberdelincuentes acelerar elementos de la secuencia de ataque, el impacto de estas brechas podría verse aún más agravado.

Estas deficiencias comparten un patrón. En casi todos los casos de los que se ocupa Control Risks, la organización no detectó la intrusión con la suficiente antelación, no pudo contenerla una vez que comenzó a propagarse, no pudo continuar sus actividades sin el sistema que perdió y no se había preparado adecuadamente para ninguna de estas situaciones.

28 Verizon, Informe de investigaciones de filtraciones de datos de 2025: la explotación de vulnerabilidades como vector de acceso inicial experimentó un aumento interanual del 34 % y estuvo presente en el 20 % de las brechas, fundamentalmente problemas conocidos y solucionables mediante un parche en dispositivos perimetrales y VPN. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

29 El programa de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures, CVE) de CISA informó en septiembre de que las notificaciones de CVE en el primer trimestre de 2026 fueron un tercio más altas que durante el mismo periodo en 2025. El Grupo de Inteligencia de Amenazas de Google informó en septiembre de una duplicación de la notificación de vulnerabilidades entre enero y agosto de 2026. https://www.cisa.gov/sites/default/files/2026-09/cve-program-establishing-a-quality-era-framework-508c.pdf https://therecord.media/google-vulnerabilities-cyberattacks-ai

Según la experiencia de Control Risks, son estas deficiencias las que separan un incidente contenido de una crisis de empresa:

Figura 6: Por qué los incidentes se convierten en crisis

El fallo	Qué aspecto tiene	Por qué el incidente escala
No pudieron verlo	Cobertura de vigilancia parcial, alertas sin revisar fuera del horario laboral	Los atacantes pueden propagarse por los sistemas de una organización en apenas 30 minutos;[30] el acceso no detectado permite un control total
No pudieron contenerlo	Redes sin segmentar, credenciales compartidas, acceso privilegiado permanente	Un punto de apoyo corporativo llega a los sistemas operativos y de producción
No podían funcionar sin él	Servicios críticos nunca se han relacionado con los sistemas y proveedores que los sustentan	La interrupción técnica se traduce en pérdida de actividad comercial; el tiempo de inactividad por ransomware ahora alcanza un promedio de alrededor de 24 días[31]
No se habían puesto en práctica	Planes redactados pero no probados, y que nunca se han llevado a la práctica más allá del equipo técnico	Las decisiones ejecutivas se toman por primera vez bajo máxima presión

Fuente: Casos de respuesta a incidentes de Control Risks.

30 https://www.crowdstrike.com/en-us/global-threat-report/
31 Informe trimestral de ransomware de Coveware by Veeam y análisis del sector asociado, 2025.

Las propias áreas de negocio también pueden convertirse en objetivos de un ciberataque

Los atacantes no eligen a sus objetivos al azar. Incluso los grupos más oportunistas tienen sus propias estrategias y preferencias, y buscan las vías que ofrecen menor resistencia, identificando dónde encuentran las oportunidades más fáciles para acceder a una organización. Suelen centrarse en las áreas que gestionan accesos, dinero, datos o relaciones de confianza, porque pueden ofrecer la vía más rápida para interrumpir la actividad y ejercer una mayor presión sobre el conjunto de la organización mediante la extorsión.

Según los casos gestionados por Control Risks, las siguientes áreas son las que aparecen con mayor frecuencia como punto de entrada inicial en las organizaciones, y no siempre coinciden con aquellas que las empresas consideran más expuestas:



Sistemas informáticos, seguridad y administradores privilegiados: El robo de credenciales y la suplantación del servicio de asistencia técnica amplían el alcance de una única brecha de seguridad a toda la empresa.



Finanzas, nóminas y adquisiciones: La autoridad de pago convierte a estos puestos en objetivos atractivos para el control de correo electrónico empresarial, el fraude en facturas y el desvío de pagos mediante deepfakes.



Operaciones, ingeniería y tecnología operativa: Donde la disrupción digital puede volverse física y el tiempo de inactividad puede conllevar costes operativos significativos.



Atención al cliente y ventas: Expuestos al exterior y un puente a los datos y sistemas de los clientes.



Ejecutivos y directivos: Tienen autoridad de aprobación y son objetivos preferentes para la suplantación de identidad.



RR. HH. y personal: Poseen datos personales y gestionan la recepción de solicitudes, lo que genera exposición a tácticas que incluyen la infiltración fraudulenta de empleados de tecnología de la información

Algunos puestos se enfrentan a niveles desproporcionadamente altos de selección como objetivo. El personal dedicado a las fusiones y adquisiciones y aquellas personas que desempeñan funciones estrechamente relacionadas con la negociación de operaciones, las desinversiones y las inversiones constituyen un objetivo clave para los ciberdelincuentes con motivaciones tanto financieras como comerciales.

Según los estudios y el trabajo de Control Risks con clientes del mercado privado, aproximadamente el 18 % del total de víctimas de ransomware y filtraciones de datos habían participado en una fusión o adquisición pública en los últimos 12 meses, lo que indica una selección desproporcionada como objetivo de las organizaciones involucradas en actividades públicas de fusión y adquisición. En las organizaciones del mercado privado, el personal de fusiones y adquisiciones es objeto de intentos de phishing e ingeniería social con más frecuencia que los equipos de tecnología de la información o de finanzas internas. Esta tendencia se observa en todos los mercados, y el personal dedicado a las fusiones y adquisiciones se ve afectado de manera desproporcionada en otros sectores ajenos al mercado de capitales.

Las funciones empresariales pueden aumentar la exposición y los retos de resiliencia en tres áreas clave:

Selección directa
Tal y como se ha mencionado anteriormente, los ciberdelincuentes se centran en puestos concretos dentro de las organizaciones, utilizando diversas técnicas de ingeniería social para posibilitar el control de los sistemas, provocar interrupciones, sustraer datos o llevar a cabo extorsiones.

Gestión de vulnerabilidades
Las deficiencias a la hora de identificar software no autorizado, incluidas las herramientas de IA no autorizadas, aplicar parches a los sistemas heredados e implementar controles de seguridad de manera coherente en todos los dispositivos pueden generar vulnerabilidades fácilmente explotables.

Planificación deficiente de la resiliencia
Aunque los sistemas y las tecnologías se gestionan cada vez más de forma centralizada, los planes de resiliencia no siempre tienen en cuenta las diferentes necesidades de cada área de negocio en términos de disponibilidad, dependencias y sistemas de respaldo. Esto puede aumentar el impacto y el coste de una interrupción de la actividad.

Cinco recomendaciones para fortalecer la resiliencia operativa y reducir el tiempo de recuperación

La resiliencia no consiste simplemente en alcanzar un determinado nivel de preparación o madurez. Según la experiencia de Control Risks, las organizaciones que consiguen recuperarse con mayor rapidez suelen tener en común unas pocas prácticas clave, y ninguna de ellas requiere incorporar nueva tecnología. Lo realmente importante es definir claramente quién debe identificar aquello sin lo que la organización no puede funcionar y revisar esta cuestión de forma continua, a medida que cambian las necesidades del negocio.

Figura 7: Cinco actividades de resiliencia que determinan el tiempo de recuperación



1 **Seguridad proactiva**	Implantar la autenticación multifactor (MFA) siempre que sea técnicamente posible, eliminar los accesos privilegiados permanentes, priorizar la aplicación de parches para vulnerabilidades conocidas y que ya están siendo explotadas, y mantener separados los entornos de IT y OT para evitar que un acceso a la red corporativa pueda extenderse a los sistemas de producción.
2 **Gobernanza y responsabilidad**	Evaluar el perfil de riesgo, acordar el nivel de riesgo asumible con la alta dirección y designar a un único responsable de gestionar las dependencias y la continuidad del negocio. Cuando esta responsabilidad queda repartida entre ciberseguridad, Compras y Continuidad de Negocio, se corre el riesgo de que nadie la asuma realmente.
3 **Análisis de dependencias**	Identificar qué sistemas, proveedores y terceros sustentan los servicios críticos de la organización, incluidos los proveedores indirectos. Determinar en qué casos la recuperación depende de terceros y acordar soluciones alternativas. Siempre que sea posible, establecer también por contrato los tiempos y prioridades de recuperación, así como alternativas viables en caso de interrupción.
4 **Pruebas y ejercicios**	Probar los planes de recuperación ante la posible pérdida de un proveedor, y no solo ante la caída de un sistema, e involucrar en estos ejercicios tanto a la dirección como a los equipos técnicos. Un plan que nunca se ha puesto a prueba se basa en supuestos, y los supuestos son lo primero que falla.
5 **Preparación y respuesta**	Contar de antemano con los recursos necesarios en materia forense, legal y de comunicación, establecer y poner a prueba los criterios para la toma de decisiones, y revisar periódicamente el perfil de riesgo a medida que evolucionan los sistemas y la red de proveedores. Anticipar estas decisiones reduce el número de cuestiones que habrá que resolver por primera vez en plena crisis, lo que permite una recuperación más rápida y reduce el impacto en la actividad.

Fuente: Control Risks

En conjunto, estas cinco actividades dan respuesta a cuatro preguntas que toda organización debería poder contestar con datos.

- ¿Puede detectar una intrusión lo suficientemente pronto como para actuar?
- ¿Puede contener la intrusión antes de que llegue a los sistemas operativos?
- ¿Puede seguir prestando sus servicios más críticos mientras el sistema afectado no está disponible?
- ¿Ha puesto a prueba su capacidad para hacerlo, involucrando tanto a la dirección como a los equipos técnicos?

Las organizaciones que pueden responder a las cuatro preguntas tienden a recuperarse más rápidamente. Aquellas que no pueden, tienen menos control sobre la duración y el impacto de la interrupción, especialmente cuando la recuperación depende de terceros. Eso es lo que convierte la dependencia en una cuestión que compete al consejo de administración: determina el tiempo de recuperación, el coste real del tiempo de inactividad y en qué medida la continuidad de la organización se decide fuera de su propio perímetro.

La visión de Suscripción



Fernando Oliver
Cyber Underwriter

Una de las conclusiones más claras que extraemos de los siniestros cyber que vemos es que la gravedad de un incidente no depende necesariamente de lo sofisticado que haya sido el ataque. A menudo, lo que realmente marca la diferencia es lo que ocurre después. Puede depender de hasta qué punto la interrupción afecta al conjunto de la organización, qué servicios críticos dejan de estar disponibles, cuánto tiempo se tarda en recuperarlos o en qué medida la recuperación depende de terceros. Esto cambia la forma en que entendemos la resiliencia cibernética y también cómo deberían abordarla las empresas.

Unos controles de seguridad sólidos serán siempre fundamentales, pero prevenir todos los incidentes no es un objetivo realista. Las organizaciones también necesitan comprender cómo seguirían funcionando cuando dejen de estar disponibles un sistema, un proveedor o una plataforma tecnológica críticos, y cuánto control tienen realmente sobre sus propios plazos de recuperación.

Para las aseguradoras, se trata de una distinción importante y valiosa. Dos empresas con controles de ciberseguridad aparentemente similares pueden tener exposiciones a pérdidas muy diferentes. Es posible que se hayan identificado los servicios críticos, se hayan segmentado las redes, se hayan comprobado las copias de seguridad, se hayan identificado proveedores alternativos y se hayan ensayado las respuestas con la alta dirección. Otra puede poner de relieve las dependencias críticas solo después de que haya ocurrido un incidente.

El ciberincidente inicial podría ser similar, pero la interrupción del negocio posterior puede ser muy diferente.

Esto es particularmente importante a medida que las organizaciones son más y más dependientes de un número relativamente pequeño de proveedores tecnológicos. Los servicios gestionados, las plataformas y los sistemas han creado unas eficiencias fantásticas, pero también pueden generar grandes puntos comunes de dependencia.

Por tanto, las empresas deben ir más allá de la gestión tradicional del riesgo de terceros. Ya no basta con saber quiénes son sus proveedores directos. La pregunta clave es: ¿de quién más dependemos para poder seguir operando? La respuesta puede incluir al proveedor cloud de uno de sus proveedores, una plataforma de software u otros subcontratistas con los que la propia organización ni siquiera mantiene una relación directa.

Sin embargo, si uno de estos proveedores falla, los tiempos de recuperación pueden dejar de depender de la propia empresa y quedar en manos de terceros.

Es también la razón por la que el riesgo de concentración es importante. Las empresas por sí solas no pueden diversificar un mercado en el que un gran número de organizaciones dependen de los mismos proveedores esenciales. Los organismos reguladores y los gobiernos desempeñan un papel importante a la hora de analizar cómo se identifican y gestionan las dependencias tecnológicas sistémicas, junto con las responsabilidades de cada organización.

La recuperación debe diseñarse, no darse por sentada

Uno de los ejercicios más valiosos que puede llevar a cabo una empresa es partir de sus servicios críticos y realizar un análisis retroactivo.

¿Qué debe seguir funcionando? ¿Qué sistemas y proveedores lo hacen posible? ¿Cuánto tiempo podría funcionar la empresa sin ellos? ¿Cuáles son las alternativas? ¿Quién tiene la autoridad para tomar decisiones cuando se produce una interrupción?

Esas preguntas deben responderse antes de un incidente, no cuando este se produce. Las pruebas son igualmente importantes. Un plan de respuesta a incidentes puede parecer exhaustivo sobre el papel, pero aun así incluir supuestos que nunca se han probado. Recomendamos que las organizaciones también realicen pruebas de estrés ante la pérdida de un proveedor, así como ante la pérdida de un sistema interno, y que los ejercicios alcancen a los responsables de la toma de decisiones a nivel ejecutivo junto con los equipos de ciberseguridad y sistemas de tecnología de la información. Las empresas deben saber y planificar con antelación cuándo deben recurrir a los acuerdos de continuidad de negocio, comunicarse con los clientes, contratar asistencia especializada o adoptar otras decisiones críticas.

La dedicación a la preparación puede afectar materialmente a la magnitud de una pérdida. El objetivo no acaba en la restauración de la tecnología: la prioridad debe centrarse en preservar la capacidad de prestar los servicios más importantes mientras se lleva a cabo la recuperación.

No hay que pasar por alto a las empresas más pequeñas

Existe también un reto importante para los gobiernos, las aseguradoras y el sector de la ciberseguridad en general en torno a las pequeñas y medianas empresas (pymes). Las grandes organizaciones se enfrentan a presiones normativas y comerciales para demostrar su resiliencia cibernética, pero las pymes suelen disponer de menos recursos internos, al tiempo que dependen de muchas de las mismas tecnologías y de cadenas de suministro interconectadas.

Es importante que exista una mayor concienciación y un apoyo práctico. La resiliencia cibernética no exige necesariamente tecnología sofisticada o costosa. Medidas sensatas como la autenticación multifactor, eliminar el acceso privilegiado innecesario, aplicar parches en las vulnerabilidades explotadas, realizar copias de seguridad de forma eficaz y comprender las dependencias críticas de los proveedores pueden mejorar significativamente la capacidad de resistir un incidente.

Para las organizaciones de mayor tamaño, esto también es una cuestión de la cadena de suministro. Ayudar a los proveedores más pequeños a mejorar su resiliencia puede, en última instancia, proteger la continuidad de las empresas que dependen de ellos.

Contar con el apoyo adecuado marca la diferencia

Por último, las empresas no deberían considerar el seguro cyber únicamente como un mecanismo financiero que entra en juego después de un siniestro. La relación con la aseguradora puede facilitar el acceso a conocimiento especializado antes, durante y después de un incidente.

Brokers y aseguradoras pueden ayudar a las organizaciones a entender mejor su exposición al riesgo, identificar áreas en las que sería conveniente reforzar la planificación de la resiliencia y aprovechar mejor los servicios especializados que tienen a su disposición.

En caso de incidente, saber de antemano a quién recurrir, ya sean especialistas forenses, asesores legales, expertos en comunicación o proveedores especializados en respuesta a incidentes, puede ahorrar un tiempo muy valioso durante las primeras fases de una crisis.

Alcance y notas

Mercados incluidos (14):

El análisis abarca 14 mercados en los que QBE tiene actividad: Reino Unido, Suecia, Dinamarca, Francia, Alemania, España, Italia, Países Bajos, Canadá, Estados Unidos, Australia, Nueva Zelanda, Singapur y Hong Kong.

Periodo

2023-26, con una proyección a 2027.

Fuentes y método

El análisis se basa en los datos sobre incidentes, inteligencia y respuesta de Control Risks en los 14 mercados analizados, complementados con informes de fuentes públicas y datos de mercado de terceros, cuando así se indica. Las cifras para 2026 toman los números del año hasta la fecha y realizan una previsión hasta el cierre del año; las cifras de 2027 se prevén basándose en el crecimiento medio.

Metodología de los datos

El conjunto de datos de Control Risks se basa en información elaborada para un público corporativo, generalmente grandes multinacionales, y se centra en incidentes estratégicamente significativos. Esto difiere de los proveedores que obtienen datos de herramientas de detección y respuesta en los terminales implementadas en su propia base de clientes, que normalmente abarcan tanto a grandes multinacionales como a empresas más pequeñas. Los datos de Control Risks no recogerán todos los incidentes que recogería una herramienta automatizada, pero son una buena representación de los incidentes que afectan a las grandes empresas en los mercados analizados.



Para más información puedes visitar nuestra página web **qbeespana.com**

QBE European Operations
QBE Europe SA/NV, Spain
Paseo de la Castellana
31 – 5ª Planta
28046 Madrid
España
+34 91 789 39 50

qbeespana.com

Todos los productos y servicios son proporcionados por QBE Insurance Group Limited o sus filiales («QBE»), o por terceros proveedores seleccionados por QBE, y pueden estar sujetos a términos y condiciones, limitaciones y exenciones de responsabilidad adicionales [disponibles previa solicitud]. La información y las orientaciones proporcionadas por QBE no pretenden constituir asesoramiento financiero o profesional adaptado a sus circunstancias particulares y pueden haber sido elaboradas sin un conocimiento detallado de sus sistemas o de los riesgos específicos de su empresa. Asimismo, no contemplan todas las situaciones posibles ni todas las medidas que puedan resultar necesarias para responder a un incidente de ciberseguridad. QBE no ofrece garantía alguna en relación con los resultados que puedan obtenerse ni sobre la reducción de la exposición a siniestros, Es responsabilidad del usuario aplicar su propio criterio independiente para valorar las recomendaciones proporcionadas y la idoneidad de cualquier producto. Esta información no sustituye el asesoramiento de profesionales jurídicos o expertos en ciberseguridad a la hora de prepararse para un incidente de ciberseguridad o responder ante el mismo. QBE no asume responsabilidad alguna por los servicios prestados por terceros proveedores. QBE y su logotipo son marcas registradas de QBE Insurance Group Limited, y las marcas de terceros se utilizan bajo las correspondientes licencias. © 2026 QBE Insurance Group Limited.

Este documento se facilita a título informativo siendo su contenido confidencial para el destinatario. La entrega de esta documentación no pretende crear ninguna obligación ni relación jurídica a cargo de ninguna de las partes ni constituirá asesoramiento ni oferta alguna. No podrá copiarse ni distribuirse, ni en su totalidad ni en parte, sin el consentimiento previo por escrito de QBE. Pese a que este documento ha sido redactado de buena fe, en ningún caso QBE garantiza la exactitud, integridad, atemporalidad o idoneidad de la información contenida en el mismo. QBE no se hace responsable del contenido de esta información para los fines a los que se destina. El término QBE mencionado en el presente documento se refiere a QBE Europe, SA/NV Sucursal en España. QBE European Operations es un nombre comercial que abarca a QBE Europe SA/NV, QBE UK Limited y QBE Underwriting Limited. QBE Europe SA/NV, con CIF BE 0690.537.456, RPM/RPR Bruselas, está autorizada por el Banco Nacional de Bélgica bajo el número de licencia 3093. QBE Europe SA/NV Sucursal en España, con domicilio en Paseo de la Castellana 31, 5ª planta 28046 Madrid y con C.I.F. W0174445G está inscrita en el Registro Mercantil de Madrid Tomo 37.059 – Libro 0 – Folio 190 – Sección 8 – Hoja M-661870-Inscripción 1, y en el Registro de la Dirección General de Seguros y Fondos de Pensiones (DGSFP) con la clave E-0230. Tanto QBE UK Limited como QBE Underwriting Limited están autorizadas por la Prudential Regulation Authority y sometidas a la regulación de la Financial Conduct Authority y la Prudential Regulation Authority.

1475304/2611-ESP

QBE Insurance