QBE
At the heart of it

Ciberamenazas en la nube:

Estrategias frente a la disrupción digital

Tres ideas a tener en cuenta:

1. La adopción de la nube y la inteligencia artificial puede mejorar la eficiencia, pero también aumentar la exposición a riesgos.

2. Los ciberdelincuentes están evolucionando: combinan herramientas nuevas con tácticas antiguas para atacar y generar interrupciones.

3. Cómo pueden las empresas integrar la gestión de riesgos en la tecnología para que la resiliencia forme parte del diseño desde el inicio, y no se añada después como un parche.

La adopción de la inteligencia artificial y el desarrollo de las plataformas en la nube están transformando los negocios, pero la velocidad y la magnitud de este rápido cambio ofrecen grandes oportunidades para el ransomware, el fraude y las interrupciones causadas por terceros.

El paso a plataformas de nube públicas, privadas e híbridas está generando nuevas formas de operar, impulsando la automatización y favoreciendo la adopción de la inteligencia artificial (IA). Estos avances están generando ventajas competitivas, pero se están desarrollando en un entorno de amenazas que evoluciona aún más rápido. Conforme las empresas aumentan su dependencia de los servicios en la nube, los actores maliciosos aprovechan debilidades tales como controles de identidad deficientes, configuraciones erróneas y datos no protegidos.

La inteligencia artificial generativa (IA generativa) amplifica el riesgo, ya que permite a los intrusos actuar con mayor rapidez y precisión, al tiempo que reduce las barreras técnicas para los ciberdelincuentes principiantes. Dado que los actores maliciosos utilizan la IA generativa para violar los sistemas de seguridad, las empresas se ven expuestas a interrupciones operativas, lo que tiene repercusiones financieras, reputacionales y potenciales repercusiones normativas. Las amenazas relacionadas con el uso de la IA generativa se han manifestado en estafas con deepfakes‡, fraudes de identidad y ataques de phishing† automatizados. Como resultado, los incidentes de ransomware siguen aumentando: IT-ISAC registró 1537 ataques de ransomware en el primer trimestre de 2025, frente a los 572 del primer trimestre de 2024, y las perturbaciones que causan representan ahora un riesgo fundamental para las organizaciones que dependen de terceros, incluidos los proveedores de servicios en la nube.

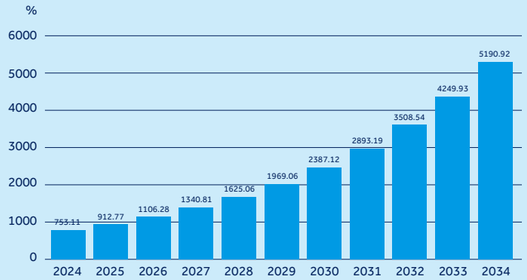
Glosario

‡ **Deepfake:** tecnología basada en la inteligencia artificial que se utiliza para producir contenidos de vídeo o audio artificiales que parecen reales.

† **Phishing:** un intento de obtener información privada y confidencial de los usuarios de Internet, como nombres de usuario, contraseñas y datos de tarjetas de crédito. Por lo general, los ciberdelincuentes envían correos electrónicos o se ponen en contacto con las víctimas a través de mensajería instantánea, haciéndose pasar por contactos legítimos u oficiales. Estos correos electrónicos o mensajes de phishing suelen contener enlaces infectados con malware.

Actuar con anticipación y priorizar la resiliencia es esencial. Las empresas deben incorporar la gestión de riesgos en sus sistemas tecnológicos, anticiparse a las vulnerabilidades de terceros e integrar planes de continuidad en sus operaciones.

Gráfico 1: Valor proyectado del mercado global de tecnología en la nube por año (miles de millones de dólares estadounidenses)



Control Risks Fuente: Precedence Research[1]

La magnitud de la adopción de la nube hace aún más urgente la necesidad de controlar los niveles de exposición. Se prevé que el mercado mundial supere los 5 billones de dólares estadounidenses en 2034, frente a los 912 000 millones de dólares estadounidenses de 2025.[2] A medida que más organizaciones transfieren su infraestructura y sus datos a los servidores en la nube, estos servidores se convierten en objetivos de gran valor. Las alertas críticas relacionadas con la nube aumentaron un 235 % a lo largo de 2024 en comparación con el año anterior[3], lo que refleja tanto el aumento en la adopción como la creciente capacidad de los atacantes.

La mayoría de los ciberataques que se originan en la nube tienen como objetivo el correo electrónico corporativo (Business Email Compromise, BEC).[4] Los delincuentes aprovechan plataformas como Microsoft 365 para lanzar campañas de phishing BEC, que pueden abrir la puerta a la apropiación de cuentas o la recopilación de credenciales, utilizando una plataforma en la nube de confianza en lugar de recurrir a dominios falsificados typosquatted‡ o suplantación de correo electrónico**. Esto significa que estos ataques pueden completarse sin activar muchas medidas de seguridad habituales.[5] Además, tanto actores vinculados a gobiernos como grupos de ciberdelincuentes están apostando por ataques dirigidos específicamente a infraestructuras digitales en la nube.

1 precedenceresearch.com/cloud-computing-market
2 precedenceresearch.com/cloud-computing-market
3 unit42.paloaltonetworks.com/2025-cloud-security-alert-trends
4 ibm.com/thought-leadership/institute-business-value/report/2025-threat-intelligence-index
5 guardz.com/blog/sophisticated-phishing-campaign-exploiting-microsoft-365-infrastructure

Glosario

‡ **Typosquatting:** la práctica de registrar versiones mal escritas de nombres de dominio legítimos para propagar malware a través de enlaces en correos electrónicos de phishing o descargas no solicitadas. Por ejemplo, una variante del dominio legítimo example.com podría registrarse de forma maliciosa como exxample.com.

** **Suplantación de identidad por correo electrónico:** táctica en la que un atacante falsifica la dirección del remitente de un correo electrónico para ocultar su verdadero origen, haciendo que parezca que ha sido enviado desde una fuente fiable.

Doble exposición: ransomware y phishing

Casi la mitad de los datos corporativos almacenados en servidores en la nube se clasifican como sensibles,[6] lo que los hace atractivos para los operadores de ransomware. Las nuevas variantes de ransomware están diseñadas para buscar y atacar herramientas de colaboración basadas en la nube, y los atacantes son cada vez más capaces de moverse lateralmente entre los sistemas locales y los sistemas en la nube, cifrando o filtrando datos a medida que avanzan.[7]

El phishing sigue siendo el principal punto de acceso para los incidentes relacionados con la nube, representando un tercio de las intrusiones en 2023 y 2024.[8] A menudo, los atacantes utilizan tácticas de phishing para robar credenciales mediante ataques de tipo "adversario en el medio" (AITM)‡. Los actores maliciosos también han logrado explotar fallos en aplicaciones en la nube, utilizando credenciales legítimas robadas y obteniendo acceso a usuarios privilegiados o cuentas de servicio.

6 cpl.thalesgroup.com/resources/webinars?commid=615147&bt_tok=%7b%7bRecipient.ID%7d%7d

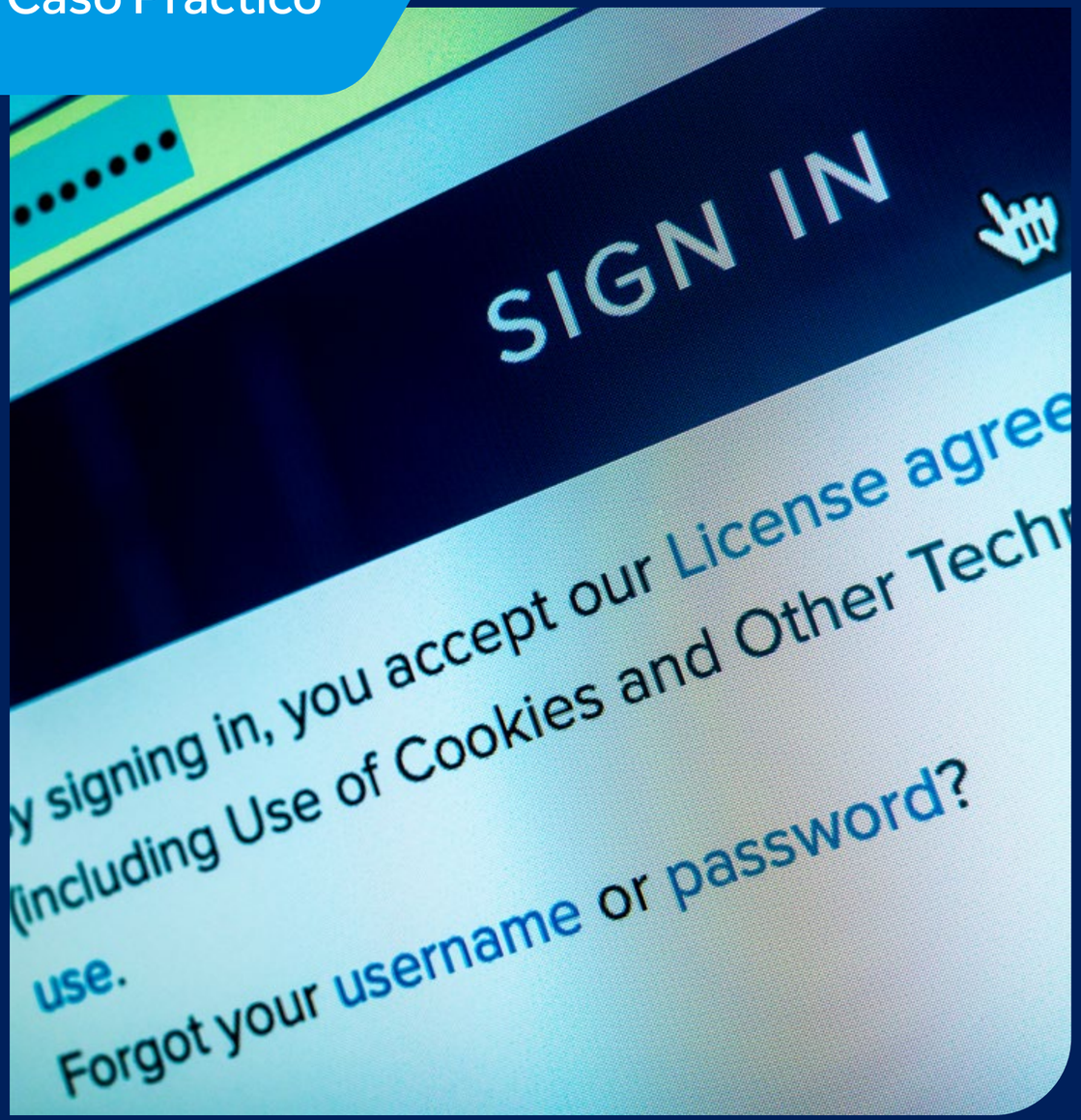
7 microsoft.com/en-us/security/blog/2024/09/26/storm-0501-ransomware-attacks-expanding-to-hybrid-cloud-environments

8 ibm.com/new/announcements/x-force-cloud-threat-landscape

Glosario

‡ **Ataque de adversario en el medio (Adversary-In-The-Middle, AITM):** también conocido como ataque de hombre en el medio (Man-In-The-Middle, MITM), se refiere a un actor malicioso que se interpone entre una conversación que tiene lugar entre el usuario (víctima) y el sistema. La posición del atacante le permite interceptar, enviar y recibir datos destinados a uno de los extremos de la conversación legítima o que no están destinados a ser enviados en absoluto.

Caso Práctico



Okta, 2023

Okta, proveedor de inicio de sesión único (Single Sign-On, SSO), sufrió una brecha de seguridad cuando unos atacantes no identificados robaron credenciales y obtuvieron acceso a su sistema de gestión de casos de soporte técnico. Se robaron datos confidenciales, incluyendo cookies y tokens de sesión, lo que permitió suplantar la identidad de usuarios reales.

Uno de los clientes, 1Password, un gestor de contraseñas con más de 100 000 usuarios empresariales, detectó actividad sospechosa en su cuenta de Okta (utilizada para aplicaciones destinadas a los empleados) el 29 de septiembre, momento en el que inmediatamente detuvo la actividad e investigó el asunto.[9] Okta no notificó a 1Password sobre la violación hasta el 19 de octubre, 16 días después, a pesar de que otro cliente de ciberseguridad, BeyondTrust, alertó a Okta sobre una violación el 2 de octubre.[10]

En total, 134 clientes empresariales de Okta se vieron afectados, y Okta sufrió una pérdida de 2000 millones de dólares en valor de mercado.[11,12]

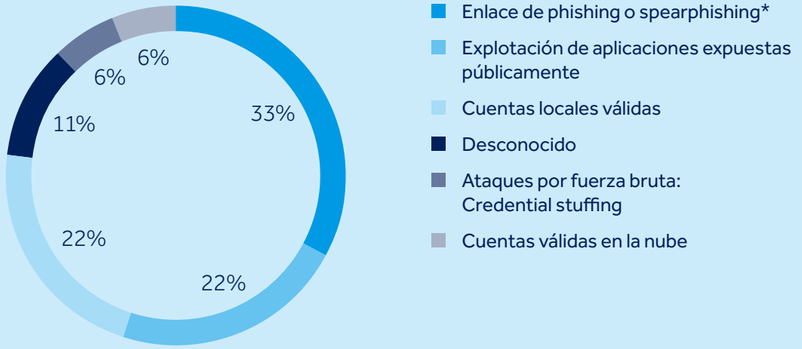
9 arstechnica.com/security/2023/10/1password-detects-suspicious-activity-in-its-internal-okta-account
10 portnox.com/blog/cyber-attacks/unpacking-the-okta-data-breach
11 nightfall.ai/blog/okta-data-breach-what-happened-impact-and-security-lessons-learned
12 cnbc.com/2023/10/23/okta-hack-wipes-out-more-than-2-billion-in-market-cap.html

Cadena de suministro y dependencias de terceros

La integración cada vez mayor entre el alojamiento y la gestión de datosha convertido a los proveedores externos en un objetivo atractivo para los ciberdelincuentes. La vulneración de un solo proveedor puede poner en riesgo a muchas empresas al mismo tiempo, incluso a cientos. El almacenamiento en la nube y de datos se ha convertido en un objetivo atractivo para atacantes de todo tipo, ya que la información tiene cada vez más valor en los mercados cibercriminales.

Para 2025, se prevé que el volumen de datos almacenados en todo el mundo alcance los 200 zettabytes (200 billones de gigabytes) en infraestructuras informáticas privadas y públicas, infraestructuras de servicios públicos, centros de datos en la nube privados y públicos, dispositivos personales y dispositivos del Internet de las cosas (Internet of Things, IoT).[13] La mitad de estos datos se almacenarán en la nube, en comparación con el 43 % de los datos almacenados en la nube en 2024[14], un 15 % estimado en 2020[15] y solo un 10 % en 2015[16]. Esta concentración de datos valiosos hace que los proveedores de servicios en la nube y los servicios de almacenamiento resulten atractivos para los atacantes.

Gráfico 2: Ataques a entornos en la nube, por vector de acceso inicial (2022-24)



Control Risks – Fuente: IBM[17]

13 cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025/
14 storagenewsletter.com/2023/01/25/43-of-data-to-be-stored-in-public-cloud-by-2024-on-average/
15 gartner.com/en/documents/3989101
16 statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/
17 ibm.com/new/announcements/x-force-cloud-threat-landscape

Glosario

* **Spearphishing:** una forma más específica de phishing que se centra en grupos concretos de personas que comparten una característica común. Por ejemplo, pueden trabajar en la misma empresa, asistir a la misma universidad, utilizar los mismos servicios o instituciones financieras, o realizar pedidos en los mismos sitios web.

Caso Práctico

MURKY PANDA, 2023-presente

MURKY PANDA, un prolífico actor malicioso vinculado al Estado chino, ha sido observado explotando vulnerabilidades de día cero en proveedores de software como servicio (Software-as-a-Service, SaaS) para obtener acceso a su red. El grupo puede burlar las defensas para permanecer sin ser detectado en los sistemas de los clientes durante largos periodos de tiempo, lo que les permite beneficiarse de un acceso prolongado a datos privados. MURKY PANDA también logró comprometer a un proveedor de soluciones en la nube de Microsoft al abusar de los privilegios administrativos delegados al personal técnico y de TI.[18]

El grupo representa una grave amenaza para las entidades gubernamentales, tecnológicas y de servicios profesionales de Norteamérica, especialmente a través del compromiso de proveedores con acceso a información confidencial. Los entornos en la nube son extremadamente vulnerables a las capacidades avanzadas y los conocimientos de MURKY PANDA sobre la lógica de las aplicaciones personalizadas, que le permiten explotar la funcionalidad de las aplicaciones en lugar de aprovechar las vulnerabilidades técnicas.

18 crowdstrike.com/en-us/blog/murky-panda-trusted-relationship-threat-in-cloud

Actores estatales nacionales

Los grupos vinculados al Estado están explotando cada vez más las debilidades de los sistemas en la nube.

IA generativa: ¿defensa o arma?

La IA generativa está transformando el panorama de las amenazas cibernéticas. Su uso y sus mercados parecen destinados a crecer de forma exponencial durante los próximos cinco años en Norteamérica y Europa, ya que las herramientas de IA generativa aportan beneficios en términos de productividad en la mayoría de los sectores, si no en todos.

- ChatGPT tendrá 755 millones de usuarios activos y Microsoft Copilot 88 millones en 2025.[19]
- Los usuarios de ChatGPT aumentaron un 33 % entre diciembre de 2024 y febrero de 2025.[20]
- El 78 % de las organizaciones implementarán la IA en al menos una función empresarial en 2025, frente al 55 % en 2024.[21]
- Entre el 20 % y el 40 % de los empleados utilizan activamente la IA en sus funciones, especialmente en la programación.[22]

Sin embargo, el uso indebido de la misma tecnología con fines de fraude y extorsión se ha convertido en una amenaza generalizada. El fraude mediante deepfakes es una tendencia especialmente alarmante, en la que los ciberdelincuentes se hacen pasar por ejecutivos, miembros de juntas directivas y figuras públicas utilizando voces, vídeos e imágenes. Estas tácticas se emplean para engañar a los empleados y que transfieran importantes sumas de dinero a cuentas no autorizadas controladas por redes delictivas. En 2024, los deepfakes estuvieron implicados en casi el 10 % de los ciberataques exitosos, con pérdidas económicas que oscilaron entre los 250 000 y los más de 20 millones de dólares estadounidenses.[23]

19 firstpagesage.com/seo-blog/chatgpt-usage-statistics
20 demandsage.com/chatgpt-statistics
21 sqmagazine.co.uk/ai-tools-usage-statistics
22 sqmagazine.co.uk/ai-tools-usage-statistics
23 Control Risks

Empresa sin nombre de Singapur, 2024

Un empleado de una empresa multinacional en Singapur fue engañado por un estafador que se hizo pasar por el director financiero. Creyendo que la videollamada era auténtica, el empleado autorizó una transferencia de casi 500 000 dólares estadounidenses.[24] Aunque las fuerzas policiales de Singapur y Hong Kong localizaron y retuvieron el dinero, es probable que el incidente haya generado importantes costes de respuesta y reparación.

24 channelnewsasia.com/singapore/deepfake-scam-impersonate-ceo-company-finance-director-5048706

Los atacantes respaldados por Estados también utilizan IA generativa para escribir código malicioso, utilizando grandes modelos de lenguaje (Large Language Models, LLM) para llevar a cabo operaciones de reconocimiento y ampliar las operaciones de malware. Estos actores también pueden atacar los LLM utilizados por las empresas para funciones internas posteriores, provocando interrupciones y problemas que afectan el funcionamiento operativo.

Los grupos de ciberdelincuentes aprovechan cada vez más las tecnologías de IA generativa y deepfake para llevar a cabo ataques con fines económicos en todos los sectores a escala mundial. La IA generativa es capaz de crear plantillas de phishing eficaces o llevar a cabo campañas de ingeniería social muy sofisticadas a gran velocidad. Los ciberdelincuentes con poca capacidad han utilizado la IA para ayudar en el desarrollo de scripts y la codificación de malware.[25] Es probable que las empresas se enfrenten a un aumento de los ataques por parte de grupos que antes se descartaban por ser demasiado incompetentes técnicamente o por carecer de los recursos necesarios para suponer una amenaza realista.[26] Los casos de extorsión con ransomware que se hicieron públicos aumentaron un 54 % entre enero y abril de 2025 en comparación con el mismo periodo del año anterior.[27]

25 hp.com/us-en/newsroom/press-releases/2024/ai-generate-malware.html
26 anthropic.com/news/detecting-countering-misuse-aug-2025
27 Control Risks

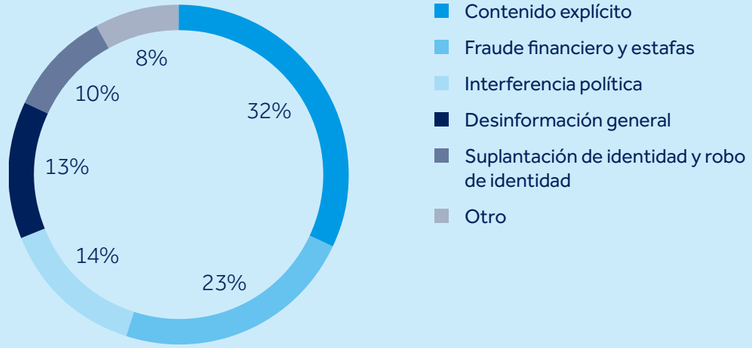
Caso Práctico

Amazon, 2025

Un “hacker ético” puso de manifiesto las graves deficiencias de la extensión Q de Amazon para Visual Studio Code al enviar una solicitud de extracción maliciosa. El hacker, utilizando únicamente una cuenta de GitHub sin privilegios, recibió por error credenciales con permisos administrativos. Este acceso les permitió ordenar al asistente que restableciera la configuración predeterminada de fábrica, borrara los sistemas de archivos locales y eliminara las bases de datos de recursos en la nube. El atacante, que describió el ejercicio como una exposición del “teatro de seguridad de la IA” de Amazon, no necesitó ningún malware sofisticado para tener éxito, lo que pone de relieve las debilidades de la arquitectura y los controles de seguridad de terceros.[28] Aunque no se destruyeron datos confidenciales, el incidente podría inspirar ataques similares contra la seguridad y los servicios de asistencia basados en inteligencia artificial de Amazon.

28 404media.co/hacker-plants-computer-wiping-commands-in-amazons-ai-coding-agent

Gráfico 3: Tipo de contenido de los ataques deepfake, primer trimestre de 2025



Control Risks – Fuente: Resemble AI[29]

El coste del compromiso

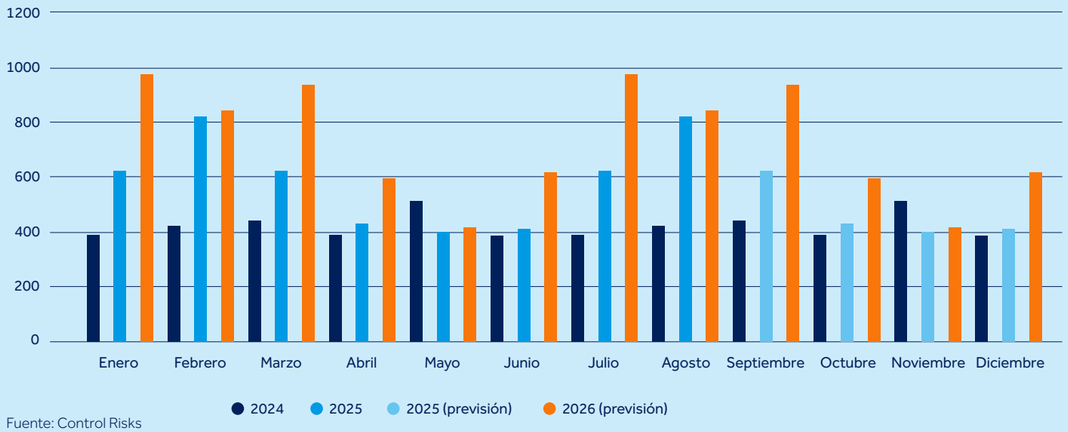
Los ataques de ransomware eficaces pueden provocar pérdidas económicas, daños a la reputación e incluso litigios, no solo para la empresa afectada, sino también para los proveedores externos y sus clientes. La adopción generalizada de los servicios en la nube y otras tecnologías emergentes ha coincidido con un aumento constante de la actividad del ransomware en los últimos años. Una importante oleada de ataques contra organizaciones del sector minorista y financiero del Reino Unido en mayo de 2025, liderada por el grupo ciberdelincuente Scattered Spider, pone de relieve esta tendencia. El grupo utilizó técnicas avanzadas de ingeniería social y phishing para obtener acceso, suplantando plataformas de confianza mediante dominios typosquatted de proveedores SaaS externos y kits de phishing que engañaban a las víctimas para que revelaran sus credenciales y datos de sesión. [30]

29 resemble.ai/wp-content/uploads/2025/04/ResembleAI-Q1-Deepfake-Threats.pdf
30 reliaquest.com/blog/scattered-spider-cyber-attacks-using-phishing-social-engineering-2025

Las organizaciones de todo el mundo siguen enfrentándose a importantes trastornos provocados por fallos de terceros. En los últimos dos años, los cortes masivos y los incidentes cibernéticos originados por los proveedores han afectado a múltiples sectores. Uno de los más notables fue la actualización defectuosa de CrowdStrike a su Falcon Sensor en 2024, que afectó a alrededor de 8,5 millones de dispositivos Windows. Aunque afectó a menos del 1 % de los equipos con Windows, la interrupción tuvo consecuencias a nivel global, siendo los sectores de salud, aviación y transporte algunos de los más impactado.

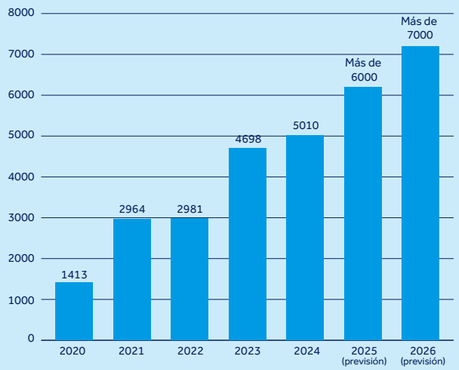
Los ciberdelincuentes aprovecharon rápidamente la situación y lanzaron campañas de phishing posteriores que utilizaban señuelos relacionados con CrowdStrike para comprometer sistemas, robar datos y extorsionar a las víctimas. Aunque el incidente no fue un ataque dirigido, puso de relieve el impacto sistémico que estos fallos pueden tener en las organizaciones que dependen del SaaS para funciones críticas. Ataques anteriores, como la campaña de vulnerabilidad masiva MOVEit y el ciberataque masivo NotPetya, demostraron cómo un ataque puede extenderse y perjudicar a muchas organizaciones que no fueron el objetivo directo.

Gráfico 4: Número mensual previsto de víctimas de ransomware nombradas en sitios web de filtración de datos



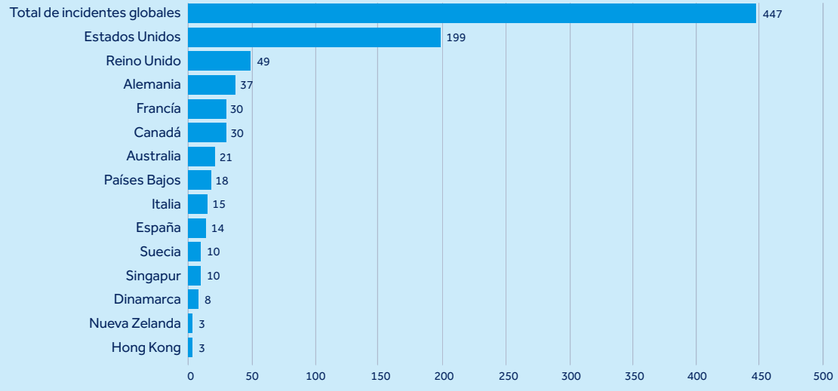
Fuente: Control Risks

Gráfico 5: Número total de víctimas de ransomware mencionadas en sitios web de filtración (a nivel mundial)



Fuente: Control Risks

Gráfico 6: Número de incidentes cibernéticos significativos registrados por zona geográfica (agosto de 2023 – agosto de 2025)



Fuente: Control Risks

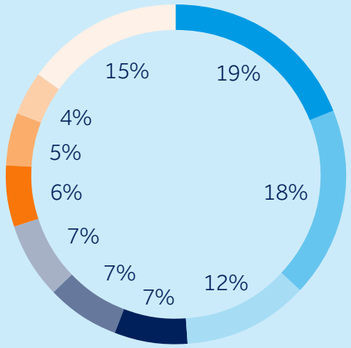
Caso Práctico

Rackspace, 2022

CASO PRÁCTICO: Rackspace, 2022
En 2022, el grupo de ransomware Play interrumpió el servicio de correo electrónico Hosted Exchange de Rackspace al aprovechar una vulnerabilidad de escalada de privilegios de día cero en Microsoft Exchange. Al menos 27 clientes de Hosted Exchange se vieron afectados después de que los atacantes obtuvieran acceso inicial a través de credenciales comprometidas, cortando el acceso al correo electrónico en todas sus organizaciones.[31] Las consecuencias fueron significativas: Rackspace se vio obligada a suspender su servicio Hosted Exchange, se enfrentó a múltiples demandas de clientes y se alegó que había incurrido en pérdidas por valor de unos 11 millones de dólares estadounidenses.[32]

31 ir.rackspace.com/news-releases/news-release-details/update-recent-cybersecurity-incident
32 msspalert.com/news/rackspace-taking-losses-of-roughly-11-million-for-hosted-exchange-ransom-attack

Gráfico 7: **Incidentes cibernéticos que afectan a mercados clave, por sector** (agosto de 2023 – agosto de 2025)



- Gobierno y administración
- Tecnología de la información y telecomunicaciones
- Finanzas y seguros
- Energía y servicios públicos, incluyendo petróleo y gas
- Fabricación
- Productos farmacéuticos y asistencia sanitaria
- Logística y transporte, incluido el marítimo
- Educación y formación, incluidos los grupos de expertos
- Hoteles y entretenimiento
- Otro

Fuente: Control Risks

Las empresas de todo el mundo están cada vez más expuestas a fallos operativos, pérdidas financieras y daños a su imagen, ya que los atacantes aprovechan nuevas vulnerabilidades. El uso cada vez mayor de servicios de terceros, como el alojamiento en la nube, el software externo o las herramientas de inteligencia artificial en las operaciones diarias, ha brindado a los actores maliciosos más oportunidades para atacar.

Resiliencia desde el diseño

Si la adopción de la nube y la integración de la IA se aceleran al ritmo previsto, los atacantes seguirán beneficiándose del aumento de oportunidades y puntos de entrada, y las empresas seguirán siendo vulnerables a los ataques. Es fundamental tener una estrategia fuerte para prevenir y afrontar ataques digitales, sobre todo los que afectan servicios externos y la nube, pilares de muchas operaciones empresariales.

Para ser más resilientes, las empresas deben incorporar la gestión de riesgos digitales desde el diseño de sus tecnologías. Esto implica implementar protocolos sólidos de gestión de identidades y accesos (Identity and Access Management, IAM), realizar auditorías periódicas de configuración y cifrar los datos confidenciales en todos los entornos de nube. Las medidas proactivas, como la supervisión continua, la inteligencia sobre amenazas y los planes de respuesta ante incidentes, ayudan a detectar y contener las amenazas antes de que se agraven.

Las empresas también deberían revisar cómo gestionan la seguridad de sus proveedores externos y definir protocolos claros para minimizar riesgos en su cadena de suministro. Al adoptar estas prácticas de forma conjunta, las organizaciones protegerán mejor sus operaciones, preservarán la continuidad y mantendrán la confianza en un panorama cibernético cada vez más volátil.

Construir resiliencia implica integrar la gestión del riesgo cibernético en todo el ciclo de vida de la tecnología. Esto significa aplicar protocolos sólidos de gestión de identidades y accesos, realizar auditorías periódicas de configuración y proteger los datos sensibles mediante cifrado.

Caso Práctico

Microsoft Azure, 2024

En julio de 2024, un ataque distribuido de denegación de servicio (Distributed Denial-of-Service, DDoS) interrumpió la plataforma en la nube Azure de Microsoft, dejando los servicios fuera de línea durante hasta ocho horas. La interrupción fue causada por un aumento repentino en el uso que afectó a Azure Front Door y Content Delivery Network.[33]

33 forbes.com/sites/kateoflahertyuk/2024/07/31/microsoft-confirms-new-outage-was-triggered-by-cyberattack

Pasos para desarrollar la resiliencia cibernética

Las empresas con mayor madurez pueden desarrollar una resiliencia cibernética adecuada a su nivel mediante diversas medidas:

Comprender e indexar los perfiles de riesgo para identificar los activos críticos, las amenazas y las vulnerabilidades, y documentar una visión clara de las exposiciones de la organización.

Definir el riesgo organizacional aceptable para que los líderes establezcan límites claros para el riesgo y la exposición aceptables.

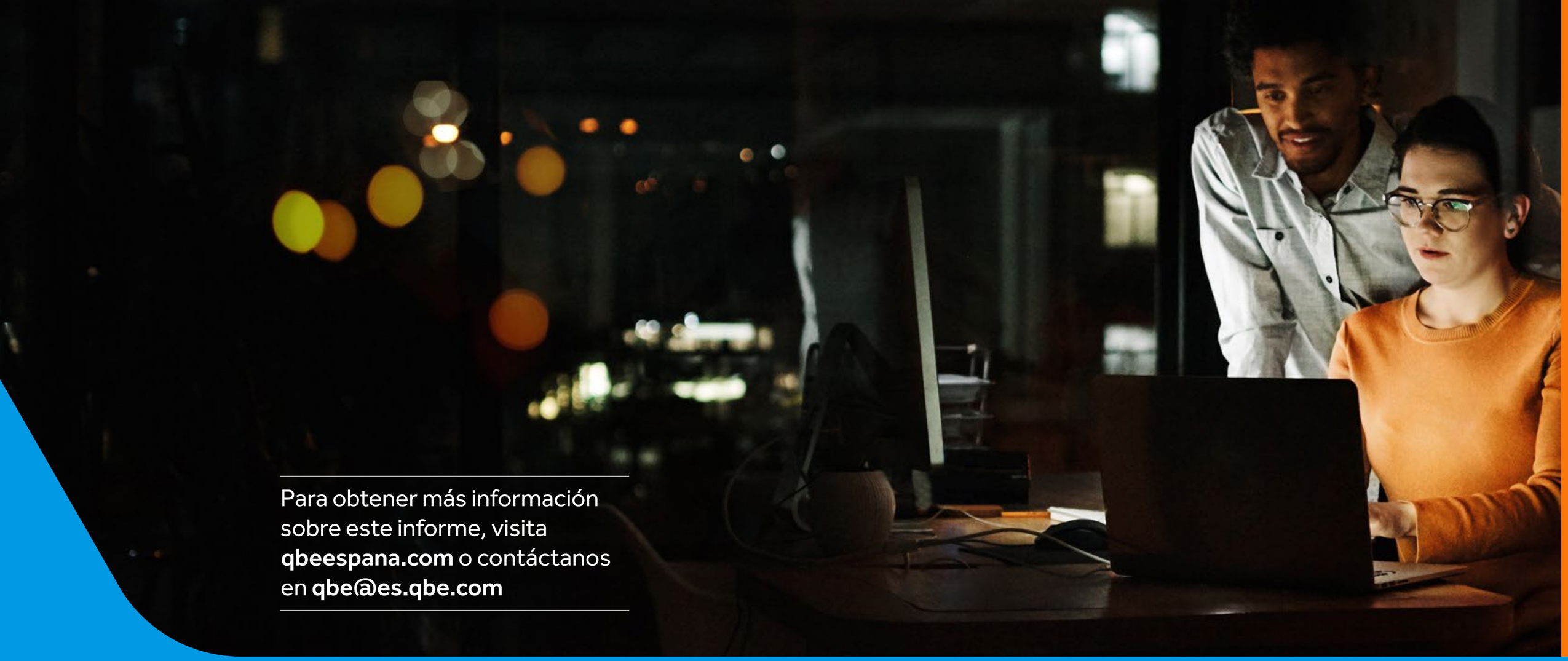
Priorizar las estrategias de mitigación de riesgos que concentran los recursos donde tendrán mayor impacto.

Prepararse para los peores escenarios con planes de contingencia y protocolos de recuperación probados.

Probar las capacidades de gestión de crisis para someter a pruebas de estrés la toma de decisiones, la comunicación y la respuesta ante crisis.

Integrar el apoyo de terceros en la estrategia de ciberseguridad para proporcionar experiencia en la gestión de riesgos residuales.

Supervisar de forma proactiva las tendencias y adaptar las ciberdefensas para adelantarse a las amenazas en constante evolución, las nuevas tecnologías y las necesidades cambiantes de las empresas.



Para obtener más información sobre este informe, visita **qbeespana.com** o contáctanos en **qbe@es.qbe.com**

QBE Europe SA/NV
Sucursal en España
Paseo de la Castellana
31-5a Planta
28046 Madrid
Spain
+34 91 789 39 50

QBEespana.com

Este informe está elaborado para QBE por Control Risks

QBE
At the heart of it

1012154/2510-ES