



CHUBB®

Gestionar la velocidad del riesgo:
**Inteligencia artificial,
litigios y resiliencia**

Informe de Siniestros Cibernéticos 2026

Sección uno

Introducción: Divergencia

La naturaleza del riesgo cibernético sigue evolucionando, mientras se amplía el alcance de las vulnerabilidades y la exposición al riesgo. Impulsados por la integración eficaz de sistemas de detección basados en IA y una mayor resiliencia, varios mercados globales han visto cómo la frecuencia de los incidentes cibernéticos se estabilizaba en 2025, según informes recientes. EE. UU., por su parte, alcanzó un máximo histórico en gravedad, con el coste medio de una brecha de datos en 2025 superando los \$10.2 millones – más del doble de la media mundial de \$4.4 millones.

En última instancia, el éxito de cualquier empresa – o de cualquier mercado geográfico – a la hora de protegerse frente a incidentes cibernéticos depende de comprender un panorama de amenazas en constante cambio, los marcos legales y regulatorios que rigen la captación y el almacenamiento de datos, y la interconexión de los socios comerciales que incrementan la exposición a lo largo y ancho de la cadena de suministro de una empresa.

.....

Esta edición del informe Chubb Cyber Claims analiza los datos históricos de siniestros de Chubb hasta diciembre de 2025 para ofrecer claves sobre las tendencias de frecuencia y gravedad de los siniestros – y los factores que impulsan estas tendencias – con el fin de ayudar a las empresas a desenvolverse en un entorno complejo de riesgo cibernético y reforzar su resiliencia financiera y operativa.

Fuente: Informe 2025 de IBM sobre el coste de una brecha de datos

Sección dos

Tendencias globales de siniestros

01

La IA acelera la velocidad del riesgo.

La misma tecnología de IA que ha permitido detectar incidentes cibernéticos con mayor rapidez y exhaustividad ha cambiado de raíz la velocidad a la que se producen: al incorporar IA agentiva y autónoma al malware, los actores maliciosos ya están comprometiendo varios sistemas en cuestión de minutos, dejando prácticamente sin margen para la intervención manual. El uso de IA avanzada por parte de estos actores, como los modelos de lenguaje de gran tamaño (LLM), crece casi al mismo ritmo que la adopción de la IA por parte del público general.

02

El reflejo de “primero, demandar”.

Un incidente cibernético ya no es solo un fallo técnico que haya que corregir: a menudo se convierte en el detonante de acciones legales poco después del suceso. En los últimos 30 años, las leyes de privacidad y protección de datos se han aprobado a un ritmo extraordinario, aumentando la complejidad del cumplimiento normativo y la frecuencia de los litigios por privacidad. La distancia entre una brecha y la primera demanda colectiva se ha acortado, y no es raro que el litigio llegue en cuestión de días, con acusaciones diversas independientemente del tamaño de la entidad o de los controles que se consideren inexistentes.

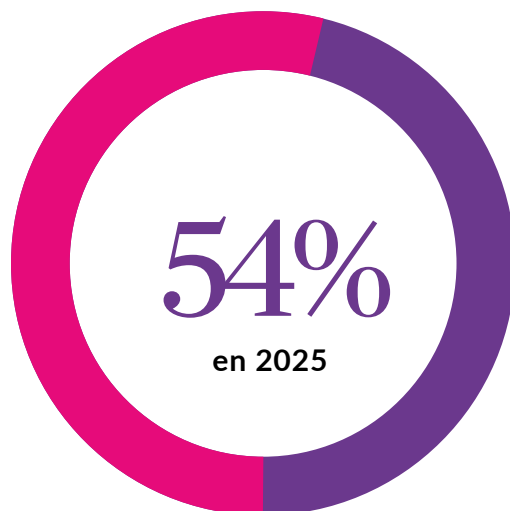
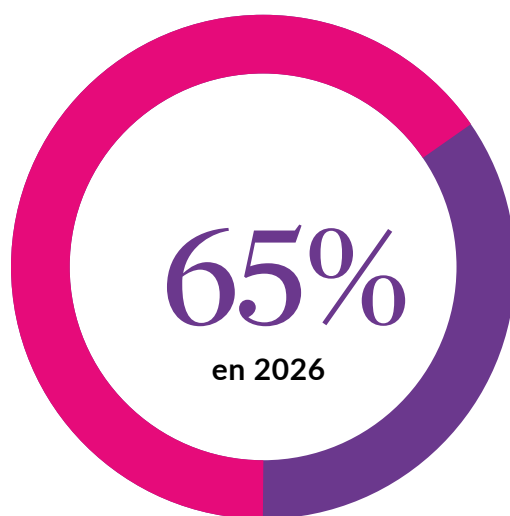
03

Interdependencia sistémica.

Hace apenas unos años, los responsables de riesgos se centraban sobre todo en evitar que sus propios fallos de ciberseguridad afectaran a sus clientes y proveedores. Hoy existe una conciencia generalizada del enorme impacto que la propia cadena de suministro de la organización puede tener en la frecuencia y la gravedad de los incidentes cibernéticos.

En todos los mercados, el aumento de los siniestros cibernéticos vino impulsado por cambios en el panorama tecnológico y legal, así como por la interconexión de las cadenas de suministro. Destacan tres tendencias.

Según el [World Economic Forum](#), el 65% de las grandes empresas considera actualmente las vulnerabilidades de terceros y de la cadena de suministro su principal reto en ciberseguridad — frente al 54% en 2025.



Un ciberincidente en un fabricante mundial de automóviles

Como se explicará con más detalle más adelante, sucesos como el incidente cibernético de agosto de 2025 que afectó a un fabricante global de automóviles pusieron de relieve el enorme impacto económico y operativo que puede tener un ciberincidente en cualquier eslabón de la cadena de suministro. El episodio sacudió toda la economía británica, provocando un efecto generalizado de forma inmediata. Además de las cuantiosas pérdidas económicas que el fabricante sufrió por las paradas de producción, ahora se enfrenta a numerosas demandas colectivas relacionadas con el incidente.

Sección tres

Frecuencia y gravedad de los incidentes cibernéticos

La frecuencia —el número de siniestros por póliza— y la severidad —el coste medio por siniestro— son los pilares del coste de siniestralidad en seguros y los principales motores de los cambios en las primas. Dado que el seguro, por naturaleza, es un negocio en el que la prima cobrada va por detrás del coste real de los siniestros, las tendencias históricas recientes en frecuencia y severidad son un indicador adelantado de las tarifas del próximo año.

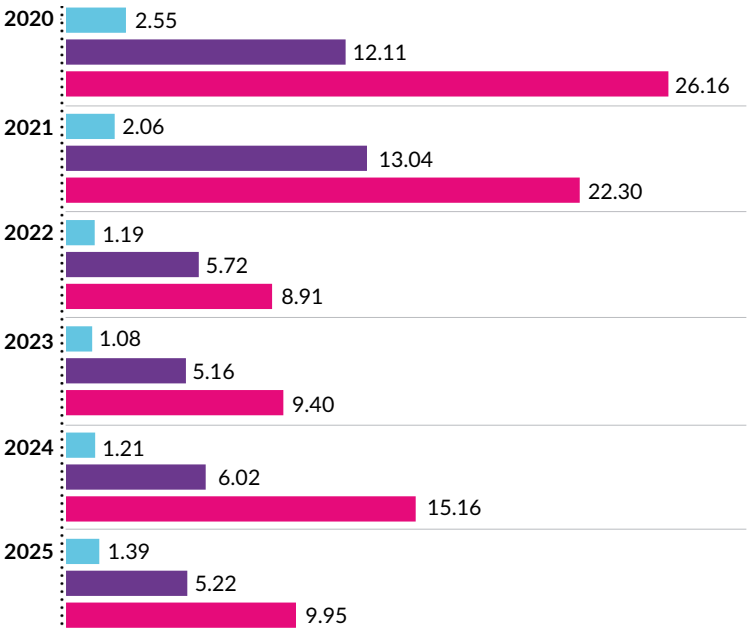


Las tablas contiguas ofrecen una visión dispar de las tendencias de frecuencia y severidad en el **panorama cibernético de EE. UU.** a lo largo de los últimos seis años.

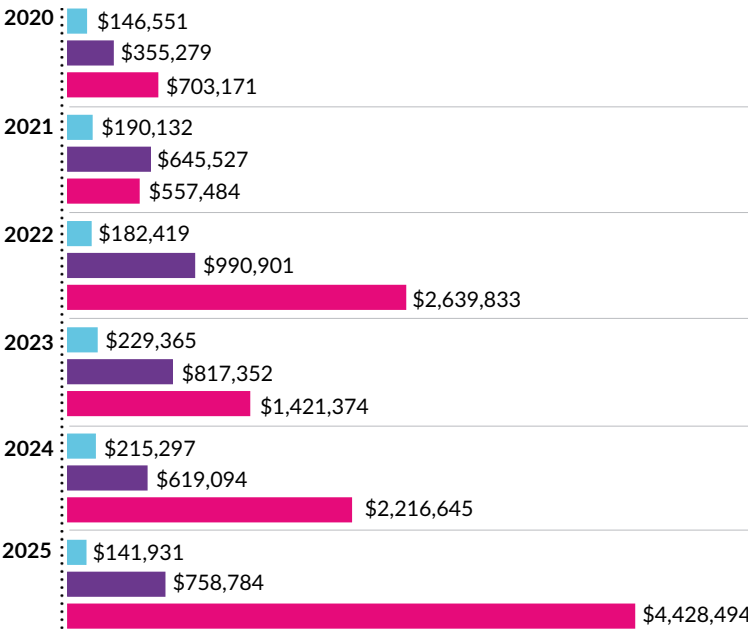
La mejora en los perfiles de seguridad de los clientes y en sus capacidades de resiliencia se refleja en la notable reducción de la frecuencia de siniestros en empresas de todos los tamaños entre 2020 y 2022. Al mismo tiempo, los datos muestran un aumento general de la frecuencia en las pequeñas y medianas empresas (PYME) y en los grupos de riesgo de gran tamaño desde 2022, mientras que el segmento mid-market se mantuvo más estable durante el mismo periodo.

La contratación de límites ha disminuido desde 2021, aunque la severidad ha aumentado. Si bien la severidad se mantuvo estable en el segmento PYME, aumentó de forma considerable en el mid-market y aún más acusadamente en el segmento de grandes cuentas. Hay varios factores que contribuyen a este incremento, entre ellos el aumento de los costes por interrupción del negocio y el encarecimiento de los litigios relacionados tanto con brechas de datos como con la privacidad.

Frecuencia de siniestros cibernéticos por cada 100 pólizas (EE. UU.)

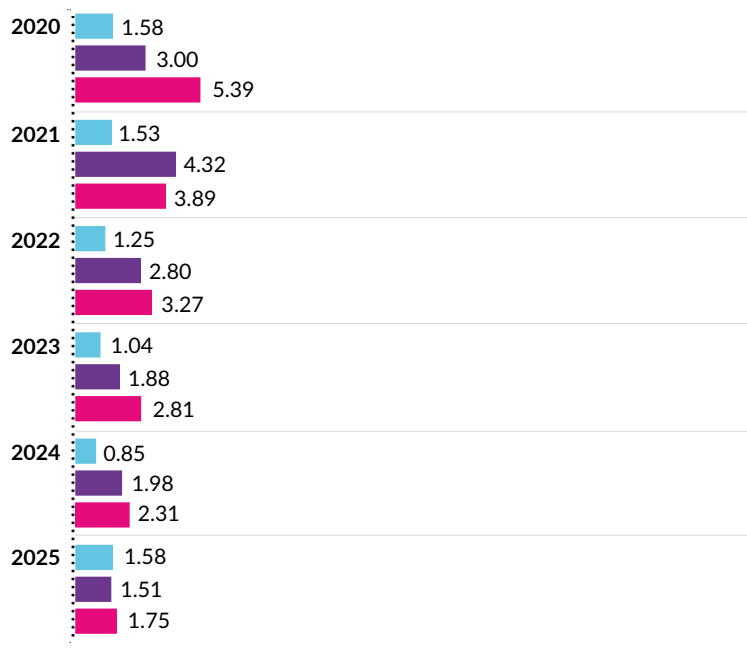


Severidad media de los siniestros cibernéticos (EE. UU.)

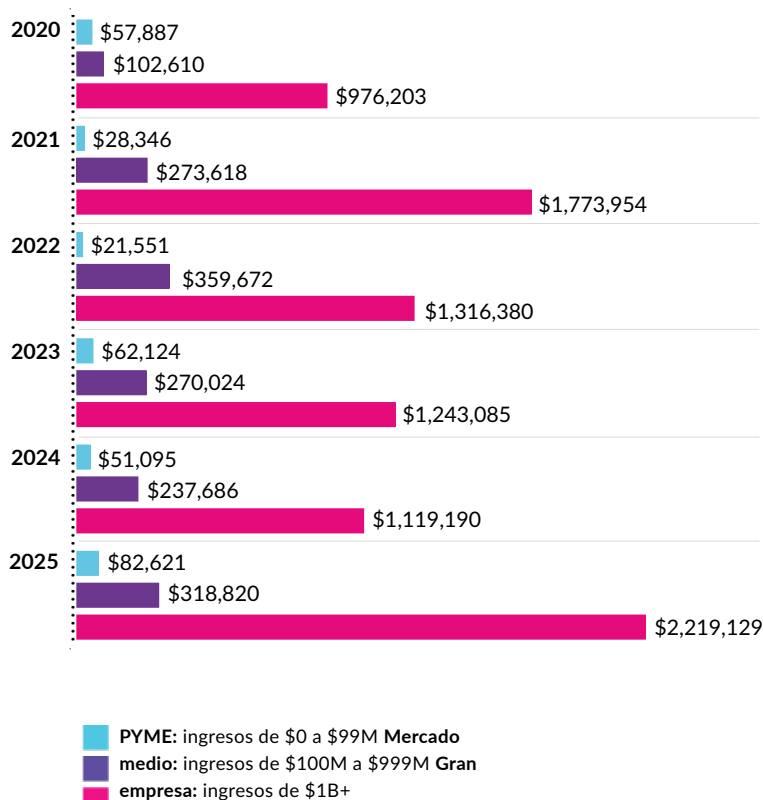


PYME: ingresos de \$0-\$99M
 Mid-Market: ingresos de \$100M-\$999M
 Grandes: ingresos de \$1B+

Frecuencia de siniestros cibernéticos por cada 100 pólizas (Europa + Reino Unido)



Gravedad media de las reclamaciones cibernéticas (Europa + Reino Unido)



Las tendencias en Europa y el Reino Unido muestran similitudes y diferencias frente a EE. UU.

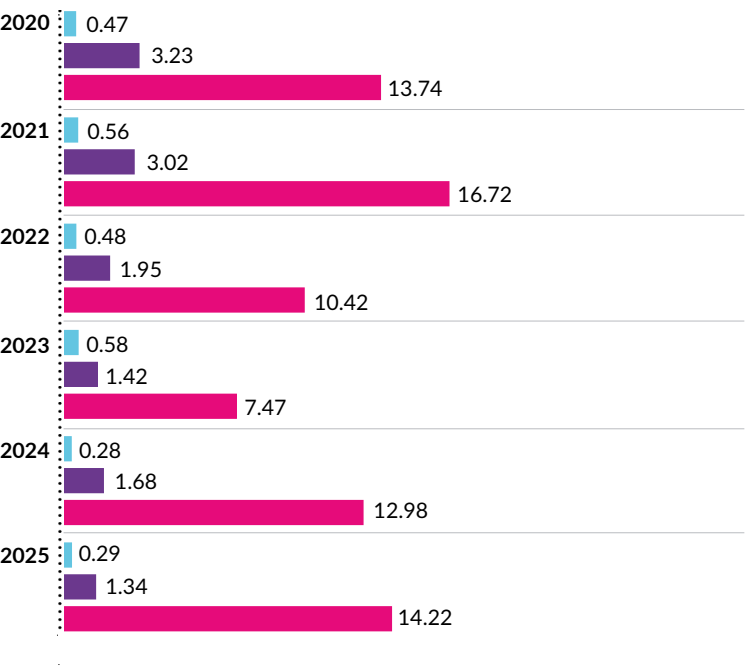
Los niveles de frecuencia son parecidos en la cohorte de pymes, pero mucho más bajos en los segmentos de middle market y grandes cuentas. Esto indica que la probabilidad de sufrir un ataque y el perfil general de seguridad, junto con los controles implantados, son similares entre las pymes de EE. UU., Europa y el Reino Unido. En cambio, se observa una reducción clara de la exposición en los segmentos de empresas medianas y grandes en Europa y el Reino Unido frente a EE. UU., debida en gran medida a la ausencia de reclamaciones vinculadas a litigios de terceros.

La severidad es menor en todas las cohortes de Europa y el Reino Unido, también en gran parte por la ausencia de gastos relevantes de litigios de terceros, tanto en reclamaciones por brecha de datos como en reclamaciones de privacidad sin brecha de datos. Aunque la severidad aumenta claramente en todas las cohortes, se mantiene más estable que en EE. UU.

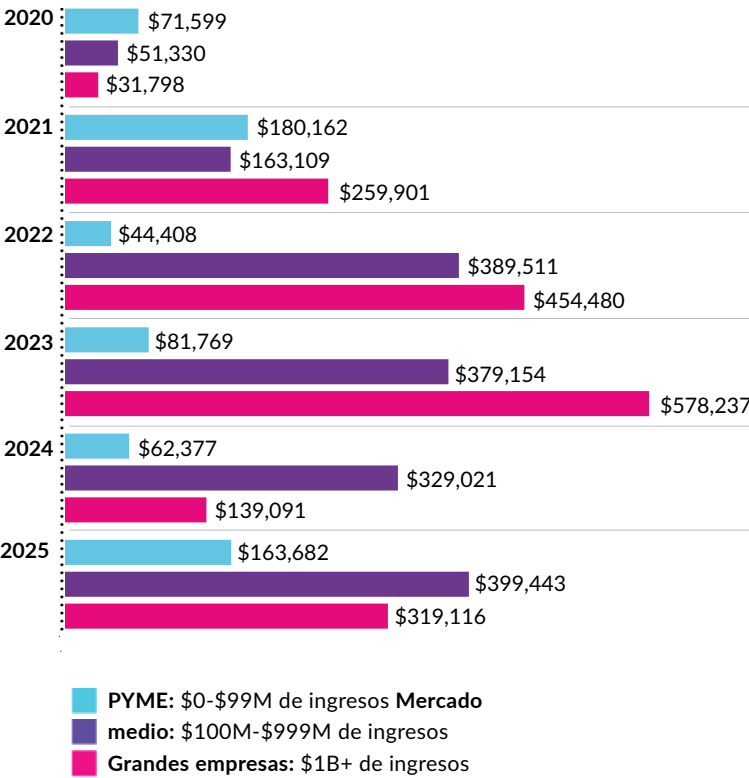
En **Australia y Nueva Zelanda**, los niveles absolutos de frecuencia y severidad, así como la tendencia general, difieren frente a otras partes del mundo, pero siguen una trayectoria general similar.

La frecuencia cayó de forma notable, mientras que la severidad, por lo general, aumentó tras 2021. La frecuencia en pymes es solo una fracción de la observada en otras regiones del mundo, aunque la severidad está más o menos en línea. En el segmento de empresas medianas, la frecuencia se sitúa en niveles similares a los de Europa y el Reino Unido —y muy por debajo de EE. UU.—, lo que refleja un entorno legal relativamente benigno en materia de brechas de datos cibernéticas y acciones de privacidad sin brecha de datos. Cabe destacar también que los segmentos de empresas medianas y grandes registraron niveles de severidad más bajos, con incrementos más moderados a lo largo del tiempo.

Frecuencia de siniestros cibernéticos por cada 100 pólizas (Australia y Nueva Zelanda)



Severidad media de las reclamaciones cibernéticas (Australia y Nueva Zelanda)



Sección
cuatro

La carrera armamentística de la IA: Ataque y defensa

La adopción y el avance de la IA a escala mundial han impulsado un uso cada vez más sofisticado de la tecnología con fines adversarios, así como herramientas eficaces de detección y corrección.



Además, **siguen produciéndose incidentes de IA menos complejos**, como cuando un empleado sube por error Información de Identificación Personal (PII) a un LLM accesible públicamente, lo que desemboca en un incidente de ciberseguridad.

En el plano defensivo, empresas y organizaciones pueden implantar herramientas de mitigación de riesgos contrastadas y centradas en la IA para responder a estas amenazas y reducir su exposición.

Entre ellas:



Defensas AI-First: Implantar operaciones de seguridad impulsadas por IA (AISO) para detectar amenazas en tiempo real.



Gobernanza de la IA: Mantener un inventario riguroso de todos los sistemas de IA y auditar las prácticas de gestión de datos de terceros.



Formación reforzada: Concienciar al personal sobre los riesgos de seguridad impulsados por IA, como el phishing avanzado y los deepfakes.

Sección cinco

El impacto del fraude por ingeniería social

Las reclamaciones por fraude de ingeniería social pueden ser muy graves, sobre todo para las pequeñas y medianas empresas. El riesgo de pérdidas económicas, interrupciones operativas y daños a la reputación pone de relieve la necesidad urgente de contar con estrategias eficaces de respuesta y recuperación.





El suceso: Tras actuar siguiendo un correo que parecía proceder de un representante de un proveedor de maquinaria habitual, una persona recién incorporada modifica los datos bancarios para el pago al proveedor, cambiándolos a una nueva entidad, sin intentar antes verificar el mensaje llamando al proveedor a su oficina.



El impacto: Más tarde, la empresa se da cuenta de que la persona empleada fue víctima de un fraude de ingeniería social cuando el empleado real del proveedor reclamó el pago y se descubrió que el correo era fraudulento y que el dinero se había enviado a un impostor.

\$100,000

La solución: Pérdida de más de \$100,000.

Sin posibilidad de recuperar el dinero ni del banco ni del proveedor.



El resultado: La póliza ciber, con una ampliación de cobertura para ciberdelito, reembolsa al tomador del seguro las pérdidas no recuperables.

Incidente cibernético por fraude de ingeniería social

Sección Seis

La nueva frontera de la privacidad y el reflejo de litigar primero

A medida que los incidentes cibernéticos se convierten cada vez más en asuntos legales, las empresas se enfrentan a nuevos retos jurídicos derivados de teorías de responsabilidad novedosas, especialmente en lo relativo a la interceptación de comunicaciones y a las tecnologías de seguimiento digital.

Entre los principales factores que influyen en la responsabilidad legal se incluyen:



El reflejo de “primero, litigar”: En EE. UU., los abogados de los demandantes están recurriendo a leyes de escuchas de hace décadas (como la **California Invasion of Privacy Act**) y a normas de privacidad de vídeo (como la federal **Video Protection Privacy Act**) para poner en el punto de mira tecnologías web estándar, incluido el seguimiento mediante píxeles.



Arbitraje masivo: En EE. UU., las empresas se ven obligadas a pagar elevadas tasas administrativas por adelantado por cada reclamación individual. En una demanda con 10.000 demandantes, por ejemplo, estas tasas no reembolsables pueden superar los \$10 millones antes incluso de que se entre a valorar el fondo del asunto.



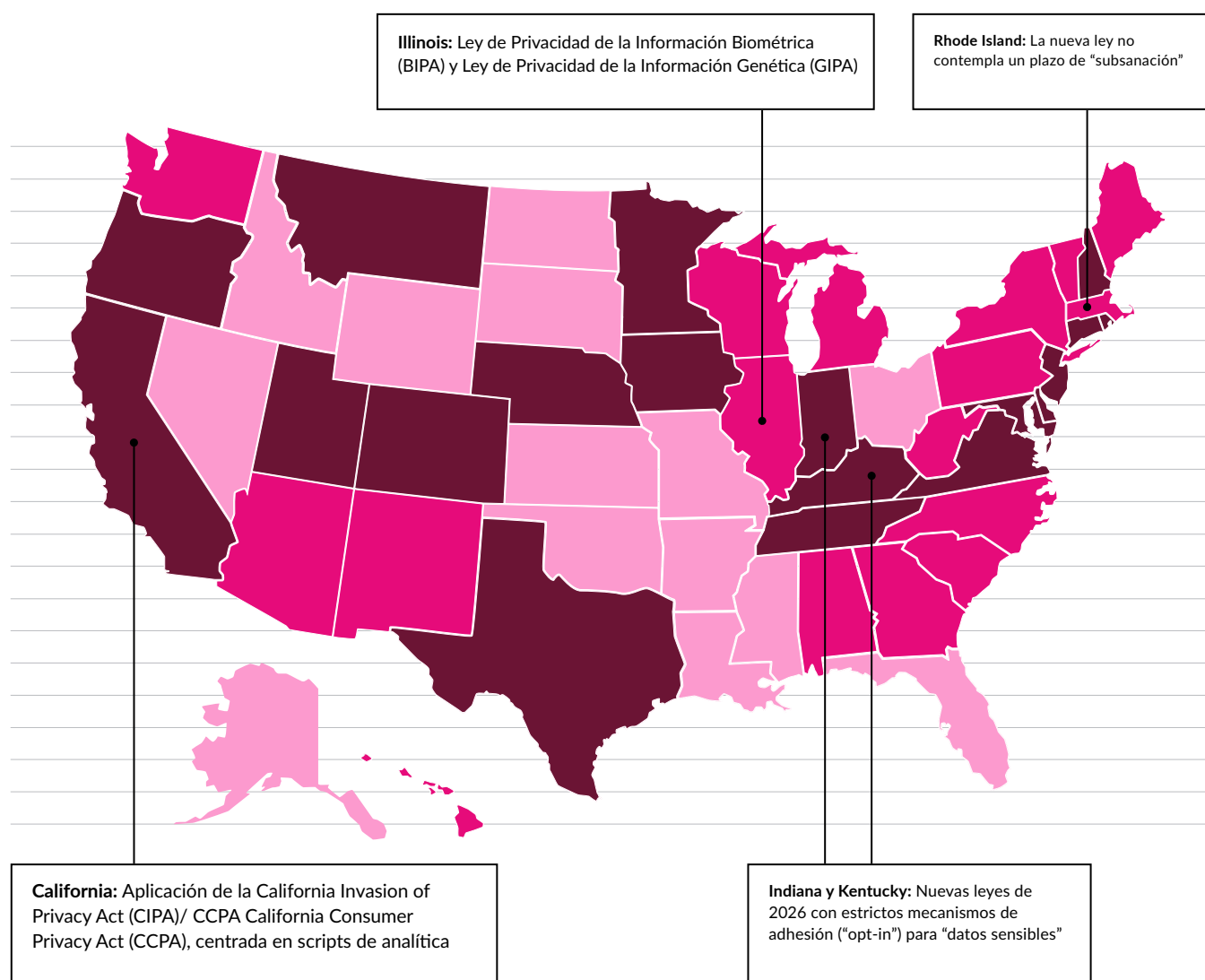
Supresión de datos: Los atacantes están optando por borrar o filtrar datos de forma deliberada en lugar de limitarse a cifrarlos, lo que provoca una “pérdida de control” permanente – y puede elevar lo que está en juego en un litigio.

Cada vez más leyes de privacidad en EE. UU. y la UE imponen obligaciones complejas y escalonadas a las empresas que almacenan y/o transfieren datos personales. Entre ellas se incluyen el derecho a excluirse del perfilado o de la toma de decisiones automatizada, requisitos de transparencia sobre el tratamiento impulsado por IA, y evaluaciones de riesgo obligatorias para casos de uso de alto riesgo.

Estados Unidos

Seguimiento de legislación sobre privacidad

No existe una ley federal, sino más bien un mosaico de normativas según el estado.



Estatuto/proyecto de ley en tramitación legislativa:

■ Legislación aprobada ■ Legislación pendiente ■ Sin legislación

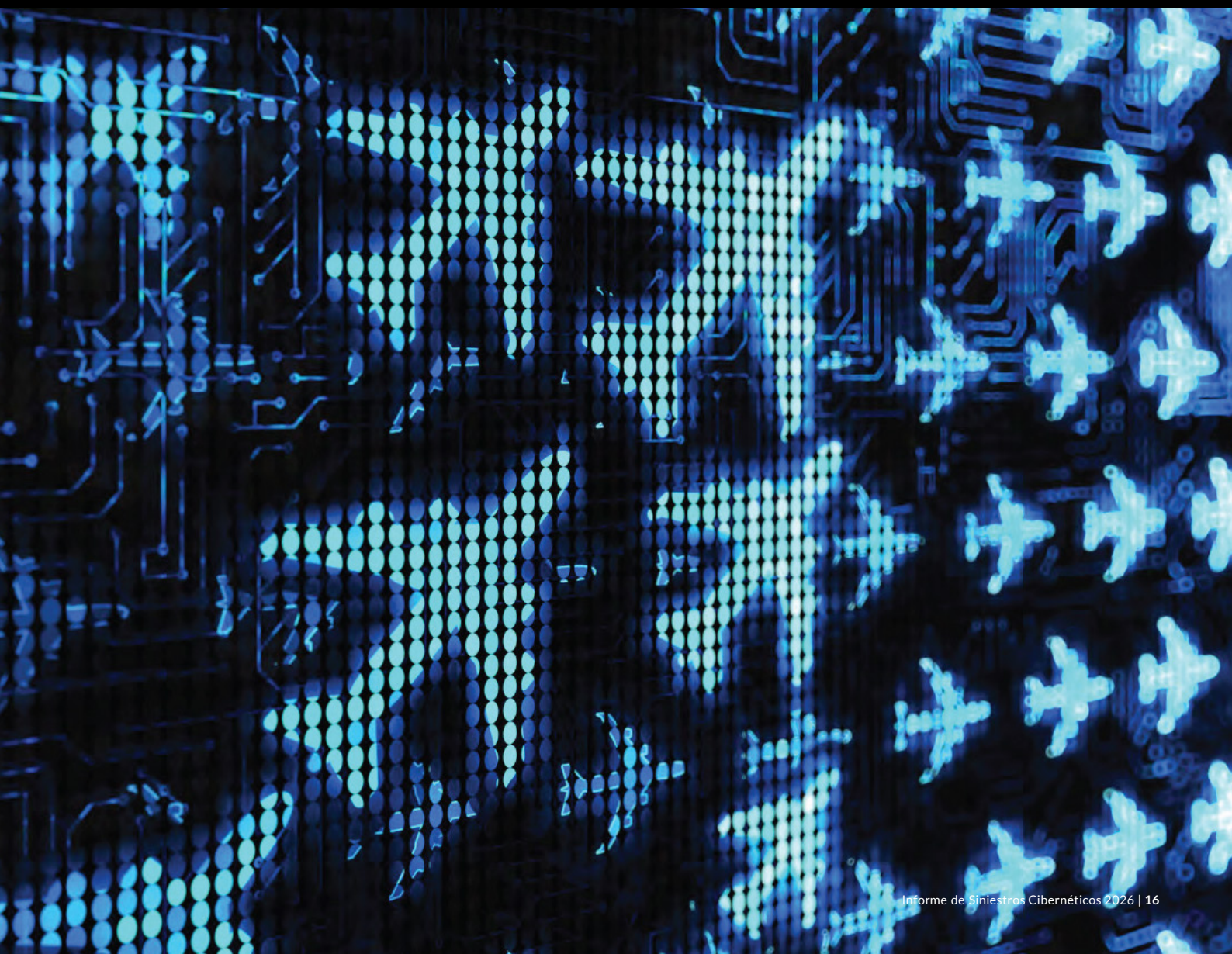
Fuente: *Rastreador de legislación federal de privacidad de EE. UU.*

Para las empresas del Reino Unido y Europa, es importante tener en cuenta este mosaico de normativas estatales al comerciar con EE. UU. o dentro del país. Para saber más, visite [Chubb Cyber Insurance](#).

Sección siete

Protección de datos sensibles

Los incidentes de privacidad se están convirtiendo en una fuente cada vez más habitual y grave de reclamaciones por ciberseguro. Con normativas en constante cambio y el auge de los litigios a gran escala, gestionar el riesgo de privacidad resulta más complejo y caro. Cada organización puede enfrentarse a retos diferentes para proteger los datos en un panorama de amenazas que no deja de evolucionar.



Gestionar los riesgos asociados a la privacidad de los consumidores es esencial. Para apoyar a nuestros asegurados, Chubb ha colaborado con **plataformas de gestión del riesgo** de privacidad que permiten a los asegurados proteger sus organizaciones mediante la evaluación y la gestión proactiva de los riesgos de privacidad, la protección de datos sensibles y el mantenimiento del cumplimiento.

Incidente de privacidad en el mercado medio



El suceso: El asegurado gestiona un sitio web de suscripción y una aplicación móvil que utilizan tecnologías de seguimiento, incluidas cookies y píxeles. El píxel registra determinados datos, como el ID del usuario del sitio web, y los transmite a terceros.



El impacto: Varios despachos de abogados emitieron miles de requerimientos previos al arbitraje alegando que el uso del píxel vulneraba la California Invasion of Privacy Act, que prohíbe interceptar comunicaciones sin consentimiento.

\$40M+

El problema: La póliza de privacidad del asegurado exigía que todas las controversias se resolvieran mediante arbitraje. Sin embargo, las normas del foro arbitral habrían obligado al asegurado a abonar varios millones de dólares en tasas iniciales de presentación incluso antes de entrar a valorar el fondo de las reclamaciones. Por ello, si las demandas se sometían a arbitraje, podía derivar en una posible indemnización por daños legales, más las costas del arbitraje, por un importe superior a \$40 millones.



La solución: Chubb contrató a un equipo jurídico con experiencia en litigios de privacidad y en el trato con los bufetes implicados, lo que condujo a una mediación del conflicto.

\$6.5M

El resultado: Las múltiples reclamaciones se resolvieron de forma global por un importe en torno a \$6.5 millones.

El impacto del ransomware en las pequeñas y medianas empresas

Chubb cuenta con una amplia experiencia en reclamaciones por ransomware y ofrece servicios muy valorados de asesoramiento legal, informática forense, relaciones públicas y otros servicios especializados para ayudar a nuestros asegurados a **responder y gestionar con eficacia los incidentes de ransomware**: reparando o sustituyendo sistemas dañados, minimizando el tiempo de inactividad y retomando la actividad.

Incidente de ransomware en una pyme



El incidente: Los intentos de un grupo de ciberdelincuentes de cifrar el equipo de la entidad asegurada se vieron en gran medida frustrados por su herramienta de detección y respuesta en endpoints. No obstante, el atacante logró filtrar información sanitaria y números de la Seguridad Social de más de 4 millones de personas.



El impacto: La entidad asegurada necesitaba identificar con rapidez y precisión qué datos e información sanitaria personal se habían visto comprometidos para cumplir con las obligaciones de notificación exigidas por las leyes y normativas aplicables.



El problema: Determinar el alcance de la brecha de datos, garantizar una notificación ágil a las personas afectadas y asegurar que las vulnerabilidades sin parche, potencialmente explotadas, se corrigieran lo antes posible.

\$4M

La solución: Se contrató de inmediato a un equipo de asesoría legal, a especialistas forenses y a un equipo de minería de datos para ayudar al asegurado a gestionar este incidente. Tras su revisión exhaustiva de los datos afectados, se notificó el suceso a 4 millones de personas y a numerosos organismos reguladores. También se implicó al equipo de Risk Advisor de Chubb para ayudar al cliente a abordar sus vulnerabilidades sin parchear.

\$4.7M

El resultado: El coste total reembolsado al asegurado fue de \$4.7 millones, incluidos \$2.4 millones en costes de notificación y \$1.2 millones en costes de monitorización de crédito para las víctimas. Además, se informó al asegurado de sus vulnerabilidades sin parchear y se le prestó apoyo para su corrección.

Sección nueve

Ransomware sin fronteras

Los ataques de ransomware siguen suponiendo riesgos graves para las organizaciones de todo el mundo. Incluso las instituciones con medidas avanzadas de ciberseguridad pueden sufrir interrupciones a gran escala cuando los actores maliciosos exfiltran datos sensibles y los publican abiertamente. Las consecuencias a menudo trascienden fronteras, lo que activa el escrutinio regulatorio, obligaciones legales y desafíos operativos.



Como demuestra este incidente en Europa, el ransomware no entiende de fronteras geográficas.

Incidente global de ransomware



El suceso: Un ataque de ransomware perpetrado por un grupo cibercriminal hasta entonces desconocido golpeó a una institución académica internacional y a su división editorial. Se filtraron más de 575.000 documentos sensibles y, posteriormente, se publicaron en el sitio de filtraciones del grupo.



El impacto: La operativa se vio interrumpida en todo el mundo. Datos sensibles, como los ingresos de autores, investigaciones gubernamentales y exámenes futuros, quedaron expuestos en más de 40 países. La recuperación resultó especialmente complicada en regiones con dependencias de TI complejas.



El problema: La institución académica tuvo que evaluar los 575.000 documentos filtrados para determinar el riesgo regulatorio. Fue necesario contar con asesoramiento legal en 40 jurisdicciones, lo que incrementó notablemente la complejidad y la presión para cumplir los requisitos globales de conformidad.



La solución: Chubb movilizó a expertos legales y forenses, y la minería avanzada de datos detectó contenido de alto riesgo, lo que permitió una revisión rápida, en gran medida automatizada. La coordinación del asesoramiento jurídico entre continentes garantizó notificaciones regulatorias precisas y puntuales.

\$14.2M

El resultado: Las pérdidas ascendieron a \$14.2 millones, incluidos los gastos de respuesta al incidente cibernético y las pérdidas por interrupción del negocio. Gracias a una actuación rápida y al apoyo jurídico coordinado, la institución académica evitó multas, investigaciones regulatorias o sanciones. A pesar de la magnitud de la brecha, los impactos reputacionales y regulatorios se contuvieron con éxito.

Eventos generalizados: los costes en cadena de la interdependencia

Ninguna empresa funciona en una burbuja: depende de socios, proveedores y clientes. Dos ciberataques relevantes de 2025 muestran hasta qué punto el impacto de un episodio de ransomware puede extenderse a varias compañías, a lo largo y ancho de la cadena de suministro de una organización. Aunque Chubb ya dio la voz de alarma sobre este asunto en 2022, la gravedad de este tipo de incidentes está cobrando ahora mucha más visibilidad en todo el ámbito de la ciberseguridad.



Reino Unido – agosto de 2025

Fabricante mundial de automóviles

El ataque de finales de agosto de 2025 contra un fabricante mundial de automóviles es el incidente cibernético más devastador de la historia británica. Los detalles del suceso son una advertencia clara, con lecciones clave para todas las empresas.



El incidente

Atribuido a “Scattered Lapsus Hunters”, el ataque obligó a desactivar las redes globales de TI para contener la brecha.



El impacto operativo

La producción se detuvo durante cinco semanas en las plantas del Reino Unido, Eslovaquia, Brasil y China. Entre los sistemas paralizados estaban los controles de la línea de producción, el equipamiento de diseño CAD/PLM y las plataformas de pedidos de los concesionarios.



Las repercusiones en seguridad y en el ámbito legal:

Los atacantes extrajeron datos de nóminas y registros de clientes de hasta 7,4 millones de personas, lo que derivó en una oleada de demandas.

Las consecuencias financieras sistémicas

£1.9B

Económico

La economía del Reino Unido registró una pérdida estimada de £1.9 mil millones (\$2.5 mil millones), lo que contribuyó a la desaceleración del PIB en el T3 de 2025.

£1.2B

Impacto en la cadena de suministro

Más de 5.000 organizaciones del Reino Unido se vieron afectadas; el Gobierno intervino con £1.2 billion en préstamos de emergencia para estabilizar la cadena.

£485M

Pérdidas de la empresa

El fabricante global de automóviles declaró unas pérdidas antes de impuestos de £485 millones, frente a un beneficio de £398 millones del año anterior.

Estados Unidos – febrero de 2025

Brecha de datos en Oracle Health

A principios de 2025, Oracle Health (antes Cerner) sufrió una **importante brecha de datos** que los analistas han calificado como una de las más grandes en la historia del sector sanitario estadounidense.



El incidente

Los atacantes utilizaron credenciales robadas para acceder a servidores heredados de migración de datos de Cerner que aún no se habían trasladado a Oracle Cloud.



La vulnerabilidad clave

La brecha se centró en un entorno heredado —con partes que no se usaban desde 2017—, dejando claro que los datos “olvidados” son un objetivo prioritario.



El impacto

El ataque se hizo con registros de aproximadamente 80 hospitales, dejando expuestos los números de la Seguridad Social de los pacientes, además de sus historiales médicos, incluidos diagnósticos e imágenes de tratamientos.



El factor de extorsión

Un cibercriminal que operaba bajo el alias Andrew exigió millones en criptomonedas para impedir la publicación de los archivos robados.

Estos y otros sucesos de 2025 – muchos de ellos causados por errores o incidentes, más que por acciones malintencionadas (p. ej., **la caída de octubre de Amazon Web Services**) – ponen de relieve la necesidad de identificar e implantar las medidas de mitigación del riesgo cibernético más estrictas disponibles.

Aunque estos escenarios puedan parecer lejanos para **las pequeñas empresas**, la experiencia de Chubb demuestra que nada más lejos de la realidad.

Incidente con un proveedor (PYME)



El suceso: El comercio asegurado contrató a un proveedor tecnológico externo para disponer del software necesario en la operativa diaria. Cuando dicho proveedor fue objetivo de un ataque de ransomware, todos sus sistemas quedaron fuera de servicio.



El impacto: Al no poder utilizar el software, el asegurado no pudo vender determinados productos, reponer inventario ni programar citas con clientes.



La solución: Chubb recurrió a un contable forense para ayudar al asegurado a calcular la pérdida derivada de la interrupción contingente del negocio. La preparación del asegurado con su plan de respuesta ante incidentes y la coordinación con el equipo de siniestros de Chubb ayudaron a gestionar un suceso que, en gran medida, escapaba al control del asegurado.

\$1.2M

El resultado: La pérdida total ascendió a \$1.2 millones.

Sección once

Chubb: Impulsando a las empresas con información clave para reducir el riesgo cibernético

Además de las herramientas para reducir el riesgo, el conocimiento es una de las mejores defensas frente a unas amenazas cibernéticas en constante evolución. Chubb ofrece a los asegurados una variedad de información y análisis para ayudar a prevenir incidentes cibernéticos y a minimizar su impacto.



El Índice Cibernético de Chubb

El **Índice Cibernético de Chubb**, lanzado en **2015**, ofrece acceso en tiempo real a los datos globales de siniestros propios de Chubb y a información clave sobre las amenazas, tendencias y costes cibernéticos actuales.

La plataforma con función de búsqueda permite a los usuarios definir parámetros y consultar tendencias históricas basadas en:



Actividad de incidentes: Desglose de las tendencias de ciberamenazas que afectan a las organizaciones, por tamaño, sector y región geográfica.



Costes de los siniestros: Desglose de los costes de los siniestros cibernéticos de Chubb por tamaño de la organización y sector.



Calculadora de riesgo cibernético: Una herramienta que ofrece información sobre el espectro más amplio de exposiciones cibernéticas y los posibles costes por pérdidas cibernéticas.

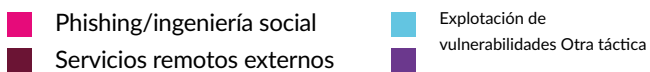


Información sobre compras entre pares: Permite a las empresas comparar su propia protección cibernética con la de organizaciones similares.

Inteligencia de amenazas de Chubb

Además de nuestro Informe de Siniestros Cibernéticos, Chubb publica un [Informe trimestral de Inteligencia de Amenazas](#) para ofrecer a los profesionales de la ciberseguridad información clara y práctica sobre las últimas tendencias en amenazas y la experiencia de Chubb en siniestros.

Un informe reciente mostró que la táctica de acceso inicial más habitual que desembocó en un incidente de ransomware en 2025 fue el phishing. La explotación de servicios remotos externos (p. ej., uso indebido de VPN, puertos abiertos) ocupó el segundo lugar, mientras que la explotación de vulnerabilidades graves se situó en tercero.



En comparación con 2022, la proporción de siniestros derivados de la explotación de vulnerabilidades graves bajó de casi el 22% al 9%, en línea con el lanzamiento por parte de Chubb de su Programa de Divulgación de Gestión de Vulnerabilidades, mediante el cual nuestro equipo de Inteligencia de Amenazas Cibernéticas prioriza las vulnerabilidades explotables más críticas y envía alertas específicas únicamente a los tomadores de póliza que podrían verse afectados por dichas vulnerabilidades. Este servicio se ofrece sin coste a todos los tomadores de pólizas de Chubb Cyber.



A través de nuestro [Programa de divulgación y gestión de vulnerabilidades Outreach Programme](#), Chubb analiza continuamente nuestra cartera y avisa a corredores y tomadores de póliza de problemas graves y explotables que requieren aplicar parches, ya sea en la renovación o durante la vigencia de la póliza. Este servicio se ofrece de forma **gratuita** a todos los tomadores de pólizas Chubb Cyber.

Además de nuestro Programa de divulgación y gestión de vulnerabilidades, Chubb ofrece servicios centrados en el phishing, diseñados específicamente para ayudar a los asegurados a reducir la exposición a ataques de phishing, entre ellos:



Formación

Cursos, juegos y actividades de concienciación en seguridad y prevención del phishing para empleados, basados en las amenazas más recientes.



Pruebas

Simulaciones de correos electrónicos de phishing, incluidas simulaciones con tecnología deepfake, para poner a prueba la toma de decisiones del personal.



Tecnología

Una herramienta de seguridad del correo con IA para ayudar a detectar la intención de phishing, el lenguaje y anomalías de comportamiento que probablemente pasarían desapercibidas para una persona.

Conclusión

Resiliencia en una era de aceleración

En 2025, el riesgo cibernético estuvo marcado por la aceleración. Los ataques de IA autónoma, la ampliación de la normativa de privacidad y las tácticas de arbitraje masivo son algunos de los factores que acortan los plazos y multiplican las posibles consecuencias de los incidentes cibernéticos.

Invertir en capacidades avanzadas de detección, reforzar la gobernanza de la IA y las prácticas de datos, y poner a prueba la resiliencia de los ecosistemas de terceros son algunas de las muchas formas en que las organizaciones pueden reducir de manera significativa su vulnerabilidad.

Como desde hace décadas, Chubb está aquí para ayudar. Nuestra experiencia global en ciberseguridad, la solidez de nuestros datos de siniestros y unas capacidades integradas de mitigación del riesgo y respuesta permiten a nuestros clientes anticiparse, resistir y recuperarse de los complejos ciberincidentes de hoy, y prepararse para lo que venga después. Esperamos seguir trabajando con clientes de todo el mundo, reforzando la resiliencia financiera y operativa frente al ciberriesgo.



Para saber más, visita

[Seguro Ciber de Chubb](#)

CHUBB®

Confía en Chubb para una protección cibernética integral y una mayor resiliencia.

Todo el contenido de este material se ofrece únicamente con fines informativos de carácter general. No constituye asesoramiento personal ni una recomendación, para ninguna persona o empresa, de ningún producto o servicio. Consulte la documentación de la póliza emitida para conocer íntegramente los términos y condiciones de la cobertura.

Chubb EuropeanGroupSE, Sucursal en España, con domicilio en el Paseo de la Castellana 141, Planta 6, 28046 Madrid y C.I.F. W-0067389-G. Inscrita en el Registro Mercantil de Madrid, Tomo 19.701, Libro 0, Folio 1, Sección 8, Hoja M346611, Libro de Sociedades. Entidad Aseguradora, cuyo capital social es de 896.176.662€, con sede en Francia y regulada por el código de seguro francés, inscrita en el Registro Comercial de Nanterre con el número 450 327 374 y domicilio social en la Tour Carpe Diem, 31 Place des Corolles, Esplanade Nord, 92400 Courbevoie, Francia. Supervisada por la Autorité de Contrôle Prudentiel et de Résolution (ACPR), 4, Place de Budapest, CS 92459, 75436 PARIS CEDEX 09 y por la Dirección General de Seguros y Fondos de Pensiones, con código de inscripción E-0155