Seguro cibernético

Riesgo, resiliencia y relevancia

Conclusiones clave

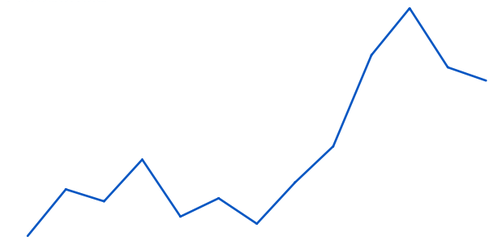
El ciberespacio continúa haciendo honor a su reputación dinámica. Sin indicios de que el panorama de riesgos vaya a disminuir (tal y como muestran el *ransomware*, la inestabilidad geopolítica y la proliferación de la IA generativa), las condiciones del mercado ofrecen a las empresas la oportunidad de asegurarse en condiciones favorables.

Entorno de amenazas variable

Frecuencia y gravedad del *ransomware*: un panorama mixto

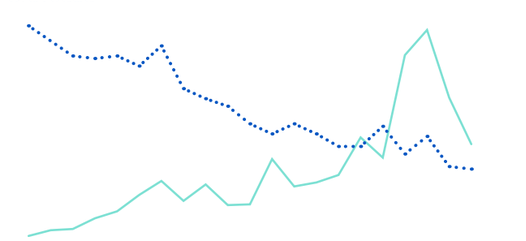
Fuente: Howden, NCC Group

Frecuencia



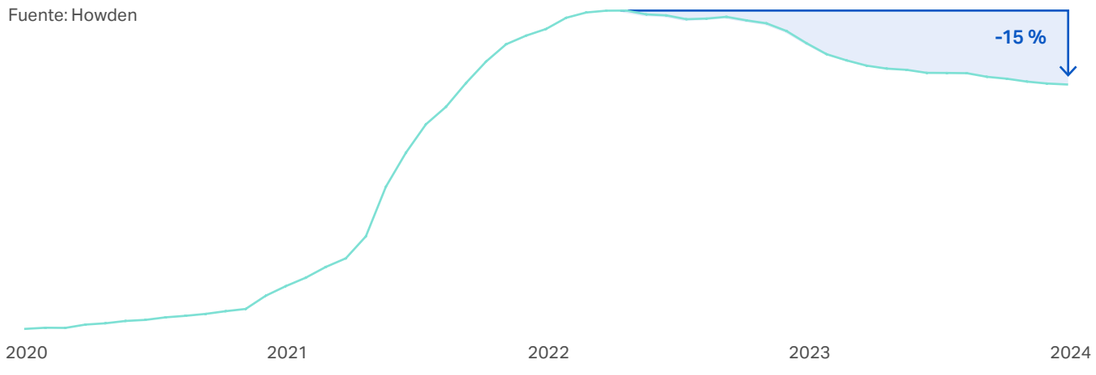
Fuente: Howden, Coveware

Gravedad



Los precios de seguros cibernéticos bajan un 15 % desde su máximo

Fuente: Howden

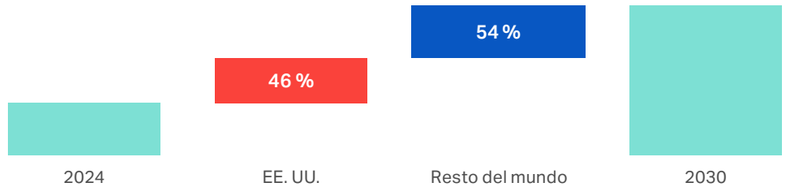


Ya se han sentado las bases para la siguiente fase de desarrollo, e incluyen oportunidades en áreas geográficas internacionales y otras zonas desatendidas preparadas para impulsar el crecimiento. Aumentar la penetración de los seguros es la vía para la resiliencia y la relevancia.

Potencial desaprovechado

Cuota del crecimiento de primas proyectado hasta 2030

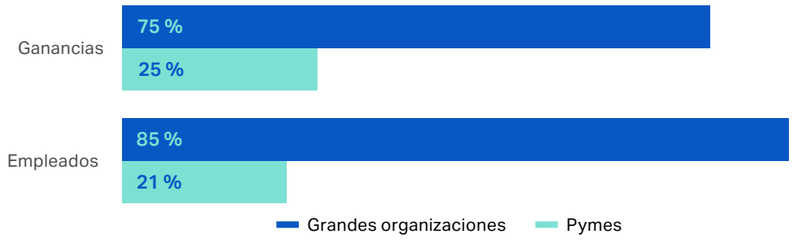
Fuente: Howden



Las principales economías de Europa, Asia y América Latina registran un potencial de crecimiento considerable dados los niveles de penetración actuales.

Cuota existente de organizaciones con seguro cibernético en todo el mundo: pymes desatendidas

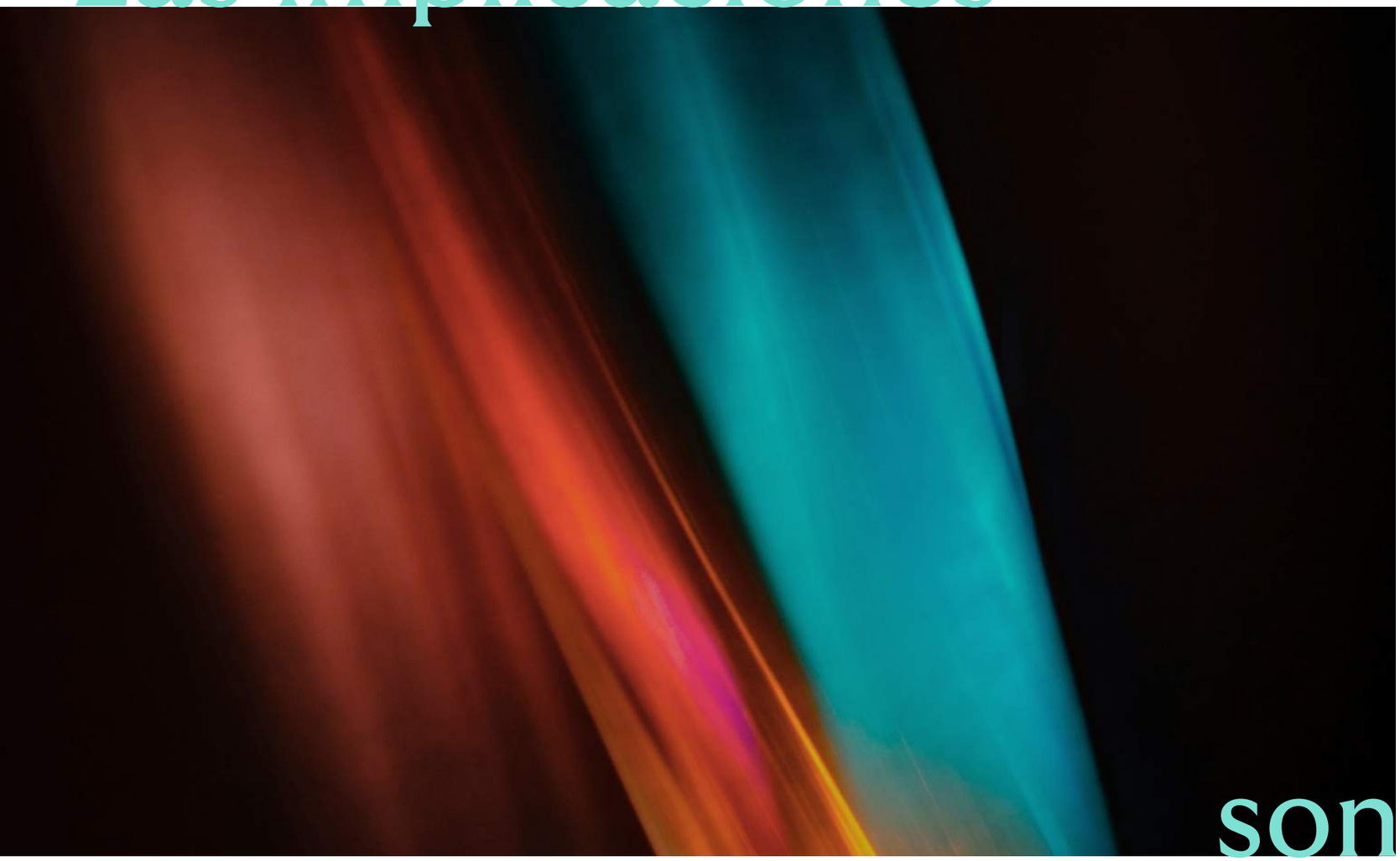
Fuente: WEF



Las pymes son la espina dorsal de la actividad económica en las economías avanzadas y dependen en gran medida de la tecnología.

La innovación es fundamental para el crecimiento, y requiere un nuevo enfoque de intermediación que tenga en cuenta los ciclos, reúna al mejor talento del sector y sea innovador, emprendedor y global. Y esto es solo parte de lo que aporta Howden. Póngase en contacto y le contaremos más.

Las implicaciones



son claras.

Le damos la bienvenida al cuarto informe anual de Howden sobre el mercado de seguros cibernéticos. Los temas de la edición de este año son riesgo, resiliencia y relevancia.

En ningún otro momento el mercado ha experimentado la combinación de condiciones que presenta en la actualidad: un panorama de amenazas crecientes con un mercado de seguros estable respaldado por controles de riesgo sólidos.

Las implicaciones son claras. Las condiciones actuales brindan una oportunidad para que los compradores obtengan protección en condiciones favorables. Para las aseguradoras, la oportunidad reside en apoyarse en un segmento con un claro potencial de crecimiento constante impulsado por la exposición, la rentabilidad continua y la innovación.

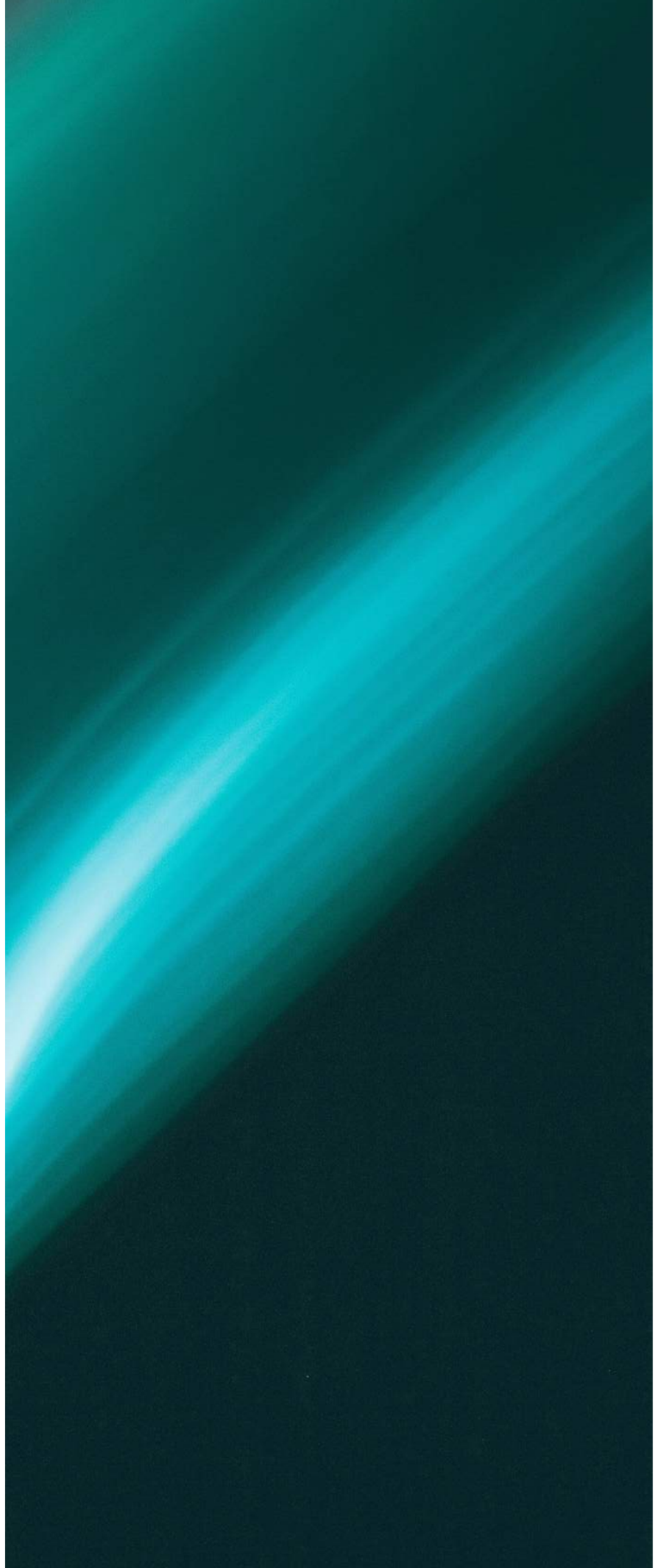
Riesgo y resiliencia

El *ransomware* continúa acechando el panorama de amenazas como la forma más costosa de ciberataque. En los últimos 12 meses se ha observado la fragmentación de los grupos de *ransomware*, una mayor colaboración entre los piratas informáticos y un apoyo tácito de gobiernos hostiles. Estas tendencias han sostenido la amenaza creciente, con datos de NCC Group que muestran que los ataques aumentaron un 85 % el año pasado en relación con 2022 (cuando la actividad disminuyó debido a la invasión rusa de Ucrania) y un 30 % del primer trimestre de 2023 al primer trimestre de 2024.

Los datos presentan un panorama más matizado en el terreno de la gravedad. Los costes de recuperación del *ransomware* vuelven a aumentar después de una disminución temporal en 2022. Además, recientemente se han producido diversos ataques de gran repercusión en el sector sanitario, lo que ha provocado perturbaciones generalizadas e importantes pérdidas económicas. Las inversiones en ciberseguridad y cobertura de seguros están dando dividendos en este entorno, ya que las compañías aseguradas ahora son menos vulnerables a interrupciones prolongadas en caso de un ataque. Esto se refleja en una marcada caída en la proporción de víctimas obligadas a pagar un rescate durante el último año.

Ir un paso por delante de los atacantes no solo hace que las organizaciones sean más resistentes a los ciberataques con motivación financiera, sino que también están mejor preparadas para afrontar incidencias de mayor escala. Los recientes ataques a MOVEit, Change Healthcare y NHS han demostrado cómo los ataques en punto único de fallo (SPoF, por sus siglas en inglés) pueden propagarse por la base de clientes o la red de TI de la organización objetivo y, en última instancia, afectar a miles de víctimas indirectas. No obstante, se espera que las pérdidas aseguradas sean asumibles y estas incidencias ofrecen valiosas lecciones sobre el potencial de acumulación de pérdidas en cualquier ataque futuro.

El auge de la IA generativa es la novedad más importante desde la valoración anterior del panorama de amenazas de Howden. Los tecnólogos, los expertos en ciberseguridad y el mercado de seguros coinciden en general en que esta nueva tecnología transformará las capacidades ofensivas y defensivas. Nuestra investigación impulsa el debate al señalar las formas específicas en que la IA generativa tiene más probabilidades de aumentar la frecuencia, la gravedad y la acumulación de reclamaciones, pero también cómo se puede implementar la tecnología, junto con los controles de riesgo existentes, para repeler a los actores de amenazas.



Relevancia

En los últimos años, las aseguradoras y los brókeres han adoptado importantes medidas para mejorar la estabilidad de precios, la claridad de la cobertura y la coherencia de los términos y condiciones. En conjunto, estas acciones constituyen unas bases sólidas para una nueva fase de desarrollo del mercado.

En este contexto, el mercado tiene dos grandes oportunidades para asegurar un crecimiento anual líder en el mercado y una relevancia a largo plazo: la expansión más allá de EE. UU. y la prestación de servicios a una base de clientes más amplia entre las pequeñas y medianas empresas (pymes) en todas las regiones.

El análisis de este informe revela que es probable que más de la mitad del crecimiento de las primas provenga de territorios fuera de EE. UU. Solo en las principales economías europeas, Alemania, Francia, Italia y España, el potencial de aumento de las primas al replicar los niveles de penetración registrados en mercados más maduros se puede medir en (muchos) cientos de millones de euros.

El espacio de las pymes, que representa cerca de la mitad del PIB en las economías avanzadas, también ofrece enormes oportunidades a medida que los brókeres y las aseguradoras encuentran mejores maneras de incorporar al mercado cibernético a este grupo demográfico actualmente desatendido.

Se han logrado avances considerables en un corto periodo de tiempo, pero nuestra investigación muestra que es necesario intensificar el trabajo para satisfacer la demanda a nivel mundial. La innovación es crucial para aprovechar nuevos fondos de capital y penetrar en mercados actualmente desatendidos.

Howden existe para hacer precisamente eso: esperamos ayudar a los clientes (nuevos y antiguos) a encontrar las mejores soluciones de transferencia de riesgos y desarrollar resiliencia cibernética en lo que sigue siendo un panorama de amenazas altamente fluido.

01

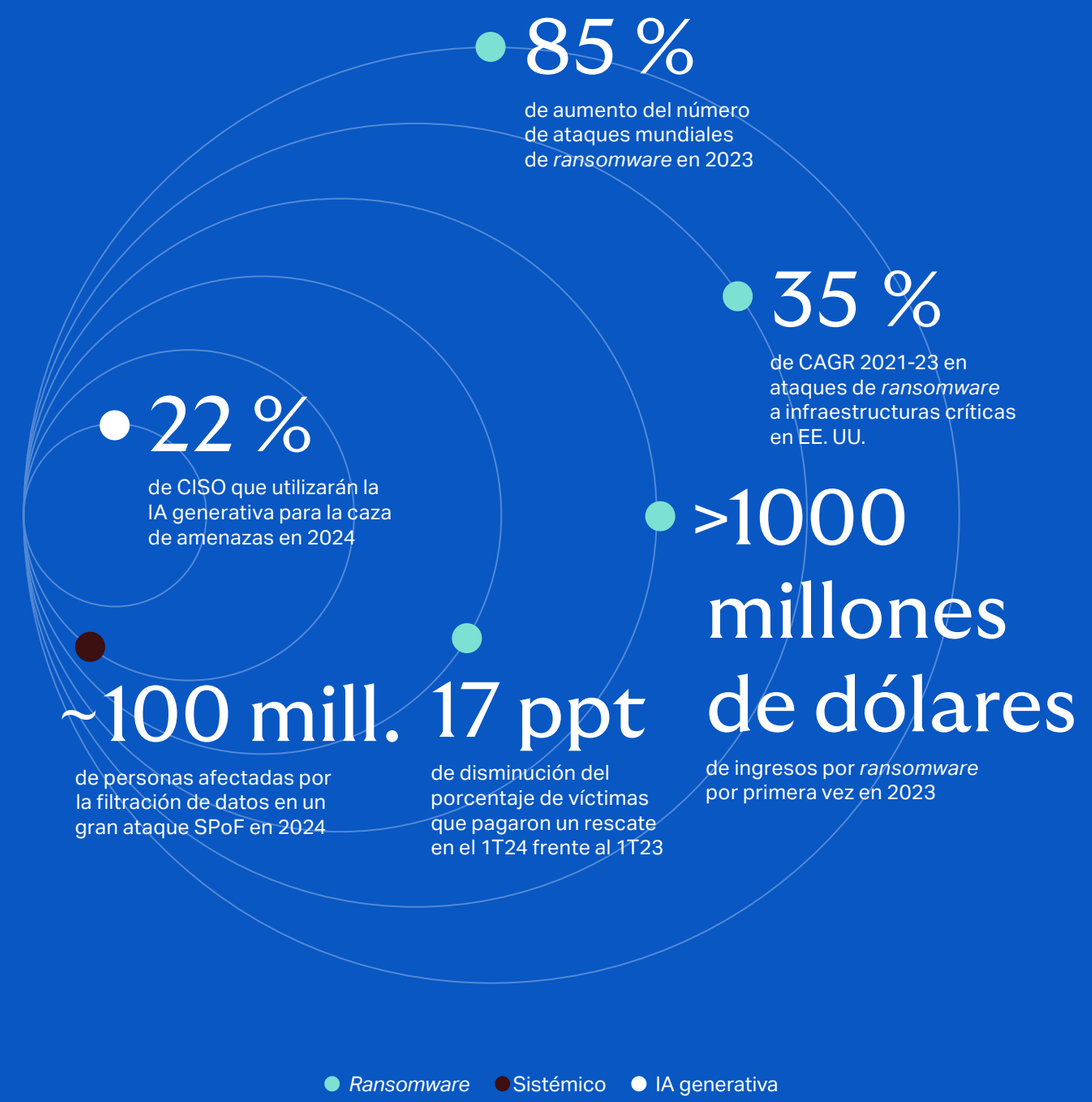
Una amenaza omnipresente

Tras una prolongada racha de crecimiento a la cabeza del mercado, el ciberseguro está entrando en una nueva fase en su camino hacia la madurez.

Tras superar las primeras fases de desarrollo que suelen acompañar a las nuevas líneas de negocio de rápido crecimiento, la competencia está aumentando, ya que las aseguradoras buscan crecer en un espacio que tiene un enorme potencial y es relevante para las empresas de todo el mundo.

Sin apenas indicios de que el entorno de amenazas vaya a remitir pronto —los últimos 12 meses han traído consigo un resurgimiento de la actividad del *ransomware* (incluidos varios ataques de gran repercusión contra entidades sanitarias), una persistente inestabilidad geopolítica y la proliferación de la inteligencia artificial generativa (IA generativa)—, las condiciones actuales del mercado ofrecen a los clientes y a los futuros clientes la oportunidad de asegurarse una protección en condiciones favorables.

Figura 1: Panorama de las ciberamenazas en 2024
(Fuente: Análisis de Howden con datos de Coveware, NCC Group, Chainalysis, Splunk, House Committee on Energy and Commerce, FBI)

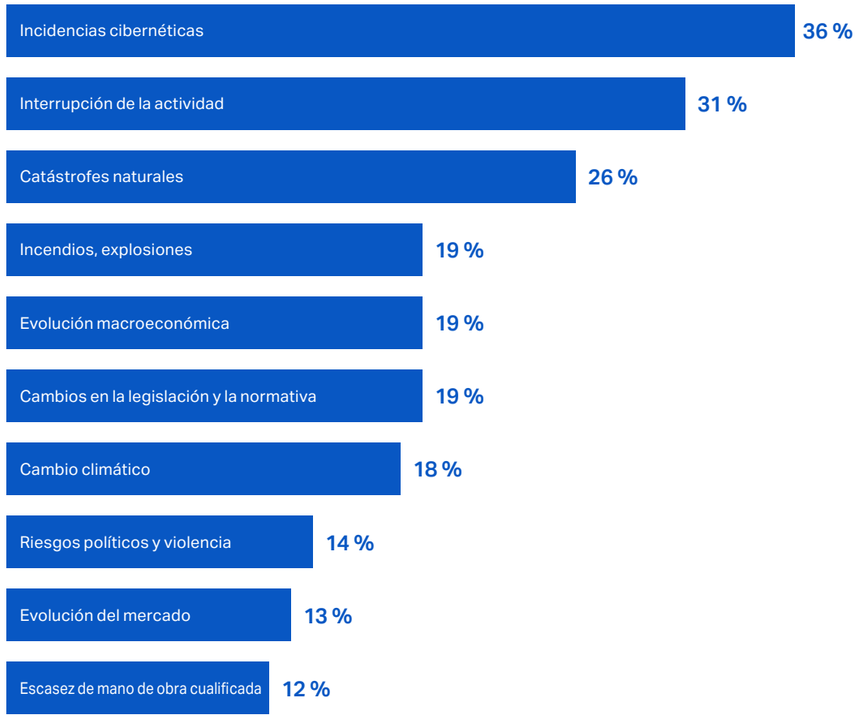


El refuerzo de la resiliencia cibernética está reportando beneficios a los asegurados, ahora que los ataques están volviendo a la tendencia al alza a largo plazo. Tras un parón temporal en 2022 debido a la invasión rusa de Ucrania, la actividad del *ransomware* ha vuelto a niveles históricamente altos. También se ha producido un aumento constante de las reclamaciones de privacidad en Estados Unidos debido al incremento de las vulneraciones biométricas y de los litigios por píxeles tras algunos acuerdos muy sonados, mientras que el resurgimiento del riesgo de acumulación se sigue cerniendo sobre el mercado. Los recientes avances en ambas áreas sirven para hablar del riesgo de cola asociado al ciberseguro.

Todo ello ha llevado a la cibernética a aumentar su liderazgo como principal riesgo mundial en el Barómetro de Riesgos de Allianz de este año (véase la Figura 2). Como reflejo de la omnipresencia del panorama de amenazas, las personas encuestadas clasificaron las vulneraciones de datos como la exposición cibernética que más preocupa (59 %), seguida de los ataques a infraestructuras cruciales y activos físicos (53 %) y el aumento de los ataques de *ransomware* (53 %).[1]

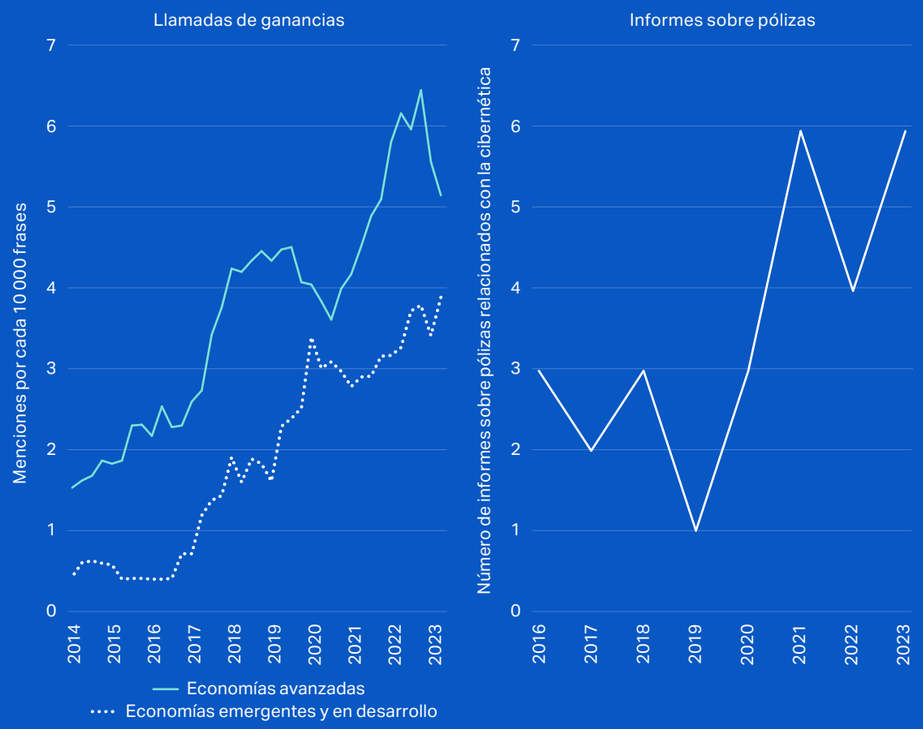
Esta mayor concienciación sobre el riesgo coincide con la aparición en los últimos años de varias publicaciones sobre políticas relacionadas con la cibernética, así como con las crecientes referencias al riesgo cibernético en las convocatorias de beneficios de las empresas (véase la Figura 3).

Figura 2: Barómetro de Riesgos de Allianz 2024[1] (Fuente: Allianz Comercial)



[1] Las cifras representan la frecuencia con que se seleccionó un riesgo como porcentaje de todas las respuestas a la encuesta. Las cifras no suman el 100 %, ya que se pidió a los encuestados que nombraran hasta tres riesgos que consideraban más importantes.

Figura 3: Creciente importancia del riesgo cibernético entre las empresas y los responsables políticos (Fuente: Análisis de Howden con datos del FMI)



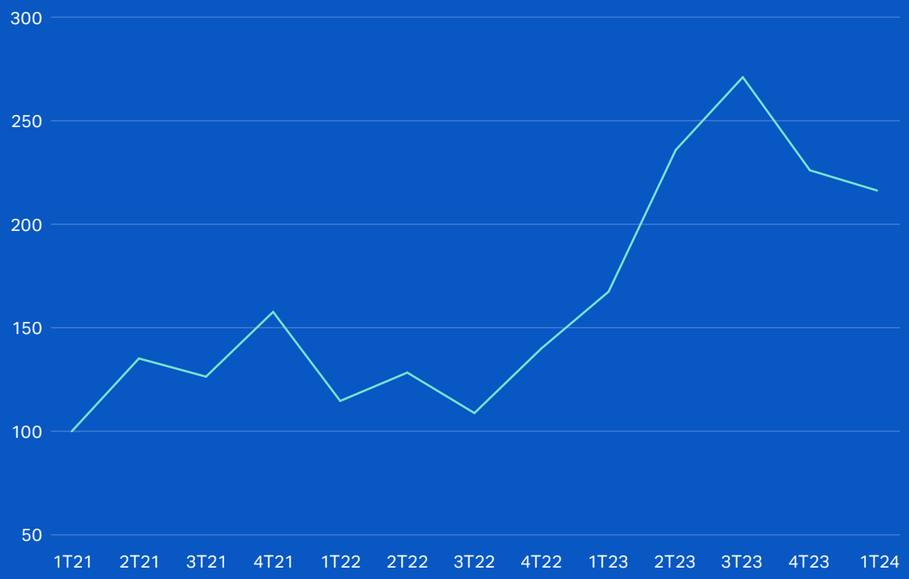
> El refuerzo de la resiliencia cibernética está reportando beneficios a los asegurados, ahora que los ataques están volviendo a la tendencia al alza a largo plazo.

Frecuencia del *ransomware*

El *ransomware* sigue dominando el entorno de las ciberpérdidas. Dados los niveles actuales de frecuencia y gravedad, parece que el *ransomware* será una fuente de pérdidas significativas para las empresas durante algún tiempo.

La Figura 4 muestra cómo ha evolucionado la frecuencia de los ataques mundiales de *ransomware* desde 2021. La disponibilidad de kits de *ransomware* asequibles (y de bajo coste), también conocidos como *ransomware* como servicio (RaaS), combinada con la continua rentabilidad de los ataques, han sido factores importantes que han impulsado la proliferación del *ransomware* durante este periodo.

Figura 4: Índice de frecuencia del *ransomware*; de 1T21 a 1T24[2]
(Fuente: Análisis de Howden basado en datos de NCC Group)



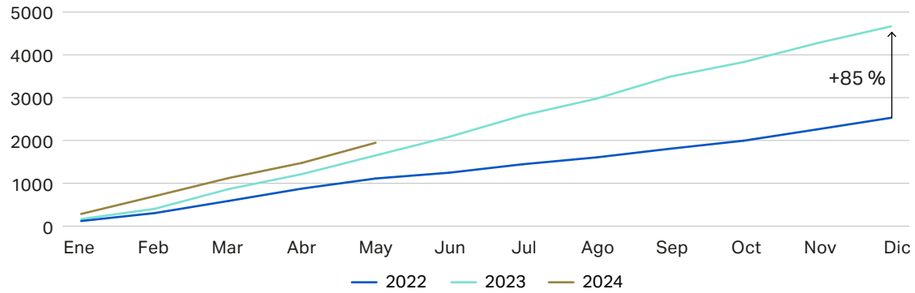
Los temores de que la invasión rusa de Ucrania a principios de 2022 avivara la actividad resultaron infundados, ya que ambos bandos enfrentados, que albergan algunos de los peores grupos de *ransomware*, centraron sus esfuerzos y recursos en la guerra cinética.

Sin embargo, la actividad del *ransomware* ha aumentado considerablemente desde entonces.)Las bandas establecidas, que se enfrentan a unos fondos agotados tras la caída de los ingresos en 2022, junto con la aparición de nuevos grupos, impulsaron una aceleración notable de la frecuencia el año pasado. La Figura 5 compara la actividad acumulada del *ransomware* por meses entre 2022 y principios de 2024, con datos de NCC Group que muestran un aumento de la frecuencia del 85 % en el año fiscal 2023 en comparación con el año fiscal 2022.

Aunque el aumento de la presión sobre las bandas por parte de las fuerzas de seguridad (incluidos los esfuerzos para acabar con grupos rusos como LockBit y BlackCat) ha contribuido a reducir la actividad desde los niveles máximos registrados en el tercer trimestre de 2013, no parece haber tenido un impacto decisivo. Las incidencias registradas en los cinco primeros meses de este año aumentaron un 18 % respecto a los ya elevados niveles de 2023.

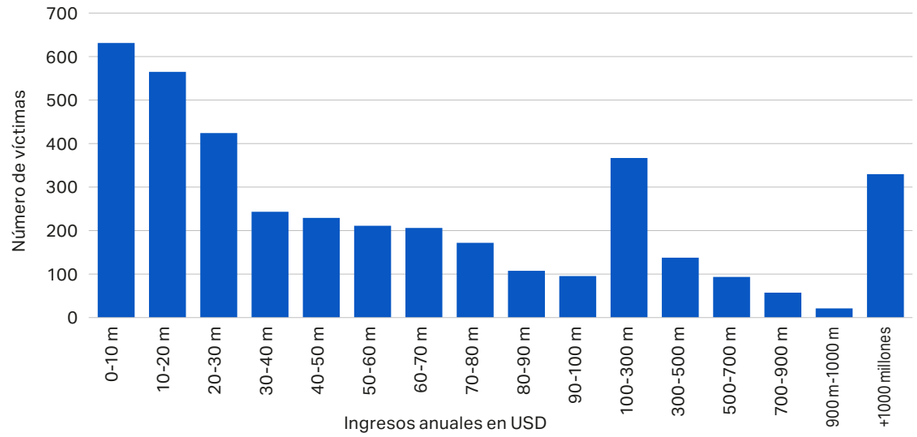
La actuación de las fuerzas de seguridad también ha envalentonado a los ciberdelincuentes para contraatacar a las infraestructuras cruciales, y los proveedores sanitarios estadounidenses Change Healthcare y Ascension fueron víctimas de ataques de *ransomware* en febrero y mayo de este año. Estos ataques causaron importantes trastornos a ambas empresas y han desencadenado cuantiosas reclamaciones de primera parte (en el caso de Ascension) y de terceros. Varios hospitales británicos también sufrieron graves trastornos en junio tras un ataque de *ransomware* a Synnovis, proveedor de servicios de patología para el NHS (servicio de salud público del Reino Unido).

Figura 5: Actividad acumulada mundial de *ransomware* por mes: de 2022 a 2T24[2]
(Fuente: Análisis de Howden basado en datos de NCC Group)



Se sigue atacando a empresas de todos los tamaños, con una clara tendencia hacia las franjas superior e inferior de la horquilla de ingresos (véase la Figura 6). Las tácticas de los atacantes se basan en maximizar los beneficios económicos y minimizar los riesgos. Las bandas sopesan la capacidad de pago de las víctimas y las medidas de seguridad adoptadas para no provocar una respuesta de las fuerzas del orden.

Figura 6: Distribución de los ataques de *ransomware* por ingresos anuales de las empresas en 2023/24 (Fuente: Análisis de Howden basado en datos de Black Kite)



[2] NCC Group rastrea a los grupos de *ransomware* que utilizan la táctica de doble extorsión de pirateo y filtración vigilando los sitios de filtración y extrayendo los datos de las víctimas a medida que se publican.

Gravedad mixta

La frecuencia del *ransomware* solo cuenta una parte de la historia desde el punto de vista de las pérdidas. El lado de la gravedad de la ecuación se compone principalmente de los costes del tiempo de inactividad (interrupción de la actividad y pérdida de productividad), pagos de rescates y otros gastos. Estos pueden ser más difíciles de medir, sobre todo si se tienen en cuenta impactos intangibles como el daño a la reputación. Los datos disponibles presentan una imagen matizada, con recientes ataques a gran escala que subrayan cómo el pago del rescate (si lo hay) puede ser solo la punta del iceberg.

Aunque los datos de Chainalysis y Sophos mostrados en las figuras 7 y 8 revelan cómo los rescates pagados en dólares han aumentado en los últimos años, ocultan una tendencia igualmente importante que se aleja del pago. Los datos de Coveware en la Figura 9 muestran una marcada disminución en la proporción de empresas que pagan rescates entre 2019 y principios de 2024, con una caída al 28 % en el 1T24 en comparación con un promedio del 70 % en 2020.

Las empresas que han invertido en controles de riesgo y gestión de crisis son ahora menos susceptibles de sufrir impactos materiales, lo que reequilibra las consideraciones de coste-beneficio para algunas empresas sobre si pagar o no rescates. Además, la creciente prevalencia de la doble e incluso triple extorsión ha socavado la suposición de que el pago de un rescate pondrá fin al pirateo.

Figura 7: Ingresos recibidos por ataques de *ransomware*: de 2019 a 2023 (Fuente: Chainalysis)

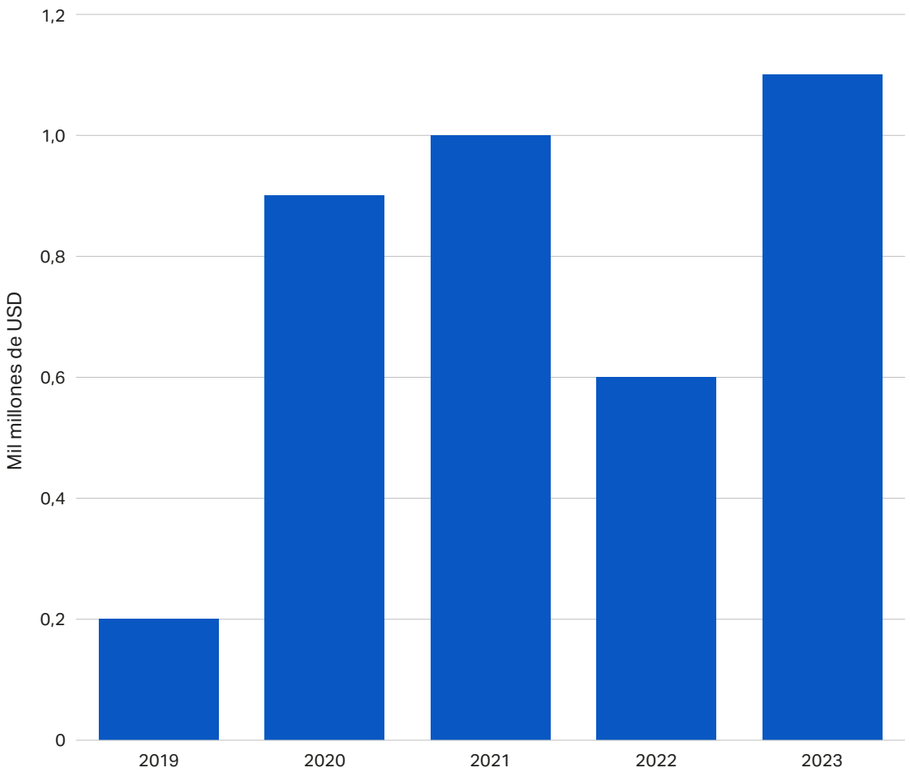


Figura 8: Distribución de los importes de pago de los rescates: de 2022 a 2024
(Fuente: Análisis de Howden con datos de Sophos)

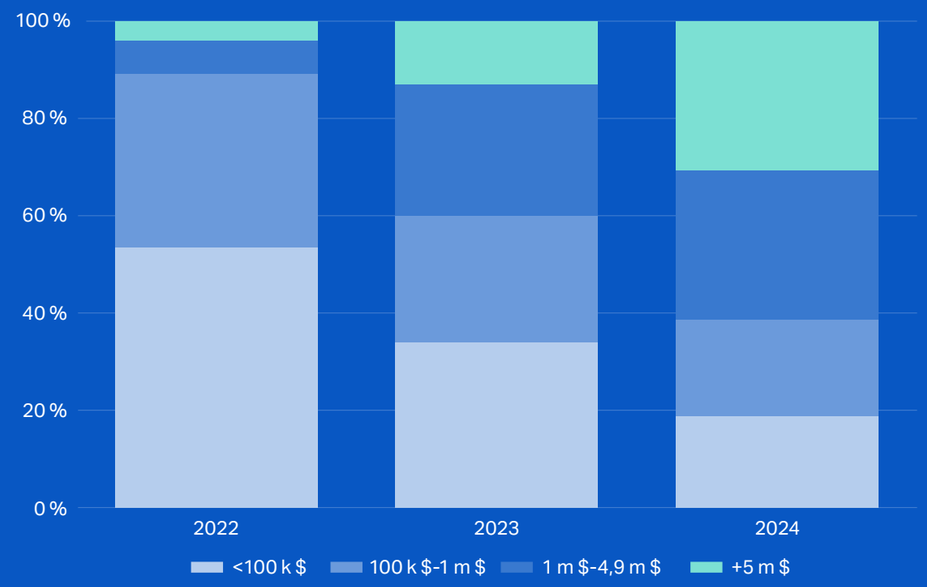
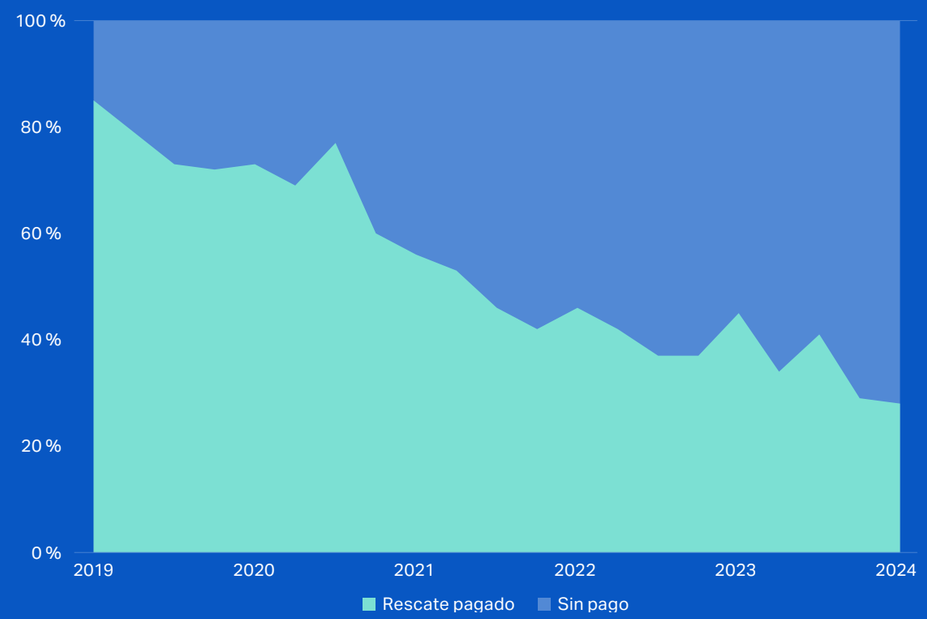


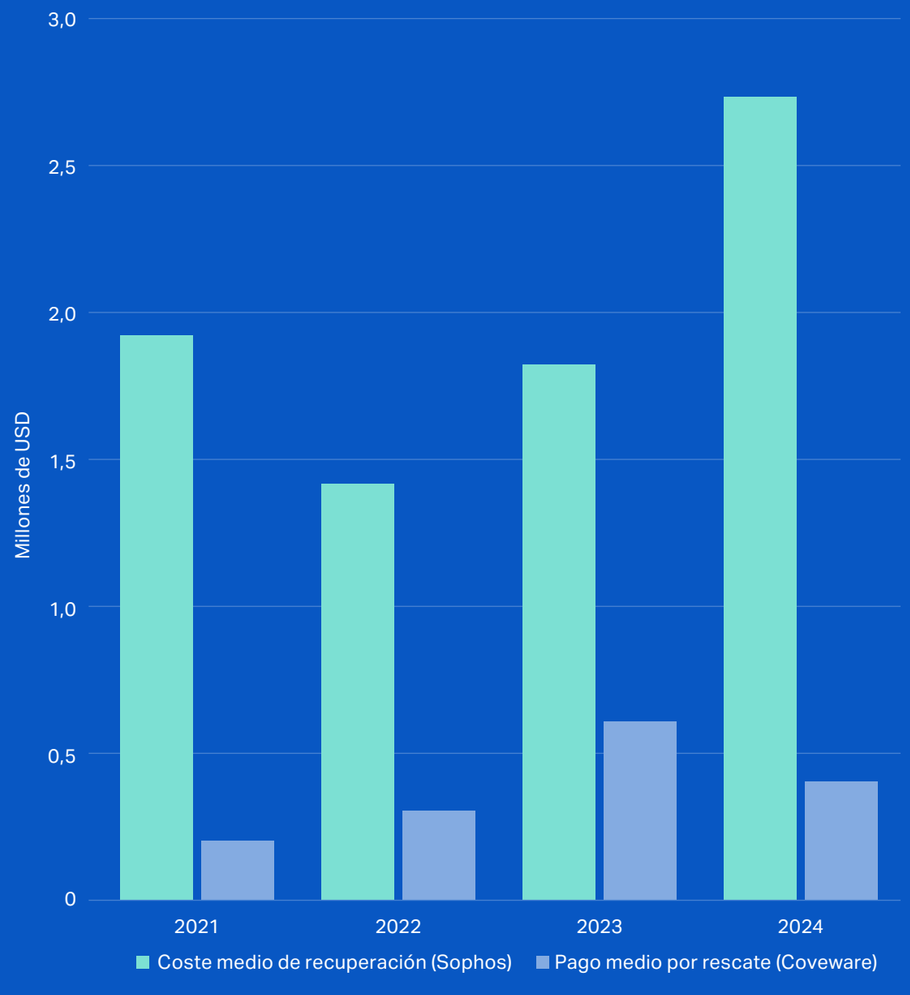
Figura 9: Proporción de víctimas de *ransomware* que pagan un rescate: de 1T19 a 1T24
(Fuente: Análisis de Howden basado en datos de Coveware)



El pago de rescates es solo una de las partidas de las pérdidas sufridas por las empresas. Los datos de Sophos y Coveware de la Figura 10 comparan el pago medio de rescates con los costes medios de recuperación, siendo estos últimos los que representan la mayor parte de los costes totales durante ese periodo.

Según S-RM, la interrupción de la actividad suele ser el componente más costoso de un siniestro importante, y representa hasta el 70 % de los costes de los siniestros cuando una empresa depende en gran medida de la disponibilidad de sistemas críticos en sectores como la fabricación y los servicios financieros. Otros costes accesorios pueden acumularse cuando existe una exposición reglamentaria significativa, o cuando la exposición multijurisdiccional conlleva la necesidad de hacer frente a diversas obligaciones reglamentarias.

Figura 10: Pagos medios de rescate y costes de recuperación por ataques de *ransomware*: de 2021 a 2024[3] (Fuente: Análisis de Howden basado en datos de Coveware y Sophos)

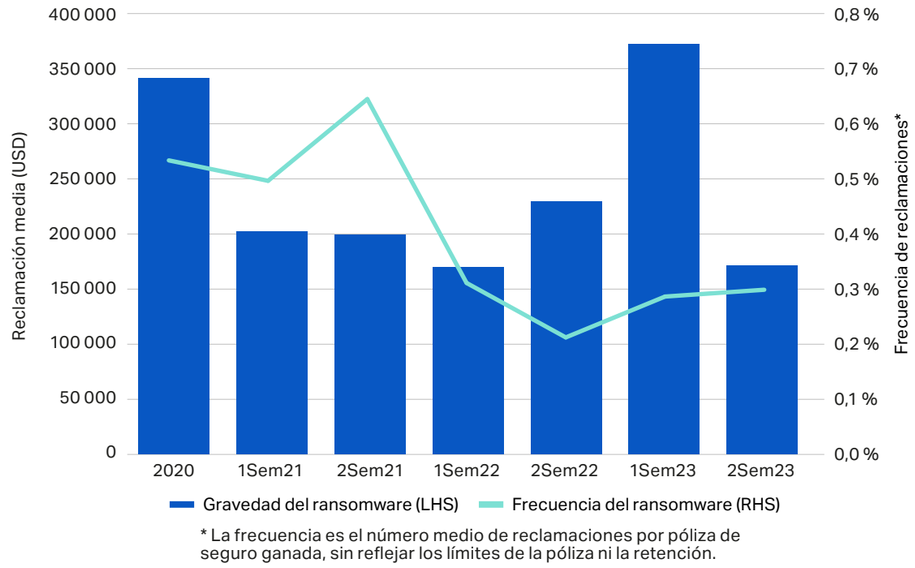


Generando resiliencia

Cada vez son más los ataques de *ransomware* que implican el robo de datos personales o comerciales confidenciales con fines de extorsión (es decir, la amenaza de filtrar datos al dominio público), lo que no solo aumenta la complejidad de las incidencias, sino que también conlleva un mayor riesgo de daños a la reputación. Las ciberdefensas reforzadas y las copias de seguridad seguras han contribuido a mitigar las pérdidas por interrupción de la actividad, aislando así a las empresas aseguradas de interrupciones prolongadas o pérdidas desmesuradas.

Estas dinámicas contradictorias siguen desarrollándose en el mercado, con picos y caídas en la frecuencia y gravedad del *ransomware* indicativos de una evolución rápida (véase la Figura 11 de los datos registrados por Coalition basados en su propio libro de negocios desde 2020).

Figura 11: Frecuencia y gravedad de las reclamaciones por *ransomware* para los asegurados de Coalition: de 2020 a 2023 (Fuente: Análisis de Howden basado en el Informe de reclamaciones de Coalition)



* La frecuencia es el número medio de reclamaciones por póliza de seguro ganada, sin reflejar los límites de la póliza ni la retención.

No obstante, los datos de 2023 y principios de 2024 siguen mostrando una fuerte rentabilidad de los seguros cibernéticos, lo que refleja la adecuación de los precios para una amplia gama de incidencias, el éxito de los controles de riesgo en la mitigación de las pérdidas y la capacidad de adaptar rápidamente los términos dada la naturaleza reciente del negocio.

Todo ello augura unas condiciones de mercado favorables en general. A medida que la cibernética hace honor a su reputación dinámica, el valor de los seguros se pone aún más de relieve, ya que incentivan (y ayudan a implementar) una mejor salud cibernética, refuerzan la resiliencia e indemnizan las pérdidas.

[3] Los costes de recuperación incluyen el tiempo de inactividad, el tiempo del personal, los costes de los dispositivos, los costes de red y las oportunidades perdidas. 2024 para el pago medio de rescate de Coveware representa los datos disponibles en el 1T24.

02

Cibernética sistémica: lo desconocido conocido

La prevención, la preparación y la protección son capas críticas de defensa en un entorno de amenazas tan intensificadas. Una gestión de riesgos mejorada no solo hace que las organizaciones sean más resilientes al ransomware y a otros ataques cibernéticos con motivación financiera, sino que también hace que estén mejor preparadas para afrontar un clima geopolítico altamente volátil que aumenta el potencial de que se produzcan incidencias a mayor escala.

> “La incertidumbre en torno a la acumulación se sigue cerniendo sobre el mercado.

Los riesgos asociados a la guerra cibernética y a los acontecimientos sistémicos en general —situaciones en las que ataques aislados desencadenan fallos generalizados en múltiples organizaciones— siguen siendo motivo de preocupación, pero los peores escenarios aún no se han hecho realidad. El riesgo y la incertidumbre en torno a la acumulación se siguen cerniendo sobre el mercado, lo que impide la entrada de capitales y modera el apetito de riesgo. Sin embargo, los datos de pérdidas hasta la fecha muestran que la amenaza más generalizada procede de ataques selectivos (y de menor nivel) perpetrados por bandas criminales y no por agentes estatales.

De hecho, gran parte de la actividad cibernética estatal relacionada con las actuales zonas de guerra se ha integrado y contenido en la campaña cinética. Esto es indicativo del cambio de prioridades durante los conflictos: las tácticas y herramientas cibernéticas consideradas más eficaces para apoyar los objetivos militares (por ejemplo, sabotaje o interrupción) probablemente tengan prioridad en ciertas fases.

Sin embargo, los gobiernos hostiles siguen protegiendo a los delincuentes en sus respectivos países, lo que les permite actuar con casi total impunidad cuando atacan a empresas e infraestructuras críticas occidentales (véase la aportación de XCyber en las páginas 28-31). La sanidad ha sido un objetivo prioritario desde hace varios años, probablemente debido a la prevalencia de sistemas heredados (e interconectados), grandes volúmenes de datos confidenciales y una disposición relativamente alta a pagar rescates para restablecer las operaciones rápidamente y proteger la vida.

La Figura 12 de la página 20 muestra que el número de ataques de *ransomware* a infraestructuras críticas de Estados Unidos aumentó en una CAGR del 35 % entre 2021 y 2023.

Figura 12: Ataques de *ransomware* notificados a infraestructuras críticas de EE. UU.: de 2021 a 2023 (Fuente: Análisis de Howden con datos del FBI)

“

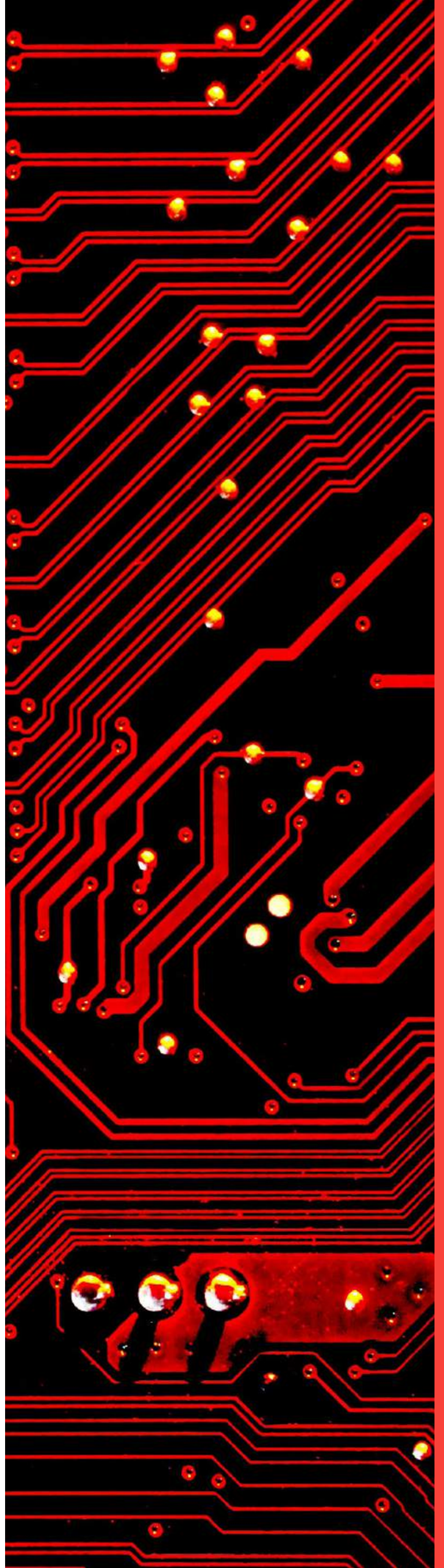
Los gobiernos hostiles siguen protegiendo a los delincuentes en sus respectivos países, lo que les permite actuar casi con impunidad cuando atacan a empresas e infraestructuras críticas occidentales.

Disparos de advertencia

Los ciberataques sistémicos son muy inciertos en cuanto a su desencadenante, probabilidad y tamaño. Por un lado, el potencial de pérdidas es evidente: la proliferación de superficies de ataque derivada de la rápida digitalización, el poco conocimiento de en qué punto y de qué manera son vulnerables las tecnologías y la escasez de datos históricos sobre catástrofes cibernéticas. No obstante, también es cierto que solo un pequeño número de agentes del Estado nación o grupos altamente sofisticados disponen de las capacidades, la experiencia y los recursos para ejecutar tales ataques. Estos actores también deben sopesar el riesgo de escalada y represalias que conlleva un ciberataque a gran escala.

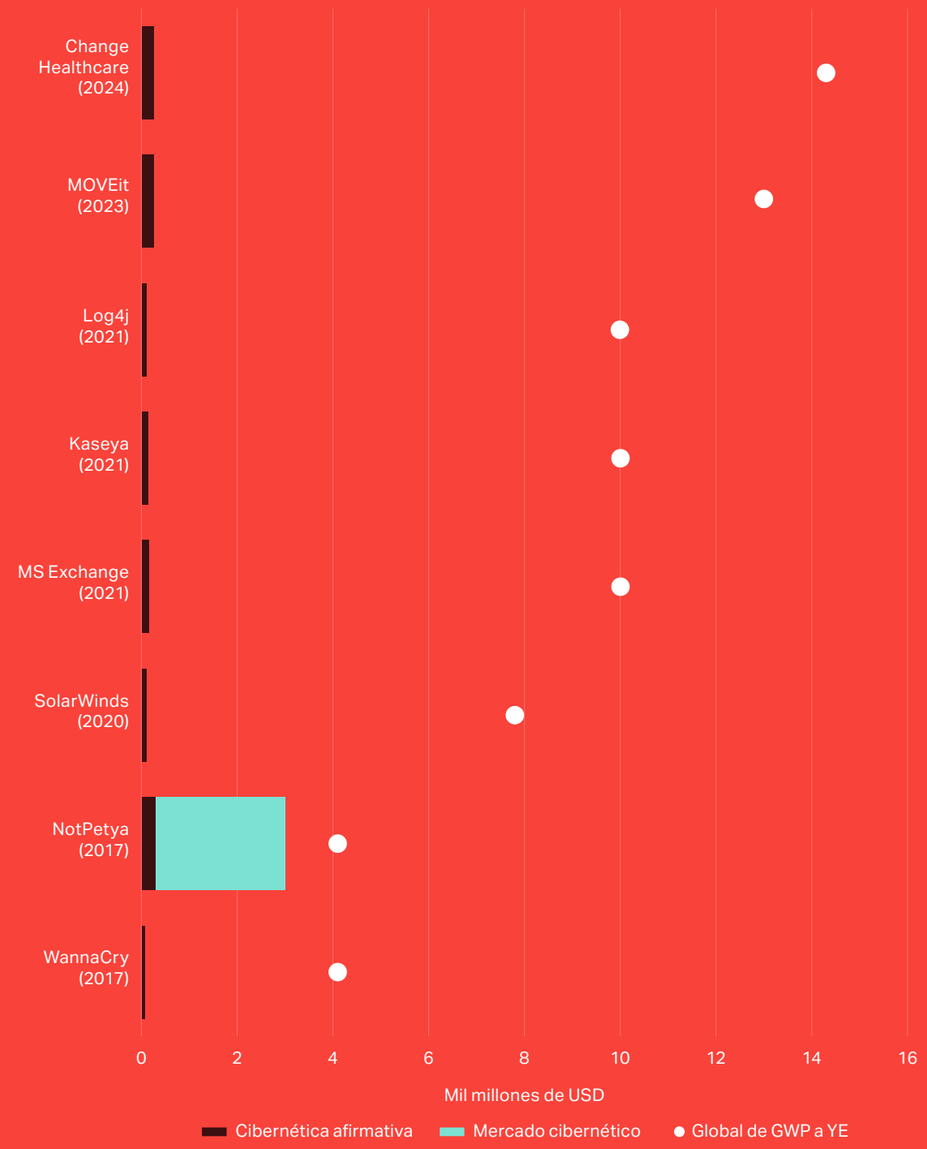
Varias incidencias ocurridas en los últimos años, como las de SolarWinds, Microsoft Exchange, Kaseya, Log4j y MOVEit, han visto cómo los actores de las amenazas se dirigían a las cadenas de suministro de *software* en un intento de maximizar las repercusiones en múltiples organizaciones, incluso si las pérdidas han sido en última instancia manejables para el mercado de seguros (véase la Figura 13).

Change Healthcare es el último acontecimiento que plantea interrogantes sobre el alcance del riesgo de acumulación. Aunque se tardará algún tiempo en saber cómo evolucionarán las pérdidas, el Property Claim Services (PCS) de Verisk, proveedor de estimaciones de pérdidas de seguros, ha calificado el suceso de cibercatástrofe, lo que apunta a unas pérdidas de mercado superiores a 250 millones de dólares.



La capacidad del mercado cibernético para absorber pérdidas de la magnitud a menudo asociada con sucesos a gran escala aumentará con el tiempo a medida que se acerque a la escala de otras grandes líneas de negocio de bienes y accidentes, y los precios se mantengan en niveles proporcionales a los riesgos. Las aclaraciones sobre la aplicabilidad de las exclusiones de guerra a todos los ataques, salvo los más remotos, de los Estados nación también deberían reducir el alcance de las disputas sobre reclamaciones y fomentar la entrada de más capacidad en el mercado.

Figura 13: Estimaciones de pérdidas aseguradas por sucesos cibernéticos de gran repercusión frente a primas brutas suscritas del mercado cibernético mundial
(Fuente: Howden, PCS)



Riesgo de acumulación

Nada de esto pretende minimizar el potencial de acumulación de riesgos. Un suceso a gran escala que diera lugar a una interrupción generalizada de la nube, interrumpiera las plataformas de pago globales o comprometiera el *software* que sustenta los sistemas digitales globales (véase la nota al lado para conocer la opinión de S-RM sobre este último) supondría un grave riesgo para el mercado y las economías en general, aunque esto es cierto para los eventos de cola en varias otras líneas de negocio.

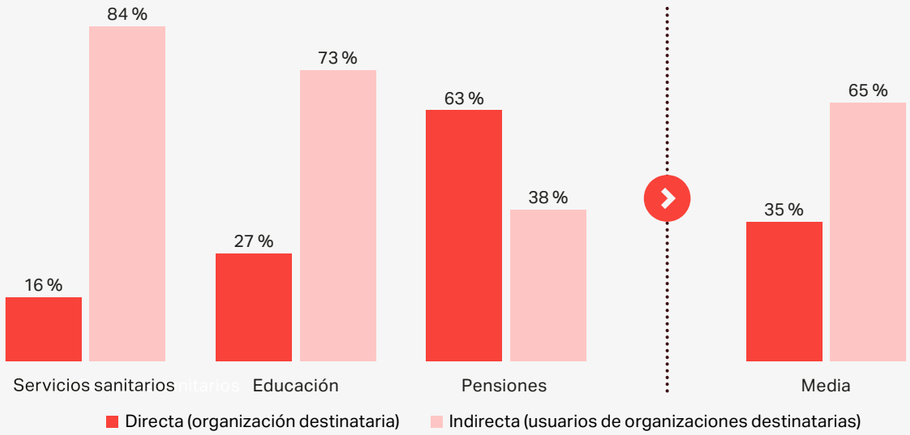
Las incidencias de MOVEit y Change Healthcare ayudan a contextualizar el potencial de pérdidas asociado a los eventos sistémicos. Recientes revelaciones muestran que la brecha en la transferencia de archivos MOVEit, que comenzó en junio de 2023, afectó a aproximadamente 2800 organizaciones y 96 millones de personas.

La base de usuarios de la plataforma de pagos y reclamaciones Change Healthcare está formada por 900 000 médicos, 33 000 farmacias y 5500 hospitales de Estados Unidos. El consejero delegado de la empresa matriz UnitedHealth ha indicado que hasta un tercio de la población estadounidense ha sufrido filtraciones de datos confidenciales. La envergadura de este tipo de ataques pone de relieve el potencial de espiralización de los costes económicos.

No obstante, se espera que el impacto de las pérdidas en el mercado de los ciberseguros sea manejable. UnitedHealth no solo ha confirmado que carecía de cobertura cibernética independiente en el momento del ataque (una gran pérdida para el mercado, dado que la empresa contabilizó 870 millones de dólares en costes relacionados con la filtración en el primer trimestre de 2024 y estimó que podrían ascender a 1600 millones de dólares para todo el año), sino que el apoyo prestado a los terceros afectados por UnitedHealth ha limitado las consecuencias y ha frenado las reclamaciones.

La Figura 14 incorpora las tendencias observadas durante los recientes ataques sistémicos de *ransomware* para mostrar cómo los costes sufridos por terceras empresas que no han sido atacadas directamente (incluyendo la interrupción del negocio, los costes de limpieza y cualquier pago secundario por *ransomware*) pueden constituir la mayor parte de las pérdidas económicas totales. Los acontecimientos subrayan el riesgo inherente de acumulación en múltiples organizaciones a través de un SPoF y revelan cómo las pérdidas se han concentrado en sectores verticales debido a la dependencia de *software* específico de la industria y plataformas de pagos/administración.

Figura 14: Distribución económica estimada de los principales ataques de *ransomware* en 2023/24
(Fuente: Análisis de Howden sobre datos de economía pública y pérdidas cibernéticas aseguradas)[4]



A medida que sale a la luz más información sobre la exposición al *ransomware*, los datos muestran que las reclamaciones por ataques indirectos han sido (mucho) más bajas de media que las reclamaciones directas. Junto con la provisión incoherente de cobertura contingente de interrupción de negocio para ciberataques y el trabajo que las empresas están llevando a cabo para reducir el riesgo de la cadena de suministro, el grado de acumulación de pérdidas (o frecuencia de pérdidas) tendría que ser múltiplo de lo que se ha experimentado hasta la fecha para generar pérdidas que amenacen la base de primas del mercado global.

Todo ello sirve para reforzar la importancia de garantizar una cobertura de seguro cibernético adaptada y completa con límites adecuados. El acceso al mejor asesoramiento de intermediación puede marcar la diferencia para lograr este objetivo en el mercado actual.

S-RM sobre el riesgo de ataques a la piedra angular digital

Texto de Roddy Priestley, director de Ciberseguridad, y Martijn Hoogesteger, jefe de Ciberseguridad, Benelux

Un ataque con éxito a una piedra angular digital tiene un impacto potencial catastrófico equivalente a una interrupción global de la nube. En tal caso, un actor malintencionado comprometería el *software* que sustenta los sistemas digitales globales. Dado que la mayoría de las organizaciones dependen de dos sistemas operativos (Windows y Linux) y estos, a su vez, de bibliotecas de código abierto desarrolladas en colaboración por colaboradores desconocidos, un solo fallo podría tener una enorme repercusión.

Una incidencia ocurrida a principios de este año subraya este riesgo sistémico después de que un ingeniero de Microsoft identificara una puerta trasera maliciosa en una biblioteca de código abierto llamada XZ Utils, integrada en la mayoría de los sistemas operativos Linux. Esto había sido implantado en el código por uno de sus colaboradores, en lo que parece ser una operación meticulosamente planificada a lo largo de varios años. Si no se hubiera identificado el ataque, el actor desconocido que estaba detrás de la operación habría tenido acceso por la puerta trasera a casi todas las organizaciones, ya que los servidores Linux se utilizan a menudo para alojar sistemas de copia de seguridad, bases de datos, hosts de virtualización, servicios en la nube, servidores web y sistemas de planificación de recursos empresariales.

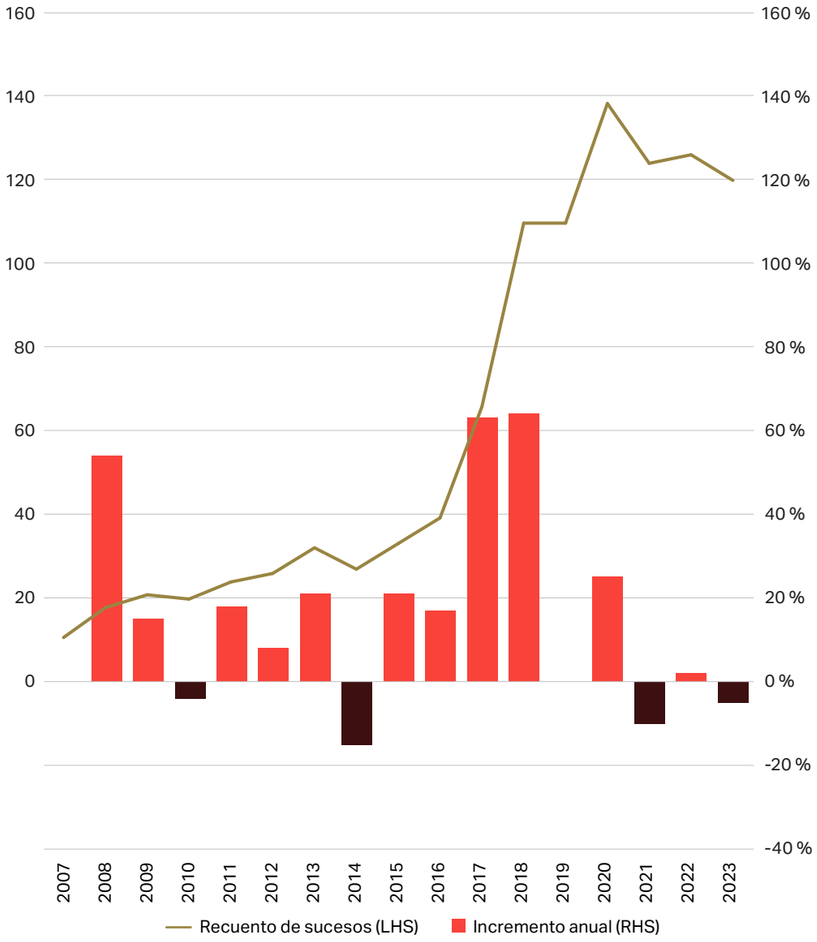
Además de los agentes estatales, se sabe que algunos grupos delictivos invierten grandes cantidades de dinero en el desarrollo de un compromiso de esta naturaleza. Aunque la probabilidad de que se produzca un suceso de este tipo sigue siendo baja, ya que se necesitaría una cascada de acontecimientos desafortunados para que ocurriera, el impacto podría ser catastrófico

[4] Las fuentes utilizadas en la Figura 14 son Change Healthcare, Coalition, At-Bay, Pension Benefit Information y National Student Clearinghouse. El análisis se basa en el número declarado de entidades afectadas y en los costes medios de los ataques de *ransomware* de primera y tercera parte.

El efecto geopolítico

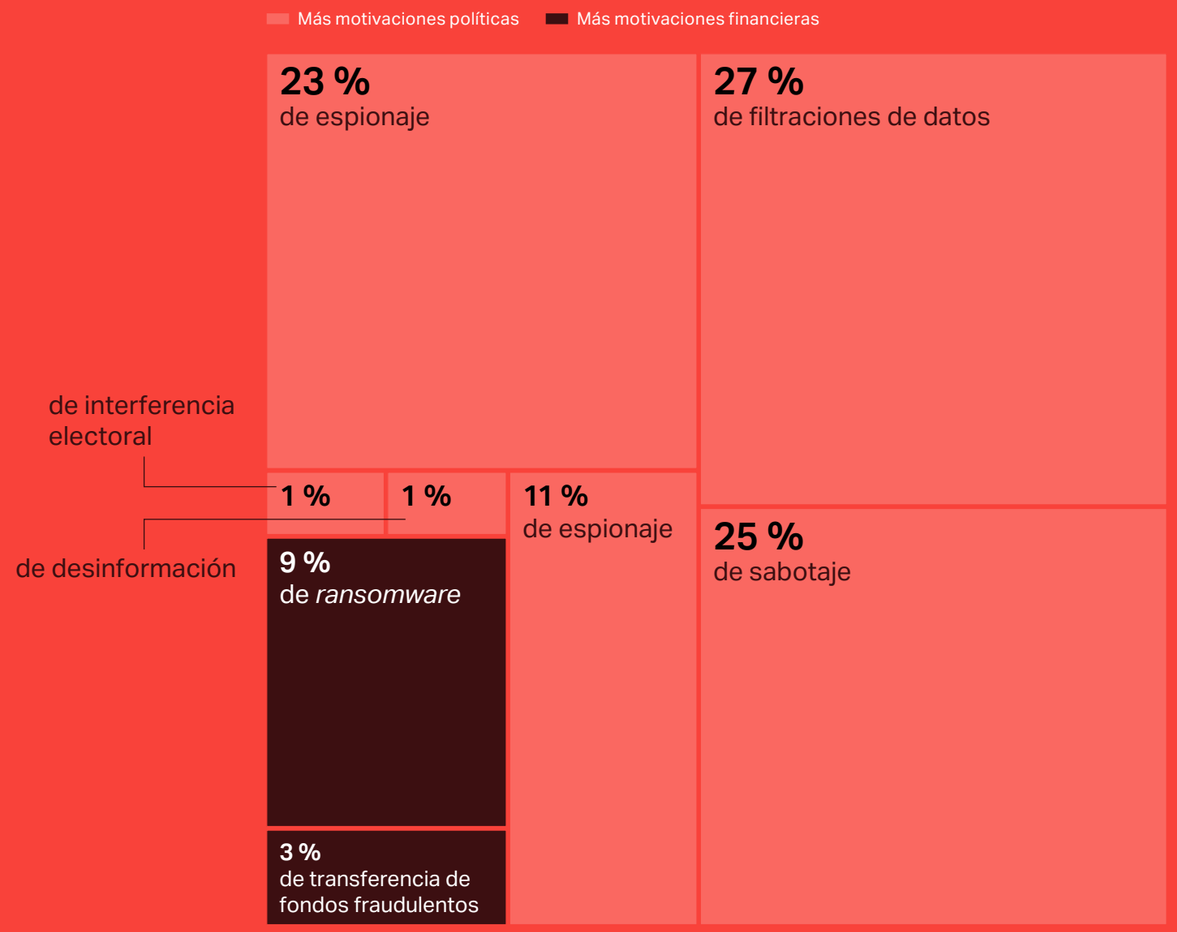
Un entorno geopolítico cada vez más febril aumenta la sensación de incertidumbre. Los datos del Centro de Estudios Estratégicos e Internacionales (CSIS, por sus siglas en inglés) que se muestran en la Figura 15, que ofrece una instantánea de la actividad afiliada al Estado al trazar los principales ciberataques contra agencias gubernamentales, defensa y empresas de alta tecnología, revelan un aumento espectacular durante la última década. Rusia y China aparecen como los autores más destacados, con el 65 % de los ataques del último año (de abril de 2023 a marzo de 2024).

Figura 15: Número de grandes ataques cibernéticos asociados al Estado: de 2007 a 2023
(Fuente: Análisis de Howden de los ataques registrados por el CSIS)



El desglose de las incidencias cibernéticas por tipo refleja las motivaciones de los Estados nación, con cerca del 90 % de las incidencias mostrando motivaciones políticas (las vulneraciones de datos, el sabotaje y el espionaje son las formas de ataque más frecuentes).

Figura 16: Principales ciberataques afiliados al Estado por tipo: de abril de 2023 a marzo de 2024
(Fuente: Análisis de Howden de los ataques registrados por el CSIS)



Es probable que el alcance y la duración de las guerras en curso en Ucrania y Oriente Próximo, junto con actividades de menor nivel dirigidas a socavar el proceso democrático en un año de elecciones importantes, tengan profundos efectos en la ciberseguridad mundial.

Esto reafirma la importante labor que está realizando el mercado para adelantarse al problema de la guerra cibernética y determinar de forma proactiva el alcance de la cobertura en caso de que se materialice cualquier pérdida importante de un Estado nación. Una encuesta reciente del Foro Económico Mundial muestra que el 70 % de los responsables de seguridad informática han declarado que la geopolítica ha influido en las estrategias de ciberseguridad de sus empresas.

Los Estados nación refuerzan cada vez más sus capacidades cibernéticas para buscar ventajas políticas, económicas y militares, difuminando así las distinciones entre los ataques orquestados por el Estado y los llevados a cabo por grupos afiliados. La información proporcionada por XCyber arroja conocimientos de inteligencia sobre lo que cabe esperar en relación con las consecuencias del aumento del riesgo geopolítico.

Geopolítica y el panorama de las ciberamenazas

Milo Wilson
Analista jefe de Inteligencia en XCyber

Bill Jarvis
Jefe de Inteligencia de XCyber

En medio de las crecientes tensiones y los cambios de prioridades entre las potencias mundiales en el ciberespacio, la amenaza más importante para las empresas es la creciente profesionalización de los ciberdelincuentes, que llevan a cabo impunemente sofisticados ataques desde países hostiles.

Las tensiones entre Estados nación se caldean en el ciberespacio

Las potencias cibernéticas mundiales parecen haber aceptado que las cibercampañas concertadas patrocinadas por los Estados, y a menudo agresivas, se han convertido en una norma. La demarcación entre Occidente y los llamados «cuatro grandes» (Rusia, China, Corea del Norte e Irán), que se ha hecho cada vez más patente en los últimos 12 meses, dará lugar probablemente a campañas cibernéticas más agresivas en el futuro.

En concreto, Rusia ha abandonado cualquier pretensión de tomar medidas enérgicas contra los ciberdelincuentes que operan dentro de sus fronteras, como demuestra la aprobación el año pasado de una ley que otorga inmunidad a los delitos cometidos por piratas informáticos «en interés del Estado ruso». La protección de los grupos de ciberdelincuentes por parte de Rusia ha agravado el panorama mundial de las amenazas, sobre todo porque las sanciones impuestas a Rusia han dejado sin empleo a un gran número de profesionales cualificados de las tecnologías de la información que podrían verse atraídos por la lucrativa ciberdelincuencia.

En última instancia, Rusia aspira a un panorama cibernético controvertido e inseguro, ya que cree que esto perjudicará desproporcionadamente a las potencias occidentales, algo que se observa en el funcionamiento de redes de desinformación dirigidas a las elecciones mundiales. Podría decirse que este panorama más amenazador también ha dado lugar a campañas de espionaje más agresivas por parte de los agentes estatales chinos, así como a respuestas más contundentes por parte de sus objetivos.

Improbabilidad de que se repita el conflicto cibernético ucraniano

Es difícil extraer conclusiones firmes de la guerra de Ucrania sobre futuros conflictos. Ucrania cuenta con un ecosistema nacional de ciberseguridad extremadamente resiliente, resultado de años de preparación contra los ataques rusos, y ha recibido el apoyo de algunas de las mayores empresas tecnológicas del mundo. Rusia también ha tenido cuidado de contener los impactos de sus esfuerzos cibernéticos en Ucrania a la zona de conflicto, a pesar de su capacidad para lanzar ataques de mayor escala y consecuencia.

Sin embargo, los futuros conflictos podrían ser diferentes, y la preocupación se centra en una guerra en la que participen ciberatacantes agresivos y competentes que revelen al resto del mundo programas maliciosos u otras técnicas altamente destructivas. China es uno de los países más agresivos en la explotación de vulnerabilidades de día cero. En 2021, el gobierno chino aprobó una ley que hacía obligatorio informar de las vulnerabilidades a las autoridades antes de hacerlas públicas.

Esto parece haber impulsado significativamente las capacidades cibernéticas ofensivas de China (los grupos chinos fueron los atacantes más prolíficos en explotar días cero en 2023). Los grupos delictivos tienen un largo historial de explotación de técnicas de piratería informática respaldadas por el Estado una vez que se revelan públicamente, sobre todo contra empresas demasiado lentas para adaptarse a las nuevas vulnerabilidades.

Rusia se vuelca en el espionaje

Los esfuerzos cibernéticos de Rusia en Ucrania en el último año se han alejado de los ataques disruptivos y destructivos (en particular, el despliegue del programa malicioso conocido como «wiper») hacia el espionaje y la recopilación de inteligencia, con la evolución de las tácticas que reflejan las expectativas de reajuste en torno a la duración de la guerra.

La resistencia de Ucrania, tanto en el ámbito militar como en el cibernético, ha hecho que cambie la naturaleza de la guerra, lo que a su vez ha repercutido en los esfuerzos cibernéticos rusos. Sandworm, el grupo más activo de los apoyados por Rusia en Ucrania, por ejemplo, ha pasado de la desarticulación a la recopilación de inteligencia, haciendo cada vez más hincapié en el espionaje para ayudar a las fuerzas rusas.

La combinación de objetivos militares y cibernéticos refleja la naturaleza de la guerra, en el sentido de que los objetivos de las operaciones cibernéticas pueden alcanzarse más eficazmente con la guerra cinética. Mientras que los ciberataques rusos de antes de la guerra contra la infraestructura energética ucraniana provocaban (como mucho) apagones de una hora, ahora se ha perdido el 80 % de su capacidad de generación eléctrica en casi 180 ataques aéreos.

Las operaciones se extienden más allá de Ucrania. Los mismos actores también están llevando a cabo campañas de desinformación coincidiendo con una serie de elecciones de alto nivel este año. La injerencia electoral forma parte de un esfuerzo más amplio de Rusia por perturbar los intereses occidentales, que incluye el uso de mercenarios en África y la financiación de partidos políticos marginales, por lo que no debe considerarse un asunto «solo cibernético».

La ciberdelincuencia sigue siendo la principal amenaza para las empresas

La ciberdelincuencia sigue siendo una enorme amenaza para las empresas de todo el mundo. Los grupos siguen favoreciendo los ataques fáciles contra las víctimas peor protegidas, y un reciente informe del FMI citaba la creciente desigualdad cibernética entre las organizaciones que son ciberresilientes y las que no lo son. Alrededor de la mitad de las ciberinfracciones afectan a empresas con menos de 1000 empleados, y muchas pequeñas empresas quiebran poco después de ser víctimas de un ataque.

Aunque muchos grupos de ciberdelincuentes actúan con independencia del respaldo estatal, ambos suelen estar interrelacionados. Prueba de ello son los crecientes niveles de ciberdelincuencia procedente de Rusia, así como la selección de empresas por parte de grupos delictivos por motivos políticos. En diciembre de 2023, una operación propalestina reivindicó decenas de filtraciones de datos contra empresas israelíes, y en el mismo mes una empresa cervecera de Estados Unidos fue objeto de ataques por utilizar *hardware* de fabricación israelí.

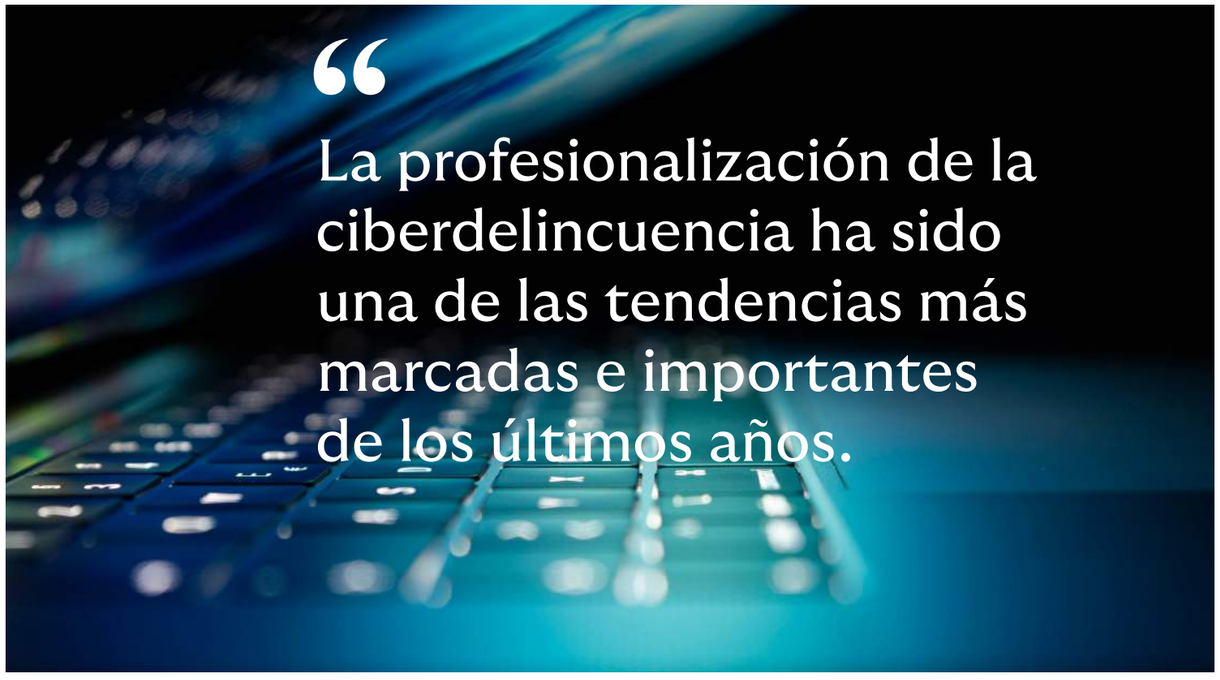
Ciberdelincuencia S.A.

La profesionalización de la ciberdelincuencia ha sido una de las tendencias más marcadas e importantes de la ciberseguridad en los últimos años. Esto ha implicado el rápido crecimiento de los actores de la amenaza, con diferentes grupos especializados en distintas partes de la cadena de suministro, y dentro de los propios grupos, lo que ha dado lugar a un entorno de amenazas más intenso.

Muchos grupos delictivos operan ahora casi como empresas profesionales, con equipos de reclutamiento e infraestructura corporativa. Un ejemplo de esta profesionalización es el grupo ruso AlphaLock, que opera un modelo de negocio en dos partes diseñado tanto para formar a los ciberdelincuentes como para convertirlos en armas con fines lucrativos contra las organizaciones, al ofrecer un programa de afiliados para unirse al grupo de piratas informáticos.

Los grupos delictivos suelen operar con un modelo de negocio que sigue el camino de menor resistencia. La explosión de las ofertas de *malware* como servicio (MaaS) y RaaS da buena cuenta de ello. Otros modelos que se están adoptando incluyen pagar a especialistas para que identifiquen objetivos fáciles. Los grupos más grandes también pueden ofrecer acceso inicial a la infraestructura empresarial de una compañía, como un escritorio remoto o la cuenta de correo electrónico de un director general, a bandas menos sofisticadas que tengan conocimientos y habilidades suficientes para explotarla con fines lucrativos.

Todo ello ha creado un ecosistema más amplio de ciberdelincuencia, en el que los grupos no necesitan ser altamente competentes , ni siquiera «piratear una empresa», para obtener beneficios significativos.



03

IA generativa: un arma de doble filo

Mientras que el *ransomware* y el riesgo sistémico siguen dominando el panorama de las ciberamenazas, otro acontecimiento importante y relativamente nuevo ha sido la explosión de la IA generativa.

A pesar del amplio consenso entre la comunidad de ciberseguridad y el mercado de seguros sobre el potencial transformador de esta nueva tecnología, tanto para las capacidades ofensivas como defensivas, hay mucha menos claridad sobre qué casos de uso demostrarán ser los más importantes y cuándo es probable que ganen tracción.

No obstante, cada vez están más claras dos conclusiones emergentes sobre cómo la IA generativa remodelará el panorama de las amenazas en los próximos años.

> “La IA generativa aumentará el potencial de acumulación, gravedad y frecuencia de los siniestros en áreas predecibles.

En primer lugar, dados los incentivos geopolíticos y financieros, los sofisticados actores de amenazas respaldados por el Estado utilizarán la IA generativa para perfeccionar sus tácticas, técnicas y procedimientos (TTP) con una eficacia y escala cada vez mayores. En febrero de 2024, Microsoft y Open AI revelaron que los actores de las amenazas de los Estados nación han estado utilizando ChatGPT para facilitar las actividades de piratería establecidas, con una banda rusa, por ejemplo, a cargo del reconocimiento de satélites.

En segundo lugar, y lo que es más importante para el mercado de los seguros, la IA generativa aumentará la acumulación potencial, la gravedad y la frecuencia de los siniestros en áreas predecibles al mejorar las capacidades de los piratas informáticos comerciales.

La Figura 17 puntúa el grado en que la IA mejorará las capacidades de los actores de amenazas entre 2024 y 2026 en cinco dimensiones clave y extrae las implicaciones para las reclamaciones. Todos los tipos de atacantes, desde los agentes estatales altamente capacitados hasta los grupos de delincuencia organizada y los piratas informáticos menos expertos, verán cómo la IA mejora sus capacidades. Más allá de esto, el impacto será muy matizado.

Figura 17: La IA generativa mejora las capacidades de los actores de amenazas: de 2024 a 2026
(Fuente: Análisis de Howden con información del Consejo Nacional de Ciberseguridad)

	Reconocimiento	Ingeniería social, *phishing*, contraseñas	Herramientas (*malware*, *exploits*)	Movimiento lateral	Exfiltración	Puntuación de aumento	Principales consecuencias de los siniestros
Agentes estatales altamente capacitados						19	**Acumulación**: mayor riesgo de propagación de ataques de programas maliciosos patrocinados por el Estado (por ejemplo, NotPetya 2.0) debido a la mayor capacidad de generación de dichos programas.
Agentes estatales capacitados, empresas comerciales que venden a Estados, grupos organizados de ciberdelincuencia						20	**Gravedad alta**: los cibergrupos avanzados se dirigen cada vez más a las empresas más propensas a pagar grandes rescates con ataques sofisticados como, por ejemplo, *deepfakes*. **Gravedad alta**: aumento de la doble y triple extorsión debido a una identificación y robo de datos de gran valor más avanzados y basados en IA, es decir, capacidad de exfiltración. **Gravedad alta**: más filtración de datos confidenciales en la red oscura con un mayor número de grupos (colaboradores) que exigen rescates por pirateo informático.
Piratas informáticos a sueldo menos cualificados, ciberdelincuentes oportunistas, hacktivistas						24	**Frecuencia alta**: más actores de amenazas novatos entran en el mercado utilizando capacidades (por ejemplo, chatbots de IA para *phishing*, buscadores de vulnerabilidades ML) desarrolladas y vendidas por grupos avanzados. **Gravedad baja**: más ataques de gran volumen y baja sofisticación que se enfrentan a una mayor salud cibernética.

Nota: Las puntuaciones de aumento son inexistentes (0), posibilidad (1), mínimo (2), moderado (4), aumento (6) o significativo (8)

Piratas informáticos menos cualificados

Este grupo es el que más verá aumentar sus capacidades. Y lo que es más importante, muchos actores de amenazas novatos obtendrán acceso a herramientas, código e inteligencia que les permitirán empezar a piratear. Esto será impulsado por piratas informáticos sofisticados con profundos conocimientos en IA que monetizarán sus habilidades vendiendo capacidades en línea, un modelo de negocio de riesgo relativamente bajo. Como resultado, la IA acelerará la tendencia de los últimos años a la democratización de la piratería informática, visible en el auge de la piratería subcontratada, como RaaS.

La principal consecuencia de la democratización de la piratería impulsada por la IA será un aumento de la frecuencia de las reclamaciones de bajo nivel. Los actores de amenazas novatos lo tendrán más fácil para llevar a cabo *phishing*, que fue el vector utilizado en el 84 % de los ataques a empresas del Reino Unido en 2023.[5] También tendrán acceso a chatbots que les ayuden a redactar contenido de *phishing* de alta calidad, similar a ChatGPT sin barreras de seguridad, reconocimiento generado por IA sobre qué empresas atacar (por ejemplo, a partir de aprendizaje automático entrenado para detectar patrones de vulnerabilidad) e incluso código de *ransomware* generado por IA.

Grupos delictivos organizados

Los grupos de ciberdelincuentes organizados y tecnológicamente avanzados verán reforzadas sus capacidades de tal forma que se prevé un aumento significativo de la gravedad de un pequeño número de siniestros. Estos grupos se centrarán cada vez más en el pirateo más lucrativo, es decir, en las empresas más proclives a pagar grandes rescates con ataques sofisticados.

Uno de estos vectores es la ingeniería social a través de deepfakes, donde la IA genera llamadas de voz e incluso videollamadas falsas convincentes para embaucar a los empleados para que transfieran fondos o compartan datos de acceso. Además, la IA generativa mejorará las capacidades de exfiltración al aumentar la velocidad y precisión con la que se pueden identificar y robar datos de gran valor.

Con el tiempo, los grandes modelos de lenguaje (LLM, por sus siglas en inglés) se entrenarán en conjuntos de datos robados para aprender qué buscar. Esto, a su vez, provocará más extorsiones al obligar a las empresas a pagar para mantener la confidencialidad de los datos exfiltrados.

Agentes estatales altamente capacitados

Los piratas informáticos más sofisticados cuentan con el respaldo de los Estados nación y siguen muy centrados en los conflictos y los objetivos geopolíticos más que en ganar dinero. No obstante, estos agentes podrían utilizar la IA generativa para mejorar las capacidades de los programas maliciosos en caso de que cambien las prioridades, lo que a su vez presentaría un mayor riesgo de propagación y acumulación de pérdidas.

[5] Ministerio de Ciencia, *Encuesta sobre Innovación y Tecnología, y vulneraciones de ciberseguridad*, 2024

Capacidades de defensa

El impacto neto de la IA en los ciberataques y las pérdidas de seguros resultantes dependerán inevitablemente de cómo respondan los defensores. En este frente, las empresas tienen motivos para el optimismo. Y lo que es más importante, las defensas actuales deberían ser lo suficientemente fuertes como para resistir el aumento de la frecuencia de ataques relativamente sencillos y predecibles.

De cara al futuro, los expertos en ciberseguridad ven con buenos ojos la capacidad de la IA para reforzar las defensas. Ya hay varios casos de uso que destacan por su potencia y facilidad de aplicación.

Escaneado de *software* previo al lanzamiento	Los desarrolladores de *software* pueden utilizar la IA para escanear el código en busca de errores y vulnerabilidades antes de su publicación. Esto significaría que ya no tendrían que apresurarse a solucionar las vulnerabilidades una vez publicadas, un desfase crítico que aprovechan los piratas informáticos.
Mantenimiento de *software* de código abierto	Los LLM pueden utilizarse para actualizar *software* de código abierto, por ejemplo, traduciendo código obsoleto a un lenguaje más seguro. Esto es importante porque el *software* de código abierto es una puerta trasera infravalorada en muchas redes (véase la contribución de S-RM sobre «piedras angulares digitales» en la página 25), ya que puede ser a la vez ampliamente utilizado y relativamente inseguro debido a su mantenimiento por la multitud en lugar de los vendedores.
Clasificación de datos	La IA puede utilizarse para automatizar el proceso de clasificación de datos en función de su confidencialidad. Se trata de un caso de uso importante porque los enfoques actuales de clasificación de datos a menudo dependen de empleados, propensos a cometer errores, para hacerlo manualmente. Además, esto ayudaría a defenderse de la amenaza emergente de que los piratas informáticos utilicen los LLM para localizar datos de gran valor a gran velocidad.
Caza de amenazas	Los analistas pueden utilizar la IA para ayudar a rastrear la red con mayor rapidez y precisión en busca de agentes de amenazas que se hayan colado bajo el radar. Por ejemplo, un LLM podría entrenarse para detectar actividades sospechosas, como picos en los volúmenes de tráfico de la red. Más de una quinta parte (22 %) de los CISO han empezado a hacerlo.[6]

[6] Splunk, *El informe CISO*, octubre de 2023.

Impacto de la IA generativa en el panorama de las amenazas cibernéticas

Matt Hull
Director de Inteligencia Global sobre Amenazas de NCC Group

Jon Renshaw
Director adjunto de Investigación Comercial de NCC Group

La IA generativa brinda oportunidades tanto a los ciberatacantes como a los defensores y parece que tendrá un impacto significativo en el panorama de las amenazas, ya que permitirá ataques más avanzados por parte de actores sofisticados y reducirá las barreras de entrada para los piratas informáticos novatos. La buena noticia es que las nuevas defensas basadas en la IA se están desarrollando a buen ritmo y que el uso eficaz de los controles de riesgo más tradicionales puede apuntalar la resistencia.

Puerta abierta a la ciberdelincuencia

La amenaza de los sistemas de IA sigue siendo relativamente desconocida. En medio de una considerable especulación e incluso sensacionalismo en torno a cómo afectará la IA generativa al panorama de los riesgos cibernéticos, es importante comprender la verdadera amenaza. En esta fase relativamente temprana del ciclo de desarrollo, vemos tres casos de uso principales para los que las empresas deben prepararse:

1. **Permitir la ingeniería social**
Los LLM ya están permitiendo a los delincuentes crear contenidos verosímiles de forma rápida y sencilla. Se utiliza para tareas sencillas, pero importantes, como corregir el lenguaje, el tono, la ortografía y la gramática de los correos electrónicos de *phishing*, lo que significa que son más selectivos y creíbles.

2. **Falsificaciones profundas (*deepfakes*) y clonación de voz**
Los delincuentes y los grupos de hacktivistas ya clonan la voz y las imágenes de una persona auténtica para cometer fraudes en línea, ingeniería social y, en algunos casos más recientes, para difundir desinformación en las redes sociales. Los casos de gran repercusión en los que se han utilizado vídeos falsos para engañar a objetivos y obtener cuantiosos pagos revelan un cambio en la sofisticación de los actores de amenazas.

3. **IA como posibilitadora**
Los ciberdelincuentes principiantes están utilizando servicios como OpenAI para acelerar (rápidamente) la curva de aprendizaje en la ejecución de ataques, mientras que los individuos más experimentados se centran en maximizar la eficiencia. Algunos ejemplos son la depuración de código, la traducción de documentos, la generación de scripts, la recuperación y cotejo de información disponible públicamente sobre objetivos y la investigación de posibles formas de poner en peligro los sistemas.

Amenaza creciente en ambos extremos del espectro de sofisticación

Como se ha mencionado anteriormente, ya estamos viendo el uso sofisticado de falsificaciones de audio y vídeo en fraudes de pagos *push* autorizados muy selectivos. Actualmente se trata de ataques de baja probabilidad y alto impacto. A medida que aumenten las capacidades, esperamos que se reduzcan las barreras de entrada para este tipo de fraude sofisticado y selectivo.

No obstante, seguirán requiriendo un grado de sofisticación (y esfuerzo) que debería impedir su despliegue a escala masiva, pero es importante que las empresas comprendan que el realismo de las falsificaciones es cada vez mayor, al igual que la probabilidad de que los ataques tengan éxito.

En el otro extremo de la escala de sofisticación, los ciberdelincuentes utilizan los LLM para mejorar la calidad de las comunicaciones escritas en ataques de *phishing* y otras estafas con motivaciones económicas. Es probable que esto aumente las posibilidades de éxito de los ataques de gran volumen (más que dirigidos).

La IA también reduce las barreras a la ciberdelincuencia, el pirateo por encargo y el hacktivismo. Este acceso más sencillo dará lugar probablemente a un mayor volumen de ciberactividad con motivaciones financieras, como el *ransomware*, y a una actividad hacktivista más amplia e impactante.

Por lo que se ha registrado hasta ahora, esperamos ver un aumento del impacto y el volumen de los ataques, sobre todo debido a un aumento de la capacidad de investigación, reconocimiento e ingeniería social.

Ataques a la IA

Las investigaciones de NCC Group[7] ya han puesto de relieve el potencial de los actores de amenazas que atacan los sistemas de IA para denegar el servicio o provocar grandes costes a las víctimas. Es poco probable que este tipo de ataques estén motivados por un beneficio económico para el atacante, sino más bien para ganar notoriedad o por motivaciones ideológicas.

Además, los modelos entrenados representan una importante inversión en propiedad intelectual (PI) por parte de los desarrolladores de IA. Los grupos sin escrúpulos podrían lanzar ataques para extraer datos de entrenamiento y ponderaciones de modelos, asegurándose así el acceso a la propiedad intelectual para obtener una ventaja competitiva. NCC Group publicó recientemente un aviso sobre una vulnerabilidad de reenlace del sistema de nombres de dominio en el marco LLM de Ollama, lo que demuestra que la seguridad de las aplicaciones tradicionales sigue siendo igual de relevante, incluso cuando esa aplicación es IA.

Las defensas de IA evolucionan a buen ritmo

Los modelos de aprendizaje automático se han incorporado a las herramientas de ciberdefensa desde hace muchos años, proporcionando capacidades de automatización que permiten a las organizaciones amplificar sus esfuerzos de ciberdefensa. También se han añadido interfaces de lenguaje natural para la búsqueda, y ahora la disponibilidad de LLM permite a los desarrolladores de herramientas integrar interfaces conversacionales que facilitan el acceso a datos y funcionalidades.

El uso de la IA para detectar y defenderse contra ataques de IA es relativamente incipiente, pero sin duda es un área que se está desarrollando a buen ritmo. Por ejemplo, el Entorno de Capacidad Acelerada del Ministerio del Interior del Reino Unido lanzó recientemente un concurso de detección de *deepfakes*.[8] Las grandes organizaciones tecnológicas y los desarrolladores de IA también están explorando técnicas de marcas de agua[9] y procedencia[10] para detectar cuándo los medios han sido generados por IA o para demostrar que no lo han sido.

Aunque el ritmo del cambio puede parecer abrumador, los consejos a las empresas siguen centrándose en la concienciación de los empleados y en consejos prácticos como evitar actuar bajo presión, desconfiar de escenarios que parezcan demasiado buenos como para ser verdad, comprobar con un colega independiente o a través de otro medio e incluso pedir a los posibles estafadores que demuestren su autenticidad, por ejemplo, poniéndose gafas de sol o un sombrero.

Prepárese ya

Cada vez hay más pruebas que sugieren que la IA actuará como un acelerador de ataques en el futuro próximo de uno a tres años y que las empresas deben estar preparadas tanto para un aumento de estafas novedosas/sofisticadas como para más ataques a vectores ya establecidos.

La buena noticia es que existen factores de mitigación probados y eficaces: formación y concienciación entre el personal, buena salud cibernética, incluida la gestión de parches, escaneado de vulnerabilidades y pruebas de penetración, así como planificación y pruebas de respuesta ante incidencias. Todos ellos son vitales para la ciberresiliencia de las organizaciones y son ahora más necesarios que nunca.

> “Las empresas deben estar preparadas tanto para un aumento de las estafas sofisticadas como para más ataques a vectores ya establecidos.

[7] research.nccgroup.com/2022/07/06/whitepaper-practical-attacks-on-machine-learning-systems
[8] ace.blog.gov.uk/2024/04/16/unmasking-deception-join-the-deepfake-detection-challenge
[9] deepmind.google/technologies/synthid
[10] c2pa.org

04

El camino hacia la madurez

A pesar de la gran variabilidad del entorno de amenazas, ya se han sentado las bases de un mercado maduro de (re)aseguros cibernéticos, con la perspectiva de un crecimiento constante impulsado por la exposición, la rentabilidad continua y la innovación.

La competencia está volviendo al mercado, ya que la mejora de la salud cibernética ha mitigado las pérdidas y ha proporcionado unos buenos resultados de suscripción.

> “Las oportunidades en zonas geográficas internacionales y en el ámbito de las pymes están preparadas para impulsar el crecimiento.

A pesar de una pausa en el crecimiento mundial de las primas el año pasado debido a la transición del ciclo del mercado, las oportunidades en zonas geográficas internacionales y otras áreas con poca penetración (pymes en particular, junto con los rápidos avances tecnológicos) están preparadas para impulsar un rápido crecimiento para el resto de la década. La evolución del panorama de las amenazas, la mayor concienciación sobre los riesgos y las normativas más estrictas también respaldarán la demanda.

Las condiciones del mercado ofrecen una propuesta atractiva tanto para los compradores como para los operadores, ya que los operadores existentes desean aumentar sus despliegues, impulsados además por una serie de nuevos participantes (incluidas las InsurTech centradas en el mercado de las pymes).

Reciclaje en materia cibernética

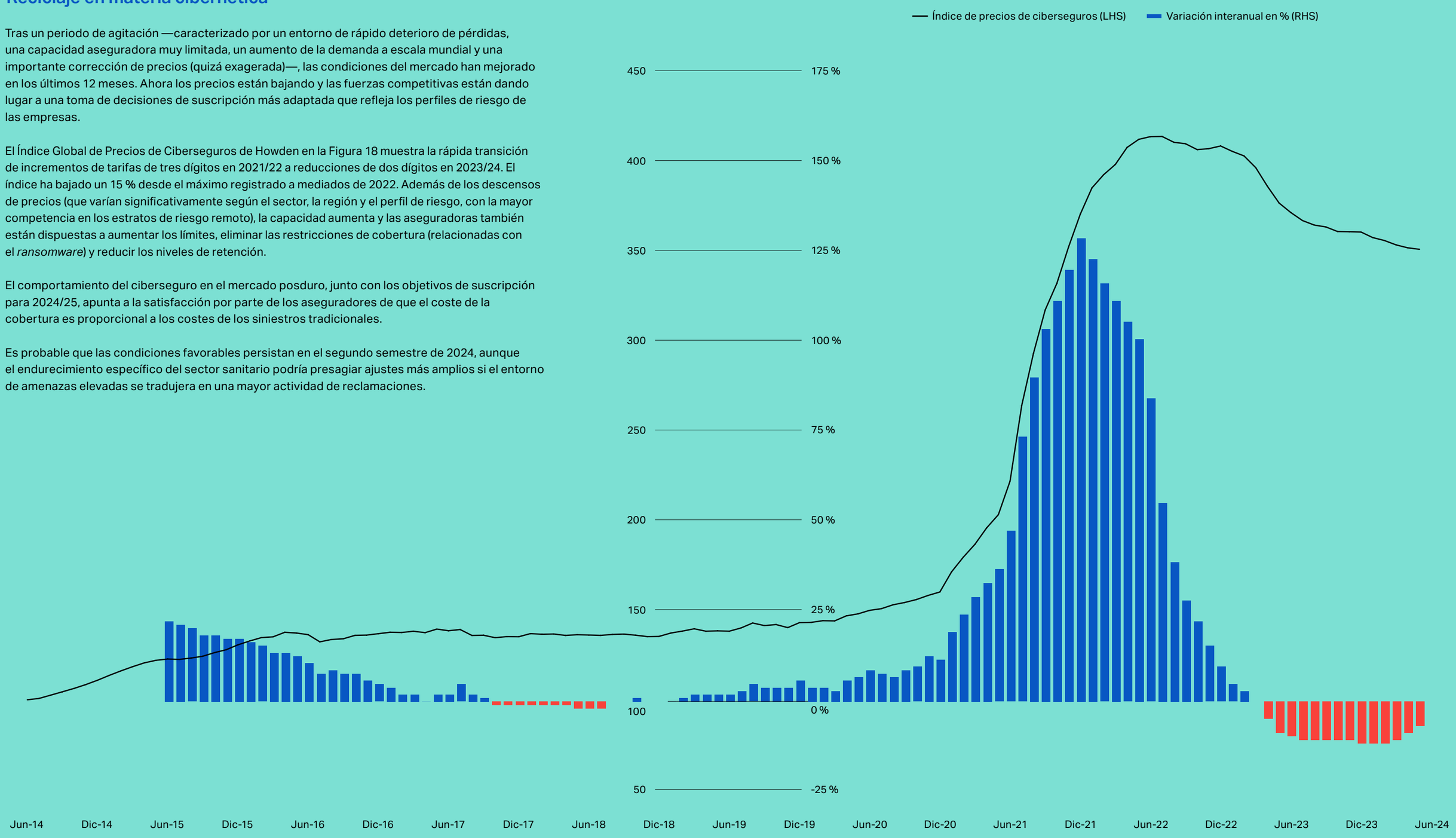
Tras un periodo de agitación —caracterizado por un entorno de rápido deterioro de pérdidas, una capacidad aseguradora muy limitada, un aumento de la demanda a escala mundial y una importante corrección de precios (quizá exagerada)—, las condiciones del mercado han mejorado en los últimos 12 meses. Ahora los precios están bajando y las fuerzas competitivas están dando lugar a una toma de decisiones de suscripción más adaptada que refleja los perfiles de riesgo de las empresas.

El Índice Global de Precios de Ciberseguros de Howden en la Figura 18 muestra la rápida transición de incrementos de tarifas de tres dígitos en 2021/22 a reducciones de dos dígitos en 2023/24. El índice ha bajado un 15 % desde el máximo registrado a mediados de 2022. Además de los descensos de precios (que varían significativamente según el sector, la región y el perfil de riesgo, con la mayor competencia en los estratos de riesgo remoto), la capacidad aumenta y las aseguradoras también están dispuestas a aumentar los límites, eliminar las restricciones de cobertura (relacionadas con el *ransomware*) y reducir los niveles de retención.

El comportamiento del ciberseguro en el mercado posduro, junto con los objetivos de suscripción para 2024/25, apunta a la satisfacción por parte de los aseguradores de que el coste de la cobertura es proporcional a los costes de los siniestros tradicionales.

Es probable que las condiciones favorables persistan en el segundo semestre de 2024, aunque el endurecimiento específico del sector sanitario podría presagiar ajustes más amplios si el entorno de amenazas elevadas se tradujera en una mayor actividad de reclamaciones.

Figura 18: Índice global de precios de ciberseguros de Howden: de 2014 a 2T24 (Fuente: Howden)

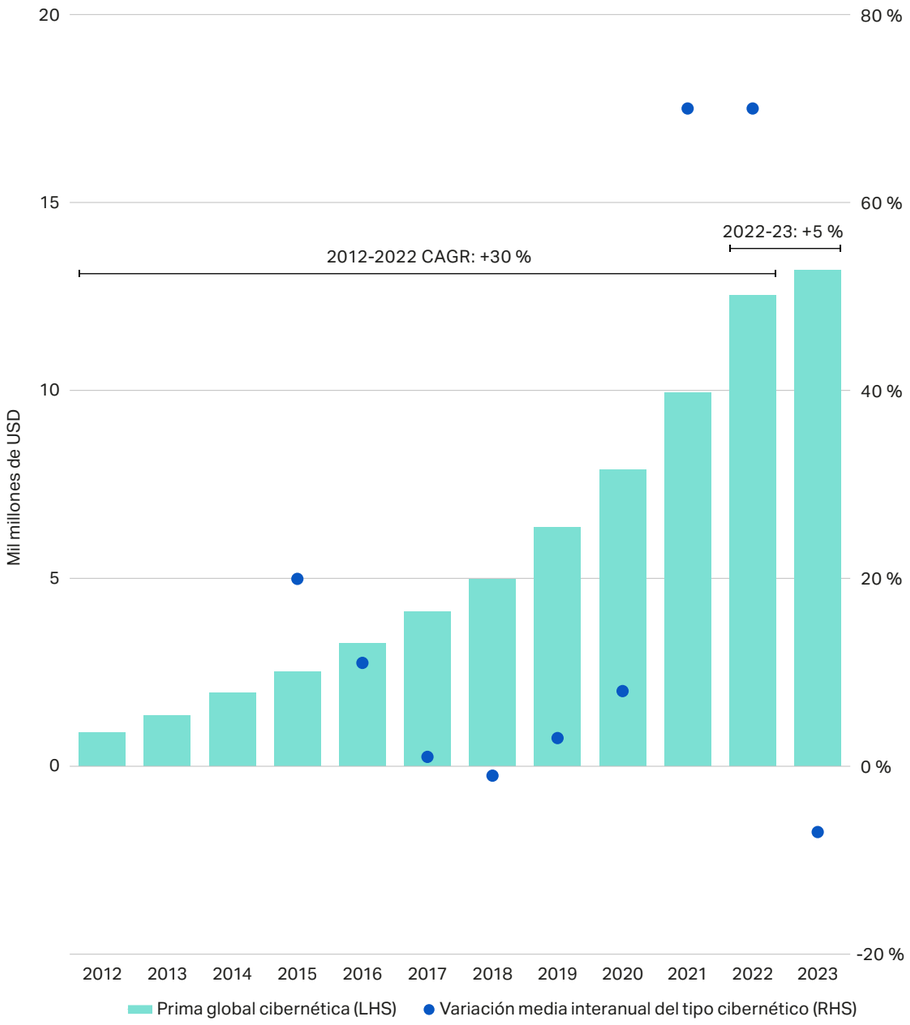


Perfil de crecimiento

El ciberseguro ha sido una de las áreas de seguros de más rápido crecimiento (si no la que más) durante casi una década. El crecimiento anualizado del 30 % durante este tiempo (como muestra la Figura 19) se compara con el rango porcentual de un solo dígito del sector comercial de bienes y accidentes más amplio.

Los volúmenes de primas están impulsados por una combinación de exposición y tarificación, y aunque ambos factores contribuyeron a impulsar el crecimiento hasta 2020 (aunque mucho más sesgado para el primero), el entorno de tarificación precipitó un cambio notable en 2021/22, cuando los elevados aumentos de precios anualizados de dos dígitos compensaron con creces las acciones de suscripción y la consiguiente reducción de las exposiciones globales.

Figura 19: Primas brutas suscritas cibernéticas mundiales: de 2012 a 2023 (Fuente: Howden)



> “Es poco probable que la fijación de precios a partir de aquí impulse la expansión del mercado en la medida en que lo hizo durante la corrección de 2020-2022.

2023 marcó el ritmo de crecimiento más lento desde la creación del mercado (+5 %). El año pasado no se cumplieron los objetivos de suscripción y varios de los principales actores no alcanzaron sus objetivos de ingresos. Si no se producen perturbaciones, es poco probable que la fijación de precios a partir de aquí impulse la expansión del mercado en la medida en que lo hizo durante la corrección de 2020-2022, lo que exige planes ambiciosos de crecimiento de la exposición.

Aliviar la presión

La mejora de las condiciones del mercado refleja las medidas de suscripción adoptadas por las aseguradoras durante el mercado duro, junto con las inversiones en curso realizadas por las empresas para reforzar sus posturas de riesgo y sus prácticas de gestión de reclamaciones.

El análisis proporcionado por S-RM explica cómo una combinación de acciones en múltiples frentes ha mitigado el coste de las reclamaciones y, en última instancia, ha facilitado un cambio positivo en las condiciones del mercado.

S-RM sobre la cesión de reclamaciones cibernéticas

En un momento de cambios complejos y rápidos en el entorno de las reclamaciones cibernéticas, sigue siendo difícil acumular y aprovechar los datos entre los participantes en el mercado. Aunque el número absoluto de reclamaciones no haya disminuido en los dos últimos años, el coste medio de estas se ha reducido claramente.

Varios factores impulsan esta tendencia.

Mejoras en las prácticas de suscripción. Las aseguradoras han mejorado notablemente sus prácticas de suscripción invirtiendo en programas de formación para mejorar la cualificación de los equipos de suscripción. El corolario ha sido una comprensión más desarrollada de las prácticas de gestión del riesgo, la adopción de herramientas de cuantificación del riesgo y el perfeccionamiento de la modelización del riesgo para adaptarla a los perfiles de riesgo de las empresas.

Prácticas de gestión de reclamaciones. Las empresas confían más en la utilización de proveedores de paneles, lo que se traduce en un mayor control de los costes de las reclamaciones y en mejores prácticas de contención y gestión de riesgos. Esto se debe a una mayor concienciación sobre el valor de los proveedores de paneles experimentados y al aumento de la inversión de las aseguradoras para mantener una experiencia de alta calidad en los paneles.

Acceso a experiencia técnica. Los modelos de tramitación de reclamaciones están dando prioridad al acceso a los conocimientos técnicos para los siniestros de primera mano que requieren asistencia técnica inmediata. La primera notificación de pérdidas se dirige cada vez más a expertos técnicos internos o externos equipados para proporcionar asesoramiento inmediato con el fin de limitar la propagación y el impacto de un suceso de seguridad, mejorando así el control de los costes.

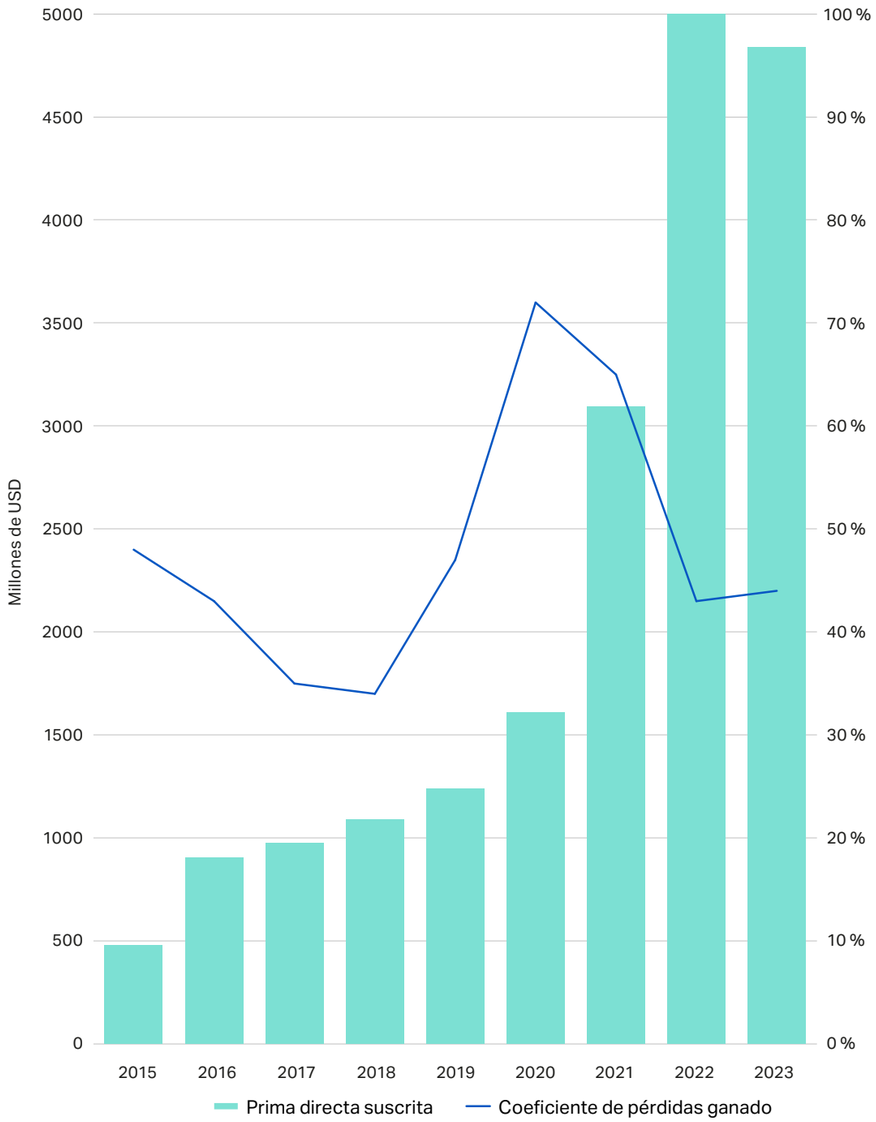
Atención en la preparación para la respuesta y la recuperación. Las organizaciones llevan varios años invirtiendo de forma proactiva en controles de prevención, detección y respuesta, lo que significa que los sucesos potencialmente importantes se interceptan en una fase temprana de la cadena de ataque, lo que limita el impacto en la empresa. La mayoría de las organizaciones están pasando de la inversión en prevención a la resiliencia operativa, con el fin de mejorar su capacidad para recuperarse rápidamente, minimizar el tiempo de inactividad y evitar pérdidas por interrupción de la actividad.

Aplicación de la ley. Las fuerzas del orden son cada vez más eficaces a la hora de desarticular algunos de los grupos de *ransomware* más activos. A finales de 2023, dos grupos, LockBit y BlackCat, eran responsables de un tercio de todos los ataques de *ransomware* conocidos. La acción selectiva de las fuerzas de seguridad a principios de 2024 desbarató ambos grupos, lo que contribuyó a que LockBit cayera de los tres grupos más prolíficos. Al parecer, BlackCat cerró sus servidores después de piratear con éxito a Change Healthcare.

> “Las organizaciones llevan varios años invirtiendo de forma proactiva en controles de prevención, detección y respuesta, lo que significa que los sucesos potencialmente importantes se interceptan a tiempo.

Todos estos factores atenuantes se reflejan en los datos de las declaraciones complementarias en Estados Unidos, que ofrecen una instantánea de las tendencias de las reclamaciones y los resultados de la suscripción. La Figura 20 muestra que la rentabilidad se mantuvo fuerte en 2023, ya que el mercado estadounidense registró un índice de siniestralidad del 44 %, en línea con 2022 y significativamente mejor que 2021 (65 %) y 2020 (72 %).

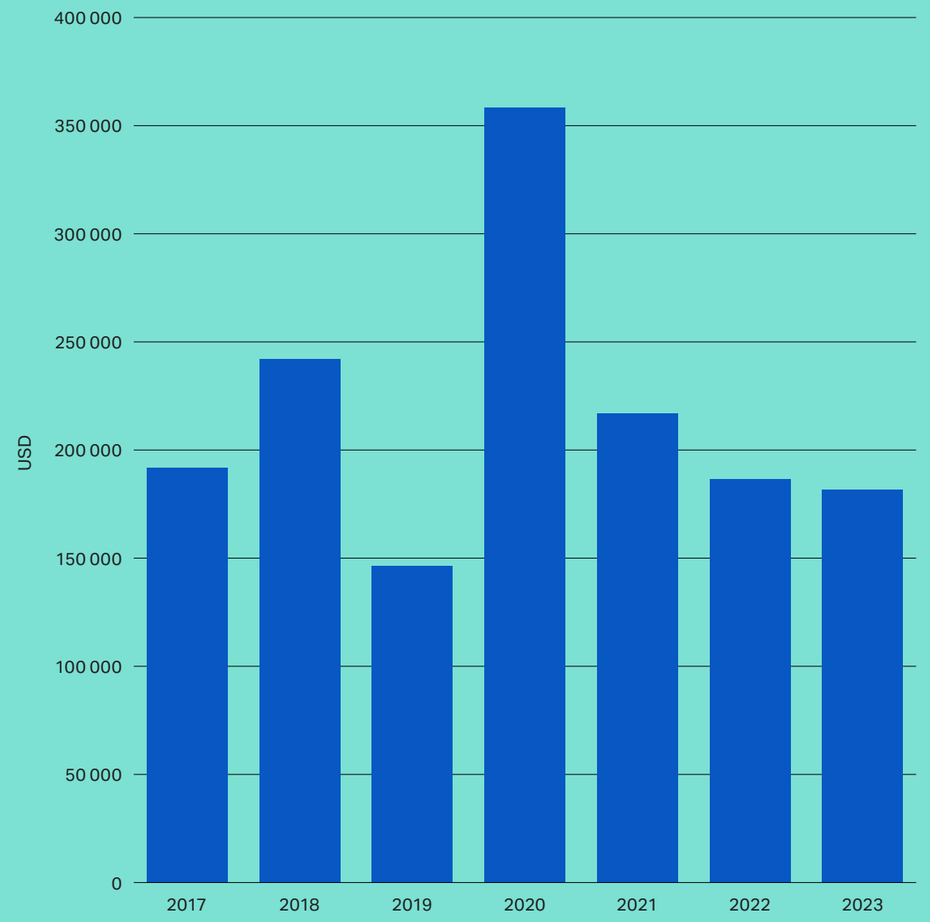
Figura 20: Coeficiente de siniestralidad y prima directa suscrita para las pólizas cibernéticas independientes de Estados Unidos: de 2015 a 2023 (Fuente: Howden, NOVA, NAIC)



La reducción marginal del flujo de primas en las líneas nacionales admitidas y excedentarias de EE. UU. el año pasado (-3 % interanual, el primer descenso registrado) tuvo una incidencia limitada en los resultados, ya que la cuantía de las pérdidas y los costes de defensa se mantuvieron relativamente estables.

La Figura 21 muestra la gravedad de las reclamaciones registradas por el mercado estadounidense desde 2017, con el notable descenso de los últimos años coincidiendo con la mejora de las posturas de riesgo que, en última instancia, han ayudado a contener los costes. Estas tendencias subyacentes se repiten en la mayoría de los demás grandes mercados cibernéticos.

Figura 21: Promedio de reclamaciones del mercado independiente estadounidense: de 2017 a 2023[11] (Fuente: Howden, NOVA, NAIC)



[11] Pérdidas directas y gastos de defensa divididos entre el número de reclamaciones pagadas.

S-RM sobre los costes de contención

Roddy Priestley
Director de Ciberseguridad en S-RM

Martijn Hoogesteger
Jefe de Ciberseguridad, Benelux en S-RM

La imposición efectiva de controles como la autenticación multifactor (MFA, por sus siglas en inglés) y las copias de seguridad ha tenido un enorme impacto en la mejora del riesgo subyacente de las carteras de ciberseguros. La ausencia o mala configuración de estos controles ha sido uno de los principales factores que han provocado importantes pérdidas.

Incluso en el caso de que se eludan estos controles, se pueden prevenir incidencias y contener los costes gestionando adecuadamente los controles en tres fases clave del ciclo de vida de los ataques.

P1

Fase de «entrada»

En 2023, el método de entrada más común en nuestros casos de respuesta a *ransomware* fue a través de servicios remotos externos. Seis de los 10 casos de mayor envergadura a los que respondió S-RM se debieron al acceso directo a la red a través de VPN no protegidas por MFA.

La MFA debe utilizarse no solo para proteger el perímetro de la red, sino también para impedir que los actores de amenazas accedan a las cuentas privilegiadas necesarias para completar pasos clave en la cadena de ataque, como borrar copias de seguridad y eliminar antivirus.

P2

Fase intermedia

La gestión de identidades y accesos (IAM, por sus siglas en inglés) bien gestionada, la segmentación de la red y la supervisión son fundamentales para detectar y contener las intrusiones. Una vez que un actor está dentro de una red, el control más valioso para evitar la escalada es la detección y respuesta gestionadas (MDR, por sus siglas en inglés). Un buen servicio de MDR supervisa la actividad en cortafuegos, puntos finales, servicios en la nube, correo electrónico y otros sistemas clave.

Un componente básico de un servicio MDR eficaz es el *software* de detección y respuesta de puntos finales (EDR, por sus siglas en inglés). En más de dos tercios de los casos de S-RM entre 2022 y 2023, no había herramientas EDR. El *software* EDR, aumentado con el registro adicional de otras herramientas de seguridad y supervisado por un proveedor externo experto, es la forma más eficaz de identificar la actividad maliciosa y contenerla antes de que se convierta en una reclamación.

P3

Fase de salida

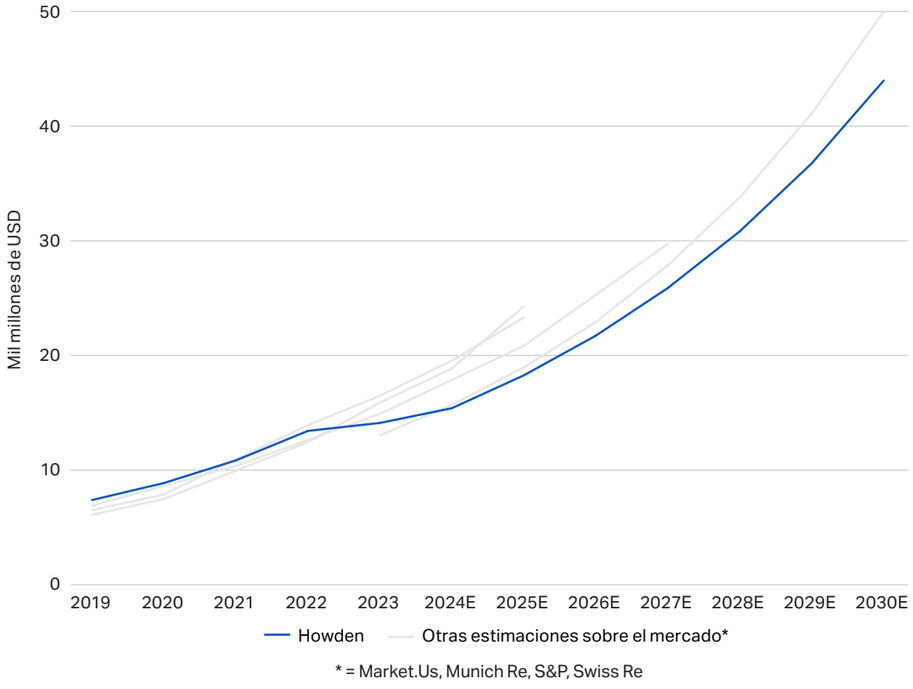
Aunque la interrupción de la actividad suele ser el mayor coste en una incidencia, las pérdidas pueden mitigarse con copias de seguridad adecuadas, inmutables y comprobadas periódicamente. Los actores de amenazas rara vez consiguen acceder a las copias de seguridad alojadas en la nube, e incluso cuando lo hacen, la inmutabilidad en proveedores de nube como Azure y AWS significa que no pueden eliminar las copias de seguridad de forma irreversible.

Esto ofrece a los responsables de la respuesta la opción de recuperar las redes sin necesidad de pagar un rescate, lo que abarata los costes de la respuesta y, a largo plazo, reduce el número de pagos que se realizan a los grupos de *ransomware*.

Cambios en la dinámica de crecimiento

La mejora de la salud cibernética y un entorno de suscripción más estable sitúan al mercado cibernético en una posición sólida para restablecer la trayectoria de crecimiento tras la estabilización de la base de primas en 2023. Ahora que los vientos de cola de los precios se están invirtiendo, el mercado necesita volver a centrarse en la innovación para aumentar su base de exposición y alcanzar las trayectorias de crecimiento esbozadas por Howden y otras empresas en la Figura 22. Esta previsión es inferior a nuestra estimación de 50 000 millones de dólares realizada el año pasado, debido en gran parte a un crecimiento plano en Estados Unidos.

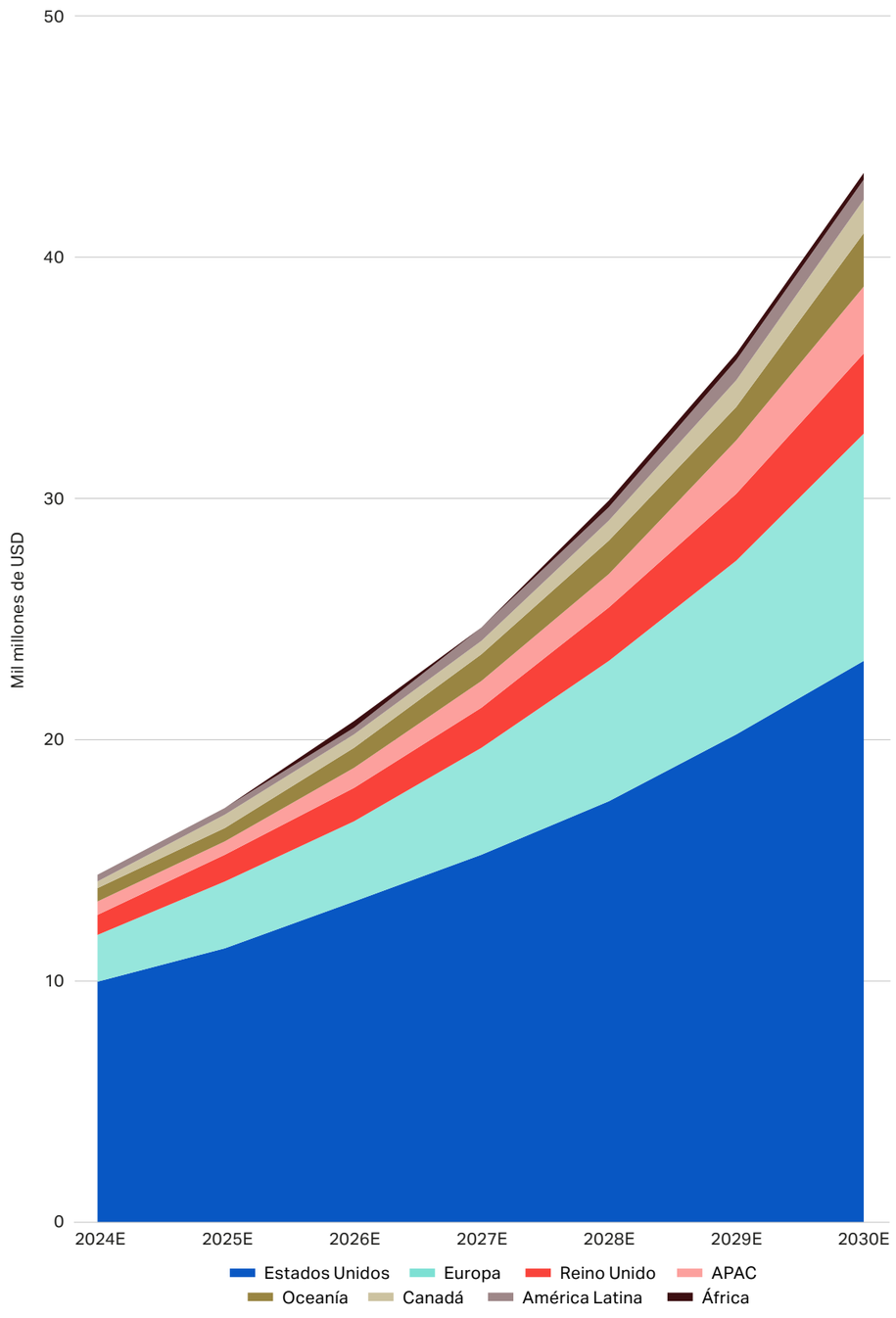
Figura 22: Proyecciones brutas globales de primas cibernéticas contratadas hasta 2030
(Fuente: Howden, Market.Us, Munich Re, S&P, Swiss Re)



Incluso teniendo en cuenta la ralentización en 2023, el mercado podría alcanzar una base de primas cercana a los 40 000 millones de dólares a finales de la década. La realización de este potencial estará inevitablemente ligada a factores externos como la macroeconomía y la geopolítica, pero si se centra en cuestiones clave que están bajo su control —incluida la penetración de las pymes (por ejemplo, facilitando el proceso de compra), la expansión geográfica y el desarrollo continuado del modelo—, el mercado puede asegurar su relevancia a largo plazo.

Howden está a la vanguardia de estos esfuerzos. Al trabajar con las aseguradoras para ofrecer soluciones pioneras que ayuden a penetrar en segmentos de empresas y geografías actualmente desatendidos por el mercado, consideramos que estas proyecciones son eminentemente alcanzables (necesarias, de hecho) para satisfacer las demandas de los clientes de todo el mundo.

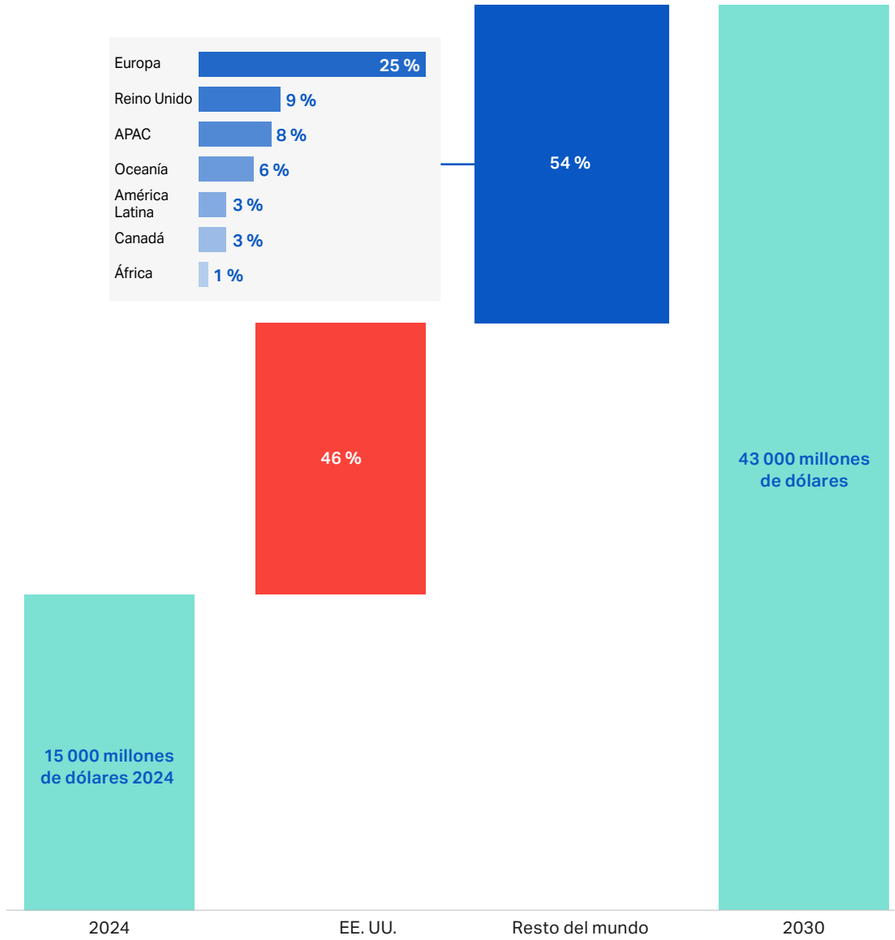
Figura 23: Estimación de las primas brutas suscritas cibernéticas por región: de 2024 a 2030
(Fuente: Howden)



Expansión geográfica

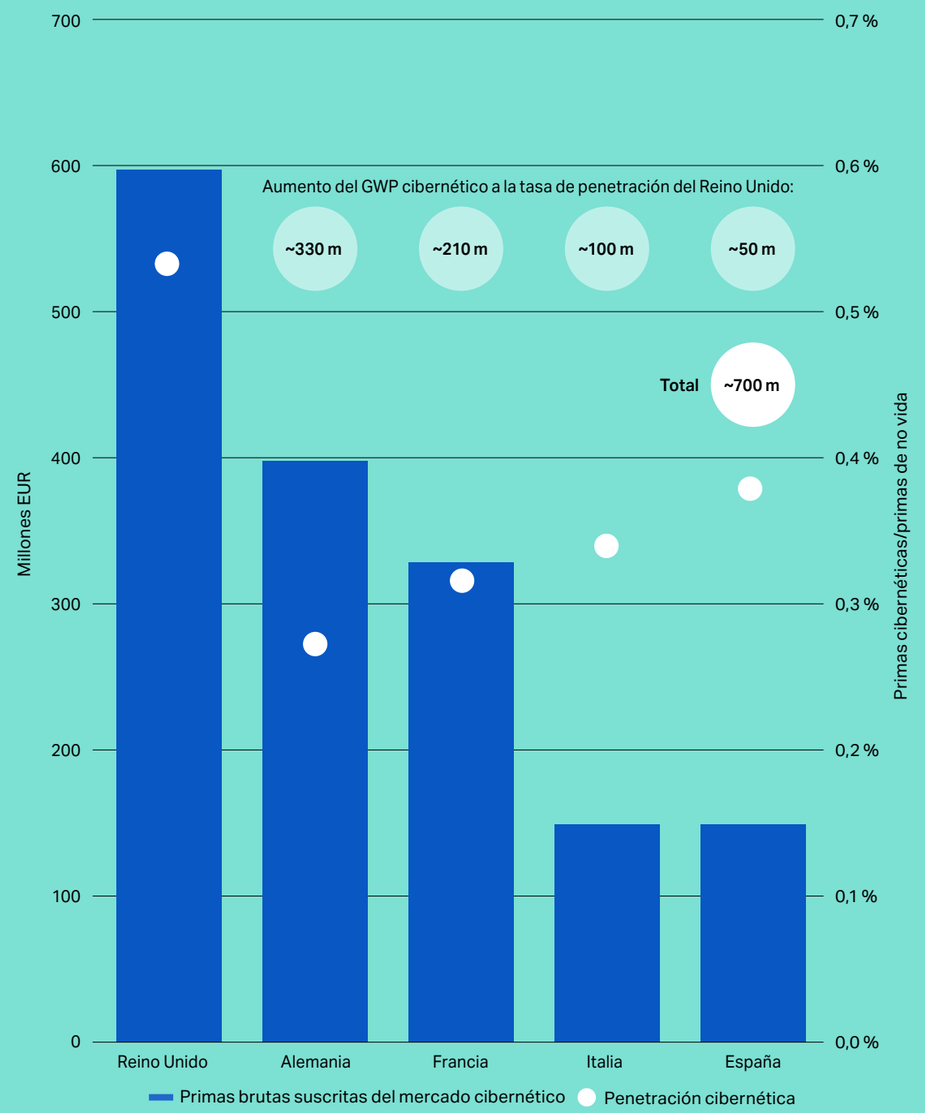
Hasta hace poco, los ciberseguros estaban dominados por Estados Unidos, que representaba aproximadamente dos tercios del mercado mundial. Como este segmento está cada vez más penetrado, el ímpetu de crecimiento se está desplazando a otros territorios para satisfacer la demanda acumulada de las empresas en medio de amenazas cada vez mayores, una mayor conciencia del riesgo y cambios normativos. La Figura 24 muestra que el negocio internacional representará la mayor parte del crecimiento hasta 2030, destacando Europa, junto con el Reino Unido, Asia-Pacífico, Oceanía y América Latina, como las principales regiones internacionales de alto crecimiento.

Figura 24: Porcentaje de crecimiento de las ciberprimas mundiales por región: de 2024 a 2030 (Fuente: Howden)



En especial, las principales economías de Europa registran un potencial de crecimiento considerable dados los niveles de penetración actuales. La Figura 25 muestra cómo los índices de primas y penetración cibernéticas en Alemania, Francia, Italia y España se comparan con los del Reino Unido, uno de los mercados cibernéticos más maduros.

Figura 25: Índices de penetración y primas cibernéticas en 2023 en el Reino Unido frente a las principales economías europeas (Fuente: Howden, AMRAE, BaFin, Swiss Re)

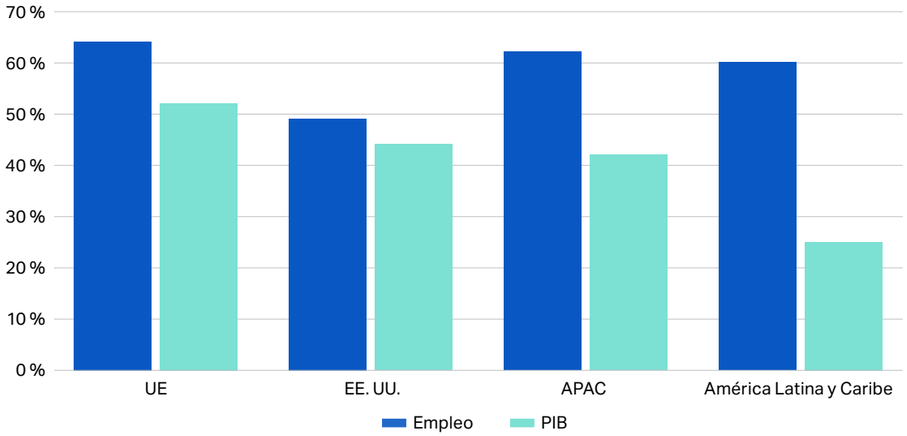


Mientras que las primas brutas suscritas del mercado cibernético en el Reino Unido se acercan actualmente a los 600 millones de euros, otras economías comparables de Europa se quedan muy atrás. La diferencia aumenta aún más si se tiene en cuenta el tamaño relativo del mercado de no vida en cada país, con Alemania a la cabeza. En total, estos territorios podrían experimentar un aumento combinado de las primas de aproximadamente 700 millones de euros con solo replicar los actuales niveles de penetración en el Reino Unido.

Penetración de las pymes

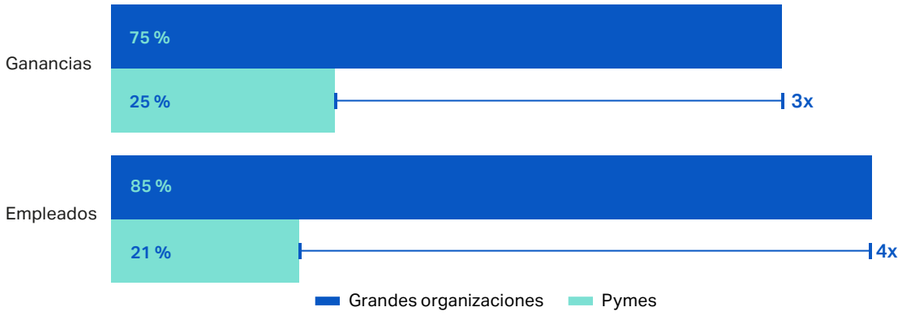
También hay que trabajar más en el compromiso con las pymes, un segmento que sigue en gran medida sin explotar para el mercado cibernético. Las pymes son la espina dorsal de la actividad económica en las economías avanzadas (véase la Figura 26) y dependen cada vez más de la tecnología para sus operaciones. A pesar de ser la incubadora de la innovación con un alto potencial de crecimiento, las pymes han estado históricamente desatendidas por el mercado de los ciberseguros.

Figura 26: Cuota de pymes en la economía por regiones
(Fuente: Comisión Europea, Cámara de Comercio de EE. UU., Banco Asiático de Desarrollo, Cooperación Económica Asia-Pacífico, OCDE, Banco de Desarrollo de América Latina y el Caribe)



Un estudio del Foro Económico Mundial pone de manifiesto la oportunidad que existe en este ámbito, ya que solo una de cada cuatro pymes está actualmente protegida por un seguro cibernético (véase la Figura 27). Por si fuera poco, muchas carecen de los recursos y los conocimientos necesarios para recuperarse de un ciberataque.

Figura 27: Cuota de organizaciones con ciberseguro en todo el mundo en 2023
(Fuente: Foro Económico Mundial)

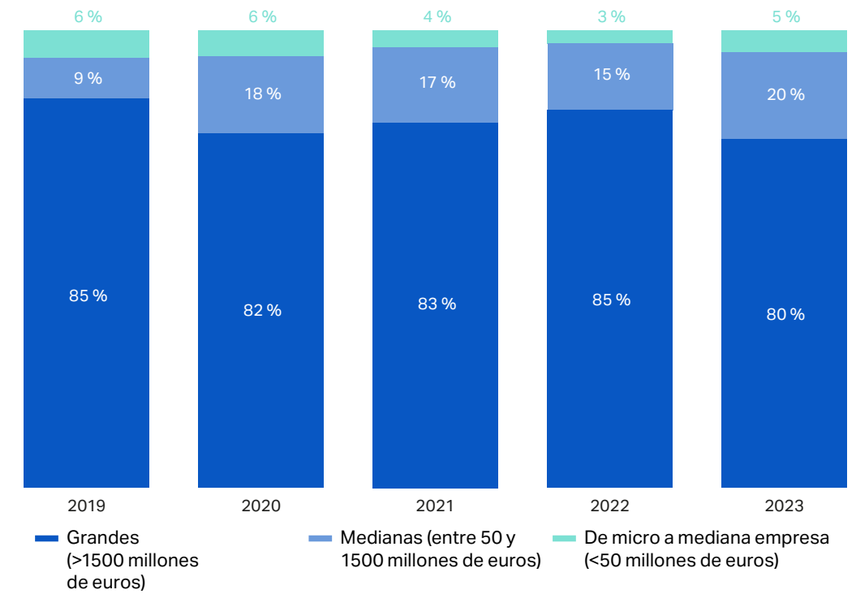


Nota: Las pymes se definen como empresas con <250 empleados o <250 millones de dólares de ingresos. Las grandes organizaciones se definen como empresas con >100 000 empleados o >5500 millones de dólares de ingresos.

En algunos mercados ya se está avanzando, con datos específicos de Francia que muestran que las empresas categorizadas de microempresas a medianas empresas han aumentado su participación en el conjunto de primas de ciberseguro del 15 % en 2019 al 25 % en 2023 (véase la Figura 28).

No obstante, se necesita un enfoque más transformador para acelerar la penetración y consolidar la relevancia entre las pymes. Entre las oportunidades importantes cabe citar el aumento de la concienciación sobre el riesgo, una mayor vinculación de las tarifas a los niveles de salud y la simplificación del proceso de compra.

Figura 28: Distribución de primas de ciberseguros en Francia por tramos de ingresos de las compañías: de 2019 a 2023 (Fuente: AMRAE)



Ciberplataforma para pymes de Howden

En mayo de 2024, Howden lanzó una plataforma que permite a las pymes con ingresos inferiores a 250 millones de dólares adquirir hasta 6 millones de dólares de cobertura cibernética en cuatro sencillos pasos. Lo más importante es que esta solución solo requiere el nombre, el sector, los ingresos y el sitio web para elaborar un presupuesto para las empresas. Los datos complementarios se recopilan a través de API abiertas, lo que significa que las normas de suscripción se mantienen durante el proceso de compra, muy simplificado.

Nuestra plataforma tiene el potencial de revolucionar el proceso de compra para las pymes, que normalmente carecen de los recursos necesarios para hacer frente a las exigencias de presentación existentes. Combina la ciberintermediación diferenciada y la experiencia de las aseguradoras con la tecnología de vanguardia y es el mayor ejemplo de cómo Howden amplía los límites para penetrar en este segmento vital, pero actualmente desatendido de la economía.

05

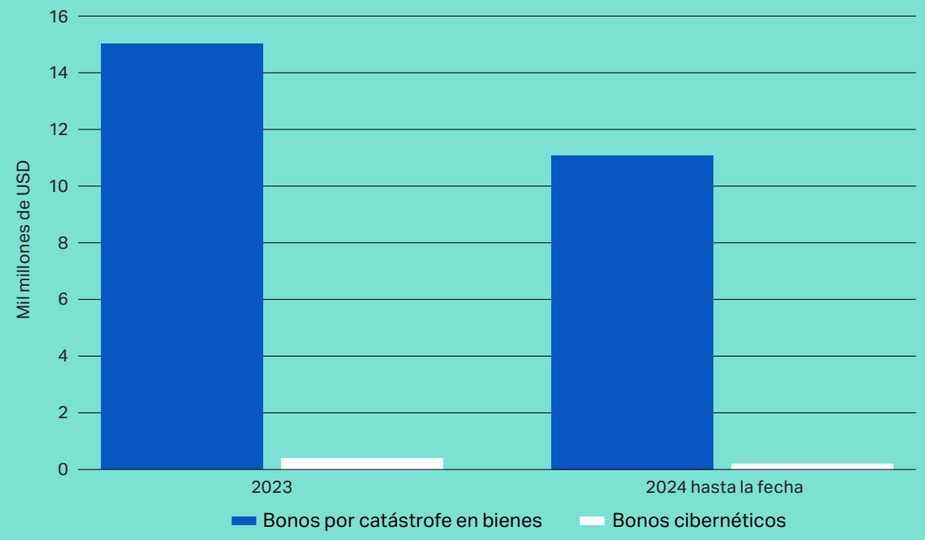
Equiparación del riesgo al capital

Las perspectivas del ciberseguro son sólidas, respaldadas por una base de capital creciente y cada vez más diversificada.

Esto será crucial a medida que el mercado vaya más allá de los grupos de primas existentes para satisfacer las demandas de las empresas de todo el mundo.

En los últimos doce meses se han producido varios acontecimientos positivos en el frente del capital. Más allá de la abundante oferta en el lado directo, las condiciones en el mercado del reaseguro cibernético también han mejorado, con una suavización de los precios y una capacidad más que suficiente para satisfacer la demanda.

Figura 29: Emisión de bonos para catástrofes en bienes frente a las cibernéticas 144A: 2023/24
(Howden, Artemis)



Es importante señalar que las cesiones de cuotas están disminuyendo a medida que las aseguradoras se sienten más cómodas con las ratios de siniestralidad por desgaste y grandes pérdidas, una tendencia que probablemente continuará a medida que las cedentes exploren estructuras de capital más eficientes, como los productos de exceso de pérdida basados en sucesos.

El creciente interés en este ámbito ha facilitado una serie de emisiones históricas de bonos de cibercatástrofe desde el 4T23. Además de casi duplicar el tamaño del mercado de exceso de pérdidas basado en sucesos, estas transacciones también apuntan a un nivel de apetito inversor que impulsará una actividad adicional a partir de ahora. El margen de crecimiento es considerable; la emisión de bonos para catástrofes para el riesgo de catástrofes en bienes, un mercado que existe desde hace casi 30 años, rondaba los 15 000 millones de dólares en 2023, frente a los apenas 400 millones para el cibernético. En 2024 se han cerrado otros acuerdos cibernéticos.

Las inversiones continuas en soluciones de modelización para gestionar y valorar las exposiciones sistémicas han sido (y seguirán siendo) cruciales para liberar más capacidad de los mercados de capitales (véase el informe de Howden Re, *Replanteamiento del riesgo cibernético*, sobre los distintos enfoques que pueden adoptar las aseguradoras). Habrá que seguir trabajando en este ámbito para acelerar las entradas (al precio adecuado). El camino hacia la relevancia a largo plazo y hacia nuevas posibilidades consiste en detener la tendencia al autoseguro y las retenciones más altas.

Los intermediarios desempeñan un papel crucial en la realización del potencial de crecimiento del cibermercado, especialmente aquellos con la experiencia y las capacidades locales (genuinas) necesarias para penetrar en nuevas geografías y atraer capital a escala. El mercado actual demanda un nuevo enfoque de intermediación que tenga en cuenta los ciclos, reúna al mejor talento del sector y sea innovador y marcadamente emprendedor. Y esto es solo parte de lo que aporta Howden. Venga y cuéntenos.

Estos son los expertos

Julian Alovisi
Jefe de Investigación

+44 (0)7593 576 024
julian.alovisi@howdengroup.com

Peter Evans
Director de Investigación

+44 (0)7443 377 340
peter.evans@howdengroup.com

Shay Simkin
Director global de Ciberseguridad

shay@howden.co.il

Jean Bayon de La Tour
Jefe de Ciberseguridad, Internacional

jean.bayon@howdengroup.com

David Rees
Jefe de Ciberseguridad, Reino Unido

david.rees@howdengroup.com

Sarah Neild
Jefa de Comercio Minorista Cibernético, Reino Unido

sarah.neild@howdengroup.com

Colaboradores expertos

S-RM

Roddy Priestley
Director, Ciberseguridad

r.priestley@s-rminform.com

Martijn Hoogesteger
Jefe de Ciberseguridad, Benelux

m.hoogesteger@s-rminform.com

XCyber

Milo Wilson
Analista jefe de Inteligencia

milo.w@xcybergroup.com

Bill Jarvis
Jefe de Inteligencia

bill.j@xcybergroup.com

NCC Group

Matt Hull
Director de Inteligencia Global sobre Amenazas

matthew.hull@nccgroup.com

Jon Renshaw
Director adjunto de Investigación Comercial

jon.renshaw@nccgroup.com

Escríbanos a info@howdenbroking.com
o llámenos al 020 7623 3806.

One Creechurch Place, Londres, EC3A 5AF

T +44 (0)20 7623 3806
Fax +44 (0)20 7623 3807
E-mail info@howdenbroking.com

howdenbroking.com