Perspectiva del Mercado de Seguros Cibernéticos 2026

Gallagher

Introducción

Al reflexionar sobre los desarrollos en el mercado de seguros cibernéticos en 2025, está claro que la industria de seguros continúa evolucionando rápidamente en respuesta a amenazas complejas y emergentes, cambios regulatorios, avances tecnológicos y requisitos de suscripción en constante cambio. El mercado actual de seguros cibernéticos es sólido y se proyecta que crezca significativamente. Sin embargo, es un mercado que no está exento de desafíos: el aumento de la capacidad ha llevado a una disminución general de las tasas, más recientemente en cifras de un solo dígito. Estamos observando un mayor escrutinio en la suscripción en ciertos sectores de la industria, como el de la salud, donde se han producido aumentos en las tasas. Aunque parece que estas tendencias continuarán en 2026, la comunidad de suscripción ha sido constantemente recordada del potencial de los riesgos sistémicos. Recientes interrupciones en la nube y ataques a la cadena de suministro han alimentado esta preocupación y han llevado al mercado a un punto de inflexión. Nuestra Perspectiva del Mercado Cibernético 2026 describe las principales tendencias y expectativas para el mercado de seguros cibernéticos en el próximo año y más allá, centrándose en las tendencias de reclamaciones cibernéticas, la postura de suscripción, la influencia del reaseguro, la regulación de la privacidad y la creciente influencia de la inteligencia artificial (IA).

Authors:

John Farley, Director General, US Cyber Practice

Dan Burke, Vicepresidente Ejecutivo, US Cyber Practice

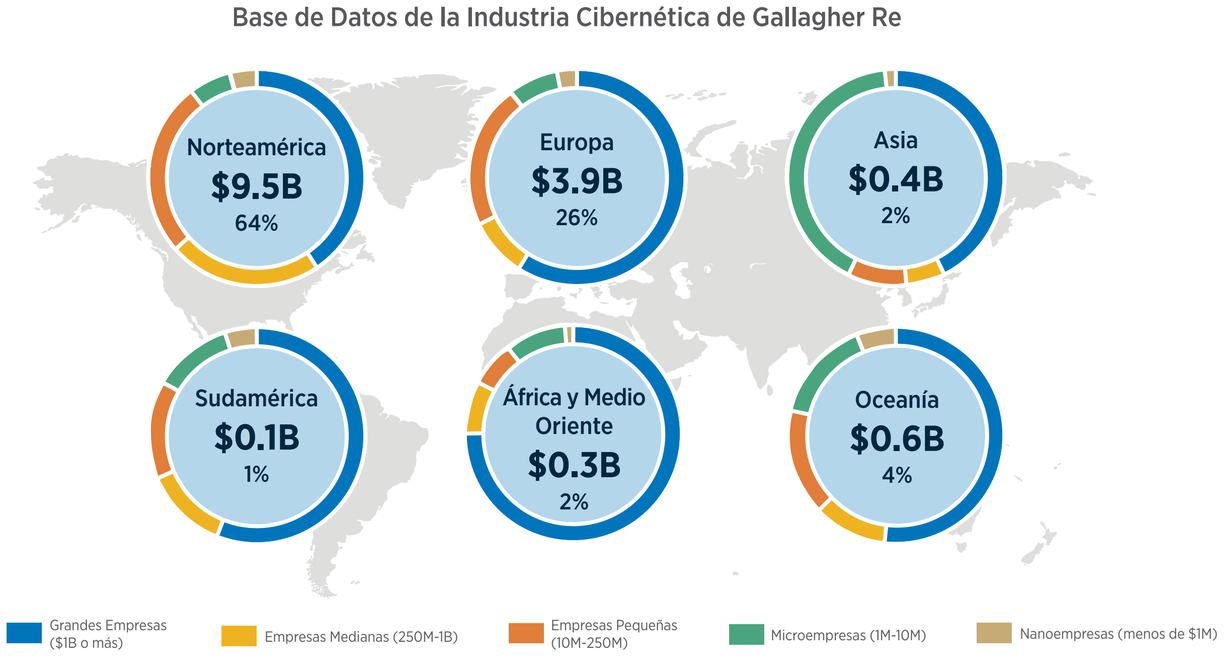
El Estado Actual

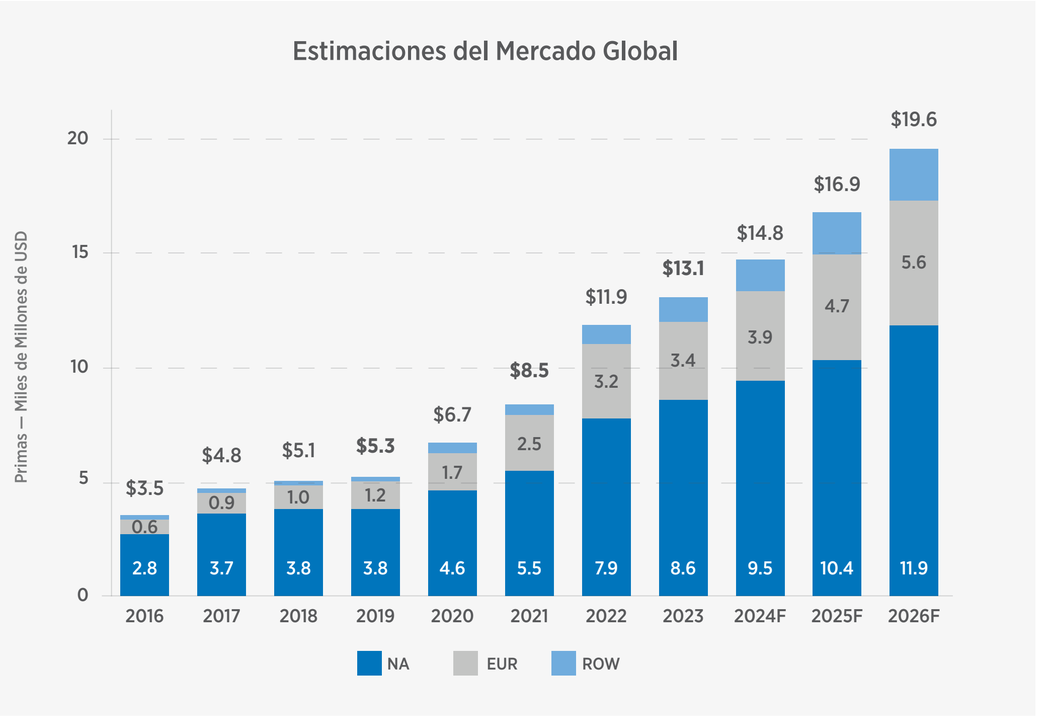
Mercado Global de Seguros Cibernéticos

Desde el endurecimiento del mercado de seguros cibernéticos a principios de 2021, el mercado global de seguros cibernéticos ha experimentado un crecimiento significativo en las primas suscritas brutas (GWPs, por sus siglas en inglés). La demanda de seguros cibernéticos sigue siendo sólida en todas las geografías. La mayoría de las proyecciones de crecimiento futuro coinciden en que el tamaño del mercado de 2025, estimado entre $1616y20 mil millones, podría escalar razonablemente a 30a50 mil millones para 2030.[1]

Las tasas de crecimiento más altas en algunas perspectivas a largo plazo reflejan una aceleración anticipada debido a los riesgos asociados con la inteligencia artificial IA, las amenazas de la computación cuántica y las vulnerabilidades en la cadena de suministro. Desde una perspectiva regional, esperamos que América del Norte continúe dominando, con una participación de mercado del 60%-70%. Se espera que Asia-Pacífico experimente el mayor crecimiento debido a la rápida digitalización y las regulaciones emergentes.

Distribución del Mercado Cibernético y Expectativas de Crecimiento





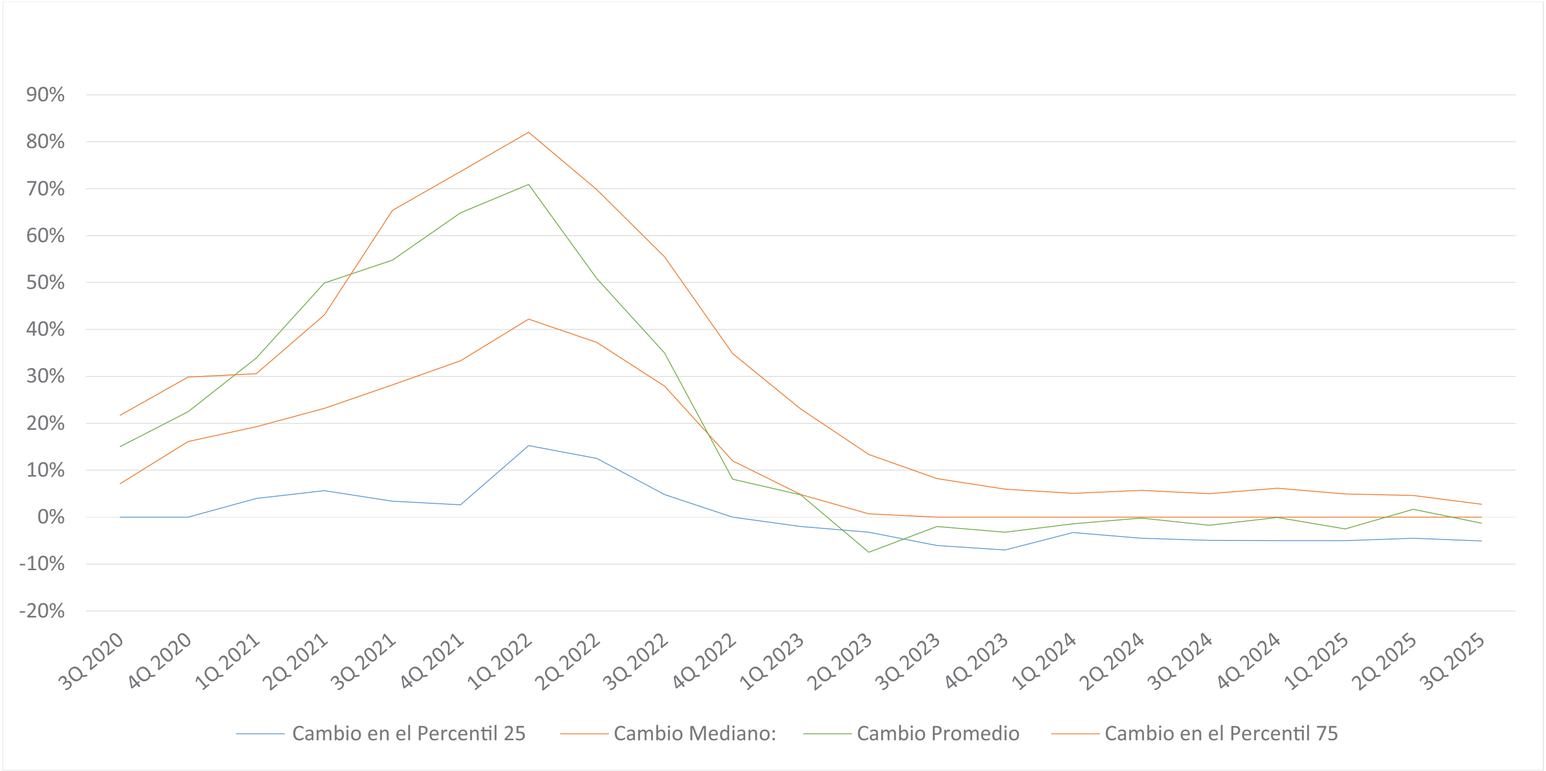
Mercado de Seguros en EE.UU.

El mercado de seguros cibernéticos continúa evolucionando para reflejar las preocupaciones en torno a nuevas amenazas y avances tecnológicos. Las condiciones de mercado más flexibles que comenzaron hace tres años se estabilizaron en gran medida a lo largo de 2025. En general, los compradores de seguros cibernéticos están experimentando precios estables. Aunque esperamos que estas tendencias continúen al menos durante la primera mitad de 2026, observamos que la experiencia de nuestros clientes varía según la industria.

El sector de la salud es un ejemplo donde la competencia es menos intensa debido al entorno de reclamaciones, y esa falta de competencia está impulsando un ligero aumento en los precios de los seguros cibernéticos. Al menos una aseguradora importante está adoptando un enfoque cauteloso hacia el sector de la salud, donde las tasas han aumentado en porcentajes de un solo dígito. Queda por ver si esto es un indicador de que el mercado podría estar cambiando de rumbo.

En general, los precios de los seguros cibernéticos han retrocedido desde los máximos del mercado duro más reciente a niveles más comparables con el inicio del ciclo de mercado duro en la primera mitad de 2021. Atribuimos esto a la dinámica del mercado y la competencia entre aseguradoras, ya que los suscriptores sienten la presión de alcanzar ambiciosos objetivos de crecimiento.

Ciberseguridad — Mediana, Promedio y Percentil 75 a lo Largo del Tiempo



Mercado de Reaseguros

El reaseguro continúa siendo una piedra angular, impulsando el crecimiento y la expansión del mercado de seguros cibernéticos al proporcionar estabilidad financiera, mecanismos de reparto de riesgos y desarrollo de capacidad para las aseguradoras. La afluencia de capacidad al mercado de seguros cibernéticos, que ha dado lugar a las actuales condiciones competitivas del mercado, está impulsada por la innovación en el mercado de reaseguros cibernéticos, incluyendo:

Valores Vinculados a Seguros (ILS, por sus siglas en inglés): Estos instrumentos permiten la transferencia del riesgo cibernético de las aseguradoras a los mercados de capital, diversificando la exposición entre múltiples inversores.

Transacciones de Reaseguro Proporcional: Estos acuerdos permiten a las aseguradoras compartir una cantidad proporcional de primas y pérdidas con las reaseguradoras, distribuyendo efectivamente el riesgo.

Reaseguro Paramétrico: Los pagos se activan en función de parámetros predefinidos, como la duración de una interrupción en lugar de las pérdidas reales, para agilizar la resolución de reclamaciones.

Bonos Catastróficos CAT Bonds: Diseñados para activar pagos después de eventos cibernéticos extremos, estos bonos están respaldados por los mercados de capital, proporcionando una sólida red de seguridad para las aseguradoras.

Al aprovechar estos mecanismos de transferencia de riesgos, las aseguradoras de ciberseguros pueden transferir una parte de su exposición al riesgo a los mercados de capital más amplios, mejorando su capacidad para gestionar amenazas cibernéticas a gran escala.

Además, la integración de tecnologías avanzadas, como la inteligencia artificial y el aprendizaje automático, en los procesos de modelado de pérdidas y evaluación de riesgos podría mejorar aún más la eficiencia y precisión de las soluciones de reaseguro. Estas tecnologías pueden analizar grandes volúmenes de datos para identificar tendencias emergentes y vulnerabilidades, permitiendo estrategias de gestión de riesgos más proactivas.

El papel del mercado de reaseguros en el sector de seguros cibernéticos no se limita a proporcionar capacidad, sino que también impulsa la innovación y la colaboración para abordar uno de los desafíos más apremiantes de la era digital.

Panorama de Amenazas Cibernéticas

Según el Comité de Seguridad Nacional de la Cámara de Representantes de los EE.UU.[2], el costo promedio de una violación de datos en los EE.UU. fue de $10 millones en 2025. Los grupos de actores de amenazas más destacados incluyeron:

Trabajadores de TI Remotos de la RPDC: Actores estatales asociados con la República Popular Democrática de Corea RPDC desplegaron trabajadores de TI encubiertos para infiltrarse en empresas estadounidenses obteniendo empleos remotos en el sector de TI.

Scattered Spider: Una organización criminal que utilizó esquemas de ransomware y extorsión mediante robo de datos para lanzar ataques con fines financieros contra grandes organizaciones globales.

Interlock: Un actor de amenazas que lanzó ataques de alto perfil contra víctimas en los sectores gubernamental y manufacturero.

Salt Typhoon: Actores estatales asociados con China que infiltraron puertas traseras en importantes empresas de telecomunicaciones y proveedores de servicios de internet en los EE.UU.

Ransomware

Las tendencias de reclamaciones cibernéticas en 2025 siguieron un patrón similar al de años anteriores, con el ransomware continuando como una amenaza para empresas de todos los tamaños e industrias. Sin embargo, las tácticas de los actores de amenazas han cambiado: han pasado de encriptar datos a simplemente exfiltrarlos.

Los actores de amenazas han adoptado la idea de que los datos son más valiosos para la empresa de la que fueron robados que para un tercero en el mercado negro. En lugar de extorsionar a las empresas para que paguen por descifrar los datos, los actores de amenazas han recurrido a amenazas de simplemente publicar datos sensibles si no se realizan los pagos de extorsión. En una nota positiva, estamos viendo una disminución notable en el número de víctimas que acceden a pagar, y aquellas que lo hacen están pagando montos menores. Diversos estudios muestran que solo entre el 28% y el 32% de las víctimas pagaron rescates en 2025, frente al 37% en 2024.[3] Cuando se pagaron, los rescates promedio oscilaron entre 1.2 y 1.8 millones, una disminución del 10% respecto a 2024.[4]

El porcentaje de víctimas que pagaron rescates en 2025 fue solo del

28% al 32%,

según diversos estudios, una disminución respecto al

37% en 2024.[3]

Ataques a la Cadena de Suministro

Los incidentes cibernéticos que involucran a actores clave en la cadena de suministro continuaron en 2025, y vemos esto como una amenaza persistente en el futuro. Los ataques a la cadena de suministro suelen dirigirse a proveedores de tecnología y proveedores de servicios gestionados. Al infiltrarse en uno de estos proveedores, los actores de amenazas pueden afectar a todos los clientes de los proveedores de tecnología o servicios gestionados, creando potencialmente miles de víctimas con un solo ataque.

En 2025, hemos visto ataques dirigidos a empresas de software como servicio (SaaS), proveedores de servicios en la nube y empresas de repositorios de código, con un enfoque en comprometer actualizaciones de software, integraciones de API y tokens de autenticación.

Estos ataques destacan la importancia de la gestión de riesgos de proveedores y la implementación de controles adecuados para evaluar la ciberseguridad de sus proveedores, así como el impacto comercial de una interrupción en proveedores clave de terceros.

Violaciones de Privacidad sin Brechas de Datos

Quizás una de las tendencias más alarmantes en reclamaciones cibernéticas involucra pérdidas relacionadas con el seguimiento de píxeles en sitios web. Hemos observado un aumento significativo en litigios basados en acusaciones de incumplimiento de una variedad de leyes de privacidad estatales recientemente desarrolladas y leyes de décadas de antigüedad, incluyendo la Ley de Invasión de Privacidad de California (1967), la Ley Federal de Intervenciones Telefónicas (1968) y la Ley de Protección de Privacidad de Videos (1988). Los abogados de los demandantes han sido hábiles en aprovechar estas leyes para iniciar acciones colectivas y demandas de arbitraje masivo, buscando acuerdos y sanciones legales que oscilan entre $250 y $10,000 por violación.[5]

Estas reclamaciones han afectado a una amplia gama de industrias, incluyendo tecnología, atención médica, servicios financieros y empresas minoristas orientadas al consumidor.

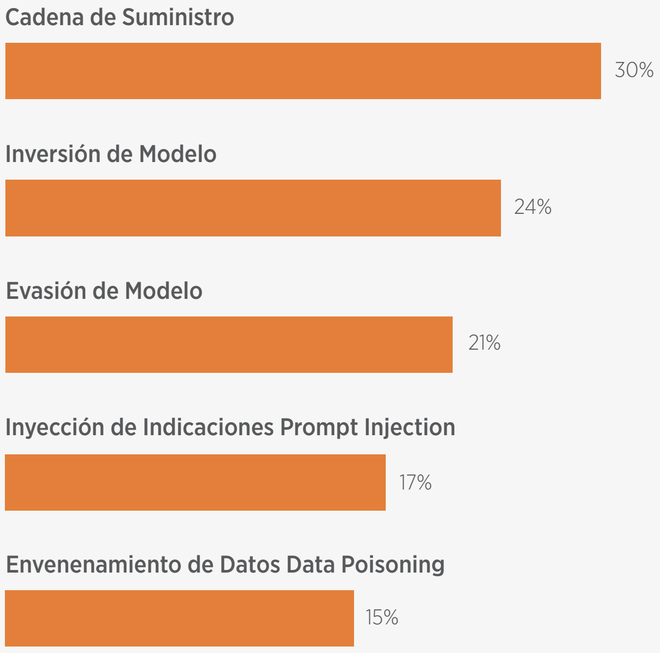
La mitigación adecuada de este riesgo incluye la coordinación entre múltiples partes interesadas dentro de una empresa, desde los equipos legales y de TI hasta los de marketing y desarrollo de productos.

Reclamaciones de Inteligencia Artificial

También estamos comenzando a ver evidencia creciente de pérdidas cibernéticas impulsadas por la inteligencia artificial. Según el Informe de Costos de Brechas de Datos de IBM-Ponemon de 2025, varias organizaciones están reportando incidentes de seguridad que involucran modelos y aplicaciones de inteligencia artificial.

El compromiso de la cadena de suministro fue la causa más común de los incidentes.

De las organizaciones que reportaron un incidente de seguridad que involucraba un modelo o aplicación de inteligencia artificial; se permitió más de una respuesta.



Fuente: IBM-Ponemon 2025 Cost of a Data Breach Report

Panorama de Riesgos Regulatorios

El panorama regulatorio de ciberseguridad en los Estados Unidos sigue siendo fragmentado y complejo. Las órdenes ejecutivas federales, las acciones legislativas impulsadas por los estados y los requisitos específicos de la industria continúan imponiendo una abrumadora variedad de obligaciones a las organizaciones.

A nivel federal, las amenazas contra la infraestructura crítica siguen siendo una prioridad principal. La Ley de Reporte de Incidentes Cibernéticos para Infraestructura Crítica CIRCIA, por sus siglas en inglés, que impone un mandato de reporte de incidentes en un plazo de 72 horas, está programada para entrar en vigor en mayo de 2026.[6] Diversas órdenes ejecutivas reflejan un enfoque en las ciberamenazas extranjeras y en la seguridad del software en la cadena de suministro mediante guías voluntarias lideradas por el NIST.

A nivel estatal, se introdujeron 200 proyectos de ley de ciberseguridad en 2025.[7] Estos se centraron generalmente en la notificación de brechas de datos, la defensa contra ransomware, la protección de infraestructuras críticas y las protecciones de privacidad relacionadas con el uso de diversas tecnologías de rastreo. La aplicación de estas leyes está aumentando, con sanciones por incumplimiento y regulaciones que permiten derechos privados de acción contra organizaciones que no cumplan con las normativas.

La regulación sobre el uso de la inteligencia artificial sigue siendo incipiente y descentralizada. Están surgiendo tensiones entre un enfoque federal que enfatiza la innovación y el enfoque estatal centrado en la mitigación de riesgos específicos para la protección de los derechos humanos básicos, la transparencia y la explicabilidad de los modelos de aprendizaje masivo. Muchas organizaciones están recurriendo al Marco de Gestión de Riesgos de IA del NIST[8] como la piedra angular para integrar la gestión de riesgos de IA en los programas de gestión de riesgos empresariales.

Mirando hacia 2026

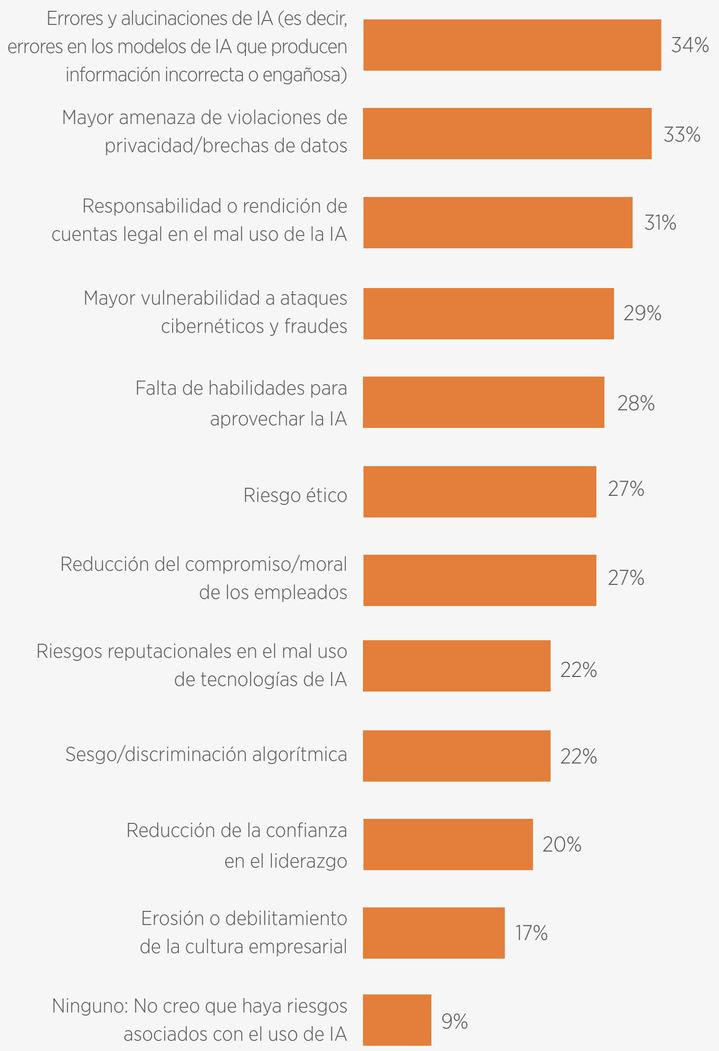
El mercado de seguros cibernéticos difícilmente podría describirse como predecible. Como se señaló anteriormente en este panorama, el estado actual del ciberespacio está influenciado por el mercado de reaseguros y un aumento de capacidad en los últimos años, la competencia entre las aseguradoras y el panorama de amenazas que evoluciona rápidamente. Al mirar hacia 2026, aquí hay algunas áreas que esperamos que impacten en el mercado de seguros cibernéticos.

Inteligencia Artificial (IA)

La aparición repentina de ataques basados en inteligencia artificial IA ha generado la necesidad inmediata de estrategias de defensa cibernética más avanzadas. De hecho, las preocupaciones quedaron claramente reveladas en la Encuesta Global de Gallagher 2025 sobre Actitudes hacia la Adopción de IA y el Riesgo:

A pesar de los beneficios, los líderes empresariales están cada vez más conscientes de los riesgos asociados con el uso de la inteligencia artificial (IA) en sus negocios.

Riesgos percibidos con el uso de IA en los negocios



Fuente: "Attitudes to AI Adoption and Risk Global Survey," *Arthur J. Gallagher & Co.*, 2025.

Esperamos un mayor enfoque por parte de los suscriptores en 2026 en torno a los marcos de gestión de riesgos de IA. Se espera que estos sean exigidos tanto a los desarrolladores como a los adoptantes de IA e incluirán probablemente:

1. Establecimiento de marcos de gobernanza sólidos.
2. Implementación de modelos de IA transparentes y explicables.
3. Técnicas de IA explicable (XAI).
4. Garantizar la calidad de los datos y la mitigación de sesgos.
5. Mejorar las medidas de seguridad.
6. Adoptar principios éticos de IA.
7. Considerar nuevos roles de liderazgo en IA:
   El Director de IA (Chief AI Officer).
8. Revisar los planes de respuesta a incidentes cibernéticos:
   El Plan de Respuesta a Incidentes de IA.

Tecnología Deepfake y ingeniería social

Los ataques de deepfake utilizan audio, video o imágenes generados por inteligencia artificial para hacerse pasar por personas de confianza con un realismo alarmante. Estos ataques se están utilizando cada vez más en campañas de phishing, donde los actores malintencionados imitan a ejecutivos o proveedores para engañar a los empleados y lograr que autoricen pagos o compartan datos sensibles. A diferencia del phishing tradicional, los deepfakes explotan la confianza visual y auditiva, lo que dificulta su detección y amplifica los riesgos de ingeniería social. A medida que estas herramientas se vuelven más accesibles, las organizaciones enfrentan una mayor exposición al fraude financiero y al daño reputacional.

Los ataques de ingeniería social continúan siendo una ventaja para los actores malintencionados. Los ataques de phishing/suplantación encabezaron la lista de quejas reportadas a la división IC3 del FBI, con 193,407 quejas reportadas en 2024. Las pérdidas totales por fraude mediante transferencias electrónicas en 2024 superaron los $109 millones. Dado el bajo costo de entrada para crear estas campañas de phishing con deepfakes y el éxito que han tenido los actores malintencionados en el pasado, esperamos que este vector de ataque continúe siendo una fuente prominente de riesgo cibernético en 2026.

Cobertura de Seguros

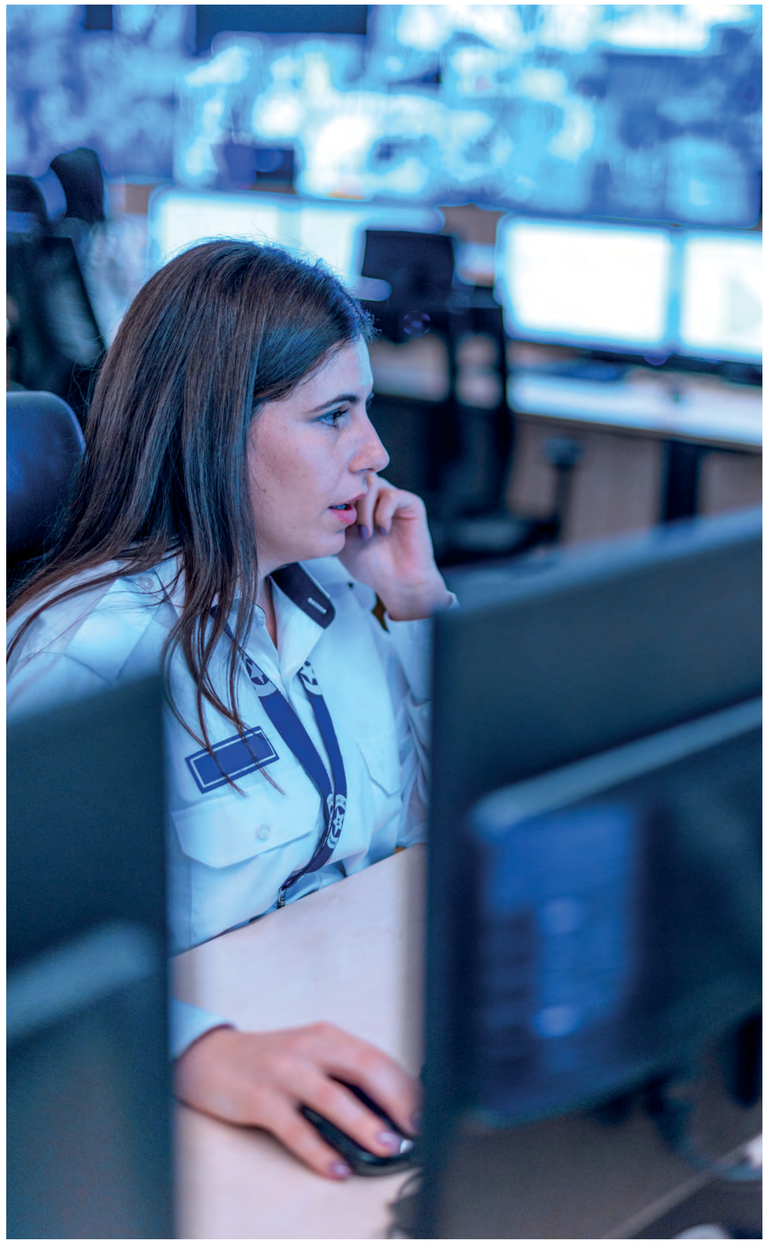
En medio de un entorno competitivo, las aseguradoras están lidiando con la redacción de pólizas en relación con algunas exposiciones clave:

Riesgo Cibernético en la Cadena de Suministro

El año 2025 presenció varios incidentes de alto perfil relacionados con ciberataques a proveedores clave de software en la cadena de suministro, así como fallos en los sistemas de dos proveedores globales de servicios en la nube con pocos días de diferencia. Aunque ninguno de estos incidentes resultó en un temido evento cibernético "sistémico," las aseguradoras están modificando el lenguaje de las pólizas para reflejar estas preocupaciones.

Las aseguradoras que ofrecen cobertura por pérdidas de interrupción de negocios contingentes pueden requerir que el asegurado tenga un contrato escrito con el proveedor afectado por la pérdida en la cadena de suministro. Sin este contrato, podría imponerse un lenguaje de exclusión. Además, algunas aseguradoras están limitando la cobertura de interrupción de negocios contingentes para pérdidas sufridas por proveedores de TI, excluyendo las pérdidas ocasionadas por proveedores que no sean de TI.

Por último, los compradores de seguros cibernéticos deben prestar atención al lenguaje relacionado con la cobertura de elementos temporales, incluyendo términos como "período de espera," "período de calificación" y "período de interrupción." Estos términos, y la forma en que se definen específicamente, pueden tener un impacto significativo en la recuperación de costos relacionados con la interrupción del negocio y los gastos adicionales.



Reclamaciones de Privacidad sin Incumplimiento

Los suscriptores también son cautelosos al cubrir reclamaciones de privacidad sin incumplimiento. Las reclamaciones relacionadas con la recopilación indebida de datos, especialmente aquellas que involucran tecnologías de seguimiento en sitios web y datos biométricos, están volviéndose más comunes. Estas acusaciones están fundamentadas en diversas leyes estatales que continúan evolucionando, algunas de las cuales permiten derechos de acción privada. Muchas aseguradoras están excluyendo esta cobertura, mientras que otras están dispuestas a ofrecerla, siempre que se cumplan ciertos requisitos de suscripción. Estamos observando que algunos suscriptores están utilizando nuevas tecnologías de escaneo para medir el riesgo relacionado con las prácticas de recopilación y compartición de datos.

Inteligencia Artificial Generativa

Se espera que la adopción generalizada de herramientas de inteligencia artificial IA generativa continúe acelerándose hasta 2026. Esta tendencia ya ha llevado a los suscriptores a prestar atención a los riesgos asociados con el uso de la IA, ya que están surgiendo reclamaciones. Actualmente, hay más de 200 casos legales activos relacionados con la inteligencia artificial y el aprendizaje automático, derivados de sesgos en los datos, infracciones de propiedad intelectual y marcas registradas, responsabilidad por privacidad, discriminación y riesgos regulatorios.

Estos riesgos van más allá del seguro cibernético y se extienden a líneas de cobertura establecidas, incluyendo la responsabilidad por prácticas laborales, responsabilidad por productos, errores y omisiones, negligencia médica, entre otras. Aunque todavía existe incertidumbre sobre cómo se cubrirán o excluirán los riesgos relacionados con la IA en las distintas líneas de cobertura, el mercado de seguros cibernéticos está comenzando a adaptarse a estas exposiciones en evolución. Por ejemplo, al menos un asegurador ha introducido una póliza independiente para IA, mientras que otros están emitiendo endosos para cubrir los costos asociados con el reentrenamiento de grandes modelos de aprendizaje. En 2026, anticipamos que un número creciente de aseguradoras ofrecerá cobertura para pérdidas relacionadas con la IA, atendiendo tanto a los proveedores de plataformas de IA como a las organizaciones que utilizan estas tecnologías. Esperamos negociaciones significativas en torno a cómo se define "pérdida" dentro de estas nuevas concesiones de cobertura.

Conclusión

Nuestra Perspectiva del Mercado de Seguros Cibernéticos para 2026 destaca la naturaleza dinámica y en rápida evolución de la industria de seguros cibernéticos, moldeada por amenazas emergentes, avances tecnológicos, cambios regulatorios y prácticas de suscripción en constante transformación. Aunque el entorno es mayormente favorable para los compradores, persisten desafíos como los riesgos sistémicos, el ransomware, las vulnerabilidades en la cadena de suministro y las violaciones de privacidad sin incumplimiento. El mercado de seguros cibernéticos se encuentra en un punto crítico, equilibrando las oportunidades de crecimiento con la necesidad de abordar riesgos cibernéticos emergentes y desafíos regulatorios en constante evolución que exigen una variedad de obligaciones de cumplimiento. La perspectiva subraya la importancia de la colaboración, la innovación y la adaptabilidad para dar forma al futuro de los seguros cibernéticos. A medida que la industria avanza hacia 2026, se espera que las aseguradoras refinen el lenguaje de las pólizas, aborden las exposiciones relacionadas con la inteligencia artificial y se enfoquen en estrategias proactivas de gestión de riesgos para mitigar el impacto de la tecnología deepfake, la ingeniería social y las interrupciones en la cadena de suministro.

Fuentes

1. Empresas de Investigación Primaria
   - "Cybersecurity Insurance Market by Offering, Coverage, Type, Provider Type, and Vertical — Global Forecast to 2030," *MarketsandMarkets*, July 2025.
   - "Cybersecurity Insurance Market — Growth, Trends, COVID-19 Impact, and Forecasts (2025-2030)," *Mordor Intelligence*, June 2025.
   - "Cyber Insurance Market Size, Share & COVID-19 Impact Analysis Source," *Fortune Business Insights*, 2025.
   - "Cyber Insurance Market by Component, Deployment Mode, Organization Size, Industry Vertical: Global Opportunity Analysis and Industry Forecast, 2023-2032," *Allied Market Research,* 2025.
   - "Cyber Insurance Market: Global Industry Trends, Share, Size, Growth, Opportunity and Forecast 2025-2033," *IMARC Group*, September 2025.
   - "Global Cyber Security Insurance Market: Industry Analysis and Forecast (2024-2030)," *Maximize Market Research*, August 2025.
   - "Cyber Insurance: Risks and Trends 2025," *Munich Re,* April 2025.
   - "Cyber Insurance: A Maturing Market Faces New Challenges," *S&P Global Ratings,* mid-2025.
2. https://homeland.house.gov/wp-content/uploads/2025/10/Cyber-Threat-Snapshot.pdf
3. Coveware Ransomware Market Reports (Q1–Q3 2025 updates.
4. Multiple sources: Sophos State of Ransomware 2025; Coveware Q2 2025 Ransomware; Deepstrike.io; GetAstra 100+ Ransomware Attack Statistics; Exabeam Ransomware Statistics 2025.
5. "A Guide to Website Tracking for Nonprofits," *AJG United States.*
6. https://news.bloomberglaw.com/privacy-and-data-security/cyber-agency-pushes-data-breach-reporting-final-rule-to-2026
7. "Cybersecurity 2025 Legislation."
8. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf
9. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

AJG.com **The Gallagher Way.** Desde 1927

Gallagher