

RIESGOS CIBERNÉTICOS Y CONTRATO DE SEGURO: UNA APROXIMACIÓN INTEGRAL A SU NOCIÓN, CARACTERIZACIÓN Y TRATAMIENTO ASEGURADOR.

CYBER RISKS AND INSURANCE COVERAGE: A COMPREHENSIVE APPROACH TO THEIR CONCEPT, CHARACTERIZATION, AND INSURANCE TREATMENT

Juan Camilo Bedoya Chavarriaga
Nicolas Uribe Lozada
María Alejandra Zona Malaver
Germán Andrés Cajamarca Castro
María Camila Sánchez Lozano

Resumen: El presente trabajo analiza el fenómeno de los riesgos cibernéticos y su aseguramiento. Para ello, se delimita conceptualmente la noción de riesgo cibernético y su taxonomía operacional; se examina el panorama empírico de incidentes a nivel global y regional; se describe la dimensión del mercado de ciberseguros y la brecha de protección latinoamericana; y se estudian, a la luz de las normas del contrato de seguro, sus elementos esenciales, las modalidades de delimitación temporal de la cobertura, los amparos de primera y tercera parte previstos en el producto, así como las exclusiones más frecuentes. El trabajo concluye que el seguro para riesgos cibernéticos constituye un instrumento complementario —y no sustitutivo— de la gestión de riesgos de seguridad de la información, pero de una importancia fundamental en el mundo moderno, cuyo desarrollo en América Latina exige una adecuada delimitación contractual, mayor estandarización de clausulados y una lectura armónica de los diferentes ordenamientos jurídicos.

Palabras Claves: *Riesgo cibernético; ciberseguro; contrato de seguro; responsabilidad civil; protección de datos personales; claims made; Colombia; América Latina.*

Abstract: This paper analyses, from a legal and technical standpoint, the phenomenon of cyber risk and the contractual mechanisms designed to transfer it to the insurance market, taking a cross-cutting look at Latin American legal systems. It conceptually delimits the notion of cyber risk and its operational taxonomy; reviews the empirical landscape of incidents at the global and regional levels; describes the size of the cyber insurance market and the Latin American protection gap; systematizes the regulatory framework applicable in the main jurisdictions of the region; and examines, under the rules of the Colombian Commercial Code, the essential elements of the contract, the temporal delimitation of coverage, the first-party and third-party insuring agreements usually marketed, and the most frequent exclusions, including the war exclusion controversy, silent cyber and the insurability of administrative fines. The paper concludes that cyber insurance is a complementary —not a substitute— instrument of information security risk management, whose development in Latin America requires precise contractual delimitation, greater standardization of wordings and a harmonious reading with the mandatory insurance contract regimes in force in each jurisdiction.

Key Words: *Cyber risk; cyber insurance; insurance contract; civil liability; data protection; claims made; Colombia; Latin America.*

Introducción

“Good cyber maturity and good cyber insurance go hand-in-hand. We buy insurance for our home, but this does not mean we leave the front door unlocked, and the same should be said for cyber security. The cyber market is shifting to a service-oriented offering that combines insurance policies with technology, risk engineering and response services. Through the underwriting process, and

throughout the policy period, insurers can help organizations understand the continually changing exposures and focus their investment in cyber security and resilience” (Allianz, 2022)

El seguro para riesgos cibernéticos representa una pequeña, pero creciente porción de los ingresos del mercado de seguros a nivel internacional que, en el marco de la digitalización acelerada de la economía, el auge del teletrabajo -a partir de la pandemia del Covid-19- y el ascenso de la inteligencia artificial, así como de la integración de esta última en los procesos operativos de las entidades del sector público y privado, ha tomado una especial relevancia a partir del lugar central que ocupan los riesgos cibernéticos para las organizaciones contemporáneas como consecuencia del incremento, no solo de los ataques cibernéticos, sino también del lugar nuclear que los datos (información) ocupan en los modelos económicos actuales (Gumenyuk, 2021; Paz, 2018; Signorino, 2015).

En efecto, el Foro Económico Mundial (World Economic Forum, 2025) ha ubicado de manera reiterada al espionaje cibernético y a la guerra cibernética, así como a la desinformación habilitada tecnológicamente, entre los riesgos globales más severos de corto y mediano plazo, y por su parte, los reaseguradores internacionales coinciden en señalar que el *ransomware* se mantiene como la primera causa de pérdidas aseguradas en el ramo (Munich Re, 2025).

América Latina no ha sido ajena a esta problemática. La región concentra un volumen significativo de intentos de ciberataques -más de trescientos sesenta mil millones registrados en 2022 según los laboratorios de inteligencia de amenazas de Fortinet, con México, Brasil, Colombia y Perú como los países más afectados- (Fortinet — FortiGuard Labs, 2023), al tiempo que presenta rezagos estructurales en materia de preparación institucional, talento especializado y marcos normativos de ciberseguridad, tal como lo documentó el reporte conjunto del Banco Interamericano de Desarrollo y la Organización de los Estados Americanos sobre el estado de la ciberseguridad regional (Banco Interamericano de Desarrollo & Organización de los Estados Americanos, 2020)¹. Este desbalance entre exposición creciente y protección limitada configura una brecha de aseguramiento que constituye, simultáneamente, un desafío de política pública y una oportunidad de desarrollo para el mercado asegurador regional².

En este contexto, así como en un panorama de rápida transformación, el seguro de riesgos cibernéticos —o ciberseguro— ha emergido como uno de los productos de mayor dinamismo y proyección dentro de la industria aseguradora, al ofrecer protección patrimonial y reputacional frente a la filtración de datos, el robo de identidad, la denegación de servicios, la extorsión informática y, en general, los incidentes derivados de la vulneración de los sistemas de seguridad de la información; sin perjuicio de lo cual afronta grandes desafíos para su consolidación debido a la imposibilidad de predecir los

¹ En efecto, la “(...) creciente dependencia de la sociedad moderna en los servicios digitales ha llevado a las organizaciones a hacer inversiones significativas en contramedidas administrativas y técnicas para prevenir incidentes de ciberseguridad accidentales o maliciosos. Sin embargo, los ataques cibernéticos modernos y los incidentes de ciberseguridad que tienen graves repercusiones han demostrado que la gestión de la ciberseguridad de las organizaciones no puede depender exclusivamente de medidas de mitigación del riesgo; en cambio, el seguro cibernético está aumentando como complemento necesario a las salvaguardas organizativas” (Tsohou et al, 2023, p. 373)

² La relevancia del fenómeno fue reconocida tempranamente igualmente por los organismos internacionales de normalización. En agosto de 2019, la Organización Internacional de Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) expidieron la norma técnica ISO/IEC 27102:2019, para la gestión de la seguridad de la información, así como para el establecimiento de directrices generales para la contratación de ciberseguros. Esta define los estándares internacionales para considerar la adquisición de estos seguros como una opción de tratamiento de riesgos, así como para aprovechar la cobertura en la gestión del impacto de un incidente y para articular el intercambio de información entre asegurado y asegurador en las etapas de suscripción, seguimiento y reclamación (International Organization for Standardization & International Electrotechnical Commission, 2019). La propia norma advierte, sin embargo, que el ciberseguro no sustituye la seguridad robusta ni los planes eficaces de respuesta a incidentes, sino que debe considerarse un componente del plan general de tratamiento de riesgos orientado a aumentar la resiliencia organizacional.

riesgos futuros y su impacto³, la falta de datos históricos⁴, la posibilidad de pérdidas en cascada, la incertidumbre del alcance de las coberturas -particularmente en ausencia de lenguajes estandarizados y claros para su comercialización- y/o de la responsabilidad legal de los involucrados y la falta de entendimiento del producto (Gumenyuk, 2021, pág. 33; Sariva Lima, H.J.M., 2020; Sales Porto & Novoa Rubiano, 2025; Vivas & Bedoya, 2022).

Para efectos de abordar la discusión planteada, resulta necesario realizar algunas precisiones preliminares, siguiendo para tal fin la doctrina existente, así:

“(…) La posición del seguro en el proceso de gestión y administración de riesgos: Un aspecto que, en muchas ocasiones, principalmente en Latinoamérica, es olvidado o del que no se tiene real conocimiento conceptual ni práctico, es que el seguro en general, en cualquiera de sus modalidades, y el que nos ocupa no es la excepción, si bien tiene como finalidad la protección contra pérdidas que puedan afectar una actividad, corresponde solo a uno de los posibles mecanismos de transferencia de riesgos, ubicado en la última etapa de un procedimiento mucho más importante y amplio, cual es el de la “Gerencia del Riesgo” o “Risk Management”. (...) la correcta, eficaz y eficiente contratación de un seguro, debe suponer que, previamente, aquella persona que está expuesta a las consecuencias nocivas que produce la realización de un riesgo, ha debido recorrer un camino en el que haya, como mínimo, en una descripción muy sencilla y básica -pues no es este el momento para profundizar en esta área-, cumplido con las siguientes actividades: En primer lugar, identificar especial y específicamente los riesgos a que está expuesta su actividad; en segundo término, cuantificarlos adecuadamente para conocer sus posibles o probables efectos teniendo en cuenta su severidad y frecuencia; y, finalmente, de acuerdo con su realidad concreta, tomar la decisión de administración que más convenga, esto es, eliminarlos (que en sentido real supone decidir no continuar desarrollando la actividad), retenerlos en su patrimonio (ya sea con la creación de fondos de autoseguro, reservas provisiones etc., o simplemente, imputándolos al capital o al patrimonio en el caso que se realice el riesgo) o transferirlos a terceros, a través de diversos mecanismos, entre los cuales, se encuentra el seguro no siendo, por tanto, lógicamente el único.

(…) La expresión “Ciber Seguros” y su alcance técnico: Es también indispensable aclarar de antemano, que la variada gama de riesgos que, en la práctica, se engloban bajo el concepto genérico de “Riesgos Cibernéticos” o “Ciber Riesgos”, involucran diversos esquemas de seguros, independientes y diferenciables en su funcionamiento y que, no obstante, pueden o no ser incluidos en una sola póliza, deben ser plenamente diferenciados para su correcto entendimiento y gestión, para lograr una cobertura eficaz y completa. En efecto, mediante los

³ En efecto, sostiene la doctrina autorizada que: “(...) los ciberataques están evolucionando constantemente a medida que hackers privados y estatales desarrollan nuevos métodos para infiltrarse en las redes. La rápida evolución de las capacidades y estrategias de piratería informática hace difícil que los aseguradores, que dependen de clientes con perfiles de riesgo relativamente consistentes, evalúen el verdadero riesgo de que un cliente potencial sea pirateado. El aumento de la sofisticación de los hackers es evidente, en que tanto la frecuencia como los costos de los ciberataques han aumentado en los últimos años: en los EE.UU. el costo promedio del ciberataque aumentó un 29%, pasando de 21,2 millones de dólares en 2017 a 27,4 millones de dólares en 2018. A pesar de esto, el mercado de los seguros cibernéticos siguió siendo rentable para los aseguradores. En tercer lugar, los ciberataques son altamente escalables ya que pueden afectar potencialmente a miles de empresas simultáneamente, causando grandes pérdidas interrelacionadas para las aseguradoras. Debido al diseño de internet, hay nodos centrales muy importantes. Este tipo de centralización de la red crea dos problemas para las aseguradoras cibernéticas. Un tipo de problema se produciría si un servicio importante, como una gran plataforma de computación en la nube utilizada por muchos titulares de pólizas, fallara. La aseguradora puede tener que pagar las reclamaciones de todos sus tomadores de seguro al mismo tiempo. Una dinámica similar se puede ver en los desastres naturales, donde las aseguradoras privadas a menudo son reacias a ofrecer un seguro contra inundaciones, porque si una sola casa en un vecindario fue golpeada por una inundación, es probable que muchas casas alrededor de ella también fueron golpeadas al mismo tiempo. Por ejemplo, en la década de 1920, después de una serie de inundaciones catastróficas a lo largo del río Misisipi, las aseguradoras privadas comenzaron a excluir explícitamente la cobertura contra inundaciones de sus pólizas de seguro de vivienda, lo que finalmente resultó en la creación del Programa Nacional de Seguro contra Inundaciones (NFIP) para llenar el vacío” (Granato & Polacek, 2019)

⁴ Al respecto pueden verse el trabajo de Biener, C. et al. (2015) o Romanosky, S. et al. (2019).

que se conocen genéricamente como “Seguros de Ciber” se pueden encontrar, por la variada naturaleza y origen de los riesgos a amparar, individualmente o en forma conjunta, tanto esquema (sic) conocidos como de “primera parte” como de “tercera parte” (o de responsabilidad civil), de forma que, podemos afirmarlo sin hesitación, en la práctica, no existe uniformidad en el alcance de dichos seguros tal como la norma ISO (...) lo pone de presente en su numeral 6.3.2, (...) Lo expuesto conlleva a la necesidad de establecer, en cada caso concreto, la extensión real del producto ofrecido por las distintas aseguradoras que vienen comercializando este tipo de productos (aunque ello debería hacerse con todo seguro), pues, como se dijo, bajo una misma denominación podrían encontrarse seguros que incorporen amparos de uno u otro esquema en forma exclusiva o conjunta, todo lo cual será tenido en cuenta, para mayor claridad y rigor, al momento de hacer el desarrollo de las distintas coberturas y elementos característicos de cada una de las categorías indicadas” (Vivas & Bedoya, 2022, págs. 657-660).

En el panorama anterior, el objetivo del presente trabajo es ofrecer un análisis sistemático del aseguramiento de los riesgos cibernéticos desde una perspectiva amplia y transversal. Para ello, el estudio se estructura en diversos apartados que buscan delimitar conceptualmente el riesgo cibernético y presentar su taxonomía operacional; revisar el panorama empírico de incidentes a nivel global y regional; el describir la dimensión del mercado de ciberseguros; sistematizar el marco regulatorio aplicable; examinar los elementos esenciales del contrato de seguro de riesgos cibernéticos; y analizar los amparos y las exclusiones más comunes en los clausulados del mercado. La metodología empleada es de carácter dogmático y descriptivo, apoyada en fuentes normativas, jurisprudenciales y doctrinales verificables, así como en informes técnicos de organismos internacionales y de la industria aseguradora y reaseguradora⁵.

1. El concepto de Riesgos Cibernéticos: Delimitación conceptual y taxonomía.

El riesgo cibernético⁶, más ampliamente conocido en el panorama internacional como *Cyber Risk*, es un concepto amplio y en construcción, bajo el cual la literatura especializada agrupa un conjunto de

⁵ Es importante destacar que el presente texto toma como punto de partida los desarrollos doctrinales previos sobre la materia en el ámbito iberoamericano, actualizándolos y reorientándolos hacia el contexto regulatorio y de mercado vigente en la región (Vivas & Bedoya, 2022; Sales Porto & Novoa Rubiano, 2025; Sobrino, 2017).

⁶ “Los riesgos cibernéticos se definen como “riesgos operativos a la información y activos tecnológicos que tienen consecuencias que afectan la confidencialidad, disponibilidad y/o integridad de la información o sistemas de información” (Cebula et al. 2014). Entre los principales eventos de riesgo cibernético se encuentran las violaciones de datos y los ciberataques (Agrafiotis et al. 2018). La creciente exposición y el impacto potencial del riesgo cibernético han sido destacados en informes recientes de la industria (por ejemplo, Allianz 2021; Foro Económico Mundial 2020). Los ciberataques a infraestructuras críticas ocupan el quinto lugar en el Informe de Riesgo Global del Foro Económico Mundial. El ransomware, el malware y la denegación de servicio distribuida (DDoS) son ejemplos de los modos en evolución de un ciberataque. (...) Otro ejemplo del alcance de los ciberataques es el ransomware NotPetya en 2017. El daño ascendió a 10 mil millones de dólares, ya que el ransomware explotó una vulnerabilidad en el sistema Windows, lo que le permitió propagarse independientemente por todo el mundo en la red (GAO 2021). En el mismo año, el ransomware WannaCry fue lanzado por los ciberdelincuentes. El ciberataque al software de Windows tomó como rehenes los datos de los usuarios a cambio de criptomonedas Bitcoin (Smart 2018). Las víctimas incluyeron al Servicio Nacional de Salud en Gran Bretaña. Como resultado, las ambulancias fueron redirigidas a otros hospitales debido a que los sistemas de tecnología de la información (TI) fallaron, lo que dejó a personas necesitadas de asistencia urgente esperando. Se ha estimado que las 19.000 citas canceladas generaron pérdidas de 92 millones de libras (Field 2018). Durante la pandemia de COVID-19, los ataques de ransomware aumentaron significativamente, ya que trabajar desde casa aumentó la vulnerabilidad (Murphey 2021b). Además de los ciberataques, las violaciones de datos también pueden causar altos costos. Según el Reglamento general de protección de datos (RGPD), las empresas están obligadas a proteger los datos personales y salvaguardar los derechos de protección de datos de todas las personas en el área de la UE. El RGPD permite a las autoridades de protección de datos en cada país imponer sanciones y multas a las organizaciones que consideren infractoras. “Para las violaciones de datos, la multa máxima puede ser de 20 millones de euros o el 4% del volumen de negocios global, lo que sea más alto” (GDPR.EU 2021). Las violaciones de datos a menudo implican una gran cantidad de datos sensibles que han sido accedidos, sin autorización, por partes externas y, por lo tanto, se consideran importantes

hechos y circunstancias derivados del uso, implementación y/o adopción de las tecnologías de la información y las comunicaciones (TIC) que, en mayor o menor medida, “(...) *comprometen la confidencialidad, disponibilidad o integridad de datos o servicios*” (Wrede, Stegen & Graf Von der Schulenberg, 2020). De allí que Eling y Schnell (2016) sostengan que el riesgo cibernético comprende todo riesgo operacional sobre los activos de información y tecnología que tenga como consecuencia afectaciones a la confidencialidad, la disponibilidad o la integridad de la información o de los sistemas de información. En sentido similar, la Organización para la Cooperación y el Desarrollo Económicos (OCDE, 2017) ha caracterizado los incidentes cibernéticos como eventos que afectan la disponibilidad, la integridad o la confidencialidad de los sistemas y datos digitales, con potencial para producir la interrupción de un negocio, la afectación de infraestructura crítica e incluso daños físicos a personas y bienes (Granato & Polacek, 2019; CRO Forum, 2016)⁷

En este contexto, siguiendo la taxonomía y premisas propuestos por parte de Cebula, J. & Young, A. (2019) para el *Software Engineering Institute* de la *Universidad Carnegie Mellon*, corresponde indicar que:

1. Los riesgos cibernéticos trascienden el limitado concepto de actividades informáticas ilegales encaminadas, entre otras, a sustraer, modificar, alterar, inutilizar y/o destruir información y/o activos -e.g. hackeo y/o crímenes por computador-, extendiéndose a errores humanos no intencionales, fallas tecnológicas, deficiencias en los procesos internos y eventos externos ajenos al control de la persona u organización -e.g. problemas legales y/o desastres de la naturaleza-. El factor común a todos ellos es que ocurren en el mismo escenario, esto es, el ciberespacio, entendido como el dominio interactivo conformado por las redes, conexiones digitales y los sistemas de información utilizados para el almacenamiento, la modificación y la comunicación de información y datos (The Geneva Association, 2016)⁸. Esta amplitud conceptual resulta determinante para el derecho de seguros, pues de la delimitación del riesgo asegurado dependerá, en cada clausulado concreto, la extensión real de la cobertura otorgada.
2. Los riesgos cibernéticos son susceptibles de ser entendidos, por lo tanto, como el conjunto de riesgos de tipo “operacional” para la información y activos tecnológicos de una persona u organización, sea esta gubernamental o una corporación, que tienen como consecuencia afectaciones a sistemas de información o a la confidencialidad, disponibilidad o integridad de los datos y/o información (Cebula & Young, 2019) que se presentan en entornos virtuales y/o tecnológicos -software, hardware, etc.-. Estos riesgos “operacionales” pueden a su vez, clasificarse en cuatro clases: acciones de personas, fallas tecnológicas y de sistemas, procesos internos fallidos y eventos externos. La tabla 1 sintetiza dicha clasificación, permitiendo evidenciar que el riesgo cibernético no se agota en la conducta dolosa de terceros, sino que

para la seguridad de la información debido a su impacto de amplio alcance (Goode et al. 2017) (...)” (Cremer, 2022, Pág. 700-701)

⁷ Sin perjuicio de comentarios ulteriores en relación con el riesgo cibernético silente, simplemente a manera de contexto de la forma en que un evento cibernético puede conllevar afectaciones a las personas y/o sus bienes, corresponde indicar que: “El riesgo cibernético silencioso es un tercer tipo de cobertura que, más que ser un amparo propiamente de una póliza de seguro cibernético, es un término que se refiere a las posibles pérdidas relacionadas con la ciberseguridad derivadas de pólizas tradicionales de bienes y accidentes (P&C) no diseñadas específicamente para cubrir los riesgos cibernéticos. Consideremos un escenario en el que el sistema informático de un hotel está infectado con malware, lo que desactiva el sistema de rociadores, dañando el interior y haciendo que un cliente se resbale y caiga. Si no se excluyen explícitamente los riesgos cibernéticos, se espera que la cobertura tradicional de propiedad y siniestralidad del hotel cubra los daños al hotel causados por los rociadores y las facturas médicas del cliente lesionado. La ciberseguridad silenciosa se está volviendo cada vez menos un riesgo para las aseguradoras a medida que pasan a pólizas de responsabilidad civil que excluyen explícitamente o incluyen pérdidas causadas por ciberataques” (Traducción libre; Granato & Polacek, 2019).

⁸ Véase la definición de cyberspace del glosario del National Institute of Standards and Technology (NIST), Computer Security Resource Center. Disponible en: <https://csrc.nist.gov/glossary/term/cyberspace>

comprende también la negligencia interna, la obsolescencia tecnológica y los desastres naturales y la exposición legal o regulatoria que afectan los entornos digitales.

Tabla 1. Categorías taxonómicas de los riesgos cibernéticos				
Acciones de personas	Fallas tecnológicas y de sistemas	Procesos internos fallidos	Eventos Externos	Descripción de clase
Derivadas del comportamiento de un individuo — interno o externo a la entidad— en determinada situación.	Derivadas del comportamiento problemático, anormal o inesperado de los activos tecnológicos de la organización.	Asociadas a fallos en los procesos internos que impiden su ejecución según lo esperado o requerido.	Asociadas con eventos generalmente fuera del control de la organización, cuya ocurrencia no puede ser planeada ni prevista.	Descripción general de cada clase de riesgo cibernético.
SUBCATEGORÍAS				
Inadvertida Acciones no intencionales, sin malicia, derivadas de equivocaciones, errores u omisiones en la ejecución de procesos.	Hardware Fallo de equipos físicos por capacidad insuficiente, rendimiento inadecuado, falta de mantenimiento u obsolescencia.	Diseño o ejecución Resultados inadecuados por errores en el diseño del flujo, mala documentación, falta de claridad en responsabilidades, alertas, acuerdos de nivel de servicio o traspaso de tareas.	Desastres Riesgos inherentes a eventos naturales o de origen humano sin control organizacional: fenómenos climatológicos, incendios, inundaciones, terremotos, terrorismo o pandemias.	Primer nivel Riesgos de primer nivel: acciones humanas no planificadas, fallas físicas del sistema, errores de diseño procedimental y desastres de fuerza mayor.
Deliberada Acciones intencionales orientadas a causar daño mediante fraude, sabotaje, hurto o vandalismo.	Software Riesgos derivados del software utilizado, por ausencia de compatibilidad, control de cambios, ajustes de seguridad, prácticas de codificación deficientes o configuraciones inadecuadas.	Control de procesos Control inadecuado de procesos por errores de monitoreo, fallos en la medición de estándares, ausencia de revisiones periódicas o prácticas deficientes de gobierno corporativo.	Problemas legales Riesgos derivados de la imposibilidad de cumplir requerimientos normativos sobre manejo de información y TI, o de acciones legales iniciadas por accionistas, empleados o clientes tras un incidente cibernético.	Segundo nivel Riesgos de segundo nivel: conductas maliciosas internas o externas, vulnerabilidades de software, deficiencias de control y exposición normativa o litigiosa.
Omisión Ausencia de acción en un momento determinado por falta de habilidades, conocimiento, guía o disponibilidad del personal requerido.	Sistemas integrados Fallas de sistemas integrados por errores de diseño, especificaciones inadecuadas, integración indebida dada su complejidad o incompatibilidad entre componentes.	Procesos de soporte Insuficiencia de recursos en procesos de apoyo institucional: escasez de personal capacitado, falta de financiación, déficits en entrenamiento y retención de talento, o fallas en la cadena de suministro operacional.	Dependencia de terceros Riesgos inherentes al entorno operativo derivados de la incapacidad temporal o permanente de un proveedor para entregar los bienes o servicios necesarios, así como de condiciones de mercado o económicas adversas.	Tercer nivel Riesgos de tercer nivel: inacción humana, interdependencias sistémicas, déficits de soporte operativo y exposición por dependencia de la cadena de valor externa.

Otras propuestas taxonómicas para los riesgos cibernéticos dejan a un lado los eventos o supuestos que aumentan la vulnerabilidad y/o facilitan la configuración de un incidente cibernético, para centrarse única y exclusivamente en aquellos hechos que, ya sea por un error, omisión y/o conducta desplegada por una persona u organización -incluidos los cibercriminales-, comprometen la seguridad, integridad y/o disponibilidad de la información⁹. Así, por ejemplo, Chong et al. (2025), clasifican los distintos tipos de incidentes cibernéticos en:

“(1) Ciberextorsión, (2) violación maliciosa de datos, (3) datos físicamente perdidos y/o robados, (4) divulgación no intencional de datos, (5) denegación de servicio (DDoS) / interrupción del sistema, (6) violación digital o robo de identidad, (7) uso de identidad fraudulento / acceso no autorizado a cuentas, (8) controles y operaciones de la industria, (9) errores de configuración y/o implementación por parte de los equipos de tecnología de la información, (10) errores de procesamiento – tecnologías de la información, (11) interrupción de la red / sitio web, (12) phishing, spoofing o ingeniería social, (13) violación a la privacidad por contacto o divulgación no autorizada, (14) violación a la privacidad por recopilación de datos no autorizada, y (15) hurto, manipulación física. Similar a Kesan y Zhang (2020b), en este artículo, estas 15 categorías se agrupan en cuatro tipos, que son (1) violación de datos, (2) fraude y extorsión, (3) error de TI, y (4) violación de privacidad (PV). Lo que sigue proporciona una breve descripción de cada tipo de ciberincidente clasificado (...)

- *Los incidentes de violación de privacidad (PV) ocurren cuando las empresas recopilan o revelan información sensible de personas, como información personal identificable e información financiera, sin recibir el consentimiento de esas personas.*
- *Las brechas de datos (DB) son incidentes en los que se violan dispositivos de almacenamiento de datos, causando una posible fuga de información confidencial. Estos incidentes pueden ser causados por [actividades de pirateo] o la pérdida de dispositivos físicos.*
- *Los incidentes cibernéticos en la categoría de fraude y extorsión (FE) son similares a los fraudes tradicionales y eventos de extorsión, pero tienen lugar en el ciberespacio. Los fraudes cibernéticos típicamente han implicado la falsificación de identidad digital, como los ataques de phishing, y comúnmente en eventos de extorsión cibernética, la información y los sistemas de información son tomados como rehenes por intrusos para obtener ganancias financieras.*
- *En los eventos de error de TI (ITE), no hay intención maliciosa involucrada. Son causados por errores al configurar o utilizar sistemas de TI” (traducción libre, Pág. 405)*

⁹ A manera de ejemplo Castillo Díaz (2020) plantea, siguiendo la clasificación propuesta por CRO Forum (2016, p.25), que los riesgos cibernéticos se pueden catalogar en cuatro (4) categorías principales, así: “a. *Mal funcionamiento del sistema:* ocurre cuando un hacker toma el control de un computador del sistema o la red y a través de ese canal lleva a cabo actividades ilícitas en contra de un tercero. Esto puede ser ejecutado a través de un DoS o un Botnet, según lo hemos expuesto en el acápite que antecede. Este evento se denomina en Inglés como “Inadvertent disruption of third-party system”. b. *Confidencialidad de datos:* un sujeto (compañía o persona) detecta que los datos de otra persona están siendo almacenados o procesados por fuera de su sistema o red (perímetro). Por ejemplo, percibe que los datos personales del tercero están siendo vendidos, tratados o expuestos en la Deep web. Este tipo de incidente se denomina “Theft of third party data”. c. *Integridad y disponibilidad de los datos:* un sujeto (compañía o persona) detecta que los datos de otra persona están siendo almacenados o procesados tergiversados. Usualmente es difícil detectar los cambios porque son pequeños y puede tardarse mucho tiempo en la detección de los cambios. Este tipo de incidente se denomina en Inglés “Corruption of third party data”. d. *Actividad maliciosa:* un hacker inicia una transferencia de dinero haciendo mal uso de unas credenciales y actuando como el sujeto (víctima) en un sistema determinado. Normalmente esta conducta es denominada “Cyber Fraud” o “Cyber theft””.

Esta última taxonomía, como puede verse, otorga especial relevancia a la implementación de diversos métodos técnicos desplegados por los criminales -en un entorno cibernético- que, bajo la clasificación propuesta por Cebula, J. & Young, A. (2019) encajan dentro de la categoría de acciones deliberadas y representan un conjunto de vectores o métodos de ataque cuya comprensión resulta indispensable para la suscripción y comprensión del riesgo que atañe a los seguros bajo estudio:

1. **Ataque de día cero (Zero-day Exploits)¹⁰:** Se corresponde con un “(...) vector de ataque cibernético que usa una falla de seguridad desconocida o no abordada en software, hardware o firmware de computadora. “Día cero” se refiere al hecho de que el proveedor de software o dispositivo tiene cero días para arreglar la falla porque los actores maliciosos ya pueden usarla para acceder a sistemas vulnerables” (IBM, 2023).
2. **Ataque de intermediario (Man in the middle o MITM):** Permite al atacante - cibercriminal- interponerse en un canal de comunicación para leer, insertar, modificar o eliminar la información transmitida, bien sea entre dos o más víctimas, bien entre una víctima y un servidor -real o fraudulento-¹¹ (Mallik et al., 2019). De esta forma, el ciber atacante puede interceptar datos confidenciales como números de tarjetas de crédito, información de acceso bancario y/o credenciales para inicio de sesión en plataformas, misma que, a la postre, es utilizada para cometer otros delitos en el entorno cibernético (Callegati et al., 2009).
3. **Cryptojacking (Criptominería maliciosa):** Tipología de ataque, asociada comúnmente a la implementación de malware, en la cual un ciberdelincuente secuestra recursos informáticos de un dispositivo con miras a extraer criptomonedas de forma no autorizada valiéndose de la energía de procesamiento y electricidad de la víctima. De acuerdo con Schneider, J. & Smalley, I. (2025):

“(...) los ataques de cryptojacking, a veces denominados criptominería maliciosa, intentan apoderarse de los dispositivos informáticos o máquinas virtuales (VM) de los usuarios. El cryptojacking funciona filtrando en secreto el poder de procesamiento de víctimas desprevenidas para extraer monedas digitales. Los delincuentes cibernéticos recaudan las ganancias generadas por las criptomonedas, mientras que las víctimas pagan la factura”.
4. **Denegación de servicio (Denial of Service – DoS):** La denegación de servicio (DoS) y su variante distribuida (DDoS) buscan restringir o impedir el acceso de usuarios legítimos a los recursos de la red, el computador o el servicio de la víctima mediante la saturación con tráfico malicioso. Estos son conceptualizados por la literatura especializada, en los siguientes términos:

“Los ataques de denegación de servicio (DoS) buscan restringir parcialmente o negar completamente el acceso de usuarios legítimos a los recursos proporcionados por la red, computadora o servicio de la víctima. Cuando este intento se inicia desde un solo host, el ataque se llama un ataque DoS. Si bien los ataques DoS se pueden montar con éxito usando un solo host con recursos limitados, la mayoría de los ataques requieren un grupo de hosts maliciosos conocidos como “bots” que inundan la red de la víctima con una cantidad abrumadora de paquetes de ataques” (Martínez Lozano & Atencio-Ortiz, 2019)

¹⁰ Para una mejor comprensión del funcionamiento y particularidades de esta tipología de ataque véase: Guisao & Toro Rendon (2014).

¹¹ Catálogos actualizados de estas amenazas, su frecuencia y su evolución pueden consultarse en los informes anuales de la Agencia de la Unión Europea para la Ciberseguridad y en el reporte de investigaciones de filtraciones de datos de Verizon (European Union Agency for Cybersecurity — ENISA, 2024).

5. **Envenenamiento de datos:** Tipología de ataque relativamente reciente y ligado al ascenso de la inteligencia artificial y los modelos de aprendizaje automático en la cual los cibercriminales:

“(…) manipulan los datos de preentrenamiento, ajuste fino o incrustación para introducir vulnerabilidades, puertas traseras o sesgos. Esta manipulación puede comprometer la seguridad, el rendimiento o el comportamiento ético del modelo, lo que conlleva resultados perjudiciales o capacidades reducidas. Entre los riesgos comunes se incluyen la degradación del rendimiento del modelo, el contenido sesgado o tóxico y la explotación de sistemas posteriores” (OWASP Gen AI Security Project, 2025)

6. **Inyección SQL (Structured Query Language Injection):** De acuerdo con la literatura especializada:

“Los ataques SQLI explotan los campos de entrada del usuario a través de la manipulación de consultas de base de datos para inyectar código SQL dañino que otorga a los atacantes acceso a datos y capacidades de modificación y borrado desde bases de datos. Estas amenazas a la seguridad crean un daño significativo a la confiabilidad de los datos mientras destruyen la protección de la privacidad junto con los estándares de seguridad financiera que requieren sistemas defensivos fuertes” (Al-olaqi et al., 2025)

7. **Kerberoasting:** Tipología de ataque que tiene como finalidad recuperar u obtener indebidamente las credenciales de las cuentas del servicio “Active Directory” sin permiso ni escalado de privilegios con miras a vulnerar el protocolo de autenticación Kerberos.

“Los ataques de kerberoasting son prevalentes porque requieren habilidades básicas para implementarlos y su propia naturaleza protege a los perpetradores de ser detectados. Un ataque de Kerberoasting exitoso permite a un atacante navegar por un sistema enmascarado como un usuario aprobado. Es atípico que una herramienta de detección de ciberseguridad analice el comportamiento de los usuarios aprobados. Actuar como un usuario aprobado hace improbable que estas herramientas detecten la actividad del adversario. Estos ataques tampoco requieren el uso de malware, lo que los hace inmunes a tecnologías defensivas como el software antivirus. El hecho de que los atacantes puedan realizar la penetración de contraseñas sin conexión a internet significa que no generan tráfico de red sospechoso ni transmiten paquetes de datos” (Demers & Lee, 2022, págs. 30-31).

8. **Malware (Software Malicioso):** Es un software malicioso que amenaza a los usuarios de sistemas informáticos:

“(…) El rootkit, la botnet, el gusano, el spyware y el caballo de Troya son los tipos más comunes de malware que pueden causar daño a la red y los sistemas operativos (Feizollah et al., 2015; Rieck et al., 2008). Los autores sin escrúpulos diseñan malware con objetivos y funciones específicos. Cuando se activa, el malware se propaga por Internet y causa defectos en los sistemas operativos. El malware utiliza vulnerabilidades en las aplicaciones informáticas y los sistemas operativos para explotar datos a través de código malicioso. También utiliza la ingeniería social para atraer a los usuarios a ejecutar el código malicioso con herramientas y aplicaciones útiles. Las actividades mencionadas anteriormente causan problemas de computadora, dispositivo móvil, rendimiento de la red y estabilidad. Para combatir este problema, los investigadores de seguridad han diseñado aplicaciones anti-malware y antivirus que se utilizan para detectar malware. Esto se hace monitoreando las actividades de la computadora

mediante algoritmos específicos y firmas o patrones predefinidos. Hay muchos tipos de malware disponibles actualmente en Internet. Verizon informó que alrededor de 170 millones de eventos de malware ocurren en las organizaciones, con una frecuencia de cinco casos cada uno (1) segundo (Verizon, 2015). Se dice que PandaLabs logró neutralizar 75 millones de nuevos malware en 2014, el doble del récord de 2013 (Lopez, 2015) mientras que Symantec identificó más de 317 millones de nuevas piezas de malware creadas en 2014, una cifra que sugiere que casi un (1) millón de nuevas amenazas son lanzadas cada día (Symantec, 2015)” (Ab Razak et al., 2016)

9. **Ransomware:** Forma de software malicioso diseñada para bloquear el acceso a un sistema informático o a los datos, frecuentemente mediante su cifrado, con el fin de extorsionar a las víctimas a cambio de restablecer el acceso, a lo cual se suma, en muchos casos, la amenaza de divulgación pública de los archivos confidenciales sustraídos. De conformidad con lo establecido por el Departamento del Tesoro de los Estados Unidos de América se trataría de una forma de “malware” diseñada específicamente para:

“(…) bloquear el acceso a un sistema informático o datos, a menudo encriptando datos o programas en sistemas de tecnología de la información para extorsionar pagos de rescate a las víctimas a cambio de descifrar la información y restaurar el acceso de estas a sus sistemas o datos. En algunos casos, además del ataque, los ciber actores amenazan con revelar públicamente los archivos confidenciales de las víctimas” (U.S. Department of the Treasury — Office of Foreign Assets Control, 2020)

Esta modalidad de doble extorsión —cifrado más exfiltración— constituye en la actualidad la principal fuente de siniestralidad del ramo: de acuerdo con Munich Re, el *ransomware* se mantuvo en 2024 como la primera causa de pérdidas amparadas bajo el seguro de riesgos cibernéticos, con demandas de rescate promedio cercanas a los seiscientos mil dólares (USD\$600.000) (Munich Re, 2025).

“(…) El ransomware es un método generalizado y en aumento mediante el cual los ciberdelincuentes buscan extraer valor. También parece que la ola aún no ha alcanzado su punto máximo. En su estudio de las técnicas de ransomware, McIntosh y sus colegas señalan que existe un consenso sobre la expectativa de que los ataques de ransomware no solo seguirán creciendo, sino que también se desplazarán hacia tácticas más disruptivas que son más difíciles de combatir. (...)

- 1. Habrá una reducción de los ataques a particulares y un aumento de los ataques a organizaciones, optimizando aún más la relación tiempo-valor en favor de los atacantes.*
- 2. Habrá un cambio en las tácticas hacia la explotación activa de las vulnerabilidades tecnológicas y se alejará de las infiltraciones pasivas (por ejemplo, a través de phishing, vishing o fraude).*
- 3. Habrá una ampliación del mecanismo para privar a las empresas del acceso a sus sistemas, posiblemente renovando el foco en los ataques de denegación distribuida de servicios (DDoS) en lugar de solo la encriptación de archivos.*

Con estos pronósticos como telón de fondo, la proliferación de dispositivos industriales conectados en red de la Internet de las cosas (IoT) en los que se basan múltiples empresas (...) plantea graves preocupaciones. Muchos de estos han sido resumidos por Yaqoob et al., que enfatizan las funciones vitales que realizan los dispositivos IIoT conectados. Estos dispositivos también han demostrado ser significativamente vulnerables a los ataques de ransomware. En el nivel macro, Yaqoob et al. discuten los riesgos del ransomware para los centros hospitalarios, las instalaciones de tratamiento de agua, la red eléctrica, la producción farmacéutica y los reactores nucleares. En el nivel micro, los vehículos autónomos y los dispositivos médicos implantables parecen

estar particularmente en riesgo. La sociedad se está volviendo cada vez más dependiente de la tecnología, y los dispositivos conectados juegan un papel cada vez más vital en la seguridad humana y el bienestar social. Es insuficiente considerar los ataques de ransomware dentro de la visión limitada de las exploits técnicas y las contramedidas. El ransomware requiere una respuesta similar a los enfoques que abordan otras amenazas sociales graves. Una respuesta así, sostenemos, debe reconocer las motivaciones de los malos actores involucrados y realinear sus intereses con los de la sociedad en general” (Traducción libre, Jae & Floridi, 2024)

10. Suplantación de identidad (Phishing): Se considera la tipología de ciberataque más común (Nykodymet al., 2010) y ha sido definida por la literatura especializada:

“(…) como "un acto escalable de engaño por el cual se utiliza la suplantación para obtener información de un objetivo". (...), todos los tipos tienen el objetivo de convencer a las personas para que compartan información personal o confidencial (por ejemplo, datos bancarios, ID de cuenta y contraseñas). La motivación detrás de los ataques de phishing varía dependiendo del objetivo del atacante, y el phishing se utiliza cada vez más como una fachada para promover diferentes ataques como robo de identidad, ransomware, espionaje y chantaje.

(...) Los ataques de phishing tienen diferentes formas, aunque los correos electrónicos son el medio de comunicación más común utilizado en los ataques de phishing debido a su facilidad de uso y bajo costo. Otros medios utilizados incluyen mensajes de texto engañosos o llamadas telefónicas que se hacen pasar por empresas o individuos legítimos. Por lo tanto, se debe considerar el tipo de ataque de phishing, las víctimas específicas y el medio utilizado para promover estos ataques a fin de entender los riesgos asociados e implementar los mecanismos de protección apropiados.” (Jabir et al., 2025).

En este contexto, es importante precisar que los diferentes tipos de ataques, eventos y/o vectores de ataque abordados presentan como eje común la afectación de la información —su adquisición, modificación, bloqueo o eliminación—, lo que explica que, en el seguro de riesgos cibernéticos, los datos constituyan simultáneamente el bien sobre el que recae el interés asegurable en razón del valor que los mismos tienen para el patrimonio del asegurado, así como determinan el espectro del riesgo asegurado porque se brindaría amparo a las diferentes causas que pueden afectar la integridad de estos. En este sentido, los ataques cibernéticos implican una actuación indebida encaminada a:

“(…) adquirir, modificar, impedir el acceso o eliminar la información y/o datos de una persona u organización almacenados en un determinado dispositivo, sistema o servidor, en la medida en que aquellos constituye (sic) un importante activo a partir del cual dichos terceros pueden obtener provecho, al tiempo que su afectación tiene la potencialidad de comprometer tanto la capacidad operativa del asegurado, como su patrimonio y reputación como consecuencia de la filtración, destrucción o modificación de la información y/o datos que, en tratándose del seguro de riesgos cibernéticos, constituye tanto el componente esencial del riesgo asegurado como el bien objeto de cobertura, al constituir su afectación, y no el hurto o desaparición de dinero como suele acontecer en las pólizas de líneas financieras, el requisito sine qua non para la existencia de un siniestro indemnizable.

Así las cosas, es del caso precisar, que tal y como se mencionó brevemente con anterioridad, la ocurrencia de un incidente como los mencionados se puede encuadrar en cuatro (4) a tipologías básicas que afectan el flujo de datos, a saber, la denegación de su circulación, su interceptación, modificación y/o la fabricación de un nuevo flujo ajeno al sentido original existente entre el emisor y el receptor, todos los cuales revisten la potencialidad de causar diferentes tipos de pérdidas u afectaciones, incluyendo, pero sin limitarse, a: i) Lucro cesante derivado de la interrupción del negocio y/o la operación asegurada con o sin daño físico; ii) Lucro cesante

contingente derivado de la afectación por un evento cibernético a proveedores, socios de negocios o consumidores; iii) Costos de reconstrucción, reemplazó o restauración y/o de reproducción de datos, información o software que, como consecuencia de un evento cibernético, haya sido perdido, robado, borrado, encriptado o corrompido; iv) Costos relativos al manejo por expertos de un evento de extorsión o solicitud de rescate ligado a la información o datos almacenados por la compañía, sean esto o no propios, así como el pago de los mismos; v) Costos y pérdidas asociados al hurto de propiedad intelectual; vi) Responsabilidad civil frente a terceros como consecuencia de una filtración de información privada y/o de datos sensibles; vii) Daño reputacional; viii) Gastos de defensa en relación con procesos regulatorios y/o legales; ix) Multas y Sanciones; x) Responsabilidad Civil de Directores y Administradores; xi) Responsabilidad Civil Profesional como consecuencia de errores u omisiones en el manejo de la información; xii) Daño u afectación a activos físicos de la compañía y xiii) Daño a la integridad física o muerte” (Vivas & Bedoya, 2022, Págs. 665-666).

De esta manera, tal y como lo sostiene la OCDE (2017) la interrelación entre los incidentes de tipo cibernético y las afectaciones que de los mismos pueden derivarse, resulta más clara al comparar las pérdidas potenciales con el hecho generador de las mismas en materia de riesgos cibernéticos. La tabla subsiguiente explicita esta interrelación a partir de la información visible en el documento “*Enhancing the role of insurance in cyber risk management*” en el cual la OCDE (2017) aborda los diversos tipos de incidentes cibernéticos siguiendo el trabajo previamente relacionado de CRO Forum (2016):

Grupo de tipo de incidente del Foro de Directores de Riesgo, CRO (2016) (tipos de pérdidas)	Alcance de la cobertura según el Foro de Directores de Riesgo, CRO (2016)
Interrupción del negocio	Reembolso de las utilidades pérdidas causadas por una interrupción de la producción que no tiene origen en daños físicos.
Interrupción contingente del negocio por daño no físico	Reembolso de las utilidades perdidas para la empresa afectada, causadas por la interrupción de la producción de terceros relacionados (proveedores, socios, prestadores de servicios, clientes) que no tiene origen en daños físicos.
Pérdida de datos y software	Costos de reconstitución y/o reemplazo y/o restauración y/o reproducción de datos y/o software que hayan sido perdidos, dañados, robados, eliminados o cifrados.
Hurto financiero y/o fraude	Pérdidas financieras puras derivadas de actividades cibernéticas maliciosas —internas o externas— orientadas a cometer fraude, robo de dinero u otros activos financieros (por ejemplo, acciones). Comprende tanto las pérdidas financieras sufridas directamente por la empresa afectada como las sufridas por terceros relacionados a consecuencia de una conducta ilícita comprobada de dicha empresa.
Rescate cibernético y extorsión	Costos de gestión especializada ante un incidente de rescate y/o extorsión, junto con el monto del pago del rescate (por ejemplo, cuando el acceso a los datos se bloquea hasta que se paga el rescate).
Hurto de propiedad intelectual	Pérdida de valor de un activo de propiedad intelectual, que se traduce en una pérdida financiera pura.
Costos de respuesta al incidente	Compensación por acciones de gestión de crisis y remediación que requieren costos de expertos internos o externos, excluyendo los costos de defensa regulatoria y legal. La cobertura incluye: (i) investigación de TI y análisis forense, excluyendo aquellos directamente relacionados con costos de defensa regulatoria y

	legal; (ii) costos de relaciones públicas y comunicaciones; (iii) costos de remediación (por ejemplo, costos para eliminar o para activar una "inundación" de los contenidos dañinos publicados contra el asegurado); (iv) costos de notificación.
Violación de privacidad (compensación)	Costos de compensación tras la filtración de datos privados y/o sensibles, incluidos los servicios de monitoreo crediticio, pero con exclusión de los costos de respuesta al incidente.
Daño reputacional (excluida la protección legal)	Compensación por pérdida de utilidades debida a la reducción de actividad comercial/clientes como consecuencia de la pérdida de confianza en la empresa afectada.
Multas y sanciones	Compensación por multas y sanciones impuestas a la empresa afectada. Los reembolsos de seguros por estos costos se otorgan únicamente en las jurisdicciones donde esté permitido.
Directores y funcionarios (D&O)	Costos de compensación ante reclamaciones interpuestas por un tercero contra los directores y funcionarios de la empresa afectada, incluidas las derivadas de incumplimiento de confianza o de deberes fiduciarios como resultado de un evento cibernético.
Errores y omisiones tecnológicos (E&O)	Costos de compensación relacionados con el incumplimiento en la prestación de servicios técnicos adecuados o en la entrega de productos técnicos como resultado de un evento cibernético.
Errores y omisiones en servicios profesionales (E&O)	Costos de compensación relacionados con el incumplimiento en la prestación de servicios profesionales adecuados o en la entrega de productos como resultado de un evento cibernético, con exclusión de los servicios y productos de carácter técnico (errores y omisiones tecnológicos).
Daño ambiental	Costos de compensación tras la filtración de productos tóxicos y/o contaminantes como consecuencia de un evento cibernético.
Daño a activos físicos	Pérdidas (incluidas la interrupción del negocio y la interrupción contingente del negocio) relacionadas con la destrucción de bienes físicos de la empresa afectada como consecuencia de un evento cibernético ocurrido en dicha empresa.
Lesiones corporales y muerte	Costos de compensación por lesiones corporales o muerte consecutiva derivadas de la conducta ilícita o negligencia de la empresa afectada o de terceros relacionados (por ejemplo, filtración de datos sensibles que conduzca al suicidio).

En este panorama, debe resaltarse que un entendimiento claro de los incidentes cibernéticos resulta determinante para precisar el alcance de los riesgos que el seguro objeto de análisis está llamado a amparar. Ello, por cuanto la correcta caracterización técnica de dichos incidentes -en cuanto a su origen, mecanismo de materialización y efectos sobre los sistemas de información- constituye el punto de partida necesario para establecer con exactitud el objeto asegurado y, por esa vía, los límites de la cobertura pactada.

2. Panorama empírico de los Riesgos Cibernéticos: Materialización del riesgo y dimensión latinoamericana.

2.1. Los riesgos cibernéticos en contexto: Breve mención a los eventos más importantes en los últimos años.

Los incidentes cibernéticos no constituyen un fenómeno reciente; sus antecedentes se remontan al incidente del Gusano Morris -especie de malware autorreplicable- que el 02 de noviembre de 1988

infectó cerca de seis mil (6000) equipos conectados a la nascente internet. Sin embargo, la severidad y la frecuencia de los eventos han crecido de manera sostenida en las últimas décadas, particularmente como consecuencia de la acelerada digitalización de la economía, circunstancia que ha traído aparejado consigo un incremento no solo en el número de eventos, sino también en su alcance y costo. Entre los eventos más importantes de los últimos años en el panorama internacional, se cuentan la filtración de datos de más de cien millones de cuentas de los servicios en línea de Sony en 2011 -incluidos aquellos asociados a los servicios de Playstation-; el compromiso de la información de pago de decenas de millones de clientes de Target en 2013; la brecha de Equifax durante más de cuatro (4) meses en 2017, que expuso datos personales de aproximadamente ciento cuarenta y siete millones de consumidores y culminó en un acuerdo global con las autoridades estadounidenses en una cuantía superior a los Quinientos Setenta y Cinco Millones de Dólares (USD\$575.000.000) (Federal Trade Commission, 2019); y los ataques globales de 2017 con los programas WannaCry y NotPetya, que afectaron a cientos de miles de equipos en decenas de países y paralizaron las operaciones de multinacionales como Telefónica, FedEx, Renault, Maersk y Merck, con pérdidas agregadas estimadas en miles de millones de dólares (OCDE, 2017; Vivas & Bedoya, 2022)¹². El costo promedio global de una filtración de datos alcanzó en 2024 la cifra récord de Cuatro Millones Ochocientos Ochenta Mil Dólares (USD\$4.880.000), según la medición anual de IBM (2024).

Sin el ánimo de ser exhaustivos, América Latina exhibe una dinámica igualmente preocupante. Además del ataque al sistema SWIFT del Banco de Chile en mayo de 2018, que derivó en transferencias fraudulentas por cerca de diez millones de dólares (USD\$10.000.000) (Casas, 2018), durante 2020 se registraron múltiples ataques de tipo ransomware contra infraestructura crítica estatal, entre ellos el que afectó a la Dirección Nacional de Migraciones de Argentina, con cifrado y exfiltración de bases de datos y posterior publicación de la información sustraída ante la negativa de pago del rescate (Brodersen & Blanco, 2020).

En el ámbito colombiano, cabe destacar como antecedente relevante el ataque de ransomware sufrido hacia finales de noviembre de 2022 por el grupo multinacional de salud Keralty —matriz, entre otras entidades, de la EPS Sanitas y de Colsanitas— el cual comprometió los sitios web y la operación de la compañía y sus subsidiarias, ocasionando fallas generalizadas en la asignación de citas médicas y en la solicitud y entrega de medicamentos y exámenes, lo que motivó la apertura de la correspondiente investigación por parte de la Fiscalía General de la Nación (Lesmes, 2022). A nivel nacional, el episodio de mayor resonancia, ocurrió en septiembre de 2023, cuando el proveedor de servicios tecnológicos IFX Networks sufrió un ataque de ransomware que comprometió más de setecientas máquinas virtuales y afectó la operación de cerca de más setecientas sesenta (760) compañías en América Latina, así como de más de cuarenta (40) entidades públicas colombianas —entre ellas el Consejo Superior de la Judicatura -paralizando el funcionamiento de la administración de justicia-, el Ministerio de Salud y la Superintendencia de Industria y Comercio—, lo que llevó al Gobierno Nacional a instalar un puesto de mando unificado y anunciar acciones legales contra el proveedor (Presidencia de la República, 2023; El Tiempo, 2023). Este incidente puso de presente, con especial claridad, la dimensión sistémica del riesgo cibernético derivada de la dependencia de proveedores tecnológicos compartidos, así como la exposición a pérdidas consecuenciales por interrupción contingente del negocio en el caso de las personas jurídicas afectadas.

¹² Sobre el impacto económico de WannaCry, véase Deloitte España. El impacto económico de WannaCry. Disponible en: <https://www2.deloitte.com/es/es/pages/governance-risk-and-compliance/articles/impacto-economico-wannacry.html>. Sobre NotPetya y sus consecuencias aseguradoras, véase Cybersecurity Dive (2024). Merck reaches settlement in closely watched NotPetya insurance case. Disponible en: <https://www.cybersecuritydive.com/news/merck-settlement-notpetya-insurance/703922/>

En este contexto, la tabla subsiguiente pretende sistematizar algunos de los incidentes más relevantes de las últimas décadas y las tipologías de pérdida asociadas, evidenciando la heterogeneidad de los impactos que abarcan desde costos de respuesta y restauración de datos, pasando por lucro cesante por interrupción del negocio, hasta responsabilidad civil frente a terceros, sanciones regulatorias y daño reputacional:

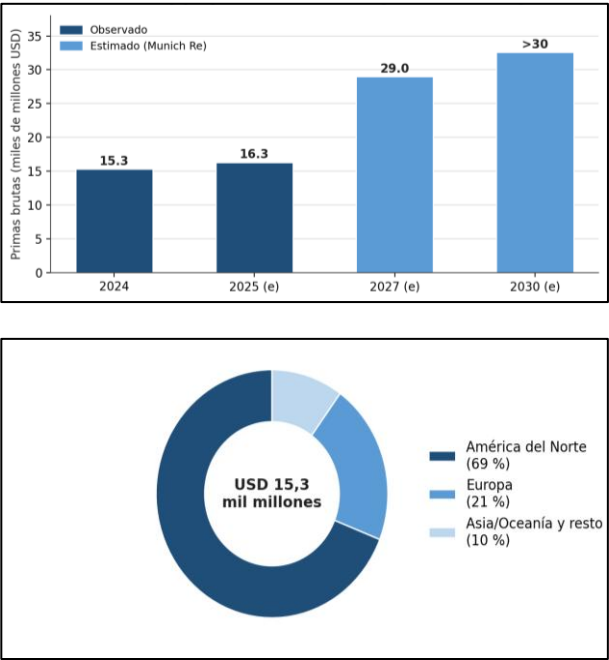
Incidente	Año	Vector / modalidad	Tipologías de pérdida documentadas
Sony (PSN)	2011	Intrusión y filtración de datos de usuarios	Costos de respuesta y limpieza estimados en Ciento Setenta y Un Millones de Dólares (USD\$171.000.000); reclamaciones de terceros; controversia de cobertura bajo póliza CGL tradicional.
Target	2013	Compromiso de credenciales de proveedor y malware en puntos de venta	Afectación de datos de pago de Cuarenta Millones (40.000.000) de clientes; costos reportados superiores a Doscientos Cuarenta y Ocho Millones (248.000.000); litigios y acuerdos con emisores de tarjetas.
Equifax	2017	Explotación de vulnerabilidad no parchada	Exposición de datos de Ciento Cuarenta y Siete Millones (147.000.000) de consumidores; acuerdo global con FTC, CFPB y estados por Quinientos Setenta y Cinco Millones de Dólares (USD\$575.000.000)
WannaCry	2017	Ransomware autopropagable (EternalBlue)	Afectación de cientos de miles de equipos en más de ciento cincuenta (150) países; interrupción de operaciones de salud, telecomunicaciones e industria.
NotPetya (Merck, Maersk y otros)	2017	Wiper/ransomware atribuido a actor estatal	Pérdidas superiores a Mil Cuatrocientos Millones de Dólares (USD\$1.400.000.000) solo para Merck; litigio de cobertura sobre la exclusión de guerra (Merck v. ACE American).
Banco de Chile	2018	Malware distractor y fraude vía SWIFT	Transferencias fraudulentas por aproximadamente Diez Millones de Dolares (USD\$10.000.000); compromiso de información financiera.
DNM Argentina	2020	Ransomware con exfiltración	Cifrado de bases de datos migratorias; interrupción del control fronterizo; publicación de información sustraída.
IFX Networks (Colombia y región)	2023	Ransomware contra proveedor de nube (RansomHouse)	Afectación de más de setecientos sesenta (760) compañías en la región y más de cuarenta (40) entidades públicas colombianas; interrupción contingente de servicios judiciales y de salud; anuncio de acciones de responsabilidad contra el proveedor.
Grupo Keralty	2022	Ransomware (RansomHouse)	Secuestro de 0,7 terabytes de información institucional, de los cuales se divulgaron trece (13) archivos con estados financieros, balances, presupuestos e información personal. Impacto operativo: interrupción de servicios digitales para ~5,5 millones de afiliados a EPS Sanitas. Vulneración de datos personales confirmada respecto de 241.589 usuarios.

En este contexto, caracterizado por la creciente frecuencia y sofisticación de los incidentes cibernéticos tanto a nivel global como nacional, el contrato de seguro se erige como un instrumento idóneo para la mitigación y gestión de los riesgos derivados de tales contingencias. Así las cosas, a través de este instrumento contractual resulta posible trasladar al asegurador el impacto económico

asociado a la materialización de eventos adversos, lo cual contribuye de manera directa a preservar la continuidad operacional del asegurado y a salvaguardar su patrimonio frente a las consecuencias derivadas de dichos riesgos.

2.2.El mercado de seguros ligados a riesgos cibernéticos: Dimensión global y brecha latinoamericana.

En el contexto previamente explicado, el mercado mundial de seguros para riesgos cibernéticos ha experimentado un crecimiento notable, aumentando casi en un trescientos por ciento (300%) su tamaño en los últimos cinco (5) años. Munich Re (2025) estima que las primas brutas globales del ramo totalizaron Quince Mil Trecientos Millones de Dólares (USD\$15.300.000.000) en 2024 —cifra que representa menos del uno por ciento (1%) del volumen mundial de primas de seguros patrimoniales y de responsabilidad—, con una proyección de Dieciséis Mil Trescientos Millones de Dólares (USD\$16.300.000.000) para 2025 y la expectativa de que el mercado duplique su tamaño hacia 2030, a una tasa media anual de crecimiento superior al diez por ciento (10%). Las figuras 1 - evolución y proyección de las primas brutas del mercado global- y 2 – Distribución regional de las primas- elaboradas a partir de los datos publicados por Munich Re (2025) ilustran, respectivamente, la evolución proyectada de las primas y la distribución regional del mercado en 2024, en la que América del Norte concentra el sesenta y nueve por ciento (69%) de las primas y Europa el veintiuno por ciento (21%), quedando para el resto del mundo —incluida América Latina— una participación marginal cercana al diez por ciento (10%) de la cual, por demás el grueso pertenece a Asia.



La participación marginal de América Latina en el mercado global contrasta con su elevada exposición. La región acumuló en años recientes una porción relevante de los intentos de explotación de debilidades y/o realización de ataques cibernéticos detectados a nivel mundial, con México y Brasil a la cabeza, encontrándose igualmente Colombia entre los países más atacados (Fortinet — FortiGuard Labs, 2023). Al mismo tiempo, la penetración del seguro en general permanece baja; en Colombia, por ejemplo, las primas emitidas del conjunto de la industria representan alrededor del tres punto dos por ciento (3,2%) del producto interno bruto, nivel similar al promedio latinoamericano, pero distante de los demás países de la OCDE (Fasecolda, 2024). Dentro de ese universo, el seguro

para riesgos cibernéticos es todavía un ramo incipiente, comercializado principalmente para grandes empresas y entidades financieras a través de programas internacionales con soporte de reaseguro facultativo, mientras que las pequeñas y medianas empresas —que constituyen el grueso del tejido productivo regional— retienen en su patrimonio casi la totalidad del riesgo. Esta combinación de alta exposición y baja transferencia configura la denominada brecha de protección cibernética, cuya necesidad de reducción ha sido identificada por la OCDE (2017) y por la industria reaseguradora como un objetivo prioritario de política pública y de desarrollo de mercado (Munich Re, 2025).

3. El seguro de riesgos cibernéticos.

“The growth of the cyberinsurance market has been shaped in large part by regulations and regulators, but cyberinsurance itself remains largely unregulated. Unlike other forms of insurance, there are no requirements governing what cyberinsurance policies must cover, who must obtain them, or to whom they must be made available” (Wolff, 2022).

3.1. Noción y evolución.

Bajo la denominación de seguro para “riesgos cibernéticos” se agrupa un conjunto más o menos amplio de Pólizas De Seguro para riesgos específicos que presentan características heterogéneas¹³ aunque con tendencia a la homogeneización a partir de los diversos esfuerzos adelantados por organismos multilaterales como la OCDE, encaminadas a brindar cobertura tanto a las pérdidas de primera parte como a las de tercera parte, como consecuencia y/o resultantes de *“(…) un ataque o mal funcionamiento informático de los sistemas informáticos de una empresa”* (Romanosky, 2019; Granato & Polacek, 2019)¹⁴. Esta tipología de productos, al igual que el grueso de los existentes en materia de seguros, generalmente distingue entre:

“(…) dos amplias categorías de pérdidas, “primera parte” y “tercera parte”. Las pérdidas de la primera parte se refieren a las sufridas directamente por el asegurado (es decir, la “primera” parte del contrato de seguro), mientras que la responsabilidad de terceros se refiere a reclamaciones presentadas por partes externas al contrato (es decir, la “tercera” parte) que sufren una pérdida supuestamente debido a la conducta del asegurado. (...) Como se mencionó, la cobertura de primera parte incluye las pérdidas incurridas directamente por el asegurado. Por ejemplo, los costos relacionados con la investigación de la causa de una violación de datos o un incidente de seguridad, los costos asociados con el restablecimiento de servicios comerciales, el costo de notificar a las personas afectadas, los servicios de supervisión del crédito, los gastos incurridos en relaciones públicas y servicios de medios para comunicar el evento, extorsión y pagos de rescate, y pérdidas asociadas con la interrupción del negocio.

(...) La responsabilidad de terceros cubre el costo de defenderse contra litigios públicos o privados, acuerdos, sentencias u otras resoluciones, así como multas, honorarios y acuerdos derivados de estas demandas. Por ejemplo, la cobertura de responsabilidad de seguridad de red del POL-35 cubre los costos debidos a “una acción civil, una disputa alternativa, un

¹³ Al respecto señala el numeral 5.2. de la ISO/IEC 27102:2019(E) que la cobertura varía de forma sustancial *“(…) entre los diferentes productos existentes en el mercado, no está estandarizada y las diferencias en su contenido dependen de: a) las necesidades del asegurado; b) las limitaciones consagradas por leyes y reglamentos locales; c) las prácticas de mercado generalmente aceptadas; y d) las decisiones comerciales del asegurador”* (Traducción propia)

¹⁴ *“Esta tipología de negocio jurídico, en la práctica de suscripción de la industria aseguradora y reaseguradora mundial se enmarca dentro de los denominados seguros de líneas financieras, en la medida en que, para muchos, su origen estructuración y alcance se puede encontrar en la evolución de los seguros de Directores y Administradores (D&O) y la sección de crímenes por computadora (“computer crime”), usualmente comercializada como un anexo de las Pólizas Globales Bancarias, como consecuencia de la falta de capacidad de tales productos tradicionales de brindar cobertura, suficiente y adecuada a los, riesgos derivados de los entornos cibernéticos, el manejo y transmisión de datos, así como la evolución de la actividad económica hacia centros no físicos de producción y la integración del internet dentro del normal funcionamiento de las organizaciones (Majuca et al, 2006)” (Vivas & Bedoya, 2022).*

procedimiento de resolución o una demanda escrita de dinero" como resultado de "[l]a violación de información comercial de terceros, [l]a propagación o reenvío involuntarios de malware, [l]a complicidad involuntaria con un ataque de denegación de servicio" (Romanosky et al., 2019, Págs. 4-6)

En este contexto, sin perjuicio del análisis que más adelante se realiza de las coberturas y exclusiones que suelen pactarse para este producto, corresponde reiterar que, aunque no existe uniformidad en el alcance de los productos comercializados bajo la denominación genérica de ciberseguro, la norma ISO/IEC 27102:2019 identifica como categorías principales de cobertura la responsabilidad civil, los costos de respuesta a incidentes, los costos asociados a extorsiones cibernéticas, la interrupción de la actividad empresarial, las multas y sanciones legales y reglamentarias, las sanciones contractuales y los daños a los sistemas, advirtiendo que con el desarrollo del producto pueden surgir nuevas categorías (ISO/IEC 27102:2019, numeral 6.3.2.). El análisis empírico de clausulados realizado por Romanosky et al. (2019) sobre una muestra amplia de pólizas estadounidenses confirma esta estructura bipartita de amparos de primera y de tercera parte, al tiempo que documenta una notable heterogeneidad en definiciones, sublímites y exclusiones entre aseguradores, siendo, tal vez, la única constante el lugar central que en todos ellos ocupa la información¹⁵ y/o los datos que la componen como objeto único de aseguramiento.

3.2. El marco regulatorio transversal en América Latina.

El aseguramiento de los riesgos cibernéticos no puede comprenderse al margen del entramado normativo que, en cada jurisdicción, sanciona los delitos informáticos, la protección de datos personales y la gestión del riesgo de ciberseguridad. Ello obedece a dos (2) razones. La primera es que buena parte de los amparos del ramo —en particular los de responsabilidad civil por violación de privacidad, los gastos de defensa en procedimientos y, donde resulte asegurable, el pago de multas— tienen como presupuesto la existencia de deberes legales de custodia de la información y de regímenes sancionatorios por su incumplimiento. La segunda es que las normas imperativas del contrato de seguro de cada país condicionan la validez y eficacia de los clausulados, muchos de ellos traducidos de formularios anglosajones cuya lógica no siempre se acompasa con los regímenes continentales de la región y que, las más de las veces, no son íntegramente ajustados para incorporar las regulaciones locales¹⁶.

¹⁵ Para efectos de las Pólizas de Seguro objeto de estudio se entiende por tal a cualquier información, siempre y cuando sea legible por algún método, "(...) *independientemente del modo de uso o presentación (texto, cifras, voz o imágenes), Software incluido, transmitida o almacenada en formato digital fuera de la memoria de acceso aleatorio (RAM) propiedad del Asegurado o por este operada. El término Datos abarcará también Archivos Digitales*" (Hass & Hofmann, 2013).

¹⁶ En el caso colombiano, el marco normativo para la comercialización de Seguros de Riesgos Cibernéticos se articula sobre cuatro (4) pilares. En primer lugar, la Ley 1273 de 2009 creó el bien jurídico tutelado de la protección de la información y de los datos, tipificando, entre otros, los delitos de acceso abusivo a sistema informático, interceptación de datos, daño informático, uso de software malicioso, violación de datos personales y transferencia no consentida de activos. En segundo lugar, la Ley 1581 de 2012 y sus decretos reglamentarios consagran el régimen general de protección de datos personales, desarrollando el derecho fundamental de habeas data previsto en el artículo 15 de la Constitución Política, e instituyendo a la Superintendencia de Industria y Comercio como autoridad de protección de datos con potestades sancionatorias. En tercer lugar, en el plano de la política pública, los documentos CONPES 3701 de 2011, 3854 de 2016 y 3995 de 2020 fijaron, sucesivamente, los lineamientos de ciberseguridad y ciberdefensa, la política nacional de seguridad digital y la política de confianza y seguridad digital. Y, en cuarto lugar, en el ámbito sectorial financiero, la Circular Externa 007 de 2018 de la Superintendencia Financiera de Colombia impartió instrucciones sobre los requerimientos mínimos para la gestión del riesgo de ciberseguridad por parte de las entidades vigiladas, exigiendo, entre otros aspectos, políticas aprobadas por la junta directiva, unidades especializadas de seguridad de la información, sistemas de monitoreo continuo, planes de continuidad que contemplen la materialización de ataques cibernéticos y el deber de informar a los consumidores financieros los incidentes que afecten la confidencialidad o integridad de su información. Es significativo que la propia Circular contemple la contratación de seguros como una de las medidas admisibles para la mitigación del riesgo residual, con lo cual el ciberseguro queda formalmente integrado al arsenal de gestión del riesgo operacional del sistema financiero colombiano.

El panorama regional muestra una convergencia progresiva hacia regímenes de protección de datos de inspiración europea y hacia marcos institucionales de ciberseguridad, aunque con ritmos y profundidades distintos. Brasil adoptó en 2018 la Ley General de Protección de Datos (LGPD), de clara inspiración en el reglamento europeo, con una autoridad nacional dotada de potestades sancionatorias que alcanzan el dos por ciento (2%) de la facturación de la empresa infractora¹⁷. Argentina cuenta desde el año 2000 con la Ley 25.326 de protección de datos personales, pionera en la región y reconocida con un nivel de adecuación por la Unión Europea¹⁸. Chile, a su vez, protagonizó en 2024 la renovación normativa más ambiciosa de la región, con la expedición de la Ley 21.663, Ley Marco de Ciberseguridad e Infraestructura Crítica de la Información —que crea la Agencia Nacional de Ciberseguridad e impone deberes de reporte de incidentes a los servicios esenciales—; y de la Ley 21.719, que modernizó el régimen de datos personales y creó la Agencia de Protección de Datos¹⁹. Por su parte, México renovó en marzo de 2025 su Ley Federal de Protección de “Datos Personales en Posesión de los Particulares”, en el marco de la reorganización institucional suprimió al antiguo instituto autónomo de transparencia²⁰; y Perú mantiene vigente la Ley 29733 de 2011 y su reglamento, con una autoridad nacional adscrita al Ministerio de Justicia²¹.

A partir de la síntesis anterior resulta imperativo indicar que para la práctica aseguradora resulta claro que, aunque los clausulados de Riesgos Cibernéticos comercializados en la región suelen provenir de matrices internacionales relativamente homogéneas, la exposición efectiva del asegurado —y, por consiguiente, el contenido material del riesgo transferido— varía sustancialmente de una jurisdicción a otra en función del rigor de los deberes de seguridad, de la existencia de obligaciones de notificación de brechas y de la severidad de los regímenes sancionatorios. La suscripción transfronteriza de programas regionales exige, por tanto, un ejercicio cuidadoso de adaptación local, tanto en la redacción de los amparos como en la verificación de la asegurabilidad de ciertos conceptos —señaladamente las multas administrativas— bajo el orden público de cada país.

3.3. El contrato de seguro de riesgos cibernéticos en el ordenamiento colombiano: naturaleza y ubicación sistemática.

En Colombia, al igual que acontece en la región, el seguro de riesgos cibernéticos carece de una regulación específica, por lo que se gobierna por el régimen general del contrato de seguro contenido en los artículos 1036 a 1162 del Código de Comercio, conforme al cual el seguro es un contrato consensual, bilateral, oneroso, aleatorio y de ejecución sucesiva. Desde el punto de vista de su estructura técnica, el seguro para riesgos cibernéticos puede ser entendido como un producto híbrido o complejo, dado que bajo una misma póliza pueden convivir, en los términos ya indicados, amparos de daños de primera parte —que protegen el patrimonio propio del asegurado frente a la pérdida de datos, la interrupción del negocio o la extorsión— y amparos denominados en mercados internacionales como de tercera parte, típicos de los seguros de responsabilidad civil (*third party liability*), que cubren la obligación de indemnizar los perjuicios causados a terceros con motivo de

¹⁷ República Federativa do Brasil. Lei nº 13.709, de 14 de agosto de 2018 — Lei Geral de Proteção de Dados Pessoais (LGPD). Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm

¹⁸ República Argentina. Ley 25.326 de Protección de los Datos Personales. Disponible en: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm>

¹⁹ República de Chile. Ley 21.663, Ley Marco de Ciberseguridad e Infraestructura Crítica de la Información (2024), y Ley 21.719, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (2024). Disponibles en la Biblioteca del Congreso Nacional de Chile: <https://www.bcn.cl/leychile>

²⁰ Estados Unidos Mexicanos. Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada en el Diario Oficial de la Federación el 20 de marzo de 2025. Disponible en: <https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>

²¹ República del Perú. Ley N.º 29733, Ley de Protección de Datos Personales (2011). Disponible en el Archivo Digital de la Legislación del Perú: <https://leyes.congreso.gob.pe/>

una determinada conducta del asegurado, producto regulado en Colombia en el artículo 1127 del Código de Comercio.

Esta dualidad de los productos de ciber impone que cada sección del clausulado se interprete y aplique conforme a las reglas propias del esquema al que pertenece, especialmente aquellas que son exclusivas y específicas para el seguro de responsabilidad, tales como las normas sobre la acción directa de la víctima dispuesta en el artículo 1133 del C. de Co. y/o el especial cómputo del término de prescripción del seguro de responsabilidad civil dispuesto en el artículo 1131 del C. de Co. que en estricto sentido solo operaría si la cobertura de responsabilidad estuviera dispuesta bajo el sistema de delimitación temporal por ocurrencia, lo cual como se verá a continuación, no aplica para este producto que es comercializado bajo el sistema *Claims Made* o por reclamación.

De otra parte, otras figuras como la de la regla proporcional por infraseguro establecida en el artículo 1102 del C. de Co. no aplicarían para la cobertura de responsabilidad civil, pero sí para los amparos de primera parte como sería específicamente el de lucro cesante, lo cual es una práctica común en el mercado colombiano (Ossa, 1991; Díaz-Granados, 2012).

3.3.1. Riesgo asegurable e interés asegurable.

El artículo 1054 del Código de Comercio define el riesgo como el suceso incierto que no depende exclusivamente de la voluntad del tomador, del asegurado o del beneficiario, y el artículo 1055 sanciona con ineficacia el aseguramiento del dolo, la culpa grave y los actos meramente potestativos del tomador, asegurado y/o beneficiario, así como las sanciones de carácter penal o policivo. Trasladadas estas categorías al ámbito cibernético, el riesgo asegurado estará constituido, según el amparo de que se trate, por la eventualidad de un incidente de seguridad de la información —acceso no autorizado, cifrado, exfiltración, denegación de servicio— que afecte los sistemas y especialmente los datos del asegurado, o por la eventualidad de que el asegurado incurra en responsabilidad frente a terceros con ocasión de tal incidente.

La incertidumbre exigida por la ley no se ve comprometida por la alta frecuencia estadística de los ataques, pues lo incierto es que su materialización se concrete respecto del asegurado individualmente considerado; en cambio, sí resultaría inasegurable el siniestro ya ocurrido y conocido al momento de la celebración del contrato, lo que explica la generalizada inclusión de fechas retroactivas y de exclusiones de hechos previos y circunstancias conocidas en los clausulados del ramo, especialmente para las coberturas de responsabilidad civil que operan bajo el sistema por reclamación.

En cuanto al interés asegurable, el artículo 1083 del Código de Comercio lo radica, para los seguros de daños, en toda persona cuyo patrimonio pueda resultar afectado, directa o indirectamente, por la realización de un riesgo, y el artículo 1127 lo extiende, en el seguro de responsabilidad, al patrimonio del asegurado expuesto a las consecuencias de su responsabilidad o al nacimiento de un débito u obligación de reparar a otro. La particularidad del seguro para riesgos cibernético reside en que el objeto sobre el cual recae primariamente el interés asegurable, es un bien intangible -los datos o información- es decir un activo inmaterial cuya valoración económica plantea dificultades notorias, tanto en la determinación de la suma asegurada, como en la cuantificación de la pérdida indemnizable, sin que por dicho simple hecho se pierda la naturaleza eminentemente indemnizatoria del grueso de los amparos que integran la Póliza de Seguro.

La práctica internacional -y, en ello América Latina no es la excepción- ha respondido a esta dificultad mediante la fijación de sublímites por amparo, la indemnización por costos de reconstrucción, reparación o restauración de los datos —y no por su valor intrínseco o comercial— y la determinación de utilidades brutas en lo que respecta a los amparos de interrupción del negocio,

técnicas todas compatibles con el principio indemnizatorio del artículo 1088 del Código de Comercio²².

3.3.2. La declaración del estado del riesgo y el formulario de suscripción.

El grueso de los ordenamientos jurídicos latinoamericanos -entre ellos Colombia por virtud del artículo 1058 del Código de Comercio- impone al tomador el deber de declarar sinceramente los hechos y circunstancias que determinan el estado del riesgo, según el cuestionario que le sea propuesto por el asegurador, sancionando con la nulidad relativa del contrato la reticencia o inexactitud sobre hechos que, conocidos por el asegurador, lo hubieren retraído de celebrarlo o inducido a estipular condiciones más onerosas. En el seguro para riesgos cibernéticos, este deber adquiere una intensidad singular, pues la evaluación del riesgo depende casi por completo de la información que el propio candidato suministre acerca de su infraestructura tecnológica, sus controles de seguridad —autenticación multifactor, copias de respaldo, segmentación de redes, gestión de parches, planes de respuesta a incidentes—, su historial siniestral y su dependencia de terceros proveedores. El formulario de solicitud o “proposal form” cumple aquí una doble función, como instrumento de suscripción y delimitación del marco de la declaración, de suerte que, conforme al inciso final del artículo 1058, si la aseguradora omite indagar sobre determinados aspectos, no podrá luego alegar la nulidad por reticencia respecto de ellos, salvo dolo o mala fe del tomador. La norma ISO/IEC 27102:2019 recomienda precisamente articular el intercambio de información entre asegurado y asegurador sobre la base de los sistemas de gestión de seguridad de la información, lo que en la práctica se traduce en cuestionarios técnicos detallados, auditorías externas de postura de seguridad y, crecientemente, escaneos no intrusivos de superficie de ataque realizados por el propio asegurador.

3.3.3. La delimitación temporal de la cobertura: Ocurrencia y Claims Made como modelos centrales de delimitación temporal del riesgo asegurado.

La delimitación temporal de la cobertura constituye uno de los aspectos más sensibles del producto. Para los productos ciber en los amparos de primera parte, la regla general sigue siendo la ocurrencia del evento durante la vigencia de la póliza, es decir, el incidente cibernético debe acaecer dentro de la vigencia de la póliza para que se activen los amparos destinados a cubrir pérdidas patrimoniales sufridas por el asegurado. En los amparos de responsabilidad civil o de daños causados a terceras partes —siguiendo la práctica internacional— de manera generalizada aplica la modalidad de delimitación temporal por reclamación o “claims made”, conforme a la cual en el seguro de responsabilidad la cobertura se circunscribe a las reclamaciones formuladas por la víctima al asegurado o a la compañía de seguros durante la vigencia de la póliza, siempre que el hecho generador ocurra dentro del mismo periodo del seguro o con posterioridad a la fecha retroactiva pactada.

Ahora bien, dada la creciente sofisticación y complejidad de los incidentes cibernéticos, cada vez es más común, que entre la intrusión inicial o ataque y su descubrimiento puedan transcurrir incluso meses -como por ejemplo ocurrió en el caso de Equifax, en el que los atacantes operaron inadvertidos durante más de cuatro (4) meses-, lo que hace especialmente sensible en este producto la delimitación

²² No puede dejar de observarse, sin embargo, que la ISO/IEC 27102:2019(E) consagra en punto de los límites de cobertura en su numeral 6.8.: “(...) Las posibles afectaciones para el negocio y las pérdidas correlativas que pueda sufrir el asegurado deben ser revisadas y aclaradas para considerar y determinar cuidadosamente el monto de la cobertura de la póliza de seguro cibernético a adquirir. La cantidad de cobertura que el asegurado puede comprar puede variar dependiendo de su situación financiera, la industria, las operaciones que realiza y la exposición al riesgo cibernético (...) Para ayudar a evaluar las posibles pérdidas cibernéticas que permitirían determinar la cantidad adecuada de cobertura a comprar, se puede solicitar asesoramiento a las organizaciones de investigación que publican regularmente información de referencia para o de la industria sobre el costo de incidentes cibernéticos pasados en todo el mundo” (Traducción libre).

temporal de cobertura y pueda conducir a que la realidad técnica y tecnológica pueda exigir que se adopte un sistema de delimitación temporal por descubrimiento en el cual el detonante de la cobertura de primera parte, ya no sea el acaecimiento del incidente cibernético, sino la conciencia o conocimiento por parte del asegurado de haber sido atacado.

En este panorama, la principal dificultad práctica radicará en que no en todos los ordenamientos jurídicos se permite la utilización de sistemas de delimitación temporal diferentes al tradicional por ocurrencia para la mayoría de los productos de seguros, sino únicamente para algunos expresamente autorizados como por ejemplo ocurre en Colombia donde el artículo 4 de la Ley 389 de 1997 autoriza que los seguros de responsabilidad pueden operar bajo el sistema por reclamación (Claims Made) y los seguros de manejo e infidelidad y riesgos financieros puedan operar bajo el sistema por descubrimiento; sin embargo, ese tratamiento excepcional no estaría autorizado para el producto de riesgos cibernéticos en las coberturas de primera parte lo cual podría requerir una actualización normativa.

Así las cosas, una correcta articulación entre fecha retroactiva, período de vigencia, plazos de descubrimiento -si aplican- y períodos extendidos de reclamación para la cobertura de responsabilidad, resulta decisiva para evitar lagunas de cobertura en incidentes de larga latencia o tardía manifestación, y debe ser objeto de especial atención en la renovación o el cambio de asegurador.

3.3.4. Las garantías y las cargas de conducta del asegurado.

Las garantías han sido históricamente utilizadas en los seguros y se conciben técnicamente como la promesa en virtud de la cual la parte asegurada se obliga a hacer o no determinada cosa, o a cumplir determinada exigencia, o mediante la cual afirma o niega la existencia de determinada situación de hecho. Sea o no la garantía sustancial al riesgo asegurado, su incumplimiento es severamente sancionado, porque faculta al asegurador para dar por terminado el contrato desde el momento de la infracción en aquellos eventos en los que la garantía debe cumplirse con posterioridad a la celebración del contrato o genera la nulidad de este cuando su cumplimiento deba ser coetáneo con la celebración del seguro.

En los clausulados de ciberseguro es habitual la incorporación de garantías relativas al mantenimiento de los controles de seguridad declarados en la solicitud: la conservación de copias de respaldo (back ups) con determinada periodicidad y segregación, la vigencia de soluciones de protección de *endpoints*, la aplicación oportuna de parches críticos o el uso de autenticación multifactor para accesos remotos.

El hecho de que las sanciones por incumplimiento de las garantías operen con independencia de la relación causal entre el incumplimiento y el siniestro exige del asegurado una gestión contractual rigurosa y, del asegurador, una redacción precisa que distinga entre verdaderas garantías, condiciones de cobertura (en aquellos ordenamientos jurídicos en los que exista dicha categoría) y simples cargas informativas, distinción de la que dependerá el efecto jurídico del incumplimiento.

4. Coberturas más comunes para los riesgos cibernéticos.

4.1. Amparos de primera parte.

4.1.1. Pérdida de información o datos.

Esta cobertura comprende, en términos generales, los costos, gastos y expensas en que deba incurrir el asegurado debido a la configuración de un evento asegurado que produzca, entre otros, daño, alteración, corrupción, destrucción, pérdida, fuga, copia no autorizada, hurto o apropiación de la información, tal y como lo ha afirmado la doctrina especializada:

1. Costos y/o gastos incurridos para restablecer o reemplazar los datos, incluidos materiales, tiempo de trabajo extra de empleados del asegurado y/o gastos generales en las instalaciones afectadas, asociados como ya se indicó con el restablecimiento o remplazo de los elementos afectados, o como bien lo resumen la norma ISO/IEC 27102:2019(E), al indicar que bajo este amparo se entienden cubiertos los: “(...) *costos de sustitución o reparación de la información impactada mediante la restauración, actualización, recreación o sustitución al mismo estado en que se encontraba la información antes de la pérdida, robo o daño*” (Traducción libre)²³.
2. La contratación de expertos, esto es: investigadores, auditores forenses, etc., para establecer a ciencia cierta la causa, extensión y consecuencias de cualquier evento objeto de cobertura. Esta cobertura obedece al hecho de que el entorno tecnológico en el que se presentan los eventos de cobertura en sí mismo requiere, por su propia naturaleza y particularidades, de conocimientos de especial naturaleza técnica que normalmente no tiene la parte asegurada, lo que dificulta la acreditación de la ocurrencia de un siniestro y la cuantía de la pérdida tal como lo prevén las normas del contrato de seguro, por lo que es de gran utilidad para la parte asegurada contar con ese soporte profesional.
3. Costos y/o gastos para el manejo, respuesta y contención. Se cubren gastos incurridos para el alquiler de equipos, servicios o mano de obra de obra externa, así como los costos de operaciones adicionales -incluidas horas extras del equipo y gastos en que se incurra para la reactivación o continuidad de las operaciones del asegurado-. Este tipo de erogaciones cumple una doble función, porque permiten restablecer la operación del asegurado y a su vez reducen o mitigan cualquier pérdida por lucro cesante derivado de la interrupción del negocio.
4. La contratación de expertos y equipos para eliminar, remover y/o contener la amenaza cuando ello resulte procedente y/o, en general, para prevenir la extensión y propagación de una pérdida. Para que se puedan realizar estas acciones es indispensable que, como parte de la gerencia de riesgo, el asegurado tenga identificados los posibles proveedores de estos servicios, tal y como se sugiere expresamente por la norma ISO/IEC 27102:2019(E), en su sección 6.6. (Vivas & Bedoya, 2022).

Finalmente, con relación a cada uno de los tipos de gastos descritos, el otorgamiento de todos y cada uno de ellos y su alcance dependerá del texto de la póliza y lo usual es que ese tipo de coberturas esté sujeto a sublímites específicos y además de exigirse que se trate de gastos necesarios y razonables, solo se reconocerá su pago si se ha solicitado, para incurrir en ellos, previa autorización de la compañía de seguros.

4.1.2. Pérdidas consecuenciales por interrupción del negocio.

Resulta de la mayor importancia la cobertura de las pérdidas consecuenciales derivadas de la interrupción (total o parcial) del negocio como consecuencia de los eventos o riesgos cibernéticos

²³ Debe precisarse que, por regla general no se incluye el costo de reemplazo o el valor de los equipos (hardware) que han sufrido un daño material porque ese tipo de pérdidas normalmente debe ser solventada por productos tradicionales de daños a propiedad, específicamente de equipo eléctrico y electrónico. Sin embargo, en algunos productos disponibles en el mercado se procede con el reemplazo del hardware si un experto determina que el reemplazo de los equipos es la forma más eficiente y económica para descontaminar o reconfigurar el sistema informático.

asegurados en la póliza de seguro. Si bien no existe uniformidad en el mercado respecto del alcance de esta cobertura, es habitual que se brinde cobertura durante un periodo indemnizable para la pérdida de utilidad bruta del asegurado resultante de la interrupción del negocio con ocasión de un incidente cibernético cubierto.

Debe destacarse que, atendiendo a la realidad actual, en la cual muchos servicios de administración y custodia de datos e información son contratados con terceros proveedores especializados, es igualmente relevante, de acuerdo con las necesidades específicas de cada asegurado, que se revise la necesidad de contratación del amparo de “lucro cesante contingente”, es decir, aquella cobertura para pérdidas consecuenciales del asegurado, derivadas del cese o interrupción de actividades del tercero proveedor de dichos servicios tecnológicos necesarios para su propia operación. Esta cobertura normalmente requerirá de contratación expresa y en ocasiones de pago de prima adicional.

4.1.3. Ciberextorsión – ransomware.

Esta cobertura se encuentra encaminada a amparar al asegurado frente a los costos, gastos o sumas de dinero que se vea constreñido a pagar el asegurado como resultado de una amenaza creíble de parte de un tercero que pretenda dañar, restringir o afectar el sistema informático del asegurado o divulgar información copiada o robada al asegurado, a menos que se proceda con el pago de un rescate o extorsión.

Conforme al numeral 6.3.5. de la norma ISO/IEC 27102:2019(E), pueden ser consideradas como extorsión cibernética las siguientes acciones o conductas:

- “a) haciendo inaccesible la información del asegurado a través del cifrado por malware;*
- b) emprender o amenazar con llevar a cabo un ataque informático, denegación de servicio, o introducir malware en los sistemas de información del asegurado;*
- b) (sic) suprimir, difundir, divulgar o utilizar la información almacenada en los sistemas de información del asegurado;*
- c) dañar, destruir o alterar los sistemas de información del asegurado, y*
- d) solicitar un rescate para descifrar información”.*

Debe anotarse que en algunos ordenamientos jurídicos podría restringirse la posibilidad de aseguramiento del pago de extorsiones o rescates a cibercriminales, pues se considera que ese tipo de acciones fomenta las actividades delictivas lo cual podría poner en entredicho la validez de este amparo en particular.

4.1.4. Terrorismo Cibernético.

Conforme lo indica la doctrina especializada, se trata de un riesgo caracterizado por su severidad, circunstancia que conlleva a que este generalmente excluido de la cobertura otorgada bajo los productos básicos existentes en el mercado internacional. Sin embargo, en aquellos casos en que se otorga mediante anexo específico y/o condición particular, su alcance suele circunscribirse o limitarse a la cobertura de pérdidas derivadas de un “acto de terrorismo” perpetrado a través de medios cibernéticos, pudiendo variar la cobertura en lo atinente a si se extiende o no a los costos y gastos relativos al restablecimiento de la operación y/o contención de la amenaza, así como a la interrupción del negocio.

Debe anotarse que, esta cobertura, presenta en todo caso la dificultad práctica, ampliamente abordada por la doctrina internacional, de la ausencia o inexistencia de una definición universalmente aceptada de los conceptos de “terrorismo” y/o “acto de terrorismo” de forma que resulta indispensable que estos sean claramente delimitados en el condicionado con miras a evitar ulteriores discusiones

respecto del alcance del amparo, siendo en todo caso común encontrar que en algunos productos nacionales se define el terrorismo cibernético como cualquier acto realizado por un individuo o grupo de personas usando sistemas informáticos y que dañe, interrumpa, acceda o destruya el sistema informático del asegurado con objetivos religiosos, ideológicos o políticos con el fin de influir en un gobierno o provocar temor en la población o en una parte de esta (Vivas & Bedoya, 2022).

4.2. Amparos de tercera parte o de responsabilidad.

Mediante este amparo se cubre la indemnización de perjuicios causados a terceros ya sea por una violación de confidencialidad o privacidad de datos e información bajo custodia del asegurado o en general, por un incidente cibernético en el sistema informático del asegurado que cause daño, alteración, destrucción, acceso no autorizado o divulgación no autorizada de datos de un tercero o la interrupción o degradación de servicios del sistema informático.

La norma ISO/IEC 27102:2019(E) establece y/o considera la existencia de esta tipología de amparos como parte de los “Seguros de Ciber” en los siguientes términos:

“6.3.3. Responsabilidad Civil

Un incidente cibernético puede conducir a costos de responsabilidad para el asegurado a través de la indemnización por pérdidas a terceros. Ejemplos de esa responsabilidad pueden ser:

a) los daños causados por un incidente cibernético en el asegurado que afecte a personas u otras organizaciones; (...) c) Violación de datos de información personal, de clientes o de proveedores”
(Traducción propia)

En este escenario, es posible afirmar que se trata de una cobertura enmarcada por los regímenes de responsabilidad civil y administrativa de protección de datos personales, así como aquellos que rigen el desarrollo y/o ejecución de actividades sensibles como la financiera y bursátil.

A continuación, se describirá el alcance de la protección frente a pérdidas causadas a terceros que normalmente otorgan los productos ciber:

4.2.1. Indemnización de perjuicios.

Esta cobertura corresponde a la cobertura básica de todo seguro de responsabilidad civil, encontrándose encaminada a cubrir los perjuicios que el asegurado haya causado a terceros y por los cuales esté legalmente obligado a indemnizar o reparar, específicamente en materia de seguros ciber se cubre la responsabilidad por los siguiente s eventos

4.2.2. Responsabilidad por la publicación, revelación o exposición de información de terceros.

Para efectos de esta cobertura, el riesgo cubierto se encuentra determinado, en el grueso de los productos existentes en el mercado, no sólo por la responsabilidad civil del asegurado a la luz del ordenamiento jurídico aplicable, sino también por el hecho de que esta derive de la publicación, revelación o exposición de información sensible de terceros que se encuentre bajo custodia del asegurado y que haya sido realizada tanto sin autorización del titular, como en razón de un acto u omisión negligente del asegurado. Así mismo, el riesgo cubierto estará determinado por el hecho que efectiva y realmente se produzca y/o cause un daño al tercero titular de la información que tenga la posibilidad de materializarse como consecuencia, entre otras, de la violación de derechos de privacidad, intimidad o propiedad, la configuración de actos de plagio o apropiación indebida de

propiedad intelectual y/o la configuración de una afectación al buen nombre comercial y/o el derecho de imagen.

4.2.3. Responsabilidad civil o administrativa derivada de violaciones de seguridad o de privacidad.

Con cargo a esta tipología de cobertura se suelen amparar, en la práctica, los reclamos formulados contra el asegurado por la responsabilidad en que incurra como consecuencia de actos u omisiones negligentes, en relación con la obligación de evitar o prevenir violaciones de seguridad y/o privacidad; pérdida de información de empleados o terceros; la no divulgación o comunicación a los interesados de una violación de seguridad; la no destrucción de información -que posteriormente sea expuesta con ocasión de un evento cibernético- cuando estaba obligado a hacerlo de acuerdo con la ley sustancial vigente; y/o la materialización de cualquier acto encaminado a obtener la información de una persona mediante engaño o fraude que resulte en el hurto, pérdida, alteración, copia, corrupción o destrucción de información o datos de terceros, y/o en la transmisión de códigos maliciosos o virus a sistemas de terceros y/o en la divulgación de información confidencial (Vivas & Bedoya, 2022).

4.2.4. Gastos y costos de defensa.

Esta cobertura se encuentra encaminada a amparar los costos y gastos en que pueda incurrir el asegurado para su defensa frente a reclamaciones en su contra formuladas y/o presentadas por parte de terceros. Esta cobertura puede, según el texto del producto aplicable, circunscribirse únicamente al pago de honorarios de abogados o extenderse a otros costos y gastos como la consecución de pruebas – e.g. informes técnicos, peritajes, etc.- y/o el otorgamiento de cauciones. Debe observarse que por regla general la procedencia de esta cobertura se encuentra supeditada a la autorización previa, expresa y por escrito del asegurador respecto del apoderado y el valor de sus honorarios. Finalmente, debe anotarse que de conformidad con los productos consultados -mismos que se desarrollan en la sección pólizas de la bibliografía- la cobertura de gastos de defensa se extiende tanto a procesos civiles de responsabilidad en estricto sentido, como también a procesos, generalmente, de tipo administrativo sancionatorio, incluso en aquellos eventos en los cuales no se brinde o no se pueda brindar cobertura a las sanciones o multas que puedan imponerse en dicho trámite administrativo.

4.2.5. Multas y Sanciones impuestas al asegurado.

Se encuentra encaminado a cubrir la materialización de un ataque o incidente cibernético puede conllevar, dependiendo del marco legal aplicable a cada país, la imposición de sanciones de diversa índole al asegurado, siendo este escenario de riesgo uno de los amparos más importantes y que mayor conciencia de la necesidad de protección y apetito por el producto han generado. En efecto, muchos ataques de la tipología objeto de estudio no producen y/o generan una consecuencia y/o efecto palpable e inmediato, por ejemplo, conforme se describe por la literatura, un ataque ligado a la sustracción de información, que aun cuando sea pública o al menos no privada o confidencial, pueda ser visto como un incumplimiento de las obligaciones de seguridad, privacidad o integridad de la información de terceros que pueden producir la imposición de una sanción, multa o penalidad (Vivas & Bedoya, 2022)

5. Exclusiones usuales en materia del seguro de riesgos cibernéticos.

Dentro de las exclusiones más usuales en este tipo de seguros se encuentran las siguientes, advirtiendo que algunas exclusiones son comunes a todos los amparos del producto ciber y otras únicamente aplican para algunos de los amparos arriba descritos, pero no para todos.

5.1.Exclusiones comunes a cualquier tipo de cobertura.

Con independencia de que se trate de amparos para pérdidas de primera o tercera parte, es posible afirmar que bajo los productos existentes en el mercado se excluyen de cobertura todas aquellas pérdidas o reclamaciones derivadas o relacionadas con los siguientes eventos:

- a) La falla del asegurado o de aquellos que actúan en nombre del asegurado, en dar mantenimiento a cualquier servidor, computador, sistema de cómputo, o red, software de computador, hardware o cualquier otro equipo similar.
- b) El uso y desgaste habitual, disminución en el rendimiento, deterioro progresivo, o envejecimiento de equipo electrónico y otra propiedad, software o hardware de computador utilizado por el asegurado.
- c) Fallas de satélite; fallas eléctricas o mecánicas y/o interrupción incluyendo, pero no limitado a, perturbaciones eléctricas, picos, baja de voltaje o apagón; y los cortes de gas, agua, teléfono, cable, telecomunicaciones, u otra infraestructura. Es posible obtener el levantamiento parcial de esta exclusión, pero, restringido a las infraestructuras que se encuentren bajo el control operacional del asegurado.
- d) Fuego, humo, explosión, rayo, viento, agua, inundación, terremoto, erupción volcánica, marejada, deslizamiento, granizo, fuerza mayor, o cualquier otro evento físico sin importar la causa.
- e) Huelgas, cesación de labores de hecho o cualquier otro evento similar de acuerdo con la ley aplicable al contrato de seguro, a menos que expresamente se incluya dentro de las coberturas del seguro.
- f) Terrorismo.
- g) Uso de programas no operacionales, en prueba, no recibidos completa y a satisfacción del asegurado o que sean ilegales, no-licenciados o que violen de normas o leyes relativas a la protección del software.
- h) Propiedad intelectual o la infracción real o supuesta, directa o indirecta, de cualquier patente o la malversación, hurto, copiado, exhibición o publicación de cualquier secreto comercial por, o con la cooperación activa, participación, o asistencia de cualquier asegurado o sus empleados.
- i) Contaminación.
- j) Cualquier acto voluntario, premeditado o doloso del Asegurado y/o que implique la realización de actividades ilegales, criminales y/o fraudulentas realizadas por el Asegurado.
- k) Guerra, invasión, acto de enemigo extranjero, hostilidades u operaciones de guerra (bien sea declarada o no), guerra civil, motín, conmoción civil que asuma las proporciones de o escale a un levantamiento popular, levantamiento militar, insurrección, rebelión, revolución usurpación del poder o usurpación del poder militarmente.

- l) Competencia desleal, violaciones antimonopolio, prácticas engañosas de comercio, o la restricción del comercio o restricción de la competencia estatuto legislación, o regulación antimonopolio;
- m) Daños a la reputación o al buen nombre (“Good Will”) del Asegurado. Lo anterior sin perjuicio de las coberturas de costos o gastos intentar evitar que esto suceda.
- n) Lucro cesante del Asegurado.
- o) La existencia, emisión, o descarga de cualquier campo electromagnético, radiación electromagnética, o electromagnetismo.

5.2. Exclusiones propias del esquema de responsabilidad civil o de tercera parte.

Para las coberturas de Tercera Parte, es usual encontrar que no se brinda cobertura a las reclamaciones provenientes directa o indirectamente de:

- a) Actividades dolosas del asegurado haciendo precisión que ello no excluye necesariamente los actos dolosos de sus empleados.
- b) Un hecho, circunstancia o acto u omisión negligentes cometido, ocurrido con anterioridad a la fecha retroactiva pactada en la póliza.
- c) Cualquier reclamación derivada de un acto u omisión erróneos o negligentes ocurridos con anterioridad al inicio de la vigencia de la póliza, si el asegurado conocía o pudo haber previsto razonablemente que tales actos, hechos, o circunstancias podrían dar lugar a una reclamación cubierta por la póliza;
- d) Cualquier reclamación o circunstancia que pudiera dar lugar a tal reclamación notificada a o bajo cualquier otro seguro antes del inicio de vigencia de esta póliza;
- e) Lesiones corporales, cualquier tipo de perjuicio de tipo extrapatrimonial como el daño moral, a menos que expresamente se incluya en las coberturas.
- f) Perjuicios sancionatorios o punitivos, multas o sanciones a menos que sean expresamente aseguradas y ello sea legalmente válido.
- g) Cualquier reclamación que surja directa o indirectamente o sea resultante de transferencias o hurto de dineros, títulos valores o propiedad tangible de otros bajo cuidado, custodia o control del asegurado o;
- h) La responsabilidad del asegurado asumida bajo cualquier contrato o acuerdo escrito excepto y en la medida en que el asegurado hubiera sido responsable en ausencia de tal contrato o acuerdo.

6. Breves consideraciones en punto del seguro paramétrico de riesgos cibernéticos.

6.1. Noción, funcionamiento y diferencias con los esquemas de aseguramiento tradicional.

El seguro paramétrico —también denominado seguro por índice— es una modalidad de aseguramiento en la cual el pago de la prestación no se determina mediante el ajuste de la pérdida

efectivamente sufrida por el asegurado, sino por la verificación objetiva de un parámetro o índice predefinido en el contrato, correlacionado técnicamente con el riesgo asegurado. Materializado el índice —por ejemplo, la superación de cierta magnitud sísmica, un déficit de precipitaciones o, en el ámbito que aquí interesa, de cierto número de horas de indisponibilidad de un servicio digital—, el asegurador paga la suma o la escala de sumas preestablecidas, sin necesidad de inspección, peritaje, ni discusión sobre la cuantía del daño y/o su efectiva materialización.

Surgida en los mercados de riesgos catastróficos naturales y agropecuarios, esta tipología contractual en materia de seguros ofrece tres (3) ventajas características frente a los esquemas de seguro tradicionales: la rapidez del pago, que puede efectuarse en días y no en meses; la transparencia y previsibilidad de la cobertura, al eliminarse buena parte de las controversias de ajuste; y la reducción de los costos de transacción asociados a la verificación de la pérdida. Su contrapartida estructural es el denominado riesgo de base (Basis risk), esto es, la posibilidad de desajuste entre el pago detonado por el índice y la pérdida real, lo que puede conducir a que el asegurado reciba un pago superior o inferior al daño efectivamente sufrido, o incluso sufra una pérdida sin que el índice se realice, riesgo cuya administración constituye el problema técnico y jurídico central de la modalidad.

Trasladada al universo cibernético, la lógica paramétrica encuentra su terreno natural en aquellos eventos cuya ocurrencia y duración pueden medirse de manera objetiva, continua y verificable por terceros independientes. El ejemplo paradigmático se encuentra determinado por la interrupción de servicios de computación en la nube, de redes de distribución de contenidos, de pasarelas de pago o de plataformas de comercio electrónico; todos estos casos en los que la indisponibilidad del servicio es un hecho técnicamente observable mediante sistemas de monitoreo permanente, lo que permitiría definir, por ejemplo, el detonante de la cobertura como un período de caída superior a un deducible o franquicia temporal pactada —medida en minutos u horas— y la contraprestación indemnizatoria como una suma fija o escalonada por unidad de tiempo de interrupción.

En el mercado de Londres algunas agencias de suscripción, en su condición de *coverholders* de Lloyd's, comercializan seguros paramétricos contra interrupciones de la nube y de la cadena de suministro digital, soportados en plataformas propias que monitorean de manera continua diversos servicios de software, plataforma e infraestructura, así como múltiples centros de datos a nivel mundial, utilizando estos datos para tarifar el riesgo, verificar en tiempo real la realización del índice detonante de cobertura y liquidar los pagos en forma expedita (Lloyd's, s.f.; Parametrix, 2024). Por su parte, otros productos integran el componente paramétrico de interrupción digital a pólizas de seguro para riesgos cibernéticos “convencionales”, configurando estructuras híbridas en las que la “sección de interrupción contingente del negocio” se liquida por índice mientras los restantes amparos conservan su naturaleza indemnizatoria (Reinsurance News, 2024).

6.2. El incidente CrowdStrike como justificación empírica de la incorporación del esquema de aseguramiento paramétrico a los seguros para riesgos cibernéticos.

“Insurers often need more time and money to accurately identify risks than the period over which the attack itself occurs and the amount attackers charge to maintain data integrity” (Gumenyuk, 2021, Pág. 34)

La incorporación o comercialización de los seguros para riesgos cibernético bajo esquema paramétrico se justifica, entre otras, en eventos como el apagón informático global del 19 de julio de 2024, originado en una actualización defectuosa del software de seguridad de *CrowdStrike* que implicó y/o conllevó la inutilización y/o afectación de millones de dispositivos Windows a nivel mundial. Los análisis técnicos de dicho evento, conforme a lo informado por Cybersecurity Dive (2024), ubicaron la pérdida financiera directa de las compañías que integran el Fortune 500 —

excluido Microsoft— en alrededor de Cinco Mil Cuatrocientos Millones de Dólares (USD\$5.400.000.000) y calcularon que porcentualmente sólo entre el diez (10%) y el veinte por ciento (20%) de esas pérdidas resultaría cubierto por una Póliza de Seguro para Riesgos Cibernéticos, en razón de las elevadas retenciones, los sublímites de interrupción contingente, y los deducibles o franquicias temporales pactadas.

Este evento resulta sumamente ilustrativo -en materia del contrato de seguros que nos convoca- puesto que, de un lado, demostró que los eventos sistémicos de interrupción digital no requieren intención maliciosa —basta un error operacional como fue el caso, sin presencia de un ataque—, lo que reafirma la amplitud de la taxonomía expuesta en la sección primera del presente documento; del otro, evidenció la brecha entre la pérdida económica sufrida y la pérdida asegurada bajo un esquema tradicional, brecha que las pólizas con estructura paramétrica, con detonantes claros y pagos rápidos, están específicamente diseñadas para reducir²⁴.

6.3. La habilitación normativa en Colombia para la suscripción de seguros paramétricos y su compatibilidad con el principio indemnizatorio.

Hasta hace pocos años, la viabilidad del seguro paramétrico en los ordenamientos de tradición continental suscitaba reservas fundadas en el principio indemnizatorio: si el seguro de daños es un contrato de mera indemnización que jamás puede constituir fuente de enriquecimiento para el asegurado, un pago detonado por un índice, sin necesidad de comprobación de una pérdida física o real y de su correspondiente ajuste, parecía difícilmente conciliable con esa regla por demás de carácter imperativo en buena parte de los ordenamientos latinoamericanos. El legislador colombiano despejó el impedimento para la comercialización de seguros paramétricos y, por contera, para la suscripción de riesgos cibernéticos bajo modalidad paramétrica, en dos (2) etapas. Primero, el artículo 176 de la Ley 1955 de 2019 autorizó expresamente la modalidad paramétrica o por índice para el seguro agropecuario²⁵.

En un segundo momento, la Ley 2294 de 2023, contentiva del Plan Nacional de Desarrollo 2022-2026, generalizó la habilitación al adicionar mediante:

1. Su artículo 241 el artículo 183 del Estatuto Orgánico del Sistema Financiero para incluir la expedición de seguros paramétricos o por índice entre las operaciones autorizadas a las

²⁴ En el plano de la transferencia alternativa de riesgos, la lógica de los detonantes objetivos se ha extendido también al mercado de capitales. Desde la emisión del primer bono de catástrofe cibernética en enero de 2023, el mercado de valores vinculado a seguros ha canalizado capacidad creciente hacia el riesgo cibernético de cola. Por ejemplo, el programa PoleStar Re de Beazley habría acumulado, entre 2023 y 2025, Seiscientos Setenta Millones de Dólares (USD\$600.000.000) en bonos de catástrofe cibernética dentro de una torre de protección de exceso de pérdida superior a los Mil Millones de Dólares (USD\$1.000.000.000) (Reinsurance News, 2025; Artemis 2025). Aunque es posible intuir que buena parte de estas estructuras emplea detonantes de indemnización sobre la cartera del cedente, su desarrollo confirma la tendencia del mercado hacia mecanismos de transferencia basados en eventos definidos con precisión y verificables por terceros, tendencia de la cual el seguro paramétrico es la expresión más acabada en la relación directa con el asegurado.

²⁵ Al respecto, consagra la norma en cuestión en modificación del artículo 1° de la Ley 69 de 1993: “*Establézcase el seguro agropecuario en Colombia, como instrumento para incentivar y proteger la producción de alimentos, buscar el mejoramiento económico del sector agropecuario, promover el ordenamiento económico del sector agropecuario y como estrategia para coadyuvar al desarrollo global del país (...) Parágrafo Primero. **El seguro agropecuario podrá ofrecerse bajo la modalidad de seguro paramétrico, de manera que el pago de la indemnización se hará exigible ante la realización de un índice definido en el contrato de seguro. Esta modalidad de seguro podrá ser tomada por cualquier persona natural o jurídica de derecho privado o de derecho público.** En este último caso, la entidad de derecho público podrá actuar como tomador, asegurado y/o beneficiario del seguro agropecuario paramétrico, asumir el pago de la prima del seguro y disponer de los recursos recibidos por concepto de indemnización para resarcir a las personas o infraestructura afectada por el riesgo amparado en el seguro. En este último caso, tal erogación se entenderá como gasto público social (...)*” (Destacado fuera del texto original).

aseguradoras, exigiendo que el índice esté correlacionado con el riesgo asegurado y que el valor de la indemnización corresponda al monto definido en la póliza;

2. Su artículo 242 el artículo 1088 del Código de Comercio, consagrando y/o estableciendo que en el seguro paramétrico el pago por la ocurrencia del riesgo asegurado se hará efectivo con la realización del índice o los índices definidos en el contrato correlativo; y
3. Su artículo 243 el artículo 1077 del Código de Comercio, estableciendo que la ocurrencia del siniestro y su cuantía quedarán demostradas con la realización del índice, conforme al modelo utilizado en el diseño del seguro. La Superintendencia Financiera ha precisado, por su parte, que el seguro paramétrico no constituye un ramo autónomo sino una modalidad de aseguramiento utilizable en los distintos ramos autorizados (Brigard Urrutia, 2024), lo que, en nuestra consideración, abre formalmente la puerta a su empleo en el ramo de riesgos cibernéticos.

De esta forma, debe indicarse igualmente que la armonización con el principio indemnizatorio se deriva, en el ordenamiento colombiano, de la noción de correlación técnica: el índice detonante debe guardar una debida correlación con el daño o la pérdida que el siniestro ocasionaría, de modo que la prestación paramétrica opere como una valoración anticipada y razonable del perjuicio y no como una apuesta²⁶. En este contexto, para el mercado latinoamericano, y el colombiano en particular, la modalidad paramétrica ofrece un potencial significativo precisamente en los segmentos donde el Seguro para Riesgos Cibernéticos ha penetrado menos, como sería el caso de las pequeñas y medianas empresas, cuya capacidad de soportar procesos de ajuste complejos es limitada y cuya pérdida como consecuencia de un evento de interrupción digital podría ser relativamente homogénea y modelable. Un producto de detonante simple —caída de la plataforma de pagos o del proveedor de nube por encima de cierto umbral— con pago automático reduce drásticamente los costos de distribución y liquidación, facilitando a su vez la comercialización digital masiva y también un componente muy especial de estos productos que son los gastos expertos para manejo del incidente, manejo de crisis y restablecimiento de la operación. Para las grandes empresas y las entidades estatales, la cobertura paramétrica de interrupción contingente puede complementar los sublímites estrechos del seguro tradicional frente a “*eventos sistémicos*” de proveedores compartidos -entendidos como incidentes, situaciones o fallos que afectan a la totalidad de un sistema-, hipótesis cuya relevancia regional se demostrado con el ataque a IFX Networks analizado previamente y con ocasión del cual, centenares de empresas privadas a nivel latinoamericano sufrieron interrupciones simultáneas perfectamente medibles en su duración.

El seguro paramétrico cibernético es idóneo para los riesgos de interrupción y degradación de servicios, que admiten medición objetiva, pero no lo es para aquellas coberturas cuya esencia es la

²⁶ De allí que se sigan consecuencias prácticas relevantes para la estructuración de un contrato de seguro para riesgos cibernéticos bajo esquema paramétrico. La primera es la exigencia de un soporte actuarial robusto que vincule el parámetro —horas de indisponibilidad, degradación y/o afectación medible del servicio, número de registros comprometidos verificado por un tercero, etc.— con la pérdida esperada del asegurado, soporte que deberá documentarse en el diseño técnico del producto y conservarse para efectos de supervisión. La segunda es la persistencia del interés asegurable como requisito esencial: aun cuando la cuantía no se ajuste, el asegurado debe tener un patrimonio efectivamente expuesto al evento medido por el índice, lo que excluye la contratación meramente especulativa sobre caídas de servicios ajenos. La tercera es la centralidad contractual de la definición del índice, de su fuente de medición y del procedimiento de verificación: la designación de un agente de cálculo independiente, la publicidad de la metodología, las reglas sobre indisponibilidad del propio sistema de medición y los mecanismos de impugnación técnica deben quedar estipulados con precisión, pues en esta modalidad la controversia se desplaza del ajuste de la pérdida a la realización y medición del parámetro. Y la cuarta es la administración transparente del riesgo de base, que exige del asegurador y del intermediario un deber calificado de información precontractual acerca de la posibilidad de que la pérdida real no coincida con el pago detonado, so pena de comprometer los estándares de protección al consumidor financiero.

“heterogeneidad” del daño: la responsabilidad civil frente a terceros, los gastos de defensa, la gestión de una filtración de datos personales o el manejo de una extorsión que exigen el acompañamiento experto y el ajuste individualizado propios del esquema indemnizatorio del producto tradicional. De ahí que la arquitectura razonable no sea la sustitución de los productos para riesgos cibernéticos actualmente comercializados en América Latina por productos bajo esquema paramétrico, sino la complementariedad a partir de la implementación de programas híbridos en los que el componente paramétrico aporta liquidez inmediata para la interrupción del negocio —propia y contingente—, y gastos para la mitigación de la crisis o del incidente, mientras que se conservan bajo esquemas tradicionales de comprobación y ajuste de la pérdida los demás amparos con especial énfasis en aquellos atinentes a la responsabilidad. A ello se suman retos operativos propios de la región: la dependencia de infraestructuras de monitoreo y de agentes de cálculo radicados en el exterior, la necesidad de que los índices reflejen la realidad de la conectividad local, y la conveniencia de que la regulación secundaria desarrolle los estándares de gobernanza del índice —independencia, auditabilidad y continuidad de la medición— que la habilitación legal colombiana dejó deferidos al Gobierno Nacional.

En suma, la habilitación general del seguro paramétrico sitúa a Colombia entre las jurisdicciones latinoamericanas mejor posicionadas para el desarrollo de soluciones cibernéticas por índice, al haber resuelto legislativamente la tensión con el principio indemnizatorio que en otros ordenamientos de la región permanece abierta y librada a la interpretación. De esta forma, el desafío es de ejecución, esto es construir, índices locales confiables, asegurar la gobernanza independiente de la medición, calibrar el riesgo de base con información regional y educar al mercado sobre la naturaleza y los límites de la modalidad, de suerte que el paramétrico cumpla su promesa de liquidez y simplicidad sin degradar los estándares de protección del asegurado que informan el derecho de seguros latinoamericano.

7. Algunas notas finales: consideraciones respecto de las complicaciones de suscripción del ramo, el aseguramiento de riesgo silente y la existencia de servicios complementarios.

7.1. El riesgo cibernético silente y la delimitación afirmativa.

Conforme se analizó en precedencia, el Seguro para Riesgos Cibernéticos ofrece una gama de servicios o coberturas que tienen como objetivo minimizar los impactos adversos para las persona u organizaciones derivados de incidentes cibernéticos, a partir de la cobertura mediante “(...) *tres categorías diferentes de cobertura cibernética (...): (1) pólizas cibernéticas independientes, (2) cobertura cibernética como parte de un producto de seguro tradicional existente, y (3) Cobertura cibernética silenciosa en forma de pólizas sin exclusiones o vacíos en las exclusiones explícitas (...)*” (Schutz et al, 2023, Pág. 523). Esta última tipología de riesgo, también conocida como “riesgo no afirmativo”, se entiende materialmente como la exposición a pérdidas de origen cibernético embebida en pólizas tradicionales —sea de daños, de responsabilidad civil, de transporte, de lucro cesante o cualquier otra— que ni la otorgan, ni la excluyen expresamente. Los litigios de NotPetya se ventilaron, precisamente, bajo pólizas de daños todo riesgo y no bajo seguros de riesgos cibernéticos, evidenciando la magnitud de la exposición no tarifada de las carteras tradicionales en ausencia de una exclusión expresa.

El análisis cualitativo de Wrede, Stegen y Graf von der Schulenburg (2020) sobre productos del mercado alemán documentó la extensión del fenómeno y la necesidad de estrategias de clarificación contractual. Eventos como este han impulsado la adopción de políticas de delimitación afirmativa: cada póliza debe indicar con claridad si cubre o excluye las pérdidas de origen cibernético. Para el mercado colombiano y latinoamericano, donde conviven clausulados antiguos con productos de nueva generación, la revisión sistemática de las carteras tradicionales en busca de exposición silente constituye una tarea pendiente tanto de los aseguradores, en su gestión técnica, como de los

supervisores, en su vigilancia prudencial, y de los asegurados y sus intermediarios, en la arquitectura coherente de sus programas de seguros, a fin de evitar tanto vacíos como duplicidades de cobertura²⁷.

Como ejemplo práctico de las tensiones generadas por la incorporación posterior de exclusiones cibernéticas en pólizas tradicionales, puede mencionarse la discusión surgida en Colombia respecto del clausulado de las pólizas Todo Riesgo Construcción exigidas por la Agencia Nacional de Infraestructura (ANI) en los contratos de concesión de cuarta y quinta generación. Dichos clausulados hacían parte de la documentación contractual bajo el Apéndice Financiero 3 y servían como referente obligatorio para la contratación de los seguros por parte de los concesionarios. No obstante, en sus versiones originales no contemplaban una exclusión expresa para riesgos de origen cibernético en los términos actualmente utilizados por el mercado asegurador.

Durante varios años las pólizas fueron emitidas conforme a esas condiciones. Sin embargo, en procesos recientes de renovación y prórroga, las aseguradoras comenzaron a incorporar exclusiones generales de riesgos cibernéticos, en línea con las exigencias del mercado reasegurador internacional. Esta situación dio lugar a discrepancias entre la ANI y algunos concesionarios: mientras la entidad consideraba que tales exclusiones modificaban las condiciones previstas contractualmente, los concesionarios sostenían que su incorporación respondía a requisitos indispensables para obtener la cobertura en el mercado. Estas diferencias incluso derivaron en actuaciones administrativas relacionadas con la aprobación de las garantías exigidas contractualmente.

Inicialmente, se dispuso como solución la suscripción de un otrosí para modificar las exigencias del contrato de seguro. No obstante, finalmente, se abordó el asunto en la Circular No. 20263060000174 del 30 de marzo de 2026. En dicho documento, la ANI reconoció que las aseguradoras y reaseguradoras venían exigiendo la incorporación de exclusiones no previstas originalmente en el Apéndice Financiero 3, entre ellas las relativas a riesgos cibernéticos bajo la forma Cyber Loss Limited Exclusion Clause M 5410. Asimismo, con fundamento en la información suministrada por Fasecolda, advirtió que este tipo de exclusiones se ha consolidado como una práctica generalizada del mercado y, en numerosos casos, constituye una condición derivada de los programas de reaseguro, lo que dificulta o incluso imposibilita la obtención de cobertura sin tales limitaciones.

En respuesta a esa realidad de mercado, la ANI adoptó un mecanismo que permite autorizar la incorporación de exclusiones no contempladas inicialmente, siempre que se acredite su utilización generalizada en los mercados asegurador y reasegurador y que no se desnaturalice la finalidad esencial del seguro contratado, consistente en la protección de la infraestructura frente a daños materiales. Para ello, el concesionario debe justificar la necesidad de la modificación y demostrar la imposibilidad de obtener cobertura bajo las condiciones originales, quedando la autorización sujeta al análisis de la interventoría y a la aprobación expresa de la entidad. En todo caso, la incorporación

²⁷ Respecto de esta tipología de riesgos silentes, señalan Vivas, G. & Bedoya, J. (2022) que: “(...) aun cuando en la práctica algunos productos tradicionales pueden ofrecer lo que se ha denominado como coberturas silentes o silenciosas en materia de riesgos cibernéticos, como consecuencia de la interrelación del evento cibernético con un riesgo efectivamente cubierto bajo las mismas como pudiera serlo un incendio producido por una alteración en los datos que regulan el funcionamiento de determinado equipo, lo común es encontrar que el grueso de los clausulados excluyen de forma total o parcial los eventos cibernéticos, siendo esta también una razón para la existencia, en forma autónoma, del negocio jurídico que nos atañe. En efecto, existen a grandes rasgos tres (3) tipos de exclusiones en las pólizas tradicionales de propiedad en relación con los riesgos cibernéticos: 1. Exclusiones generales para todas las pérdidas resultantes de un ciberataque como es el caso de la cláusula CL380, usada con cierta frecuencia en las pólizas de “property”, así como en líneas especiales como marítimo u oil & gas; 2. Exclusiones generales para pérdidas derivadas de tipos específicos de incidentes, verbigracia filtración de información, siendo un claro ejemplo de esta tipología la cláusula “Exclusion - Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability – Limited Bodily Injury Exception Not Included” creada para el mercado de los Estados Unidos por la “Insurance Services Office (ISO)”; y 3. Exclusiones Generales para tipos especiales de pérdidas como las dispuestas en los endosos NMA 2914 (Electronic Data Endorsement C) y NMA2915 (Cláusula de uso general de exclusión de Datos Electrónicos)”.

de estas exclusiones no implica una modificación de la asignación contractual de riesgos, sino una adecuación de las condiciones de aseguramiento a las exigencias técnicas y comerciales vigentes del mercado.

7.2. Retos de asegurabilidad: Asimetría de la información, correlación y riesgo sistémico.

A pesar de la implementación habitual del “*Proposal Form*”²⁸ como parte del proceso de recolección de información para la suscripción de las Pólizas de Seguro para Riesgos Cibernéticos con miras a obtener del asegurado -conocedor principal de los riesgos a los que se encuentra expuesta su actividad y patrimonio- información clara, veraz, completa y precisa del estado del riesgo y necesidades de la operación que permitan a la compañía proceder a la determinación de las coberturas que han de expedirse y los valores asegurados que han de otorgarse²⁹, corresponde indicar que la suscripción del ramo se ve marcada, desde la perspectiva de la teoría económica del seguro, por una tensión frente a varios de los criterios clásicos de asegurabilidad y suscripción (Tsohou et al, 2023), determinada por el hecho de que:

“Hasta la fecha, los métodos tradicionales de evaluación de riesgos han sido insuficientes para las compañías de seguros debido a la ausencia de datos históricos sobre reclamos (Sheehan et al. 2021). Estos altos niveles de incertidumbre significan que las aseguradoras que otorgan cobertura a riesgos cibernéticos están más inclinadas a sobrevalorar la cobertura del riesgo cibernético (Kshetri 2018). La combinación de datos externos con los datos de la cartera de seguros parece, por lo tanto, esencial para mejorar la evaluación del riesgo y, por lo tanto, llevar a una fijación de precios ajustada al riesgo (Bessy-Roland et al. 2021). Este argumento también está respaldado por el hecho de que algunos (re)aseguradores informaron que están trabajando para mejorar sus modelos de precios cibernéticos (por ejemplo, creando o adquiriendo bases de datos a proveedores externos) (EIOPA 2018)” (Traducción libre, Cremer et al., 2022, Pág. 699)

Algunos estudios identifican la existencia de múltiples obstáculos para la adecuada suscripción de este riesgo, entre los cuales destacan como principales la escasez y baja calidad de los datos de pérdidas a nivel histórico, así como la fuerte interdependencia y correlación de los riesgos —que compromete la diversificación del portafolio—, y las severas asimetrías de información que alimentan la selección adversa y el riesgo moral (Biener et al., 2015). Al respecto, han sostenido Schwarcz, D. & Wolff, J. (2025) que:

²⁸ En punto de la implementación del Proposal Form, sin perjuicio de las consideraciones la norma ISO/IEC 27102:2019(E) presenta una recomendación, no taxativa, de la información mínima necesaria que debe ser recopilada de cara a la suscripción de Pólizas de Riesgos Cibernéticos, así: “7.2 Recopilación de información (...) Los datos e información requeridos por el asegurador pueden incluir aquellos indispensables para: a) la comprensión de la misión y del negocio; b) la identificación de los principales interesados, incluidos los clientes y los asociados comerciales; c) la información retenida y procesada [por la compañía]; d) los detalles de los sistemas de información y los arreglos de contratación externa; e) los detalles del [Sistema de Gestión de la Seguridad de la Información (SGSI)]; f) la lista y descripción de los controles de seguridad de la información aplicados; g) los registros de accidentes anteriores; y h) Garantías adicionales de la situación de los controles de seguridad de la información, como los informes de auditoría y los resultados del seguimiento (...)” (Traducción propia).

²⁹ Al respecto, señalan Romanosky et al (2019) que: “(...) si bien a menudo se considera que las compañías de seguros son las únicas organizaciones con capacidad especializada para cuantificar y valorar los riesgos operativos, casi no hay información pública sobre cómo las compañías realmente evalúan -y diferencian- el riesgo cibernético entre empresas e industrias. y, en particular, cómo calculan los precios de las primas del seguro cibernético. Esta falta de transparencia en las políticas y prácticas se cita como uno de los principales obstáculos que impiden la adopción del seguro cibernético, y presenta desafíos significativos para los altos ejecutivos que buscan gestionar los riesgos en sus organizaciones porque no pueden entender y comparar eficazmente las coberturas entre las compañías de seguros. Además, la falta de transparencia impide a esos encargados de adoptar decisiones utilizar esa información para aplicar controles de seguridad que podrían reducir sus costos operacionales y mejorar su situación en materia de seguridad” (Traducción propia)

“Incluso más importante que el desafío de proyectar el riesgo cibernético agregado es la dificultad que enfrentan los aseguradores de riesgos cibernéticos para evaluar la exposición específica al riesgo de los tomadores individuales. Si bien el panorama cambiante de las amenazas y los limitados datos históricos contribuyen a este problema, varios obstáculos adicionales complican los esfuerzos de las aseguradoras para evaluar la exposición de los tomadores de pólizas e identificar cómo fijar el precio de la cobertura en base a los controles y prácticas de seguridad de los asegurados.

Un desafío fundamental es que la experiencia pasada de una empresa a menudo proporciona una base poco confiable para fijar el precio de su exposición al riesgo cibernético. Aunque las filtraciones anteriores pueden parecer señales de una seguridad débil o una vulnerabilidad elevada, esta inferencia suele ser engañosa, ya que la mayoría de los ciberataques son oportunistas en lugar de deliberados. Además, algunas evidencias sugieren que las empresas que experimentan un ciber incidente a menudo invierten más en ciberseguridad como resultado, lo que puede hacer que tengan menos probabilidades de experimentar uno en el futuro³⁰.

(...) Un segundo desafío importante es que las aseguradoras de riesgos cibernéticos han recopilado históricamente solo información limitada sobre la exposición de los solicitantes durante la suscripción. Este proceso normalmente se basa en cuestionarios extensos sobre prácticas de ciberseguridad y, en algunos casos, escaneos automatizados de sistemas. Si bien estos cuestionarios pueden cubrir una amplia gama de temas, rara vez exploran a fondo los controles técnicos de una empresa o cómo se implementan las medidas de seguridad en la práctica. Un análisis de 31 de esos cuestionarios determinó que daban "poca atención" a la infraestructura técnica y empresarial, y su interdependencia con el entorno en que opera el solicitante." Reflejando esta evaluación superficial, los investigadores encontraron que ni las respuestas al cuestionario ni ninguna evaluación integral de la postura de ciberseguridad de una empresa jugaron un papel significativo en la determinación de las primas. En lugar de ello, los factores clave fueron el tamaño de la empresa, medido por el valor del activo o los ingresos, y su sector industrial”.

La literatura sobre modelación económica del ramo ha subrayado igualmente que la correlación de los incidentes —derivada de monocultivos tecnológicos y de proveedores compartidos— y la dificultad de verificar el nivel de autoprotección del asegurado -medidas de seguridad propias y cultura organizacional, entre otras, distinguen estructuralmente a este ramo de los seguros patrimoniales tradicionales (Böhme & Schwartz, 2010; Marotta et al., 2017). A lo anterior se suma el potencial de acumulación catastrófica. Conforme a las estimaciones recogidas por Munich Re (2025) el potencial de acumulación modelado para la industria global, con períodos de retorno de hasta doscientos (200) años, se encuentra entre los veinte mil y los cuarenta y seis mil millones de dólares, cifras que explican la cautela de la capacidad reaseguradora, la generalización de sublímites y la búsqueda de soluciones alternativas de transferencia, incluidos los bonos de catástrofe cibernética emitidos en años recientes.

Para América Latina, estos retos se intensifican por factores propios: la escasez, aún mayor, de datos históricos locales de siniestralidad, el déficit regional de talento especializado en ciberseguridad, la concentración de la infraestructura digital en pocos proveedores y la heterogeneidad de los marcos normativos descrita en el numeral 3.2. Frente a ello, la agenda razonable de desarrollo del ramo comprende la consolidación de deberes de notificación de incidentes que alimenten estadísticas públicas confiables, la promoción de estándares mínimos de higiene y seguridad digital como condición de acceso a la cobertura, la educación del segmento de pequeñas y medianas empresas, y la articulación entre la política pública de seguridad digital y el mercado asegurador, en línea con las

³⁰ Cfr. IBM, Cost of a Data Breach Report 2024 32 (2024), <https://cdn.table.media/assets/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf>.

recomendaciones formuladas por la OCDE (2017) para potenciar el rol del seguro en la gestión del riesgo cibernético.

7.3. Servicios Complementarios.

Finalmente, es menester indicar que una característica distintiva del ramo es la incorporación de servicios de valor agregado que trascienden la función indemnizatoria clásica y propenden a un mejor manejo de los riesgos cibernéticos y sus potenciales consecuencias, tal y como es el caso de la implementación en favor del asegurado de evaluaciones preventivas de postura de seguridad, capacitación del personal, realización de simulacros de respuesta, monitoreo de superficie de ataque y líneas de atención permanente para la gestión temprana de incidentes. Esta dimensión asistencial aproxima en apariencia el seguro para riesgos cibernéticos a un esquema de gestión compartida del riesgo, en el que el asegurador actúa como articulador de un ecosistema de proveedores especializados, y refuerza la tesis —recogida por la propia norma ISO/IEC 27102:2019— de que el seguro complementa, pero no reemplaza, los controles de seguridad de la información y los planes de continuidad del negocio del asegurado.

En punto de estos servicios complementarios, indica la OCDE (2017) que:

“(…) muchas compañías de seguros ofrecen servicios adicionales con sus pólizas, ya sea el asesoramiento en gestión de riesgos durante el proceso de suscripción, como medio para reducir la vulnerabilidad a los incidentes cibernéticos durante la vigencia o con el fin de reducir el impacto de los incidentes cibernéticos que se produzcan. Los dos primeros tipos de servicios se denominan a menudo servicios previos a la materialización del riesgo o servicios de mitigación de riesgos, mientras que el último tipo se identifica como servicios posteriores a la violación o servicios de respuesta. Algunas compañías de seguros han desarrollado una experiencia interna significativa y ofrecen este tipo de servicios directamente, mientras que otras han desarrollado redes y/o asociaciones con una variedad de proveedores de servicios, lo que a menudo implicando algún tipo de precio con descuento para sus asegurados (p. ej., consultores en seguridad de la tecnología de la información, bufetes jurídicos, bufetes de relaciones públicas, etc.) (...).

Como se señaló en la sección anterior, algunas compañías de seguros prestan servicios específicos de evaluación de riesgos como parte del proceso de suscripción (a veces incluso si no se ha establecido una cobertura de seguro) que van desde evaluaciones de seguridad en línea o in situ hasta asesoramiento sobre políticas y prácticas de seguridad, a las exploraciones de vulnerabilidad y pruebas de penetración que deberían beneficiar tanto a la compañía de seguros como a la gestión de riesgos de la compañía (Insurance Information Institute, 2014; Carrier Management, 2016d). Las compañías también están ofreciendo una variedad de servicios de mitigación de riesgos durante la vigencia, incluyendo alertas y detección de amenazas e inteligencia, acceso a tecnologías de protección especializadas, preparación y prueba de planes de contingencia, líneas de ayuda o portales de información y formación de los empleados (Betterley, 2015; Swiss Re, 2017; Wells Fargo Insurance Services, 2016; Insurance Journal, 2017e).

Una gama de servicios para gestionar el impacto de un incidente cibernético también es ofrecida, incluidos los servicios de investigación forense necesarios para identificar la fuente de cualquier violación, la asistencia jurídica para ayudar a gestionar los requisitos legales y reglamentarios y la posible responsabilidad, proveedores de capacidad de centro de llamadas, servicios de notificación, supervisión de crédito y/o protección contra el robo de identidad para apoyar la interacción con los clientes afectados, y empresas de relaciones públicas para minimizar el impacto en la reputación de los incidentes cibernéticos” (Traducción libre, OCDE, 2017, Pág. 75).

8. Conclusiones

“The insurance company and its contracts have a place in the statutes and the courts unknown to any other company and to any other contract; the company has been the sport of legislatures, and its contracts the football of the courts” John A. Finch

De conformidad con lo expuesto a lo largo del presente documento, es dable concluir que el denominado “riesgo cibernético” objeto de aseguramiento bajo las Pólizas de Seguro para Riesgos Cibernéticos constituye una categoría amplia que, contrario a la creencia popular, excede la noción coloquial de hackeo y crimen por computador comprendiendo, conforme a la taxonomía operacional dominante, las acciones de las personas, las fallas tecnológicas, los procesos internos deficientes y los eventos externos que comprometan la confidencialidad, la integridad o la disponibilidad de la información y de los sistemas. Esta amplitud conceptual impone, en el plano contractual, un esfuerzo correlativo de precisión en la definición del evento asegurado, de la que dependerá la extensión real de la cobertura otorgada bajo una Póliza de Seguro para riesgos cibernéticos determinada, bajo la premisa, en todo caso, que en esta tipología de producto los datos constituyen simultáneamente el componente esencial del riesgo asegurado y el bien sobre el cual recae el interés objeto de cobertura.

Es importante destacar que los amparos del ramo se ordenan en torno a la dualidad de esquemas de primera y tercera parte, cuya correcta diferenciación es presupuesto de la aplicación de las reglas legales pertinentes a cada uno. Las exclusiones, por su parte, concentran los principales focos de litigiosidad: la experiencia comparada del caso Merck enseña que las cláusulas concebidas para otras realidades no se extienden analógicamente al entorno digital, y que la delimitación del riesgo de ciber guerra, de los actos estatales y de las fallas de infraestructura exige redacciones expresas, precisas y compatibles con los controles de transparencia y de abusividad o ineficacia por vaciar de contenido las coberturas propios de los ordenamientos de la región.

La evidencia empírica global y regional —de Equifax y NotPetya al ataque contra IFX Networks que afectó a centenares de organizaciones latinoamericanas— demuestra que el riesgo para esta tipología de Pólizas de Seguro se materializa con severidad creciente y con una marcada dimensión sistémica o de eventos en cascada derivada de la dependencia de proveedores tecnológicos compartidos, dimensión que el diseño de los amparos de interrupción contingente y de las exclusiones de infraestructura debe administrar con especial cuidado. Así mismo, el mercado de Seguros para Riesgos Cibernéticos, en franca expansión global, mantiene en América Latina una participación marginal que contrasta con la elevada exposición regional, configurando una brecha de protección cuya reducción exige tanto desarrollo de mercado —productos adaptados al segmento de pequeñas y medianas empresas, servicios de prevención y respuesta— como acompañamiento de política pública, en los términos recomendados por la OCDE (2017) y los organismos multilaterales regionales.

Subsisten, en fin, retos estructurales de asegurabilidad —datos escasos, correlación, asimetrías de información y potencial catastrófico— que el mercado administra mediante sublímites, garantías de higiene digital, paneles de respuesta y soporte reasegurador internacional. En este escenario, el ciberseguro debe entenderse como lo que la propia norma ISO/IEC 27102:2019 proclama: un componente importante, mas no sustitutivo, del plan general de tratamiento de los riesgos de seguridad de la información, llamado a operar en la última etapa de un proceso de gerencia del riesgo que comienza, siempre, por la identificación, la cuantificación y el control del riesgo por parte de la propia organización.

Finalmente, el seguro paramétrico de riesgos cibernéticos emerge como un complemento valioso del esquema indemnizatorio tradicional, particularmente apto para las pérdidas por interrupción de servicios digitales medibles de manera objetiva, cuya brecha de cobertura quedó en evidencia con el

apagón informático global de julio de 2024. La habilitación general de la modalidad por índice introducida en Colombia por la Ley 2294 de 2023 —que armonizó expresamente el detonante paramétrico con el principio indemnizatorio y con el régimen probatorio del siniestro— posiciona favorablemente al mercado colombiano para su desarrollo, a condición de que la estructuración de los productos garantice la correlación técnica del índice con la pérdida, la gobernanza independiente de la medición y la información transparente del riesgo de base al asegurado.

Bibliografía

Ab Razak, M. F., Anuar, N. B., Salleh, R., & Firdaus, A. (2016). The rise of "malware": Bibliometric analysis of malware study. *Journal of Network and Computer Applications*, 75, 58–76. <https://doi.org/10.1016/j.jnca.2016.08.022>

Al-olaqi, M., Al-gailani, A., & Rahman, M. M. H. (2025). Comprehensive study of SQL injection attacks mitigation methods and future directions. *Journal of Cyber Security and Risk Auditing*, 2025(4), 347–365. <https://doi.org/10.63180/jcsra.thestap.2025.4.11>

Allianz. (2022). Allianz Risk Barometer. Allianz Global Corporate & Specialty.

Álvarez, J. (2020, junio). Honda se enfrenta a un posible ransomware. Una al Día. <https://unaaldia.hispasec.com/2020/06/honda-se-enfrenta-a-un-posible-ransomware.html>

Argentina. (2000). Ley 25.326 de Protección de los Datos Personales. Ministerio de Justicia y Derechos Humanos. <http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm>

ARN. (s. f.). Top 10 most notorious cyber-attacks in history. <https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/>

Artemis. (2025). Beazley targets \$200m PoleStar Re 2026-1 cyber catastrophe bond. <https://www.artemis.bm/news/beazley-targets-200m-polestar-re-2026-1-cyber-catastrophe-bond/>

Banco Interamericano de Desarrollo & Organización de los Estados Americanos. (2020). Reporte ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. BID/OEA. <https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe>

Bara, D., Coric, S., & Jurisic, G. (2015). The role of cyber insurance in managing and mitigating cyber security risk with special emphasis on the potential of Croatia and Serbia cyber insurance market. https://www.researchgate.net/publication/280237921_The_role_of_Cyber_insurance_in_managing_and_mitigating_Cyber_security_risk_with_special_emphasis_on_the_potential_of_Croatia_and_Serbia_Cyber_insurance_market

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance — Issues and Practice*, 40(1), 131–158. <https://doi.org/10.1057/gpp.2014.19>

Böhme, R., & Schwartz, G. (2010). Modeling cyber-insurance: Towards a unifying framework. Workshop on the Economics of Information Security (WEIS), Harvard University. <https://econinfosec.org/archive/weis2010/>

Brasil. (2018). Lei nº 13.709, de 14 de agosto de 2018 — Lei Geral de Proteção de Dados Pessoais (LGPD). Presidência da República. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Brigard Urrutia. (2024). ¿Qué dice la SFC sobre los seguros paramétricos en Colombia? <https://www.bu.com.co/es/insights/noticias/que-dice-la-sfc-sobre-los-seguros-parametricos-en-colombia>

Brodersen, J., & Blanco, P. (2020, diciembre). Ciberataque a Migraciones: se venció el plazo y se publicó la información robada por un ransomware. Clarín. https://www.clarin.com/tecnologia/vencio-plazo-ciberdelincuentes-publicaron-informacion-privada-robada-migraciones_0_izMLPV-xm.html

Callegati, F., Cerroni, W., & Ramilli, M. (2009). Man-in-the-middle attack to the HTTPS protocol. *IEEE Security & Privacy*, 7(1), 78–81.

Casas, L. (2018, junio). Robaron US\$10 millones en ataque informático al Banco de Chile: virus fue un distractor. BioBioChile. <https://www.biobiochile.cl/noticias/nacional/chile/2018/06/09/robaron-us10-millones-en-ataque-informatico-al-banco-de-chile-virus-fue-un-distractor.shtml>

Castillo Díaz, F. A. (2020). Contrato de seguro para riesgos cibernéticos: análisis de la cobertura de responsabilidad civil por violación de datos personales [Tesis de maestría, Universidad Externado de Colombia]. Repositorio Digital Institucional Universidad Externado de Colombia. <https://bdigital.uexternado.edu.co/handle/001/3608>

Cebula, J., & Young, L. (2019). A taxonomy of operational cyber security risks (Technical Note CMU/SEI-2010-TN-028). Carnegie Mellon University, Software Engineering Institute. https://resources.sei.cmu.edu/asset_files/TechnicalNote/2010_004_001_15200.pdf

Chong, W. F., Linders, D., Quan, Z., & Zhang, L. (2025). Incident-specific cyber insurance. *ASTIN Bulletin: The Journal of the IAA*, 55, 395–425.

Clyde & Co / CPB. (2023). War exclusions and cyber risks — Merck v ACE & Others. <https://www.cpblaw.com/publications/2023/war-exclusions-and-cyber-risks-merck-v-ace-others.pdf>

Congreso de la República de Colombia. (2023). Ley 2294 de 2023 (Plan Nacional de Desarrollo 2022-2026), arts. 241–243. Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/portaIDNP/PND-2023/Ley_2294_del_19_de_mayo_de_2023.pdf

Contreras, O. (s. f.). Derecho de seguros (2.^a ed.). Thomson Reuters.

Corte Constitucional de Colombia. (2016). Sentencia C-602 de 2016 (M. P. Alejandro Linares Cantillo). <https://www.corteconstitucional.gov.co/relatoria/2016/C-602-16.htm>

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance — Issues and Practice*, 47, 698–736. <https://doi.org/10.1057/s41288-022-00266-6>

CRO Forum. (2016). CRO Forum concept paper on a proposed categorization methodology for cyber risk. CRO Forum.

Cybersecurity Dive. (2024a). CrowdStrike disruption direct losses to reach \$5.4B for Fortune 500, study finds. <https://www.cybersecuritydive.com/news/crowdstrike-cost-fortune-500-losses-cyber-insurance/722396/>

Cybersecurity Dive. (2024b). Merck reaches settlement in closely watched NotPetya insurance case. <https://www.cybersecuritydive.com/news/merck-settlement-notpetya-insurance/703922/>

Demers, D., & Lee, H. (2022). Kerberoasting: Case studies of an attack on a cryptographic authentication technology. *International Journal of Cybersecurity Intelligence & Cybercrime*, 5(2), 25–39. <https://vc.bridgew.edu/ijcic/vol5/iss2/3>

Departamento Nacional de Planeación. (2011). Documento CONPES 3701: Lineamientos de política para ciberseguridad y ciberdefensa. <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf>

Departamento Nacional de Planeación. (2016). Documento CONPES 3854: Política nacional de seguridad digital. <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>

Departamento Nacional de Planeación. (2020). Documento CONPES 3995: Política nacional de confianza y seguridad digital. <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf>

Deloitte España. (s. f.). El impacto económico de WannaCry. <https://www2.deloitte.com/es/es/pages/governance-risk-and-compliance/articles/impacto-economico-wannacry.html>

Díaz-Granados Ortiz, J. M. (2012). *El seguro de responsabilidad* (2.^a ed.). Universidad del Rosario / Pontificia Universidad Javeriana.

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, 17(5), 474–491. <https://doi.org/10.1108/JRF-09-2016-0122>

El Español. (2020, noviembre). Filtran datos personales y financieros de millones de clientes de Booking y Expedia. https://www.elespanol.com/omicrofono/software/20201109/filtran-personales-financieros-millones-clientes-booking-expedia/534697112_0.html

El Tiempo. (2023). Ciberataque en Colombia: detalles del ataque a IFX Networks. <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberataque-en-colombia-detalles-del-ataque-a-ixf-networks-806778>

Electronic Privacy Information Center. (s. f.). Equifax data breach. <https://epic.org/privacy/data-breach/equifax/>

Estados Unidos Mexicanos. (2025). Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Diario Oficial de la Federación, 20 de marzo de 2025). Cámara de Diputados. <https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>

European Union Agency for Cybersecurity. (2024). ENISA threat landscape 2024. ENISA. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>

Federación de Aseguradores Colombianos [Fasecolda]. (2024). Cada vez más colombianos asegurados: crecimiento del sector en el tercer trimestre de 2024. <https://www.fasecolda.com/cada-vez-mas-colombianos-asegurados-crecimiento-del-sector-en-el-tercer-trimestre-de-2024/>

Federal Trade Commission. (2019). Equifax to pay \$575 million as part of settlement with FTC, CFPB, and states related to 2017 data breach. <https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach>

Fortinet. (2023). América Latina fue objetivo de más de 360 mil millones de intentos de ciberataques en 2022. FortiGuard Labs. <https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2023/fortiguards-labs-reports-destructive-wiper-malware-increases-over-50-percent>

Fortinet. (s. f.). Global threat landscape report. <https://www.fortinet.com/lat/resources/reports/threat-landscape-report>

Fruhlinger, J. (2020). What is a cyber attack? Recent examples show disturbing trends. CSO Online. <https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html>

Fuentes, L. F. (2008). Malware, una amenaza de internet. *Revista Digital Universitaria*, 9(4). <https://www.revista.unam.mx/vol.9/num4/art22/art22.pdf>

García, J. (2020, octubre). Así ha afectado un ataque de "ransomware" a una de las mayores aseguradoras de España. *El País*. <https://elpais.com/tecnologia/2020-10-16/asi-ha-afectado-un-ataque-de-ransomware-a-una-de-las-mayores-aseguradoras-de-espana.html>

Gandal, N., Riordan, M., & Bublil, S. (2020). A new approach to quantifying, reducing and insuring cyber risk: Preliminary analysis and proposal for further research (CEPR Discussion Paper No. 14461). Centre for Economic Policy Research.

Gatzlaff, K., & McCullough, K. (2008). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review*. <https://www.cs.drexel.edu/~greenie/cs467/SSRN-id1121172.pdf>

Granato, A., & Polacek, A. (2019). The growth and challenges of cyber insurance. *Chicago Fed Letter*, (426). <https://www.chicagofed.org/publications/chicago-fed-letter/2019/426>

Guisao, J. S., & Toro Rendón, J. C. (2014). Detección y mitigación de vulnerabilidades día cero. *Cuaderno Activa*, 6(1), 63–67. <https://ojs.tdea.edu.co/index.php/cuadernoactiva/article/view/201>

Gumenyuk, L. (2021). Cyber insurance: Modern requirements. *Economics & Education*, 6(4), 33–36. https://www.researchgate.net/publication/367746244_CYBER_INSURANCE_MODERN_REQUIREMENTS

Hass, A., & Hofmann, A. (2013). Risiken aus Cloud-Computing-Services: Fragen des Risikomanagements und Aspekte der Versicherbarkeit (FZID Discussion Paper No. 74). Universität Hohenheim.

IBM. (2023). ¿Qué es un ataque de día cero? IBM Think. <https://www.ibm.com/mx-es/think/topics/zero-day>

IBM. (2024a). Cost of a data breach report 2024. <https://www.ibm.com/reports/data-breach>

IBM. (2024b). How will the Merck settlement affect the insurance industry? <https://www.ibm.com/think/insights/merck-settlement-affect-insurance-industry>

International Organization for Standardization & International Electrotechnical Commission. (2019). ISO/IEC 27102:2019. Information security management — Guidelines for cyber-insurance. <https://www.iso.org/standard/72436.html>

Interpol. (2020). Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19. <https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19>

Jabir, R., Le, J., & Nguyen, C. (2025). Phishing attacks in the age of generative artificial intelligence: A systematic review of human factors. *AI*, 6(8), 174. <https://doi.org/10.3390/ai6080174>

Jae, J., & Floridi, L. (2024). Ransomware: Why it's growing and how to curb its growth. *ACIG — Academic Journal on Cybercrime and Information Governance*, 4(2). <https://doi.org/10.60097/ACIG/192959>

Lesmes, L. (2022, 4 de diciembre). Keralty, la nueva víctima de los ataques de "ransomware". El Tiempo. <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/keralty-detalles-del-ataque-de-ransomware-a-eps-sanitas-723175>

Lloyd's. (s. f.). Lloyd's Lab alumni: Parametrix — parametric insurance against outages of the cloud, CDNs or e-commerce platforms. <https://www.lloyds.com/insights/lloyds-lab/programmes-and-initiatives/lloyds-lab-accelerator/alumni/parametrix>

Mallik, A., Zaglul-Shahaday, M., Ahsan, A., & Tsou, J. (2019). Man-in-the-middle-attack: Understanding in simple words. *International Journal of Data and Network Science*, 3(2), 77–92.

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, 24, 35–61. <https://doi.org/10.1016/j.cosrev.2017.01.001>

Martínez-Lozano, J., & Atencio-Ortiz, P. (2019). Creación de un ataque DDoS utilizando HTTP-GET Flood a partir de la metodología Cyber Kill Chain. *ITECKNE*, 16(1), 41–47.

Memorando, Radicado ANI n.º 20257050215853. (2025, 2 de diciembre). Asunto: lineamientos para la aprobación del Seguro de Daños Contra Todo Riesgo. Vicepresidencia Jurídica, Agencia Nacional de Infraestructura.

Morgan Lewis. (2025). Cybersecurity insurance: A burgeoning global market. <https://www.morganlewis.com/blogs/sourcingatmorganlewis/2025/10/cybersecurity-insurance-a-burgeoning-global-market>

Mukhopadhyay, A., Saha, D., Mahanti, A., & Chakrabarti, B. (2005). Insurance for cyber-risk: A utility model. *Decision*, 32(1), 153–169.

Munich Re. (2025). Cyber insurance: Risks and trends 2025. <https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2025.html>

Narváez Bonnet, J. E. (2014). El contrato de seguro en el sector financiero (3.ª ed.). Grupo Editorial Ibáñez.

National Institute of Standards and Technology. (s. f.). Glossary: Cyberspace. Computer Security Resource Center. <https://csrc.nist.gov/glossary/term/cyberspace>

Niccolai, J. (2000). Analyst puts hacker damage at \$1.2 billion and rising. InfoWorld. <https://web.archive.org/web/20071112081103/http://www.infoworld.com/articles/ic/xml/00/02/10/000210icyankees.html>

Nykodym, N., Kahle-Piasecki, L., Ariss, S., & Toussaint, T. (2010). Cybercrime and business: How to not get caught by the online phisher. *Journal of International Commercial Law and Technology*, 5(4), 252–259.

Ógüt, H., Raghunathan, S., & Menon, N. (2011). Cyber security risk management: Public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. *Risk Analysis*, 31(3), 497–512.

Organisation for Economic Co-operation and Development. (2017). Enhancing the role of insurance in cyber risk management. OECD Publishing. <https://doi.org/10.1787/9789264282148-en>

Ossa Gómez, J. E. (1991). Teoría general del seguro: El contrato (2.ª ed.). Temis.

OWASP Gen AI Security Project. (2025). LLM04:2025 data and model poisoning. <https://genai.owasp.org/llmrisk/llm042025-data-and-model-poisoning/>

Parametrix. (2024a). CrowdStrike's impact on the Fortune 500 [Análisis de impacto]. <https://www.parametrixinsurance.com/reports-white-papers/crowdstrikes-impact-on-the-fortune-500>

Parametrix. (2024b). Parametric enterprise solutions for digital interruption. <https://www.parametrixinsurance.com/in-the-news/innovative-parametric-enterprise-risk-solutions>

Paz, A. (2018). La culpa del consumidor en la responsabilidad financiera y su proyección causal en el daño por fraude electrónico. *Revista de Derecho Privado (Universidad Externado de Colombia)*, (35), 261–289.

Perú. (2011). Ley N.º 29733, Ley de Protección de Datos Personales. Congreso de la República. <https://leyes.congreso.gob.pe/>

Popa, B. (2016). Adobe fined \$1 million for 2013 hack that affected millions of users. Softpedia. <https://news.softpedia.com/news/adobe-fined-1-million-for-2013-hack-that-affected-millions-of-users-510256.shtml>

Presidencia de la República de Colombia. (2023). Gobierno Nacional atiende ataque cibernético que afecta a varias entidades e instala PMU Ciber. <https://petro.presidencia.gov.co/prensa/Paginas/Gobierno-Nacional-atiende-ataque-cibernetico-que-afecta-a-varias-entidades-e-instala-PMU-CIBER-230913.aspx>

Reinsurance News. (2024). Parametrix launches new cyber insurance solution for digital interruption. <https://www.reinsurancene.ws/parametrix-launches-new-cyber-insurance-solution-for-digital-interruption/>

Reinsurance News. (2025). Beazley closes \$300m cyber catastrophe bond. <https://www.reinsurancene.ws/beazley-closes-300m-cyber-catastrophe-bond/>

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity*, 5(1), tyz002. <https://doi.org/10.1093/cybsec/tyz002>

Sales Porto, A. S., & Novoa Rubiano, D. C. (2025). La construcción de confianza en los seguros de riesgos cibernéticos: desafíos y perspectivas. *Revista Ibero-Latinoamericana de Seguros*, 34(62), 109–126. <https://doi.org/10.11144/Javeriana.ris62.ccsr>

Saraiva Lima, H. J. M. (2020). Seguros cibernéticos. *Revista Ibero-Latinoamericana de Seguros*, 29(53), 161–172. <https://doi.org/10.11144/Javeriana.ris53.seci>

Schneider, J., & Smalley, I. (2025, 30 de mayo). ¿Qué es el cryptojacking? IBM Think. <https://www.ibm.com/mx-es/think/topics/cryptojacking>

Schutz, F., Rampold, F., Kalisch, A., & Masusch, K. (2023). Consumer cyber insurance as risk transfer: A coverage analysis. *Procedia Computer Science*, 219, 521–528.

Schwarz, D., & Wolff, J. (2025). The limits of regulating AI safety through liability and insurance: Lessons from cybersecurity (Minnesota Legal Studies Research Paper No. 2025-46). SSRN. <https://doi.org/10.2139/ssrn.5411062>

Signorino Barbat, A. (2015). Visión jurídica sobre privacidad, confidencialidad y protección en el expediente clínico electrónico. En *IV Congreso de Nuevas Tecnologías: La influencia de internet, genética y nanotecnología en la medicina y el seguro*. Universidad Externado de Colombia.

Sobrino, W. (2017). Los seguros de cyber risk (a propósito del ciberataque mundial de fecha 12 de mayo de 2017). *Revista Ibero-Latinoamericana de Seguros*, 26(47), 137–164. <https://revistas.javeriana.edu.co/index.php/iberoseguros>

Solis, C. (2020). Querella confirma que BancoEstado ya había sufrido grave ataque cibernético en junio. *Interferencia*. <https://interferencia.cl/articulos/querella-confirma-que-bancoestado-ya-habia-sufrido-grave-ataque-cibernetico-en-junio>

Superintendencia de Industria y Comercio. (s. f.). Protección de datos personales. <https://www.sic.gov.co/tema/proteccion-de-datos-personales>

Superintendencia Financiera de Colombia. (2018). Circular Externa 007 de 2018: requerimientos mínimos para la gestión del riesgo de ciberseguridad. <https://www.fundacionmicrofinanzasbbva.org/revistaprogreso/wp-content/uploads/2018/05/Col-CE-007-ciberseguridad.pdf>

The Geneva Association. (2016). Ten key questions on cyber risk and cyber risk insurance. <https://www.genevaassociation.org/>

The Insurer. (2025). Global cyber premiums to reach \$16.3 billion in 2025: Munich Re. <https://www.theinsurer.com/cyber-risk/news/global-cyber-premiums-to-reach-163-billion-in-2025-munich-re-2025-04-03/>

Tsohou, A., Diamantopoulou, V., Gritzalis, S., & Lambrinoudakis, C. (2023). Cyber insurance: State of the art, trends and future directions. *International Journal of Information Security*, 22, 737–748. <https://doi.org/10.1007/s10207-023-00660-8>

U.S. Department of the Treasury, Office of Foreign Assets Control. (2020). Advisory on potential sanctions risks for facilitating ransomware payments. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

Valderrama Villabona, M., & Galán Pérez, N. P. (2023). Seguros paramétricos: panorama normativo y perspectivas. *Revista Fasecolda*, (190), 46–51. <https://revista.fasecolda.com/index.php/revfasecolda/article/view/916>

Verizon. (2025). Data breach investigations report (DBIR). <https://www.verizon.com/business/resources/reports/dbir/>

Vivas Díez, G. J., & Bedoya Chavarriaga, J. C. (2022). El contrato de seguro para riesgos cibernéticos: nociones preliminares y precisiones para su suscripción. En L. Sandoval (Ed.), *GPS Seguros: guía profesional* (pp. 655–712). Tirant lo Blanch.

Wolff, J. (2022). *Cyberinsurance policy: Rethinking risk in an age of ransomware, computer fraud, data breaches, and cyberattacks*. MIT Press. <https://doi.org/10.7551/mitpress/13665.001.0001>

World Economic Forum. (2025). Global risks report 2025. <https://www.weforum.org/publications/global-risks-report-2025/>

Wrede, D., Stegen, T., & Graf von der Schulenburg, J.-M. (2020). Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market. *The Geneva Papers on Risk and Insurance — Issues and Practice*, 45, 657–689. <https://link.springer.com/journal/41288>

Pólizas de Seguro

Allianz Colombia S.A. (2025). Cyber Allianz Protect [Póliza n.º 12/05/2025-1301-P-06-CYBERAZPROTECT14-000I; Nota técnica n.º 12/05/2025-1301-NT-P-06-CYBERAZPROTECT14]. Superintendencia Financiera de Colombia, Depósito Público de Pólizas. <https://www.superfinanciera.gov.co/publicacion/consulte-las-condiciones-generales-de-su-poliza-de-seguro-10090607>

Axa Colpatria Seguros S.A. (2025). Seguro de riesgos cibernéticos — Cyber Premium [Póliza n.º 03/06/2025-13-P-06-Cyber/Premium/25-D00I; Nota técnica n.º 03/06/2025-NT-P-06-CYBER/PREMIUM/25]. Superintendencia Financiera de Colombia, Depósito Público de Pólizas. <https://www.superfinanciera.gov.co/publicacion/consulte-las-condiciones-generales-de-su-poliza-de-seguro-10090607>

Chubb Seguros Colombia S.A. (2022). Póliza para la gestión de riesgos cibernéticos [Póliza n.º 28-07-2022-1305-P-06-CLACHUBB20180021-000I; Nota técnica n.º 28-07-2022-1305-NT-06-P&CNTCHUBBSEG051]. Superintendencia Financiera de Colombia, Depósito Público de Pólizas. <https://www.superfinanciera.gov.co/publicacion/consulte-las-condiciones-generales-de-su-poliza-de-seguro-10090607>

SBS Seguros Colombia S.A. (2023). Seguro de responsabilidad profesional por pérdida de datos (Cyber) [Registro condicionado n.º 01/01/2023-1322-P-06-RPROF_PD_CYBER01-D00I; Registro nota técnica n.º 01/01/2023-1322-NT-P-06-RPROF_PD_CYBER01]. Superintendencia Financiera de Colombia, Depósito Público de Pólizas. <https://www.superfinanciera.gov.co/publicacion/consulte-las-condiciones-generales-de-su-poliza-de-seguro-10090607>

Seguros Generales Suramericana S.A. (2023). Seguro de protección digital para empresas [Código clausulado n.º 26/10/2023-1318-06-P-F-13-18-0013-118-D00I; Código nota técnica n.º 04/10/2018-06-NT-N-01-13-0018]. Superintendencia Financiera de Colombia, Depósito Público de Pólizas. <https://www.superfinanciera.gov.co/publicacion/consulte-las-condiciones-generales-de-su-poliza-de-seguro-10090607>

Zürich Colombia Seguros S.A. (2024). Póliza de seguro de protección de datos y seguridad informática [Póliza n.º 23/02/2024-1309-P-06-PDSI-PROT-000003-D00I; Nota técnica n.º 23/02/2024-1309-NT-P-06-PDSI-PROT-000003]. Superintendencia Financiera de Colombia, Depósito Público de Pólizas. <https://www.superfinanciera.gov.co/publicacion/consulte-las-condiciones-generales-de-su-poliza-de-seguro-10090607>