ISSN 0123-1154 (IMPRESO)
ISSN 2500-7556 (EN LÍNEA)

LA CONSTRUCCIÓN DE CONFIANZA EN LOS SEGUROS DE RIESGOS CIBERNÉTICOS

DESAFÍOS Y PERSPECTIVAS[*]

BUILDING TRUST IN CYBER RISK INSURANCE.

CHALLENGES AND PROSPECTS

ADRIANA SOFÍA SALES PORTO[**]
DIANA CATALINA NOVOA RUBIANO[***]

Fecha de recepción: 16 de abril de 2025
Fecha de aceptación: 05 de mayo de 2025
Disponible en línea: 30 de junio de 2025

Para citar este artículo/To cite this article

Sales Porto, Adriana Sofía & Novoa Rubiano, Diana Catalina. *La construcción de confianza en los seguros de riesgos cibernéticos. Desafíos y perspectivas,* 62 Rev.Ibero-Latinoam.Seguros, 109-126 (2025). https://doi.org/10.11144/Javeriana.ris62.ccsr

doi:10.11144/Javeriana.ris62.ccsr

[*] Trabajo de reflexión, ganador del concurso ACOLDESE 2024, sobre los seguros de riesgos cibernéticos. Expuesto en el 32° Encuentro Nacional e Internacional ACOLDESE.

[**] Abogada de la Pontificia Universidad Javeriana. Especialista en Derecho de Seguros de la Pontificia Universidad Javeriana y Especialista en Derecho de Seguros de la Universidad de Salamanca, España. Maestría en curso en Derecho de Daños de la Universidad de Girona, España. Correo electrónico: salesportoadriana@gmail.com

[***] Abogada de la Pontificia Universidad Javeriana. Especialista en Derecho de Seguros y Derecho Comercial de la Pontificia Universidad Javeriana. Correo electrónico: dianacatalinanovoa@gmail.com. Cuenta con más de 8 años de experiencia en el sector de seguros y reaseguros.

RESUMEN

Recientemente, mucho se ha discutido acerca de los seguros de riesgos cibernéticos, más en realidad, no se tiene total claridad acerca de estos que implican concretamente. Este tipo de seguros, están encaminados a proteger de las consecuencias financieras y operacionales de los incidentes cibernéticos, buscando la protección de los costosos impactos de las amenazas cibernéticas y de eventos de seguridad a los que puede verse expuesto el asegurado (tanto persona natural como jurídica). Sin embargo, para que estos seguros sean efectivos, es necesario que se cuente con la confianza, por parte de los asegurados, como de las aseguradoras. Sólo de esta forma, las necesidades de los clientes serán atendidas de manera adecuada, y sólo así las compañías de seguros podrían cumplir con sus amparos, en caso de un incidente cibernético.

El presente trabajo de reflexión abordará la importancia de los seguros de riesgos cibernéticos, evaluando su importancia en el actual panorama de la ciberseguridad, destacando, como es de vital importancia que exista confianza entre las aseguradoras y sus clientes, enfatizando en la necesidad de transparencia, colaboración y compromiso mutuo, a efectos de garantizar la efectividad, y el éxito de los seguros de riesgos cibernéticos.

Palabras claves: Riesgos cibernéticos, seguros cibernéticos, seguros.

ABSTRACT

There has been much discussion recently about cyber risk insurance, but in reality, there is little clarity about its specific implications. This type of insurance is aimed at protecting against the financial and operational consequences of cyber incidents, seeking to protect against the costly impacts of cyber threats and security events to which the insured (both individuals and legal entities) may be exposed. However, for this insurance to be effective, it is necessary to have the trust of both insured parties and insurers. Only in this way will customers' needs be adequately addressed, and only then will insurance companies be able to fulfill their coverage in the event of a cyber incident. This reflection paper will address the importance of cyber risk insurance, assessing its significance in the current cybersecurity landscape. It highlights the vital importance of trust between insurers and their clients, emphasizing the need for transparency, collaboration, and mutual commitment to ensure the effectiveness and success of cyber risk insurance.

Keywords: *Cyber risks, cyber insurance, insurance.*

INTRODUCCIÓN

Uno de los temas sobre los cuales recientemente más se ha empezado a estudiar, y profundizar a nivel global, es el análisis de los seguros de riesgos cibernéticos. Lo anterior, debido al creciente aumento de ataques cibernéticos, a la conciencia en la importancia de la ciberseguridad, en la creciente regulación en el ámbito de la protección de datos y de la ciberseguridad, y en la evolución del mercado de seguros.

Lo primero a señalar al respecto, es que los seguros de riesgos cibernéticos, son productos relativamente nuevos, a comparación de los seguros más tradicionales. Y aunque no exista con claridad una fecha exacta en la cual se empezaron a asegurar los riesgos cibernéticos, se sabe que, debido a la alta dependencia en la tecnología de la información, se empezaron a desarrollar los primeros productos de seguro cibernético, buscando respuestas a las preocupaciones respecto de seguridad en la información de las empresas y de la sociedad en general, los cuales buscaban combatir incidentes cibernéticos.

Estos productos de seguros de riesgos cibernéticos inicialmente se centraban en la cobertura de responsabilidad por divulgación de datos personales – como era el tema de infracciones de seguridad y de violaciones de privacidad –, pero los mismos posteriormente evolucionaron, y ahora abarcan una amplia gama de riesgos.

Hoy en día, se ha empezado a brindar otras coberturas, a efectos de poder comprender riesgos como los costos de recuperación de datos, los costos de respuesta a incidentes, por las pérdidas de ingresos por interrupciones de negocios, y por la responsabilidad civil derivada de violaciones de datos, etc.

Así las cosas, se han diseñado los seguros de riesgos cibernéticos, como unas pólizas concebidas, para proteger y/o salvaguardar de las consecuencias financieras y operacionales de los incidentes cibernéticos, buscando la protección de los costosos impactos de las amenazas cibernéticas y de eventos de seguridad a los que puede verse expuesta una empresa.

Precisamente, como el seguro de riesgos cibernéticos se ha vuelto cada vez más relevante, al ser latentes diariamente las amenazas cibernéticas, que se ha aumentado el énfasis en desarrollar este tipo de seguros, a efectos de poder proteger financiera y tecnológicamente a las personas y empresas que los necesiten.

Es así como, el seguro de riesgos cibernéticos se ha vuelto cada vez más importante en la era digital en la que vivimos, toda vez que a medida que la tecnología ha avanzado, así mismo han progresado las amenazas cibernéticas en frecuencia y sofisticación. Precisamente por ello, se busca contar con medidas efectivas para prevenir y/o mitigar esos riesgos, brindando una capa adicional de protección financiera, buscando salvaguardar la seguridad de los datos y las operaciones comerciales.

Sin embargo, para que estos seguros de riesgos cibernéticos sean efectivos, es necesario que se cuente con la confianza, tanto por parte de los clientes que adquieren las pólizas, como de las aseguradoras que las ofrecen. Solo de esta forma, las necesidades de los

clientes serán atendidas de manera adecuada, y solo así las compañías de seguros podrían cumplir con sus amparos, en caso de un incidente cibernético.

Por lo anterior, por medio del presente escrito de reflexión, pasaremos a explicar, la importancia de los seguros de riesgos cibernéticos, evaluando su importancia en el actual panorama de la ciberseguridad, destacando, como es de vital importancia que exista confianza entre las aseguradoras y sus clientes, enfatizando la necesidad de transparencia, colaboración y compromiso mutuo, a efectos de garantizar la efectividad, y el éxito de los seguros de riesgos cibernéticos.

CONFIANZA DIGITAL Y SEGURIDAD CIBERNÉTICA

Lo primero que sería de relevancia precisar, a efectos de poder entender con mayor claridad los seguros cibernéticos, es el que se comprende por cibernético. Precisamente, en palabras de la doctora Andrea Signorino Barbat, se señala:

> ***"Como cibernético designamos todo lo relacionado con la tecnología computacional interdisciplinaria usada para la extensión de las capacidades humanas.***
>
> *(...)*
>
> *Hoy en día,* ***lo cibernético se caracteriza por ser todo lo que se relaciona con la tecnología computacional, especialmente, pero no únicamente, con Internet.***
>
> *(...)*
>
> *En especial el tema ha sido analizado con respecto al sistema bancario que sufre muchas pérdidas por estos motivos, pero asimismo,* ***se está hablando fuertemente en el mundo del seguro de estos peligros que acechan, dentro y fuera de la empresa aseguradora.***
>
> ***El tema de los Ciber Riesgos va mucho más allá de la acción de un hacker y se relaciona con actividades informáticas ilegales para sustraer, alterar, modificar, manipular, inutilizar o destruir información o activos, como ser dinero, bonos o bienes inmateriales, información, de las compañías o usuarios afectados, utilizando para dichos propósitos medios electrónicos o dispositivos electrónicos. "***[1]

Es así como, se entiende que por la palabra cibernético, se abarcan todos los aspectos afines con la tecnología digital, y los entornos digitales, que permiten extender las capacidades humanas.

Ya teniendo clara la noción de lo que se podría entender por cibernético, es forzoso continuar con el análisis de los riesgos cibernéticos, destacando que, para hacerles frente a los mismos, son de vital importancia dos conceptos principales, los cuales son la confianza digital, y la seguridad cibernética.

[1] Signorino Barbat, Andrea, *Ciber riesgos: Su dimensión social, funcional y ética,* 51 Rev.Ibero-Latinoam. Seguros, 35-56 (2019). https://doi.org/10.11144/Javeriana.ris51.crsd

Para poder hablar de confianza digital, primero se debe precisar que se entiende por confianza. Al respecto, algunas de las definiciones que se tienen de confianza en la Real Academia Española[2], son: *"(i). Seguridad que alguien tiene en sí mismo, (ii). En quien se puede confiar, y (iii) Que posee las cualidades recomendables para el fin a que se destina".* Para efectos de este texto, se entenderá la palabra confianza, como la seguridad que puede tener una persona, respecto de ciertas cualidades puntuales, respecto de otra persona u otra situación.

Cuando se habla de confianza digital, se deben hablar de aspectos como lo son, la protección de la privacidad, seguridad en las transacciones, o en la seguridad de datos.

Por el contrario, cuando se hace referencia a la por seguridad cibernética, se deben entender todo este conglomerado de prácticas, técnicas, medidas diseñadas para poder proteger contra amenazas cibernéticas. Precisamente, esta seguridad informática, se originó, para poder tomar medidas para

> *"la protección de infraestructura, software y hardware, contrarrestando las posibles amenazas mediante internet, y para desarrollar estrategias de contraataque. Esta perspectiva implicó la creación de sinnúmero de normas y sanciones para mitigar los delitos a través de esta red.*
>
> *(...)*
>
> *Por otro lado, la ciberseguridad alude al:*
>
> *Conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. [...] La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios [disponibilidad, integridad, autenticidad, confidencialidad, etc.][3]"*

En la era digital en la que actualmente vivimos, la aplicación del término de confianza digital termina siendo de gran relevancia, toda vez que lleva consigo, la fiabilidad y seguridad de las transacciones e interacciones en línea de cada uno de sus usuarios. En virtud de lo anterior, proponemos 3 alternativas, que pudieran ser de vital importancia, al momento de analizar la confianza digital y su aseguramiento. Estas son:

1. Se podrían aumentar, o iniciar campañas, a efectos que las organizaciones nacionales e internacionales, inviertan en seguridad cibernética, buscando poder proteger la confianza digital de los usuarios y sus clientes. Para ello, se podría empezar, por implementar tecnologías como cifrados de datos, autenticaciones

[2] Rae Confianza: Diccionario Esencial de la lengua española, 'Diccionario esencial de la lengua española'. Disponible en: https://www.rae.es/desen/confianza.

[3] Ospina Díaz, Milton Ricardo, & Sanabria Rangel, Pedro Emilio. (2020). *Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia.* Revista Criminalidad, 62(2), 199-217. Epub November 26, 2020. Retrieved March 31, 2024, from http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199&lng=en&tlng=es.

multifactoriales, firewalls, brindando capacitaciones, y teniendo sistemas de detección de intrusos.

2. Así mismo, se podría optar por incentivar a las organizaciones y a los gobiernos, a efectos que pudieran empezar a implementar paulatinamente regulaciones, y estándares de cumplimiento, encaminados a proteger la confianza digital.

3. Otra alternativa, y frente a la cual se le dará mayor énfasis a lo largo del presente escrito, es el poder empezar a implementar cada vez más los seguros cibernéticos, toda vez que podrían funcionar como una capa adicional en la protección financiera, contra las consecuencias adversas de los incidentes cibernéticos. Sin lugar a duda, son dos conceptos estrechamente interrelacionados entre sí.

Precisamente, para garantizar que los usuarios puedan confiar en la privacidad, integridad y seguridad de sus datos y actividades digitales, se ha optado por el aseguramiento de la confianza en lo digital.

Se ha optado por dicho aseguramiento, toda vez que los usuarios deben estar en la posibilidad de confiar en que sus datos financieros y personales estén protegidos, y ante el crecimiento de los riesgos cibernéticos, lo anterior cada vez se torna más difícil.

En relación con lo anterior, para que se pueda hablar de seguros cibernéticos, efectivamente tiene que existir una confianza de parte de los consumidores, y de parte de los inversionistas y socios comerciales, siendo ahora de relevancia, el entrar a profundizar acerca de la confianza digital, y la seguridad cibernética.

Así las cosas, la seguridad cibernética, y el aseguramiento, son dos de los principales aspectos en la actualidad del entorno digital, los cuales se complementan e interrelacionan entre sí. Precisamente, debido a esta colaboración, es que así mismo se termina teniendo un enfoque preventivo y reactivo, para poder estar preparados en caso de algún incidente cibernético, y poder mitigar así los daños, englobado lo anterior, en una gestión de riesgos.

ANÁLISIS DE LOS SEGUROS CIBERNÉTICOS, Y SUS RIESGOS – DESAFÍOS EN LA CONSTRUCCIÓN DE CONFIANZA

En la actual era digital, los riesgos cibernéticos, son una amenaza latente para todas las personas y/o empresas (independientemente de su sector o tamaño). Una de las respuestas más acertadas para poder combatir dichos riesgos, es el optar por protegerse, por medio de seguros cibernéticos, los cuales son productos que además de hacerle frente, entre muchos otros riesgos, a las violaciones de datos, interrupciones de negocios, y a los daños a la reputación, así mismo llevan a un mayor análisis de los productos, y tendencias en el mercado asegurador.

Puntualmente, se puede decir, que estos son unos productos, encaminados a brindar una cobertura financiera, legal, y de asistencia, a las empresas y/o personas naturales, que busquen salvaguardarse de los nuevos y cada vez más frecuentes, ataques cibernéticos.

Así mismo, estos seguros ayudan a los asegurados, a poder mitigar, o cubrir el impacto financiero derivado de hacerle frente a un ataque cibernético. Adicionalmente, podrían ser de utilidad, al momento de entrar a ayudar a proteger o restaurar la reputación, y la confianza de los clientes después de un ataque. Otro de los puntos por medio de los cuales los seguros cibernéticos son de gran ayuda en la actualidad, es precisamente, porque al momento de la suscripción del seguro, son las mismas aseguradoras, las que, a efectos de cumplir con los requisitos regulatorios, y proporcionar cobertura adecuada para dichos riesgos cibernéticos, revisan las regulaciones y las normas de vanguardia que potencialmente pudiesen proteger la privacidad, y la seguridad, de los sistemas informáticos de sus clientes.

Adicionalmente, otro punto importante a destacar, es que los seguros cibernéticos, ofrecen una serie de beneficios a los interesados en asegurarse, como lo son, una mejoría en la gestión del riesgo, puesto que las personas y las empresas, logran identificar y evaluar sus riesgos cibernéticos, implementando medidas para mitigarlos si buscan el aseguramiento. Lo anterior, conlleva una tranquilidad y confianza intrínseca, al saber que en caso de algún desafortunado ataque cibernético, estarían financieramente protegidos. Aunado a todos estos beneficios, en caso de un inminente riesgo cibernético, con la protección del seguro de riesgo cibernéticos tienen, asimismo, acceso a expertos, y a una asistencia de especialistas, para poder responder al ataque y minimizar el daño.

Se podría decir, entonces, que gran parte del crecimiento de este mercado, se ha dado, no solo por el crecimiento de los ataques cibernéticos, sino también, por la creciente conciencia, respecto de la importancia de poder estar protegido contra estos riesgos. De dicha manera, se ve cómo claramente se tiene una demanda de parte de los posibles tomadores y/o asegurados, respecto de querer protegerse frente a riesgos, como podrían ser las violaciones de datos, daños a la reputación, o interrupciones del negocio. Pero se cuestiona, ¿existe una oferta correspondiente y proporcional, de parte de las compañías de seguros?

La respuesta que hemos podido encontrar respecto de dicho interrogante, es que, precisamente, de parte de las diferentes compañías de seguros, si existiría una oferta, y un interés, en poder asegurar los riesgos cibernéticos, al ser un mercado en constante crecimiento, con una alta demanda, al ser productos especializados y específicos, destinadas para las necesidades de diferentes empresas y sectores. Sin embargo, no se puede desconocer, que existe una gran desconfianza en la materia, que no permite que sean tan competitivas, por los costos, y complejidades que dicho ramo trae consigo.

Si bien las compañías de seguros están constantemente adaptando sus ramos y productos, a efectos de poder satisfacer las diferentes y cambiantes necesidades del mercado, los seguros de riesgos cibernéticos, presentan sin duda, un desafío, puesto que deben ser seguros, más flexibles, y personalizados a sus clientes. Adicionalmente, una de las complejidades que podría traer consigo este aseguramiento, es el hecho que, no es posible cuantificar y evaluar, por la constante evolución de la materia, los riesgos cibernéticos, y ello es realmente lo que genera incertidumbre de parte de las compañías de seguros, de brindar estas coberturas.

Debido a lo anterior, es que las compañías de seguros han empezado a implementar alianzas estratégicas con empresas de tecnología, y consultoras de seguridad, a efectos de poder mejorar su capacidad para evaluar, entender, y mitigar los riesgos cibernéticos, así como también poder ofrecer servicios adicionales de gestión de incidentes y evaluaciones de seguridad.

Sin embargo, para que estos seguros de riesgos cibernéticos sean efectivos, es necesario que se cuente con la confianza, tanto por parte de los clientes que adquieren las pólizas, como de las aseguradoras que las ofrecen. Solo de esta forma, las necesidades de los clientes serán atendidas de manera adecuada, y solo así las compañías de seguros podrían cumplir con sus amparos, en caso de un incidente cibernético.

Precisamente entonces, unos de los latentes desafíos que se encuentran hoy en día respecto de los seguros de riesgos cibernéticos, es que este tipo de pólizas, además de ser costosas, en especial para las empresas con un alto riesgo de ataque, así mismo son complejas de entender (en gran parte por su novedad), lo cual puede llevar a que no se elijan las coberturas adecuadas y atinentes para hacerle frente al riesgo cibernético, y así mismo, puede terminar ocurriendo, que ciertos riesgos se crean cubiertos, pero en realidad estén excluidos.

Algunos desafíos a la hora de construir confianza por parte del cliente asegurado son:

- Como el panorama de amenazas cibernéticas, está siempre en constante evolución, los riesgos cubiertos por una póliza de seguro cibernético pueden llegar a cambiar con el tiempo. Precisamente por eso, se debe estar revisando constante y regularmente la póliza, actualizándola si es necesario, a efectos de poder garantizar que esté totalmente protegido contra las nuevas amenazas.

- El punto anterior, será también de relevancia, a la hora de comprender las exclusiones que pueden limitar la cobertura de este tipo de productos, puesto que por lo general, y como todavía no se tienen completamente diseñados estas pólizas –en parte también por la naturaleza cambiante de las mismas– genera que ciertos tipos de ataques, o daños a la reputación de la empresa, o de costos asociados a la interrupción del negocio, o que pérdidas que no estén totalmente respaldadas se encuentren excluidas.

- Así mismo, si bien tendrían confianza en la compañía aseguradora, y en el negocio aseguraticio, y por eso mismo buscan asegurarse, deberán propender por comparar diferentes pólizas de riesgos cibernéticos, encontrando así, la que mejor se adapte a las necesidades deseadas.

- A efectos de minimizar también el impacto financiero, en caso de que ocurra un ataque cibernético, no se deberían confiar únicamente del hecho de que tengan una póliza contratada. Por el contrario, es importante que se implementen diferentes medidas de seguridad, que logren reducir este riesgo.

- No se debe desconocer, que las primas de los seguros de riesgos cibernéticos, son, por regla general, bastante elevadas, por lo que deberían optar por ellas, las personas que tengan un alto riesgo de ataque. Por el contrario, los costos de estas pólizas, pueden llegar a no ser justificables, si ya cuentan con medidas de seguridad cibernética robustas, o si tienen un bajo perfil de riesgo.

- Así mismo, no se debe desconocer, que en caso de un ataque cibernético, las compañías de seguros, estarían en la facultad de subrogarse en los derechos del asegurado, a efectos de poder reclamar daños y perjuicios a los responsables del ataque.

Así mismo, algunos de los desafíos a la hora de construir confianza por parte de las aseguradoras son:

- Se debe partir de la buena fe del contrato de seguro. Precisamente por ello, se debe tener la confianza de parte de las compañías de seguros, frente a que sus clientes, sean transparentes al momento de efectuar la declaración del riesgo, de conformidad con el artículo 1058 del Código de Comercio, partiendo de la base de una colaboración y un compromiso mutuo, a efectos de poder garantizar el éxito y la efectividad de los seguros de riesgos cibernéticos.

- Precisamente como las compañías conocen que no siempre sus clientes asegurados declaran con exactitud el riesgo que buscan trasladar, o a veces estos mismos no conocen a ciencia cierta la magnitud de sus riesgos, se genera al momento de establecer esta relación de confianza, una especie de cautela, a la hora de asegurar los riesgos cibernéticos, lo que genera el cobro de primas más altas, para compensar la incertidumbre.

- Como estos productos de seguros de riesgos cibernéticos son muy nuevos, uno de los desafíos en la construcción de confianza de parte de las aseguradoras, también es la falta de datos históricos confiables, y la dificultad para desarrollar modelos de riesgo precisos, que puedan ser utilizados para la determinación de primas de seguro adecuadas.

- Aunque son latentes los desafíos en la evaluación del riesgo, y en el desarrollo de productos, las compañías de seguros están adaptando sus ofertas para poder satisfacer las necesidades cambiantes del mercado, pudiendo proporcionar cobertura efectiva contra las amenazas cibernéticas. Un inconveniente que se puede presentar frente este aspecto, es precisamente que los costos derivados y relacionados con la respuesta a incidentes cibernéticos, representan gastos elevados para las compañías de seguros, lo cual les puede ser perjudicial, si no tienen los recursos adecuados para gestionar eficazmente las reclamaciones.

- Así mismo, las aseguradoras en esta construcción de confianza, se tienen que enfrentar al riesgo que les presenten reclamaciones fraudulentas, por lo que es importante que las empresas, logren implementar medidas, a efectos de poder prevenir el fraude, y solo se le presenten reclamaciones legítimas.

- De la mano con el punto anterior, se puede también afirmar, que con el aumento en la gravedad y frecuencia de los ataques cibernéticos, las compañías de seguros estarían expuestas a un número mayor de reclamaciones y pérdida financieras, lo que conllevaría que las mismas terminen siendo un poco más cautelosas y prevenidas al ofrecer coberturas por riesgos cibernéticos.

- Adicionalmente, otro factor que puede influir en la disposición de ofrecimiento de seguros de riesgos cibernéticos, es el marco legal, y la regulación

del país, analizando los avances, y filosofías que se tengan respecto de la seguridad cibernética, y la privacidad de datos.

DESAFÍOS DE LOS SEGUROS DE RIESGOS CIBERNÉTICOS

A medida que las amenazas cibernéticas evolucionan en complejidad y alcance, los seguros de riesgos cibernéticos, se enfrentan a una serie de desafíos importantes. Por un lado, la continua y creciente sofisticación de los ataques cibernéticos trae consigo nuevos desafíos, y riesgos para las aseguradoras, en términos de evaluación y gestión de riesgos. Así mismo, el continuo crecimiento del mercado de seguros de riesgos cibernéticos presenta para las compañías de seguros, oportunidades para expandir la oferta de productos, y de servicios, logrando así, satisfacer la demanda de los clientes, en materia de protección cibernética.

Como se precisó en líneas anteriores, uno de los principales retos para las aseguradoras al momento de tener confianza al momento de expedir estas pólizas de seguros de riesgos cibernéticos, es la evaluación precisa de dichos riesgos. Ello se debe, dado que no se tienen datos históricos confiables, no ayudado por el hecho, que estos riesgos están en constante evolución, no pudiendo entonces las compañías poder calcular adecuadamente el riesgo (ni la exposición total al mismo), y así mismo, calcular una prima de seguro, que logre reflejar con precisión, la probabilidad y magnitud de los incidentes cibernéticos.

A pesar de los desafíos, el mercado de seguros de riesgos cibernéticos, genera así mismo, oportunidades significativas para la innovación. Esto por cuanto que, las aseguradoras están constantemente, desarrollando nuevos productos y servicios, que se puedan adaptar, cada vez más, a las necesidades específicas de las diferentes industrias y personas, siendo estos, más flexibles y personalizados. Además, con cada vez más frecuencia, las aseguradoras están explorando nuevas tecnologías y de enfoques analíticos, para poder mejorar la evaluación de riesgos cibernéticos, proporcionando soluciones, que sean cada vez más, eficaces y rentables.

ASEGURAMIENTO DE LOS RIESGOS CIBERNÉTICOS. PERSPECTIVAS

Después de explorar los desafíos, oportunidades, y el papel crucial de la confianza que existe alrededor de los seguros de riesgos cibernéticos, podemos concluir los siguientes puntos:

1. Resulta de gran importancia presentar estudios de casos, y ejemplos prácticos de cómo las empresas han utilizado los seguros de riesgos cibernéticos para mitigar los riesgos y recuperarse de incidentes cibernéticos.

2. Así mismo, se encontró que el desarrollo de un área técnica con profesionales expertos en riesgos cibernéticos, es necesario en las Compañías Aseguradoras para

la suscripción, la ejecución de las pólizas, y en el momento de las reclamaciones, determinar el siniestro.

3. La tecnología avanza muy rápido, por lo tanto, contar con monitoreo permanente es muy importante, a efectos de poder estar a la vanguardia de los diferentes riesgos cibernéticos, para así también poder identificar los cambios y modificaciones en las coberturas y condiciones de cada póliza.

4. Se debe implementar, y fortalecer la seguridad cibernética de las aseguradoras y de los asegurados, en la revisión constante de las políticas, sistemas y programas, a través del oficial de cumplimiento.

5. Se puede empezar a incluir una sección dedicada a evaluar la efectividad de los seguros de riesgos cibernéticos en la protección contra amenazas cibernéticas. Esto podría incluir análisis de reclamaciones pasadas, estudios de casos de incidentes cibernéticos, y cómo fueron manejados con la ayuda de seguros cibernéticos, así como encuestas de satisfacción de clientes y retroalimentación de la industria.

6. También es importante discutir los desarrollos tecnológicos emergentes que podrían impactar el mercado de seguros de riesgos cibernéticos, y cómo estas tecnologías podrían afectar tanto los riesgos cibernéticos, como las soluciones de seguro.

7. Se destaca como es importante el trabajo en equipo, como la unión de Gobiernos, compañías aseguradoras y reaseguradoras, entidades no gubernamentales, asociaciones nacionales e internacionales en la seguridad cibernética y fortalecimiento de los seguros cibernéticos.

8. El tiempo nos traerá mayor virtualidad en el trabajo y diferentes aspectos de la vida, tanto a las empresas como a las personas, por lo que los seguros cibernéticos tendrán mayor demanda y por lo tanto, las aseguradoras deberán estar más preparadas en el desarrollo constante de estos productos.

9. Al no tener los riesgos cibernéticos fronteras, la regulación de ciberseguridad y de riesgos cibernéticos se proyecta que va a desarrollarse más, hasta convertirse en estándares globales.

10. Si bien las aseguradoras tradicionales no tienen mucha experiencia en la gestión de riesgos cibernéticos, estas están constantemente en evolución, y con la intención de también poder asegurar este otro nuevo merado. Para poder entonces entrar a evaluar de manera precia las primas y la gestión de las reclamaciones, se deberán apoyar de modelos de riesgos precisos.

11. Los términos y condiciones de las pólizas de seguro cibernético pueden ser complejos y difíciles de entender, lo que puede generar disputas entre los asegurados y las aseguradoras. Se debe optar por lograr obtener siempre claridad en los textos, con un lenguaje claro, sencillo, y fácil de entender.

12. A medida que el mercado madure, se espera que las primas se estabilicen y la cobertura se amplíe, lo que facilitará que cada vez más empresas obtengan la protección que necesitan contra los riesgos cibernéticos.

Así las cosas, consideramos que las Compañías Aseguradoras por normatividad, deben cumplir con la obligación de seguridad cibernética, por lo que ya deben contar actualmente con esta área, sin embargo, la contratación de profesionales expertos en ciberseguridad y riesgos informáticos, sería de gran beneficio para las Compañías, para el estudio de los siniestros, el monitoreo y la suscripción.

Es inminente, que todas las personas, bien sean naturales o jurídicas, estarán o ya han estado expuestas a riesgos cibernéticos, por lo tanto, la no inversión en este producto seguros cibernéticos, es un gran error. Estos clientes, que buscan asegurar dichos riesgos, deberán tener la confianza, no solo de las medidas de seguridad cibernética ya implementadas por ellos, sino también, de los productos aseguraticios que pudieron haber contratado.

De la mano con lo anterior, las compañías de seguros, estarían desaprovechando una gran oportunidad, y un gran mercado, de no estar ofreciendo y/o implementado estos seguros de riesgos cibernéticos, al ser, hoy en día, de los productos más necesarios para todas las personas conectadas digitalmente. De su parte, se debe tener confianza en el modelo de negocio que manejan, en los datos históricos que han podido recolectar en sus investigaciones, y en el hecho de que se presente un ataque cibernético puntual, puedan contar con todas las herramientas necesarias, para poderlo atender.

Así mismo, para que las aseguradoras sientan confianza digital en los seguros de riesgos cibernéticos y puedan ofrecer cobertura de manera efectiva, es importante implementar estrategias que mejoren la seguridad cibernética y la transparencia en la gestión de riesgos. Una de las formas por medio de las cuales podrían llegar a ello, puede ser el implementar sistemas de monitoreo continuo y alerta temprana para detectar posibles amenazas cibernéticas y responder rápidamente a incidentes.

De la mano con los puntos anteriores, se ve también cómo la promoción de campañas en pedagogía del valor de adquirir seguros cibernéticos es indispensable.

CONCLUSIONES

En un mundo cada vez más interconectado, y dependiente de la tecnología digital, los seguros de riesgos cibernéticos han surgido como una herramienta esencial para mitigar las crecientes amenazas cibernéticas que enfrentan las organizaciones y los individuos. A lo largo del presente texto, hemos venido explorado los desafíos y oportunidades en el mercado de seguros de riesgos cibernéticos, así como el papel crítico de la confianza en esta relación.

La evolución tecnológica seguirá dando pasos muy grandes, con el desarrollo de la inteligencia artificial, el metaverso, entre otros, lo que indefectiblemente nos llevará a la necesidad de seguir desarrollando este producto de seguro de riesgos cibernéticos a través de sus diferentes coberturas y amparos.

Desde la evaluación precisa de los riesgos cibernéticos, hasta la innovación en productos y servicios, las aseguradoras continúan adaptándose y evolucionando para satisfacer

las necesidades cambiantes de los clientes en materia de protección cibernética. Al mismo tiempo, los clientes también juegan un papel crucial al implementar medidas de seguridad cibernética sólidas, tratando de mantener una relación de confianza con sus aseguradoras.

A medida que avanzamos hacia el futuro, es fundamental que todas las partes involucradas en la protección contra amenazas cibernéticas trabajen juntas de manera colaborativa y proactiva. La educación y la concientización sobre seguridad cibernética, el aprovechamiento de tecnologías emergentes y la adaptación continua a las tendencias del mercado son aspectos clave para garantizar la efectividad y el éxito de los seguros de riesgos cibernéticos.

El trabajo constante con profesionales especializados en ciberseguridad, ingenieros capacitados en el desarrollo constante en las diferentes amenazas que pueden surgir con el desarrollo tecnológico, es de vital importancia. En especial, en el momento de la suscripción de los seguros de riesgos cibernéticos, con el trabajo mancomunado de estos profesionales expertos será fundamental.

También es necesario implementar el monitoreo constante por parte de las aseguradoras, a través de los profesionales especialistas o empresas de ingeniería, a las empresas o personas aseguradas para fortalecer sus herramientas actuales de la ciberseguridad y reducir los incidentes.

Así mismo, es necesario impulsar la capacitación a nuevos profesionales expertos en la ciberseguridad y los riesgos informáticos, pues hoy en día son pocos, y las amenazas aumentan diariamente.

La confianza de las aseguradoras en abrir esta línea de producto de los seguros cibernéticos, sin duda alguna se logra con la capacitación, y con el contar con profesionales expertos en ciberseguridad y riesgo informático, revisando las coberturas, exclusiones y condiciones generales, así como la suscripción, monitoreo y asesoramiento a los asegurados, por lo que motivamos a las aseguradoras que inicien en el desarrollo de estos nuevos productos.

En última instancia, al centrarnos en la confianza mutua, la transparencia y el compromiso con la seguridad cibernética, podemos construir un futuro más seguro y resiliente en el ciberespacio para todos.

Los seguros cibernéticos son una herramienta importante para proteger a las empresas de los riesgos cibernéticos, sin embargo, hoy en día, estos productos no logran satisfacer a cabalidad las necesidades de protección que actualmente se está demandando en el mercado.

Aunque existen algunos desafíos, como el costo y la complejidad, los beneficios de los seguros cibernéticos pueden superar significativamente estos retos. Se espera que el mercado de seguros cibernéticos siga creciendo y evolucionando en los próximos años, ofreciendo a las empresas una mayor variedad de opciones y precios más competitivos.

BIBLIOGRAFÍA

2023 Cyber Insurance Market Update. (2023). Retrieved from https://www.youtube.com/watch?v=ju0KtELoFDU

Benito Osma, Félix (2022). *El contrato de seguro en un mercado digital,* 56 Rev. Ibero-Latinoam. Seguros, 45-72. https://doi.org/10.11144/Javeriana.ris56.csmd

Benito Osma, Félix (2022). *La digitalización en el mercado de seguros*, 57 Rev.Ibero–Latinoam. Seguros, 199-230. https://doi.org/10.11144/Javeriana.ris57.dmds

Bousakr, N. (2020). *Beazley lanza una línea de seguros de líneas financieras y cibernéticas en Colombia. Property & Casualty 360*.

Campoy, A. J., Malfatti, M. A., Malfatti, M. S. L., & Rumstain, T. D. C. (2020). *Contrato de seguro. La obligación de información y agravación del riesgo cibernético.* Revista Ibero-Latinoamericana de Seguros, 29(52). https://doi.org/10.11144/Javeriana.ris52.csoi

Campoy, Adilson José; Malfaltti, Marcio Alexandre; Malfatti, Michelle Sampaio Lopes & Rumstain, Thaís de Cássia. (2020). C*ontrato de seguro-La obligación de información y agravación del riesgo cibernético,* 52 Rev.Ibero-Latinoam. Seguros, 131-144. https://doi. org/10.11144/Javeriana.ris52.csoi

Coberturas de responsabilidad civil en las pólizas de riesgos cibernéticos frente a un evento de fuga de datos o "data breach" en Colombia tesis de maestría https://repository.javeriana.edu.co/bitstream/handle/10554/63887/Coberturas%20de%20responsabilidad%20civil%20en%20las%20p%c3%b3lizas%20de%20riesgos%20cibern%c3%a9ticos%20frente%20a%20un%20evento%20de%20fuga%20de%20datos%20o%20%e2%80%9cdata%20breach%e2%80%9d%20en%20Colombia.pdf?sequence=1&isAllowed=y

Cole, N. (2023) *23 eye-opening Cybersecurity Insurance Statistics* (2023), Network Assured. Available at: https://networkassured.com/security/cybersecurity-insurance-statistics/.

Erkan-Barlow A, Wells-Dietel BP. 2024. The Current State of Cyber Insurance and Regulation in the Context of Investment Efficiency and Moral Hazard: A Literature Review. *Journal of Insurance Regulation*. October 2023:1-27. Accessed February 28, 2024.

Freeman, R. (2022). *What is Cyber Security Insurance?* Retrieved from https://www.youtube.com/watch?v=Bw_GK1R3Gis

González, E. J. (2021). Seguro contra riesgos cibernéticos. In *CE Noticias Financieras* (Spanish ed.). ContentEngine LLC, a Florida limited liability company.

González, E. J. (2021). Seguro contra riesgos cibernéticos. In *CE Noticias Financieras* (Spanish ed.). ContentEngine LLC, a Florida limited liability company.

González, E. J. (2021). Seguro contra riesgos cibernéticos. In *CE Noticias Financieras* (Spanish ed.). ContentEngine LLC, a Florida limited liability company.

How cybersecurity insurance works (2018) YouTube. Available at: https://www.youtube.com/watch?v=J79WqSbdoYw.

Institute of Risk Management. (2022). Cyber group how the insurance industry thinks about Systemic Cyber Risk. Retrieved from https://www.youtube.com/watch?-v=MgutgZKYjgs

INSTRUCTIVO PARA LIQUIDAR Y AJUSTAR SINIESTROS QUE AFECTEN LA COBERTURA DE PÉRDIDAS PROPIAS EN LOS SEGUROS DE RIESGOS CIBERNÉTICOS EN COLOMBIA tesis de maestria https://repository.javeriana.edu.co/bitstream/handle/10554/63920/Tesis%20Trabajo%20de%20Grado__Joseph%20Mclean_versi%c3%b3n%20final%20aprobada.pdf?sequence=1&isAllowed=y

Rodríguez-Márquez, M.P. 2021. "Ciberseguridad en la justicia digital: recomendaciones para el caso colombiano" Rev. UIS Ing., vol. 20, no. 3, pp. 19-46, 2021, doi: 10.18273/revuin.v20n3-2021002

Monterrosso Casado, E. (2019). *Inteligencia artificial y riesgos cibernéticos: responsabilidades y aseguramiento.* Tirant lo Blanch.

Nava, R. (2016, Nov 16). *Apuntan aseguradoras a riesgos cibernéticos. El Norte Retrieved from* https://www.proquest.com/newspapers/apuntan-aseguradoras-riesgos-cibernéticos/docview/1847735592/se-2

Doria Arcila, N. (2012). Riesgos cibernéticos ya se pueden asegurar. *Portafolio*.

Doria Arcila, N. (2012). *Riesgos cibernéticos ya se pueden asegurar.* Portafolio, Retrieved from https://www.proquest.com/trade-journals/riesgos-cibernéticos-ya-se-pueden-asegurar/docview/1235693827/se-2

Ospina Díaz, Milton Ricardo & Sanabria Rangel, Pedro Emilio. (2020). *Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia.* Revista Criminalidad, 62(2), 199-217. Epub November 26, 2020. Retrieved March 31, 2024, from http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199&lng=en&tlng=es.

Pimienta Anaya, M. y Suarez Vanega, L. (2023). R*iesgos cibernéticos en Colombia: un estudio de la percepción y su impacto en la seguridad.* Universidad Cooperativa de Colombia, Posgrado, Maestría en Gestión de Tecnologías de Información, Bucaramanga.

Previti, L. (2023). *Public-private collaboration in the cybersecurity system: reflections from the European and Italian strategy.* REGAP: Revista Galega de Administración Pública, 1(65), 105–123.

Rae Confianza: Diccionario Esencial de la lengua española, 'Diccionario esencial de la lengua española'. Available at: https://www.rae.es/desen/confianza.

Saldívar, B. (2020). Seguro de riesgos cibernéticos toma relevancia por Covid-19. In *CE Noticias Financieras* (Spanish ed.). ContentEngine LLC, a Florida limited liability company.

Sánchez Barrios, M., Jiménez Naharro, F., & Sánchez Montañés, C. (2018). La transferencia de los riesgos cibernéticos en empresas internacionales con alto nivel de capitalización bursátil. *Revista de Pensamiento Estratégico y Seguridad CISDE*, *3*(1), 67–90.

Saraiva Lima, H. J. (2022). Nuevas tecnologías, protección de datos personales y el seguro. *Revista Ibero-Latinoamericana de Seguros*, *31*. https://doi.org/10.11144/javeriana.ris57.ntps

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

Saraiva Lima, Henrique José. Nuevas tecnologias, protección de datos personales y el seguro, 57 Rev.Ibero-Latinoam.Seguros, 249-270 (2022). https://doi.org/10.11144/Javeriana.ris57.ntps

Signorino Barbat, A. (2020). Ciber riesgos: Su dimensión social, funcional y etica. *Revista Ibero-Latinoamericana de Seguros*, *28*(51). https://doi.org/10.11144/Javeriana.ris51.crsd

Signorino Barbat, A. (2022). Los seguros cibernéticos: Alcance frente a los Ciber Riesgos. *Revista Ibero-Latinoamericana de Seguros*, *31*. https://doi.org/10.11144/javeriana.ris57.scaf

Signorino Barbat, Andrea. (2019). Ciber riesgos: Su dimensión social, funcional y ética, 51 Rev.Ibero-Latinoam. Seguros, 35-56. https://doi.org/10.11144/Javeriana.ris51.crsd

Sobrino, W. (2018). Los seguros de 'cyber risk' (A propósito del ciberataque mundial de fecha 12 de mayo de 2017). *Revista Ibero-Latinoamericana de Seguros*, *26*(47). https://doi.org/10.11144/Javeriana.ris47.lscr

Sobrino, Waldo. (2017). Los seguros de 'cyber risk'. (A propósito del ciberataque mundial de fecha 12 de mayo de 2017), 47 Rev.IberoLatinoam.Seguros, 137-164. https://doi.org/10.11144/Javeriana. ris47.lscr

Tapia Hermida, Alberto J. (2021). La responsabilidad civil derivada del uso de la inteligencia artificial y su aseguramiento, 54 Rev.Ibero-Latinoam.Seguros, 107-146.

Toro-Álvarez, M. M. (2013). El control del cibercrimen. Análisis exploratorio de sentencias y medidas de supervisión. Revista Logos Ciencia & Tecnología, 15(2), 162-173. https://doi.org/10.22335/rlct.v15i2.1768 (ESTADOS UNIDOS)

Una encuesta de AIG revela que hay más gerentes responsables de tomar decisiones sobre seguros preocupados por las amenazas cibernéticas que por otros riesgos importantes: Desarrolla la primera aplicación móvil de gestión de riesgos cibernéticos, lanza otras herramientas para complementar la solución de seguros CyberEdge y para satisfacer la demanda de información sobre amenazas cibernéticas. In *Business Wire en Español*. Business Wire.

Understanding the (cyber) insurance business. (2023b). Retrieved from https://www.youtube.com/watch?v=L-1vjCPZ91Y

Varela, C. (2023). Riesgo cibernético y ciberseguros. Revista Fasecolda, (190), 84–89. Recuperado a partir de https://revista.fasecolda.com/index.php/revfasecolda/article/view/911

Visbal, M. (2021). Un seguro de Riesgos Cibernéticos es la solución absoluta al problema? *Expansión (Mexico City, Mexico)*.

What is Cybersecurity Insurance? (2021). Retrieved from https://www.youtube.com/watch?v=lnHZkiNdqsI