El Contrato de Seguro Cibernético

Trabajo de grado para optar por el título de abogadas

Presentado por:

[1]Tatiana López Martín y [2] Karol Violeta Hernández

Asesora:

Dacmar Andrea Báez Mesa

Facultad de Derecho, Universidad Santo Tomas

Agosto 2020

[1] Facultad de derecho, Universidad Santo Tomas, correo institucional tatianalopez@usantotomas.edu.co

[2] Facultad de derecho, Universidad Santo Tomas, correo institucional karolhernadezm@usantotomas.edu.co.

Resumen

El artículo analiza las situaciones presentadas hoy en día con los desarrollos tecnológicos y su relación con la creación de nuevos riesgos que en materia de seguros suponen; riesgos que hoy por hoy son en su mayoría considerados delitos como por ejemplo ciberdelincuencia, suplantación de sitios web para capturar datos personales y phishing (técnica de ingeniería social para obtener información confidencial).

Eso ha dado lugar a la aparición del contrato de seguros cibernéticos como solución a esa problemática, tanto así que para Amparo Zabala responsable del producto de ciberriesgo en Zurich Empresas, los seguros cibernéticos unen la responsabilidad civil con la cobertura de daños propios y evolucionan con cada nuevo riesgo (Zabala,2015).

Sin embargo, no es posible establecer que en Colombia haya regulación expresa sobre el Cyber Risk (Riesgo Cibernético) es por ello que se vuelve conveniente saber cuáles serían esos factores de riesgo cibernético. Algunas de las ideas más relevantes al respecto giran en torno a la protección de la contaminación o destrucción de datos, el D.O.S (Denial of services), y la responsabilidad por la divulgación de datos personales por ejemplo clientes, proveedores o los trabajadores.

Palabras clave: Riesgo cibernético, seguros, ciberdelincuencia, seguro cibernético.

Abstract

The article analyzes the situations presented today with technological developments and their relationship with the creation of new risks that in insurance matters they entail; risks that today are mostly considered crimes such as cybercrime, spoofing websites to capture personal data and phishing (social engineering technique to obtain confidential information).

This has given rise to the emergence of the cyber insurance contract as a solution to this problem, so much so that for Amparo Zabala, responsible for the cyber risk product at Zurich Empresas, cyber insurance combines civil liability with their own damage coverage and evolves with each new risk (Zabala, 2015).

However, it is not possible to establish that in Colombia there is an express regulation on Cyber Risk (Cyber Risk), which is why it becomes convenient to know what these cyber risk factors would be. Some of the most relevant ideas in this regard revolve around the protection of contamination or destruction of data, the D.O.S (Denial of services), and the responsibility for the disclosure of personal data for example customers, suppliers or workers.

Keywords: Cyber risk, assured, cybercrime, cyber insurance.

Sumario

Glosario

- **Ciber resiliencia:** la forma con la que una compañía o entidad del gobierno va a poder mantener sus operaciones ante algún tipo de ataque informático o ataque de ciberseguridad. Es decir, la ciber resiliencia trata sobre la capacidad de una organización para prevenir, identificar y contener las amenazas contra datos o información de mucho valor. Todas estas acciones se ejecutan de forma rápida para reducir el tiempo de exposición.
- **Ciber riesgo:** Son todos aquellos riesgos a los que está sometido un sistema informático y la dependencia a este que pueda tener una empresa.
- **D.O.S:** denial of service/ ataque de negación del servicio.
- **Internet de las cosas:** es un concepto que se refiere a la interconexión digital de los objetos cotidianos con Internet, convirtiéndose así en objetos inteligentes.
- **Malware:** es una abreviación de las palabras “malicious software”, software malicioso. Esto significa que el software está diseñado y creado para causar daño a un dispositivo o a su usuario. Es un término general usado para clasificar archivos o software que causan daños una vez que entran en su sistema**.**
- **Medios electrónicos:** son todos aquellos instrumentos creados para obtener un eficiente intercambio de información de forma automatizada; tales como internet, celulares y correo electrónico.
- **Ramsonware:** es un virus que no permite al usuario acceder al sistema y archivos de su ordenador o dispositivo móvil, solicitando el pago de una cantidad a cambio de la recuperación del acceso.

- **Riesgo:** riesgo asegurable, como uno de los elementos esenciales del contrato de seguro, lo cual es en sí una incertidumbre que se refiere a si el hecho se presentara o no.

Introducción

El contrato de seguros cibernético surge como una solución a aquellos problemas de ciberdelincuencia y hackeo de la información que sufren las empresas víctimas como consecuencia del desarrollo tecnológico negativo. Es aquí, donde las compañías de seguros deberían asumir los riesgos originados por los impactos y/o efectos que producen los nuevos cambios en materia de contratos.

En lo que respecta a los contrato de seguro cibernético y en particular lo relacionado con el manejo de la información, puesto que esta enmarca desde el hurto, destrucción, contaminación de datos de la empresas hasta las mismas extorsiones por parte de los hacker para quienes les es valiosa la información, es fundamental mostrar que el marco por el cual los nombrados contratos se deben regir, no se encuentra regulado, siendo esta la razón por la cual la presente investigación pretende desarrollar ¿cuáles son los factores del riesgo cibernético y cuáles serían los elementos de protección en el contrato de seguros cibernético?.

Lo anterior con el fin de demostrar que en Colombia no existe tal regulación a este tipo de contratos; los cuales surgen con la necesidad de trasladar a una compañía de seguros los riesgos y problemas que el hackeo a una empresa trae consigo, por consiguiente, es necesario e indispensable fijar unas condiciones generales de

contratación para que, a partir de este estudio, se pueda establecer un marco normativo para tal fin.

La presente investigación tiene un enfoque jurídico, con métodos de investigación cualitativos y con herramientas de revisión documental, tomando como base cada uno de los objetivos específicos planteados en el proyecto de investigación.

Para el procesamiento y análisis de la información se tomó como base el modelo guía de "Sistematización de la Información Documental", mediante el cual se logró recolectar la información de manera precisa y ordenada, destacando los puntos claves y esenciales.

Marco jurídico nacional e internacional

Colombia

En este capítulo, abordaremos los antecedentes para la instauración de políticas y estrategias que ha adoptado el Gobierno Colombiano para combatir los delitos cibernéticos, en primera instancia encontramos el Conpes 3701, realizado en el 2011, el cual adopta la dirección de políticas para la ciberseguridad y ciberdefensa; que tenía como finalidad principal reforzar las estrategias del Estado para poder combatir los ataques cibernéticos; de la misma manera crea lineamientos de protección para salvaguardar la seguridad del Estado; de esta forma se crea el grupo de respuestas de emergencia cibernéticas de Colombia, el centro cibernético policial y el comando conjunto cibernético; con este documento se destaca la preocupación del Gobierno nacional, para combatir los delitos que trae la tecnología.

Por otro lado, teniendo en cuenta los pasos agigantados que da la tecnología, se ve la necesidad de implementar legislación que abarque la protección de información

personal en el ámbito digital, por ende, se expide la ley estatutaria 1581 de 2012, en la cual se eleva a rango constitucional el derecho que tienen todas las personas a conocer, actualizar y rectificar su información personal, es por este motivo que se implementa un entorno normativo que tiene en sí mismo el reconocimiento de los datos e información personal, como un bien tutelable.

Luego de analizar los riesgos que acarrea el avance de la tecnología, el gobierno, genera nuevas directrices, creando el Conpes 3854 de 2016, en el cual se establece la Política Nacional de Seguridad Digital, con estos nuevos lineamientos, la protección para los riesgos digitales, se expande, pues ya no solo se interesa en la seguridad digital del Estado, sino que va más allá, incluyendo a las partes interesadas que se desenvuelven en el campo de la era digital, por este motivo dicho documento incorpora estrategias para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital, pese a los esfuerzos que se hicieron, "estos lineamientos resultaron ineficientes, en cuanto a la defensa y seguridad digital". (Documento CONPES 3995 *Por la cual se establece la política nacional de confianza y seguridad digital*)

Por lo anterior, en el año 2018 se expide el decreto 1008, que establece los lineamientos generales de la política de Gobierno Digital, "esta política establece que la seguridad de la información es uno de los habilitadores transversales, es decir, que es uno de los elementos fundamentales que permiten el desarrollo del gobierno digital. Desde lo relativo a la confianza digital, esta política también busca preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos". (Documento CONPES 3995 *Por la cual se establece la política nacional de confianza y seguridad digital*)

Por otro lado, en 2019, se expide la ley 1955 de 2019, la cual contiene el plan Nacional de desarrollo 2018 -2022 Pacto por Colombia, Pacto por la Equidad. Específicamente, en el capítulo VII Pacto por la transformación digital de Colombia: Gobierno, empresas y hogares conectados con la era del conocimiento, "se busca que el país se encamine hacia una sociedad digital y hacia la industria 4.0, a través de la generación de confianza en el entorno digital y del desarrollo de estrategias sobre seguridad digital en los territorios. Por su parte, en el capítulo I Pacto por la legalidad: seguridad efectiva y justicia transparente para que todos vivamos con libertad y en democracia, se establece como estrategia para promover el control integral marítimo, terrestre, aéreo, fluvial, espacial y ciberespacial que el Gobierno Nacional fortalezca las capacidades de ciberseguridad y ciberdefensa para garantizar los intereses nacionales". (Documento CONPES 3995 *Por la cual se establece la política nacional de confianza y seguridad digital*)

En cuanto a la legislación penal nacional, encontramos sanciones dirigidas para los delitos informáticos, a partir de la ley 1273 de 2009; se tipifican estos delitos en nuestra legislación de la siguiente manera: acceso abusivo a un sistema informático, obstaculización ilegítima del sistema informático o red de telecomunicación; interceptación de datos informáticos; daño informático; uso de software malicioso; hurto por medios informáticos y semejantes; violación de datos personales; suplantación de sitios web para capturar datos personales y transferencia no consentida de activos. Esta tipificación ha ayudado, para que las entidades públicas y privadas, puedan atacar y evitar las contingencias que generan los delitos informáticos, y en consecuencia iniciar las acciones penales correspondientes, contra aquellos que incurran en estos delitos.

Internacional

Una de las primeras preocupaciones en materia de comercio electrónico se vio reflejada por la comunidad internacional en la Ley Modelo de la CNUDMI sobre Comercio Electrónico y su guía para la incorporación al derecho interno de 1996, la cual pretendía ayudar a todos los estados miembros a fortalecer la legislación existente sobre el uso de medios de almacenamiento de información y métodos de comunicación sustitutivos del papel, ofreciendo a los legisladores un compendio de reglas internacionalmente aceptadas que evitaran obstáculos jurídicos y permitieran fluidez al comercio electrónico, que con el tiempo se fue especializando y perfeccionando hasta dar a luz otros convenios y normas que a nivel internacional permiten hoy la comunicación, transacciones y regulación de contratos a nivel mundial.

Desde la perspectiva de los ciberriesgos, se torna inevitable hablar del convenio de Budapest, el cual reunió a una serie de expertos del ciberespacio, juristas, miembros de la policía y expertos informáticos, para debatir problemas del ciberespacio; 4 años después de la creación de este comité se logra la firma de un marco legislativo común para los estados miembros el cual define los delitos informáticos conteniéndolos en cuatro grupos:

1. “Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos.
2. Delitos relacionados con la informática. Se definen la falsificación y el fraude informático.
3. Delitos por su contenido. Comprende las conductas englobadas en los delitos relacionados con la tenencia y distribución de contenidos de pornografía infantil en la red.

4. Delitos relacionados con las infracciones de la propiedad intelectual y de los derechos afines.

Lo anterior con el fin de perseguir a nivel mundial el delito cibernético, estableciendo entre los países disposiciones que permitan la cooperación efectiva y fiable" (García, 2019, p. 38).

El convenio de Budapest fue adoptado en nuestro ordenamiento jurídico por medio de la ley 1928 del 24 de julio de 2018.

Adicionalmente, en el mes de mayo de 2018 se incorpora a la legislación Europea, el Reglamento Europeo en materia de Protección de Datos Personales el cual significó un cambio en la comprensión del Ciberriesgo en la Unión Europea y su tratamiento, pues no solo aplica para los países de la Unión si no que amplía su espectro a cualquiera dentro o fuera de la unión que trate datos personales de ciudadanos de la Unión Europea, los cuales deben conocer dicha normatividad y garantizar medidas para su cumplimiento.

Otras leyes a nivel internacional que desde la seguridad informática pueden afectar a las organizaciones y personas independientes, que pueden ser compiladas en el contrato de seguros son:

- Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, que reglamentan temas legales de las ocupaciones comerciales y económicas que se derivan del comercio electrónico, esto es aquellos negocios que tengan nexos con internet, así como la contratación por medio electrónico, la publicidad y servicios de intermediación, un ejemplo de la materialización de esta norma se da en el establecimientos de las "cookies" las cuales permiten el

almacenaje de la información del usuario en su dispositivo, para ello habrá que solicitar el consentimiento del usuario para que se instale.

- Ley de Propiedad Intelectual, que protege y reglamenta los derechos inherentes a la creación y uso de invenciones de tipo literario, científico, producciones en formato digital como spots, videos, contenido multimedia, entre otros. La protección se predica tanto de los derechos morales como de los patrimoniales; de aquí que ni las empresas ni las personas puedan usar estas obras sin pagar derechos de autor.

Finalmente, en lo que tiene que ver con pólizas de ciberriesgo, algunas de las leyes actuales a nivel internacional son:

- Ley Orgánica 15/1999, sobre la Protección de Datos de Carácter Personal cuya finalidad es la protección de la intimidad de las personas y sus datos personales, esto tiene que ver con las libertades públicas, tratamiento de datos y derechos fundamentales de las personas. Lo anterior teniendo en cuenta que tanto clientes, proveedores y empleados utilizan datos personales lo cual los vuelve garantes del cumplimiento de esta legislación.
- Real Decreto 1720/2007, el cual reglamentó y desarrolló la Ley Orgánica 15/1999.
- Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, que busca el amparo de las personas en lo que tiene que ver con el tratamiento de datos personales y la libre circulación de esos datos.

Naturaleza jurídica

A nivel general, es posible afirmar que el contrato de seguros es de naturaleza consensual ya que la característica que debe primar en el contrato es el consentimiento en cuanto a que el contratante es libre de contratar o en este caso tomar o no una póliza de seguros; sin embargo, por lo general son contratos preestablecidos, donde las cláusulas ya están previamente estipuladas; en este sentido, autores como el profesor Fernando Palacios se expresan al respecto en los siguientes términos:

> "Resulta extraño afirmar que el contrato de seguro es de adhesión, siendo contrato consensual, pues en este el cruce de voluntades es previo al nacimiento del contrato, es decir, sin deliberación no hay contrato consensual y los de adhesión se caracterizan por la ausencia de tal deliberación" (Palacios, 2016, p. 43)

La realidad es que para el caso de los contratos de seguros, la voluntad de la parte que se adhiere no se ve excluida, sino se ve representada al decidir si toman o dejan el ofrecimiento, ahora bien, al momento de aceptar se ve reflejado el contrato de seguros como un contrato de adhesión, puesto que quien acepta en la mayoría de los casos no puede negociar las clausulas de la póliza, es en este caso en que las condiciones generales de los clausulados se vuelven particulares para quien acepta suscribir la póliza; así mismo, no podemos generalizar los casos en que las aseguradoras son la parte dominante de la relación contractual, la excepción a la regla la muestran las grandes empresas cuándo son las aseguradas, puesto que estas son las que definen las condiciones del contrato, planteando los requerimientos económicos, técnicos y financieros que deben tener los mismos.

Al final estas dos figuras jurídicas, consensualidad y adhesión no se excluyen en el contrato de seguro, simplemente la voluntad se manifiesta en decir “lo tomo” o “lo dejo”

Características del Contrato de Seguro

Contrato Condicional

Analizando el contrato de seguro, podemos destacar que este tiene como característica una obligación condicional (hecho futuro e incierto), no sabemos cuando el siniestro va a ocurrir y de qué forma ocurrirá, en este sentido en cuanto al asegurador, la obligación tendrá que darse siempre y cuando el riesgo (contingencia) se cumpla; de este modo, como se define en la doctrina “las partes están sometidas a una contingencia, que puede representar una utilidad, para uno y una pérdida para el otro” (Burgos, 2008, p.1).

Contrato aleatorio

El contrato de seguros es un contrato aleatorio, en este sentido la ley procura un tratamiento equilibrado entre el riesgo que asume la compañía de seguros y la prima pagada por el tomador del seguro; como se observa existen dos elementos opuestos en el contrato de seguros que a su vez hacen parte de los elementos del contrato; por un lado está el tomador del seguro, que también puede tener la calidad de asegurado, por el otro la compañía de seguros como ente asegurador; además de ellos son esenciales de este tipo de contratos, el riesgo o interés asegurable y la prima, la falta de algunos de estos elementos genera nulidad en el contrato. (Sentencia Exp. 4923/19,1999).

Prevalece la voluntad

Es un contrato en el cual va a predominar la intención de los contratantes; en este sentido, se debe tener autonomía de voluntad para contratar como para modificar e intervenir en el contenido del contrato.

Cabe aclarar que en Colombia se exige que este acuerdo esté pactado por escrito, por ende, podemos decir que es de carácter formal y como lo establece el Código de comercio, dicho contrato se perfecciona, cuando el asegurador suscribe la póliza (Código de Comercio Colombiano [C.de.Co.], 1971, art. 1046), lo anterior para temas probatorios.

Contrato bajo el principio de buena fe

Por otro lado, el acuerdo de seguros se basa en el principio de la buena fe, en este sentido el Código de Comercio observa que el asegurador debe conocer el riesgo que va a amparar, con el objetivo de definir dentro de un marco de libertad si accede o no al contrato y de esta manera determinar el monto de la prima a cobrar (C.de.Co. 1971 art. 1058).

De esta manera se crea una diferencia entre la declaratoria del estado del riesgo a asegurar y la conservación del riesgo asegurado, dentro del cual la primera es responsabilidad de la aseguradora y la segunda del tomador o asegurado.

Contrato oneroso.

El contrato de seguro se caracteriza por la onerosidad, ya que ambas partes tienen obligaciones y ventajas económicas recíprocas, por un lado tenemos al asegurado, que deberá pagar una prima para que se proteja o se asegure un riesgo (objeto del contrato), por otro lado, tenemos la entidad aseguradora, que deberá cumplir con la redención de la obligación al momento de la ocurrencia del siniestro, en este

caso, el pago de una indemnización; por ende, existen posiciones recíprocas en cuanto al principio de onerosidad que rige este contrato.

Contrato de tracto sucesivo

Igualmente, el contrato de seguros es un contrato de tracto sucesivo, es decir las prestaciones se deben desarrollar en un periodo de tiempo constante, hasta que se venza el plazo pactado de la obligación.

Seguro cibernético

En lo que se refiere al fondo, el contrato de Seguro Cibernético no ofrece mayor variación, sigue siendo un contrato bilateral, en donde el pago de una prima trae consigo la protección o el aseguramiento de un riesgo cuando se cumpla la condición; sin embargo, en este punto se vuelve especial, ya que con el devenir de la era digital, nació una nueva clase de contratos; es por esto que al no encontrar definición legal en Colombia, acudimos al panorama Español, y es que de acuerdo con la definición dada por el profesor Fernández, los contratos electrónicos son aquellos "en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectado a una red de telecomunicaciones" (Fernández, 2013, p. 234) sin embargo, y para ir concretando el lugar que ocupa este tipo de contrato, encontramos en la misma obra que hay diferentes modalidades de tipos de contratos online, así que nos ocuparemos en expresar que el Contrato de Seguro Cibernético pertenece a la modalidad de contratos web en cuanto que la oferta del contrato se centra en presentar al suscriptor una serie de condiciones específicas o coberturas en forma de formulario, de manera que no hay negociación entre las partes y se formaliza con el diligenciamiento de los espacios dedicados para tal fin.

Campo de aplicación

El avance de las TICS trae consigo grandes impactos para los modelos tradicionales frente a los nuevos desarrollos y problemas que surgen de temas como el medio ambiente o el daño ecológico, temas que aún no se han desarrollado de manera oportuna y concreta y que tienen relación con riesgos extraordinarios, es decir, riesgos que no son previsibles y que al momento de aplicar las técnicas tradicionales o conocidas, no darán solución a las incógnitas generadas de estos, "lo cual lleva a sostener que el seguro y la responsabilidad civil no pueden, por sí solos, solucionar los problemas que plantean los riesgos de la era tecnológica, lo que hace necesaria la intervención activa del Estado" (Zornosa, 2009,p .141).

La toma de decisiones frente a los cambios que las sociedades en desarrollo deben acatar, son un factor importante de la relación que se presenta entre los expertos y el ciudadano común, decisiones que tendrán en cuenta los riesgos y los beneficios que el uso de la tecnología trae consigo.

> "la sociedad incorpora instituciones que abren espacios de deliberación sobre los riesgos que debemos enfrentar y legislaciones que obligan a los sectores económicos a implementar medidas preventivas y contratar seguros para garantizar recursos que permitan afrontar los daños que se desencadenan" (Zornosa, 2009, pp. 145-146).

Los nuevos riesgos son un desafío para el sector asegurador y traen consigo un gran cambio en la implementación de los mismos, es por esto que el presente trabajo ancla su campo de aplicación en función de prevenir, gestionar y mitigar los riesgos de seguridad digital en las actividades socioeconómicas que se realizan en el entorno digital y el hecho de que los riesgos que se presentan son imprevisibles, muestran la

imposibilidad que tiene el sector asegurador para cumplir su función y consigo la necesidad de presentar nuevas políticas y de aplicarlas.

El Gobierno nacional, a través del documento CONPES 3854 del 11 de abril de 2016 estableció la política nacional de seguridad digital que busca

> "fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el País". (Documento CONPES 3854 *Por la cual se estableció la política naciones de seguridad digital)*

Factores de riesgo

Uno de los elementos primordiales del contrato de seguros es el riesgo asegurable, el riesgo en sí es la incertidumbre que puede referirse a si el hecho se presentará o no o cuando se presentará; esto es en esencia la base del concepto de riesgo, de allí que el profesor Garrigues señala unas condiciones necesarias para que exista el riesgo como:

> 1ª Que el hecho o evento del que depende sea de posible realización (por ejemplo nadie puede asegurarse contra el hecho de que se caiga el sol), 2ª que no se sepa cuando se va a realizar es decir que sea incierta, tanto en cuando se producirá, en el momento de su realización o el cómo se producirá; 3ª que su producción sea fortuita, o sea, que no depende de la persona que el hecho se produzca y por último que en caso de realizarse el hecho provoque un daño. (Garrigues, 1973, p.143)

El profesor Efrén Ossa es constantemente citado por el profesor López Blanco al hablar del riesgo y la clasificación del mismo en el contrato de seguro, para el profesor OSSA por ejemplo existen los riesgos personales, los cuales amenazan la integridad de las personas ya sea física o laboral, los riesgos reales que son aquellos que afectan las cosas y los patrimoniales que de alguna forma u otra menoscaban el patrimonio que también puede verse afectado mediante la RC (Responsabilidad Civil) o el lucro cesante, entre otros (López, 2004).

En contraste con esto, el profesor López Blanco no está de acuerdo con lo anteriormente expuesto, pues para él todos los riesgos finalmente tienen un contenido patrimonial e implican por ello un menoscabo en el patrimonio; para el autor a la luz del tema en cuestión, no existe diferencia entre la pérdida de una parte del cuerpo, o de determinado bien como un vehículo o la indemnización al tercero dañado; para el profesor lo importante es que el hecho provoque un daño. (López, 2004)

En síntesis y como lo indica el profesor López Blanco “el riesgo es unitario, no susceptible de clasificación, tan solo admite la denominación patrimonial, pues todo detrimento físico que recaiga sobre una persona o cosas implica una lesión económica". (López, 2004, pp. 84-90)

Aun con las aseveraciones realizadas por los doctrinantes, cabe decir que la naturaleza del seguro es dinámica, implica precisamente el poder hacerse cargo o cubrir los riesgos y su correspondiente daño que los cambios, el futuro y en fin el progreso trae consigo.

Esta claro que el factor de riesgo en el contrato de seguro cibernético hoy por hoy es la tecnología; Amparo Zabala, responsable de producto de ciberriesgo en Zurich Insurance, establece que el uso de ciberseguros se ha generalizado gracias al interés de

los medios de comunicación y por supuesto a los escándalos por hackeo de información y ciberdelincuencia que se han dado en los últimos años. Los riesgos notables, referentes al Boom de las tecnologías de la información y la comunicación, son: el internet de las cosas, la utilización del Big Data como medio de comunicación y perfilamiento de clientes y usuarios, el cloud computing y el riesgo en la cadena de suministros. (Zabala Amparo, 2015)

Un área de creciente preocupación para las empresas a nivel mundial son los siniestros cibernéticos, estos van desde violaciones a datos almacenados hasta delitos informáticos, pero también incluyen fallas técnicas en los departamentos de tecnologías de la información (TI), según la medición realizada por Allianz Risk en 2020

> "La pérdida de reputación (69%) es la principal causa de pérdida económica para las empresas después de un incidente cibernético, según las respuestas, seguida de la interrupción del negocio (60%) y las reclamaciones de responsabilidad después de una violación de datos (52%)". (Allianz,2016.p.1)

Las empresas están cada vez más preocupadas por la creciente sofisticación de los ataques cibernéticos, según el Barómetro de riesgos de Allianz. "Los ataques de piratas informáticos están cada vez más orientados a objetivos, duran más y pueden provocar una penetración continua", explica Jens Krickhahn, experto en seguros cibernéticos de AGCS. (Allianz, 2016, p.1)

En la actualidad existen tres tipos de ciberriesgo, estos se pueden clasificar en operacional, reputacional y regulatorio, donde el primero es capaz de detener las operaciones de la empresa aunque no por un hecho físico, por ejemplo el secuestro de password de las maquinas en una empresa de manufactura robotizada podría detener la operación in situ de dicha empresa hasta encontrar la manera de acceder; frente al riesgo

reputacional, no hace falta ahondar si tenemos en cuenta que tiene que ver con temas de marca, branding y la confiabilidad de la empresa frente a sus clientes, finalmente en el campo regulatorio el riesgo se presenta con respecto a multas y sanciones prescritas por la legislación del país y reclamación de terceros frente a un hecho que los afecte, como por ejemplo, la divulgación de información sensible.

Con esto se evidencia que los riesgos cibernéticos están en constante evolución; a través del tiempo se ha evidenciado que el aumento en el número de incidentes de ransomware está ayudando a aumentar la frecuencia de pérdidas para las empresas. Es decir, a la fecha los ciberataques se están volviendo más sofisticados y dirigidos a medida que los delincuentes buscan mayores retribuciones con extorsiones multimillonarias; por ejemplo, el grupo hotelero Marriot y la agencia de puntaje crediticio Equifax en 2017 informaron violaciones de datos personales de más de 300 millones y 140 millones de clientes respectivamente, estas compañías se vieron enfrentadas con numerosas demandas judiciales, acciones regulatorias en varias jurisdicciones y multas millonarias por violación de datos personales.(Allianz,2020,p.1)

El Riesgo Asegurable

"En el derecho colombiano el riesgo asegurable, el interés asegurable, la prima y la obligación condicional son los elementos esenciales del contrato de seguro, en cuya ausencia se configura una causal de ineficacia de este último". (Código Civil, 1873)

El riesgo asegurable es aquel acontecimiento (hecho incierto), que generará el cumplimiento de la obligación condicional que ha pactado el asegurador; cabe mencionar que la ocurrencia de este hecho, no dependerá de la voluntad de las partes, es así como el doctrinante Ordóñez define como riesgo asegurable: "un evento fortuito,

el evento que por súbito e imprevisto no tiene, ni en su génesis ni en su desarrollo, relación alguna con el acto humano consciente, sea voluntaria o no su consecuencia".(Ordoñez, 2002, p.11)

El barómetro de riesgo del catálogo de negocios para el 2016 emitido por la compañía de seguros Allianz, permite aproximarnos al cambio en la realidad de las compañías de seguros con respecto al riesgo asegurable: debido a lo que hoy en día se ha llamado el "Internet de las cosas" se describe una realidad en donde todos y cada uno de los dispositivos electrónicos se encuentran o encontrarán conectados a internet, la intercomunicación de cada aspecto en la vida de las personas es inminente y esto lleva inmerso un incremento de la exposición al ciber riesgo, en consecuencia las compañías de seguros prevén un aumento en el volumen de ataques de tipo cibernético (Allianz,2016,p.1).

Este barómetro de riesgo fue una encuesta realizada entre las empresas globales, así como consultores de riesgos, aseguradoras, directivos y expertos, su atención se centró en seguros corporativos para grandes, pequeñas y medianas empresas; para esta encuesta había un registro de 824 encuestados de un total de 44 países.

Uno de los grandes hallazgos de la encuesta tiene que ver con la inclusión por primera vez y ocupando el tercer puesto de la categoría de interrupción del negocio la cual de acuerdo con el 59% de los encuestados es causada por hechos de ciber incidentes y cibercrimen, esto es muy importante ya que las empresas a nivel mundial ya no se están preocupando tanto por otros riesgos tradicionales de gran relevancia como por ejemplo las catástrofes naturales.

De acuerdo con el informe, se estima que el delito cibernético cuesta en la economía mundial cerca de US $445 bn al año, convirtiéndose en la segunda causal más

importante de pérdidas económicas para las empresa; los estudios realizados demuestran que en promedio las empresas demoran alrededor de 90 días para descubrir que han sido hackeados; a menudo el incidente no es identificado por la propia empresa si no por sus clientes, lo cual lógicamente representa una gran amenaza para la reputación y el good will de la empresa.

El hecho de que las empresas a menudo sólo reconocen la pérdida cuando el ataque haya ocurrido significa que todo lo que pueden hacer es tratar y prevenir más daños. Esta es la razón por la que la prevención es un elemento clave en la seguridad de las tecnologías de la información. La gestión del riesgo cibernético tiene que ser una parte integral de la estrategia de gestión del riesgo de cualquier empresa.

A la pregunta ¿Cuáles son las principales causas de pérdida económica después de un ataque cibernético? el 69% de los encuestados respondió la pérdida de la reputación seguido de la interrupción de negocios (sobretodo en la cadena de suministro) con el 60% y en tercer lugar se ubica las reclamaciones de responsabilidad después de una violación de datos con el 52%.

Lo anterior ha obligado a los gobiernos a endurecer las penas por pérdida de datos y esto se convierte en que las empresas deben reforzar su seguridad cibernética; tales desarrollos impulsarían un crecimiento sistemático en el mercado de seguros cibernéticos, debido a que las empresas buscarán la manera de protegerse contra los crecientes costos tangibles e intangibles asociados a una violación digital.

En últimos años, delitos tales como la usurpación de la identidad, la clonación de tarjetas de crédito o el hurto de información de compañías con el propósito de venderlo al mejor postor, se constituye en el tipo de delitos de los que hoy por hoy las empresas buscan protegerse; Zabala presenta dentro de su artículo, las estadísticas de

uno de los brókers más grandes de seguros el cual asegura que en el mercado estadounidense sus clientes para este tipo de productos aumentaron en un 32% en 2014 con respecto al año inmediatamente anterior, y aseguran que la proyección para el año 2015 es en aumento. Los seguros cibernéticos unen la responsabilidad civil con la cobertura de daños propios y evolucionan con cada nuevo riesgo planteado como por ejemplo la interrupción del negocio, daños a la reputación, entre otros., riesgos que los seguros tradicionales excluyen tal como ocurre con la protección de activos intangibles y problemas derivados del uso de la TIC'S (Zabala, 2015).

Esta es la manera en cómo se mejora el contrato de seguro, obliga a las compañías de seguros a retarse al respecto tanto en la delimitación del riesgo (por ejemplo, en la cadena de suministro), el cálculo de la prima y la elección del bien asegurable o del mismo asegurado.

> "La tecnología y el avance de las comunicaciones han modificado nuestro concepto sobre el tiempo; la cibernética y los medios de comunicación han hecho posible la simultaneidad; hoy presenciamos las guerras en vivo y en directo; sin poder hacer nada, observamos la muerte de la tripulación del submarino ruso. Ahora vivimos una aparente realidad virtual que ha hecho posible la marcación del mal concepto de la tolerancia, el de la indiferencia. La tecnología de la comunicación, el cine y la televisión nos producen la sensación de que vivimos en una realidad virtual, la misma que, en la mente, produce la ficción" (Zornoza, 2009, pp.141- 142)

Está claro que los riesgos cibernéticos, aumentan día tras día, pues la tecnología avanza a pasos agigantados, por ende, las entidades aseguradoras deben estar en

continuo avance, ampliando sus coberturas y generando conciencia para poder entender que los riesgos cibernéticos, pueden ir de un país a otro.

De este modo, cada organización debe estudiar individualmente los ciber riesgos como lo son, por ejemplo, fuga de información, suplantación de identidad, fraude, internet de las cosas, entre otros; es decir, cada entidad deberá prepararse y anticiparse a dichos escenarios para lograr una mitigación de los efectos nocivos que estos puedan causar.

¿Pero de que forma las entidades se deben anticipar a los acontecimientos? Para esto se tendrá en cuenta dos enfoques:

> "El primero consiste en ofrecer principios y lineamientos generales que las entidades deben cumplir (como un reconocimiento de la importancia del riesgo y el establecimiento de procesos generales de salvaguarda y responsabilidad de gobierno corporativo). El segundo consiste en ofrecer prescripciones específicas de acción, tales como estrategias de defensa o procesos de respuesta a ataques" (Clavijo, Osorio, & Yanquen, p.93).

Otra forma de contrarrestar los ciberataques es entrenando tanto a los funcionarios del sector público, como los trabajadores del sector privado, para que de esta forma amplíen su conocimiento en cuanto al manejo de las TIC y se dé un adecuado uso de la tecnología, para este caso tenemos el ejemplo en donde el Gobierno Nacional por medio de colCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia):

> "Adelantó procesos de capacitación en los que participaron funcionarios del Estado y de empresas del sector privado, así como programas de sensibilización y concientización para los ciudadanos en general respecto a la

ciberseguridad y ciberdefensa. Por su parte, el CCOC (Comando Conjunto Cibernético) fortaleció las capacidades de ciberdefensa propias y las de las unidades cibernéticas. De igual manera, brindó lineamientos y directrices al interior de las instituciones en este tema, con el fin de garantizar la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional". (Documento CONPES 3854 *Por la cual se estableció la política naciones de seguridad digital)*

A nivel internacional también encontramos que la agencia policial de la Unión Europea (Europol) sostiene que el ransomware es la mayor amenaza de delito cibernético, estos ataques cada vez son más sofisticados y sus consecuencias mas devastadoras, de las cuales tenemos, la interrupción del negocio y el hurto de datos personales que más que nada afecta a negocios de productos y servicios como las firmas de abogados, consultores o arquitectos, para quienes los sistemas y datos de TI son su principal motor.

"Incidentes como los que presentan el malware Ryuk se han convertido en un factor clave para las reclamaciones de seguros cibernéticos en los últimos años. Se informó por primera vez en agosto de 2018 y ha sido responsable de múltiples ataques contra grandes empresas, hospitales y gobiernos locales a nivel mundial" (Allianz, 2020, p.1)

Riesgo Inasegurable

Los hechos ciertos, salvo la muerte, son inasegurables, y no constituye riesgo la incertidumbre subjetiva sobre el acaecimiento o no de una determinada circunstancia de hecho; el concepto de riesgo inasegurable es diferente del concepto de exclusión legal.

“Se reitera que los inasegurables son los que por ningún motivo se pueden asegurar” (Allianz, 2020) “esto significa que como están prohibidos, las disposiciones que así lo regulan son de carácter imperativo, de orden público y restringen el ejercicio de la autonomía privada de la voluntad” (Zornosa, 2009).

Es importante destacar que existen riesgos no asegurables, como son aquellas acciones que se cometen con dolo; el doctrinante Nicolás Barbato establece que, en primer lugar, podemos observar que la conducta dolosa puede presentarse al tiempo de la celebración del contrato. El contratante puede haber efectuado una falsa declaración del estado del riesgo o bien haber callado intencionalmente circunstancias relativas al mismo, llevando al asegurador a evaluar erróneamente las características asegurativas de ese riesgo y otorgar una cobertura a situaciones que de haber conocido en su realidad no hubiera amparado con el seguro, o lo hubiese hecho a prima más elevada (Barbato, 1998).

El dolo también se puede manifestar en las conductas relativas que asuma el asegurado o beneficiario, es decir, conductas que conlleven la mala fe, estas conductas pueden ir desde la simulación del siniestro o la utilización de terceros para provocar el siniestro, todo esto con el fin de obtener una indemnización.

Otros riesgos que no son asegurables son los hechos ciertos, es decir, aquellos que si ocurrirán; igualmente los hechos u actos imposibles que son aquellos que por ningún motivo se realizaran; así como los hechos pasados, los cuales ya sucedieron y estaban fuera del alcance establecido inicialmente, como tampoco, aquellos que son de disposición única del tomador y de sanciones penales policivas de carácter económico, estos no ocasionan impacto alguno sobre las coberturas o pagos que se realicen, como

quiera que se informa sobre la inexistencia del amparo al no configurarse un elemento fundamental del contrato.

En este sentido, encontramos a nivel de riesgo cibernético algunos ejemplos de riesgos inasegurables además del dolo, como lo son, revelación de datos públicos de un cliente, proveedor o de un tercero, reclamación que se derive de la publicación o el mal uso de la información de terceros en su nombre, información de tarjetas de crédito, claves de portales financieros para hacer trámites bancarios o reclamaciones por daños relacionados con el uso de nubes públicas gratuitas.

Coberturas

Desde el contrato de seguro marítimo hasta nuestros días, ha sido precisamente la tecnología la que ha marcado la pauta en cuanto a riesgos y cobertura de estos, en la época industrial, por ejemplo, con el desarrollo de las máquinas se produjeron muchas pérdidas en cuanto a su mantenimiento y operación, lo cual sirvió de base para generar el seguro de rotura y maquinaria.

Para el autor Waldo Sobrino se plantean dos grandes grupos de coberturas que se manejan en el contrato de seguros cibernéticos como los son cobertura de Daños Patrimoniales (Property) y de Responsabilidad Civil (Liability) (Sobrino, 2017).

Particularmente dentro de la cobertura Property se encuentran las coberturas de: a) Sustracción de datos o dinero que soporte la compañía asegurada, b) asolamiento o contaminación de datos o información dentro del cual se cubre el costo de reparación que tenga que asumir la empresa asegurada para esto, c) se ampara también los gastos realizados en la contratación de un especialista para revelar el motivo del daño o hackeo, d) se cubre la extorsión que realice el hacker para no destruir los datos que por

su accionar haya encriptado o ransomware, e) D.O.S Denial of services o el acceso denegado, el cual hace que el asegurado no pueda acceder a sus archivos, correo, intranet, etc., f) la cobertura de business interruption en el cual la compañía básicamente paga el siniestro en sí, al igual que otros perjuicios como el lucro cesante o los gastos fijos que se producen mientras se reparan los bienes siniestrados, g) el business interruption también es contingente, porque cubre el daño que se le ocasione no solo al tomador del seguro, si no a su cliente o proveedor; por su puesto al tratarse de una nueva era, la era digital, estas coberturas no guardan relación o se encuentran inmersas en las coberturas tradicionales.

Según José Luis Pérez "el fundamento del seguro y su definición y conocimiento son la base para que la entidad aseguradora pueda asumir su cobertura" (Pérez, 2016, p. 22) y de esta manera se perfecciona desde el punto de vista del tomador el seguro; Amparo Zabala se remite a los seguros cibernéticos al afirmar que ellos unen la responsabilidad civil con la cobertura de daños propios y evolucionan con cada nuevo riesgo planteado como por ejemplo: la interrupción del negocio, daños a la reputación, entre otros., riesgos que los seguros tradicionales excluyen tal como ocurre con la protección a activos intangibles y problemas derivados del uso de la TIC'S. (Zabala, 2015)

En lo que se atañe a la cobertura de Responsabilidad Civil o Liability en el seguro cibernético o Cyber Risk, se pueden mencionar 1) el de responsabilidad por datos personales, es decir por la publicidad o divulgación de la información personal de funcionarios, consumidor, proveedores, entre otros, 2) responsabilidad por datos corporativos que al igual que el anterior protege datos personales, esta vez de clientes corporativos, lo cual es importante por ejemplo, en caso de que un asesor o un abogado

está asesorando la fusión o compra de empresas, 3) la responsabilidad por empresas contratadas, como por ejemplo, el proveedor de hosting o la nube; como se trató líneas atrás los clausulados no se han estandarizado lo cual hace que las responsabilidades sean innumerables.

Otros autores, sin embargo, analizan algunas variables que podrían cubrirse; por ejemplo, García Marcén realiza una explicación a partir de la alteración, pérdida o hurto de datos o denegación del servicio del sistema TI del asegurado en el cual se garantizaran los costos derivados de estos hechos con causa de un hecho informático voluntario, malware o equivocación humana, tema que hoy por hoy es causal de exclusión en las pólizas existentes en el mercado colombiano (García, 2019)

Dentro de ella podrían indemnizarse los gastos de restauración y recreación de la información perdida o hurtada, ampliar el acompañamiento a la compra de licencias de sustitución de software, copia y restauración de Backup, descontaminación de programa maligno, investigación del origen del ataque con el fin de limitar el impacto, así como la parametrización y restauración de firewall y capas de protección para evitar futuras brechas de seguridad.

Otro aspecto que se plantea como cobertura es la confiabilidad de datos en la industria de tarjetas de pago, en la que se asegura los gastos como resultado de la pérdida, hurto o publicación a sujetos no autorizados, de información de índole personal que se encuentra en custodia y control del asegurado y que han sido objeto de actos informáticos dolosos, malware o yerro humano que se dé en el propio sistema del asegurado; claramente, una exclusión de la aseguradora podría ser que el asegurado no contara con una certificación válida PCI DSS (Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago) emitida por un consultor certificado en seguridad.

Finalmente, se plantea la extorsión cibernética que sufra el asegurado, previa verificación de que dicha extorsión sea confiable, cierta, inmediata y comprobable; esta puede ir desde una negación de acceso a la red del garantizado, una pérdida de datos almacenados a su custodia, o hurto y exhibición de datos a un tercero que no está permitido; por ejemplo, en Colombia sucede que las empresas de telecomunicaciones venden sus bases de datos al sistema financiero para colocación de productos de este último sector. Al respecto, en Colombia ha habido desarrollo legal con respecto a la ley de protección de datos Ley 1581 de 2012 y posteriormente con el Decreto 1759 de 2016, donde también se presenta exclusión cuando el hecho delictivo es realizado por directivos, trabajadores o accionistas de la misma organización; por lo tanto, es apenas lógico que las aseguradoras fijen un limite máximo de indemnización y se fijen unos deducibles.

Para Waldo Sobrino "existe una íntima relación entre las coberturas de property y liability ya que en caso de un siniestro muchas veces el perjuicio no se concentra solamente en el asegurado, también este se puede extender a otras empresas lo cual genera por supuesto, la correspondiente reclamación por responsabilidad civil" (Waldo, 2017).

Para el caso colombiano una de las primeras aseguradoras en lanzar una póliza de protección al riesgo cibernético es Suramericana de seguros, la cual presenta su póliza bajo el nombre de seguro de protección digital empresas, que establece dentro de sus coberturas: responsabilidad civil por fallas en el tratamiento de datos personales, responsabilidad civil por fuga de información de terceros, la cual para nuestro trabajo se enmarcaría en la cobertura de liability; por otro lado asegura los costos de emergencia y gastos de defensa y de investigación oficial en lo que se enmarcaría como una cobertura

de property; cabe aclarar que riesgos como el ramsonware estas excluidos de la póliza lo cual deja al asegurado sin ninguna protección frente a uno de los ataques que mas se repite y que mayor daño puede generar.

Alcance del contrato

Con la revolución tecnológica vivida, el alcance del contrato no solo debe proveerse desde lo geográfico, es indispensable tener en cuenta las necesidades del asegurado, para ello, la revista de ciberseguridad y ciberdefensa en la Unión Europea plantea:

> "Hasta ahora el mercado asegurador se había centrado en productos dirigidos a aquellas empresas más expuestas al riesgo cibernético, siendo normalmente grandes corporaciones multinacionales y que, por tanto, necesitan mayores niveles de protección. No obstante, cada vez hay más aseguradoras que dirigen su mirada al sector de la pequeña y mediana empresa, están intentando adaptar su oferta a su realidad y necesidades. La dificultad para asegurados, aseguradores y mediadores radica en la necesidad de adaptar los productos al perfil de riesgo y la cobertura que necesitan estas empresas y no tanto al tamaño que la misma compañía tenga". (Thiber. 2016. p 1).

En el caso colombiano, el Ministerio de las TIC ha sacado un diagnóstico acerca de los sectores mas afectados por incidentes digitales en el territorio, lo cual se resume en la siguiente tabla:

Figura 1. Diagnóstico de incidentes de seguridad digital en Colombia.

Nota. Descripción de los sectores de la economía mas afectados por los incidentes digitales y tipos de delitos que se cometen a nivel digital en Colombia. Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (2016) Nueva Política Publica de Seguridad Digital, Bogotá D.C., (Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, 2016)

De acuerdo con la infografía anterior, el Ministerio de las Tic relaciona en orden de mayor a menor, quienes son los más afectados en Colombia por incidentes digitales siendo los primeros la ciudadanía y el gobierno, entre otros; sin embargo, según un estudio realizado por el Observatorio de Cibercrimen de la Policía Nacional para los años 2019 y 2020, los ciberdelincuentes se han concentrado en las pequeñas empresas y geográficamente el estudio muestra gran incidencia en la ciudades de Bogotá con 5.308 casos, Cali 1.190 casos, Medellín 1.186 casos y Barranquilla con 643 casos (Policía Nacional de Colombia, 2020)

Aún con los retos planteados, se prevé que el mercado del seguro cibernético alcance los 10.000 millones de dólares para el año 2020 (por supuesto existe una contraprestación esperada por la compañía de seguros además del pago de la prima), de acuerdo con el artículo, es necesario que las compañías consideren sus sistemas de

seguridad en internet e implementen medidas para garantizar la ciber resiliencia, que no se refiere únicamente a evitar los ataques en la red, también conlleva la capacidad de detectarlas y gestionarlas en el menor tiempo posible. (Thiber, 2016, p.1)

El alcance de este seguro también debería llegar a otros sectores como lo son, el financiero, el de telecomunicaciones y proveedores de servicios tecnológicos, puesto que los datos que estas organizaciones manejan (información y datos de terceros) son de alto impacto al momento de su pérdida.

En este punto vale la pena indicar que el "asegurador indemnizará al asegurado conforme a los términos, condiciones, límites, franquicias y exclusiones contenidas en las condiciones particulares y generales de la póliza. Delimita a su vez el lugar donde se pueden formular reclamaciones contra el asegurado". (Zabala, 2015) En el caso que nos atañe, Colombia, frente a tribunales colombianos y, por actos llevados a cabo en territorio colombiano, salvo que por voluntad de las partes se pacte lo contrario.

Conclusiones

El mundo de la tecnología, en estos momentos, nos tiene que concientizar y generar nuevos pensamientos, para que así las empresas públicas o privadas, puedan resarcir nuevos daños que se han causado gracias a los avances tecnológicos.

Al tratarse de nuevos daños, las formas de indemnización son escasas, pero en este punto se destaca que el contrato de seguro cibernético se expande día tras día.

Las organizaciones, tales como grandes, medianas y pequeñas empresas, del sector público o privado deben evaluar sus sistemas de seguridad en los sistemas

digitales y aplicar las medidas necesarias para garantizar el mínimo riesgo de la ciberdelincuencia; esto implica tener la capacidad de detectar y evitar dichos ataques, en otras palabras, ciber resiliencia.

Esta claro que los avances tecnológicos, con llevan el control de la sociedad, pero la sociedad no logra tener este mismo control preponderante en dichos avances, hoy por hoy se está respondiendo a la evolución con métodos obsoletos y una gestión insuficiente, es por ello que se han desarrollado riesgos a nivel digital, dentro de los cuales encontramos: operacional, reputacional y regulatorio, donde el primero es capaz de detener las operaciones de la empresa aunque no por un hecho físico; frente al riesgo reputacional, no hace falta ahondar si tenemos en cuenta que tiene que ver con temas de marca, branding y la confiabilidad de la empresa frente a sus clientes; finalmente, en el campo regulatorio el riesgo se presenta con respecto a multas y sanciones prescritas por la legislación del país y reclamación de terceros frente a un hecho que los afecte como por ejemplo la divulgación de información sensible.

El alcance del contrato de seguro cibernético no solamente debería tomarse por parte de las empresas privadas, sino que también se debería analizar la extensión de los riesgos y coberturas, vinculadas con daños del negocio a nivel estatal y personal, pues constantemente estamos manejando aparatos electrónicos, que en muchas ocasiones guardan no solo nuestra información personal, sino también la de nuestros familiares.

Podemos decir que, si las empresas sufren un ciberataque, el daño patrimonial que estas acarrearían pueden ser sustancialmente más gravosas, dado a toda la información que estos recopilan, como lo son la información de terceros, así mismo, se

puede llegar a interrumpir la cadena de elaboración, o se pueden robar secretos comerciales, o arruinar registros de la asociación.

Cuando existan riesgos que sean considerados como “no asegurables” por el sector privado, se puede tener la posibilidad de acudir al sector público, en este caso deberá ser el Estado el que asuma ciertos riesgos para mitigar las pérdidas patrimoniales, por los daños recibidos por los ciberataques, como también para reemplazar o estabilizar el mercado privado; esto haciendo un símil con la ya existente póliza del Ministerio de Hacienda o el terrorismo que en Colombia cubre los daños parciales o totales provenientes de ataques de grupos armados organizados, entre otros.

References

Allianz Risk. (2020). Allianz risk barometer 2020 – ciber incidentes. Retrieved from https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2020-cyber-incidents.html

Allianz risk barometer 2016: Businesses face changing risk landscape: Risk - short term. (2016). Retrieved from http://reference.sabinet.co.za/sa_epublication_article/nm_monm_feb_2016_a36

Barbato, N. (1998). Culpa grave y dolo en el derecho de seguros. Buenos Aires.: Editorial HAMURABI S.R.L.

Clavijo Felipe, Osorio Daniel, & Yanquen Eduardo. Riesgo cibernético: Relevancia y enfoques para su regulación y supervisión., 93.

Fernández, R. (2013). El contrato electrónico: formación y cumplimiento. Barcelona: J.M. BOSCH EDITOR. Retrieved from https://ebookcentral.proquest.com/lib/[SITE_ID]/detail.action?docID=3208513

García Marcén, G. (2019). Contratación de la póliza de Ciberriesgos, tratamiento del siniestro y la importancia del reaseguro. Universidad de Barcelona). , 54-60. Retrieved from http://hdl.handle.net/2445/144759

Garrigues, J. (1973). Contrato de seguro terrestre Aguirre.

José Luis Pérez. (2016). Teoría general del seguro. Https://www.Researchgate.Net/Publication/40942409, 22. Retrieved from https://www.researchgate.net/profile/Jose_Luis_Perez_Torres/publication/40942409_Conociendo_el_seguro_teoria_general_del_seguro/links/56dc897e08aebe4638c0324a/Conociendo-el-seguro-teoria-general-del-seguro.pdf

López, H. F. (2004). Comentarios al contrato de seguros (4ª ed.). Bogotá: Dupre Editores.

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (2016). Nueva política pública de seguridad digital: Desafíos y oportunidades en el escenario de posconflicto. Retrieved from https://www.mintic.gov.co/portal/604/articles-15570_recurso_2.pdf

Ministerio de Tecnologias de la Informacion y las Comunicaciones de Colombia. (2020). por la cual se establece la política nacional de confianza y seguridad digital.

Retrieved from ww.mintic.gov.co

Ministerio de Tecnologias de la Informacion y las Comunicaciones (2020, 01 de julio). Por la cual se establece la política nacional de confianza y seguridad digital (Documento CONPES 3995) Bogotá D.C., Colombia: MinTic.

Ministerio de Tecnologías de la Información y las Comunicaciones (2016, 11 de abril). Por la cual se estableció la política nacional de seguridad digital (Documento CONPES 3854) Bogotá D.C., Colombia: MinTic.

Ordoñez Andrés. (2002). Elementos esenciales, partes y carácter indemnizatorio del contrato. Colombia: U Externado de Colombia.

Palacios Sánchez, F. (2016). Seguros: temas esenciales. Bogotá: Ecoe Ediciones. Retrieved from https://ebookcentral.proquest.com/lib/[SITE_ID]/detail.action?docID=4870573

Policía Nacional de Colombia. Tendencias cibercrimen Colombia 2019 - 2020. Retrieved from https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

Thiber. The cybersecurity think tank. (2016). CIBERSEGUROS la transferencia del ciberriesgo en España., 29,30. Retrieved from https://www.thiber.org/ciberseguros.pdf

Waldo Sobrino. (2017). Cyber Risk Insurance Law (New Developments Upon May 12, 2017 Global Cyber-Attack). Revista Ibero - Latinoamericana de Seguros, 26(47) Retrieved from https://search.proquest.com/docview/2013153348

Zabala Amparo. (2015). El riesgo cibernético y su aseguramiento. Retrieved from https://communityofinsurance.es/blog/2015/11/15/el-riesgo-cibernetico-y-su-

aseguramiento/

Zornosa, H. E. (2009). El riesgo asegurable y los riesgos emergentes de las nuevas tecnologías. Revista de Derecho Privado, (17), 141-173. Retrieved from http://dialnet.unirioja.es/servlet/oaiart?codigo=3171399