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

LOS SEGUROS CIBERNÉTICOS: ALCANCE FRENTE A LOS CIBER RIESGOS[*]

CYBER INSURANCE: SCOPE FOR DEALING WITH CYBER RISKS

ANDREA SIGNORINO BARBAT[**]

Fecha de recepción: 18 de octubre de 2022
Fecha de aceptación: 30 de octubre de 2022
Disponible en línea: 30 de diciembre de 2022

Para citar este artículo/To cite this article

Signorino Barbat, Andrea. *Los seguros cibernéticos: Alcance frente a los ciber riesgos,* 57 Rev.Ibero–Latinoam.Seguros, 231-248 (2022). https://doi.org/10.11144/Javeriana.ris57.scaf

doi:10.11144/Javeriana.ris57.scaf

[*] Ponencia presentada en el XVII Congreso del Comité Ibero– Latinoamericano de Derecho de Seguros (CILA) , San José de Costa Rica, agosto de 2022.

[**] Abogada, Traductora Pública, Universidad de la República Oriental del Uruguay. Estudios de postgrado en Dirección, Habilidades Directivas y Gestión de Recursos Humanos, ORT, EDU y Universidad Católica del Uruguay. Secretaria General de AIDA World (Association Internationale du Droit des Assurances), Secretario Académico Internacional AIDA–Uruguay, Presidente del Grupo Internacional Nuevas Tecnologías, Prevención y Seguros en AIDA, Vicepresidente del Grupo Internacional Principios Generales del Contrato de Seguro en AIDA, Presidente de la Asociación Uruguaya de Derecho Marítimo. Profesor de pregrado y postgrado de seguros en Argentina, Brasil, Chile, Colombia, Panamá, España y Uruguay. Directora Académica de la Universidad de Montevideo. Contacto: andreasignorino@gmail.com.

RESUMEN

Hoy en día, lo cibernético se caracteriza por ser todo lo relacionado con la tecnología informática, especialmente, pero no sólo, con Internet. En estos momentos se habla mundialmente de los *Cyber Risks* o Ciber Riesgos, refiriéndose a los riesgos que acechan en el ciberespacio.

En este artículo se brinda una aproximación no tradicional a lo que puede considerarse un riesgo del Ciber entorno, que tiene que ver con los riesgos que acechan al consumidor–asegurado, a las empresas de seguros y en general, y la posible discriminación y afectación moral que las tecnologías basadas en la inteligencia artificial pueden generar a los seres humanos.

Sin embargo, no todos los ciber riesgos pueden ser asegurados y, en este sentido, concluiremos qué riesgos pueden ser cubiertos o gestionados por el seguro y cuáles no.

Palabras clave – seguros, tecnologías, ciber riesgos, seguros cibernéticos.

ABSTRACT

Today, cyber is characterized as everything related to information technology, especially, but not only, to the Internet. Cyber Risks are now being talked about worldwide, referring to the risks that lurk in cyberspace.

This article offers a non–traditional approach to what can be considered a Cyber Risk, which has to do with the risks that lurk for the consumer–insured, insurance companies and in general, and the possible discrimination and moral affectation that technologies based on artificial intelligence can generate for human beings.

However, not all cyber risks can be insured, and, in this sense, we will conclude which risks can be covered or managed by insurance and which ones cannot.

Key words*– insurance, technology, cyber risks, cyber insurance.*

SUMARIO:

1. INTRODUCCIÓN. 2. EL SEGURO CIBERNÉTICO FRENTE A LOS CIBER RIESGOS Y SUS DIMENSIONES. 2.1. Seguros y dimensión social. 2.2. Seguros y dimensión funcional . 2.3. Seguros y dimensión ética. 3. CONCLUSIONES. 4. BIBLIOGRAFÍA.

1. INTRODUCCIÓN

En estas líneas pretendo efectuar un análisis de las dimensiones de los riesgos generados por las tecnologías que resultan ser asegurables, es decir considerar los riesgos que implican las nuevas tecnologías y las soluciones que aporta el sector asegurador.

Para entender estas líneas, es imprescindible comenzar por un aspecto etimológico; ¿qué significa cibernético?

Con la palabra cibernético designamos todo lo relacionado con la tecnología computacional interdisciplinaria utilizada para la ampliación de las capacidades humanas.

La palabra cibernético deriva del griego *kybernetes*, que significa "el arte de manejar un barco". Posteriormente, Platón la utilizó en su obra *La Repúbli*ca para referirse al "arte de dirigir a los hombres" o al "arte de gobernar".

El concepto moderno de cibernético o cibernética, tecnología informática basada en la comunicación humana, fue acuñado por Norbert Wiener (1894–1964) en su obra Cybernetics: or Control and Communication in the Animal and the Machine[1].

Stafford Beer, filósofo de la teoría de la organización y la gestión, de quien el propio Wiener dijo que debía considerarse el padre de la cibernética de la gestión, define la cibernética como "la ciencia de la organización eficaz"[2]. Según el profesor Beer, la cibernética estudia los flujos de información que rodean a un sistema, y la forma en que esta información es utilizada por el sistema como un valor que le permite controlarse a sí mismo: esto ocurre tanto para los sistemas animados como para los inanimados indistintamente. La cibernética es una ciencia interdisciplinar, y está tan ligada a la física como al estudio del cerebro y al de los ordenadores, y también tiene mucho que ver con los lenguajes formales de la ciencia, proporcionando herramientas con las que describir objetivamente el comportamiento de todos estos sistemas.

Hoy en día, lo cibernético se caracteriza por ser todo lo relacionado con la tecnología informática, especialmente, pero no sólo, con Internet.

En estos momentos se habla mucho en todo el mundo de los *Cyber Risks* o Ciber Riesgos, refiriéndose a los riesgos que acechan en el ciberespacio.

En particular, el tema ha sido analizado con respecto al sistema bancario que sufre muchas pérdidas por estos motivos, pero también, el mundo de los seguros está hablando fuertemente de estos peligros que acechan, dentro y fuera de la compañía de seguros.

De hecho,

> "las empresas de servicios financieros son víctimas de ataques de ciberseguridad con mucha más frecuencia que las empresas de otros sectores. Las brechas de seguridad

[1] Wiener, Norbert. *Cybernetics: or Control and Communication in the Animal and the Machine.* Hermann &Cie&Camb. Mass. (MIT Press) 1948 2nd ed. 1961.

[2] Beer, Satford. *Cybernetics and Management,* English Universities Press, 1959.

> suponen una pérdida de ingresos para las entidades bancarias, interrupciones en las operaciones y pérdida tanto de reputación como de clientes"[3].

Los establecimientos financieros sufren amenazas procedentes de diversas fuentes, encabezadas principalmente por las aplicaciones móviles y los portales web. Los ciberdelincuentes pueden robar o manipular datos valiosos de los usuarios y o "clonar" aplicaciones bancarias para utilizarlas con fines nefastos[4].

El tema de los Ciber Riesgos va mucho más allá de la acción de un hacker y está relacionado con las actividades informáticas ilegales para sustraer, alterar, modificar, manipular, inutilizar o destruir información o activos, como dinero, bonos o bienes intangibles, información, de las empresas o usuarios afectados, utilizando para ello medios electrónicos o dispositivos electrónicos.

Para entender su alcance, es necesario analizar el riesgo interno, es decir, el riesgo que genera o sufre el individuo y la propia empresa, y el riesgo externo, es decir, el riesgo frente a terceros, la responsabilidad que se genera frente a terceros usuarios o terceros vinculados a los sistemas.

En este contexto, hablamos del fraude informático, que es uno de los retos más modernos para la protección de los individuos y las empresas, tanto de los delincuentes organizados como de los ocasionales. El fraude abarca desde el simple robo de información hasta el robo de identidad, el robo de cuentas en la red, la extorsión y el ciberterrorismo, así como el espionaje empresarial y la responsabilidad por los datos.

Se trata de organizaciones, pero también de individuos solitarios, cada vez más sofisticados y que ponen en peligro tanto a las personas como a las empresas, porque hoy todos estamos conectados. Los ciberataques suelen tener como objetivo el flujo de datos, ya sea impidiendo la comunicación entre el emisor y el receptor, o interceptando, modificando o inventando datos que alteran el flujo normal de información.

Por supuesto, el negocio de los seguros no es ajeno a estos riesgos. Estamos en la era de las nuevas tecnologías, el llamado mundo *Insurtech*, es decir, la aplicación de las nuevas tecnologías a la actividad aseguradora abre todo un mundo, impensable hace unos años, de nuevas formas de hacer negocio. Esto abarca desde herramientas para la venta de seguros hasta la tecnificación de toda la suscripción, emisión e incluso el pago de siniestros utilizando tecnología *blockchain* , contratos inteligentes, algoritmos y otros basados en inteligencia artificial.

En particular, proteger la identidad y los datos y proporcionar seguridad a los asegurados es crucial para las estrategias de fidelización del sector de los seguros. Los principios consagrados en las leyes de protección de datos –legalidad, consentimiento, finalidad, proporcionalidad, claridad, seguridad, protección, recurso...– deben cumplirse incluso cuando los datos son utilizados por un medio virtual[5].

[3] https://www.archonsecure.com/blog/banking–industry–cyber–threats Recuperado 29 junio 2022.

[4] https://www.archonsecure.com/blog/banking–industry–cyber–threats Recuperado 29 junio 2022.

[5] En general, estos principios están consagrados en las leyes de protección de datos de toda América Latina. Por ejemplo, la Ley uruguaya N° 18.331, de 28 de agosto de 2008, los establece en esos términos.

Asimismo, el asegurado debe ser protegido como consumidor en un contrato de adhesión, pero al mismo tiempo en un contexto en el que el intercambio de datos es algo natural en la sociedad actual. Todo esto constituye lo que yo llamo la dimensión social de los ciber riesgos.

Sin embargo, los ciber riesgos también amenazan las propias operaciones de las aseguradoras, en su gestión interna, en lo que llamo la dimensión funcional de estos riesgos.

En este sentido, es necesaria una adecuada gestión del riesgo tecnológico en un sentido amplio, que va desde la gestión del talento humano hasta la implicación de la alta dirección.

Asimismo, la lucha eficaz contra los ciber riesgos depende nada menos que de la seguridad de la propia empresa y de los asegurados que son la razón de su negocio.

Por último, pero no menos importante, el aspecto ético que implican las nuevas tecnologías y que genera lo que he venido a llamar la dimensión ética de los ciber riesgos.

Se trata de una aproximación no tradicional a lo que puede considerarse un riesgo del Ciberentorno, que tiene que ver con la posible discriminación y afectación moral que las tecnologías basadas en la inteligencia artificial pueden generar a los seres humanos.

Sin embargo, no todos los ciber riesgos pueden ser asegurados y, en este sentido, concluiremos qué riesgos pueden ser cubiertos o gestionados por el seguro.

2. EL SEGURO CIBERNÉTICO FRENTE A LOS CIBER RIESGOS Y SUS DIMENSIONES

Teniendo en cuenta las características que debe tener un riesgo para ser asegurado, y la necesidad de su delimitación, debemos distinguir cuáles de las diversas dimensiones de los ciber riesgos pueden ser cubiertas por el seguro y cuáles no.

Es decir, analizar qué ciber riesgos escapan a las posibilidades técnicas del seguro, especialmente porque no pueden ser medidos o delimitados y, por tanto, no pueden ser asegurables.

De acuerdo a una clasificación personal, que he desarrollado a efectos metodológicos, podemos distinguir una dimensión social, una funcional y una ética de los ciber riesgos.

Veremos a continuación si todas ellas pueden ser cubiertos, y con qué alcance, por los seguros llamados comercialmente como cibernéticos.

2.1. Seguros y dimensión social

En su dimensión social, cuando mencionamos los ciber riesgos se nos presentan automáticamente varios aspectos legales, en mi visión más amplia de carácter social, entre los que destaca la protección de los datos de los usuarios, su identidad y su seguridad.

Si lo aplicamos al sector asegurador, es evidente que los múltiples usos que ofrecen las últimas tecnologías para aportar mejoras en los procedimientos de las aseguradoras, pueden implicar riesgos para terceros y para las propias compañías de seguros.

En cuanto al daño interno a la propia empresa, me referiré a él al hablar de la dimensión funcional de los ciber riesgos.

En cuanto al riesgo a terceros, en realidad si nos referimos al asegurado no es un tercero respecto a la aseguradora, es su cliente con el que tiene un contrato celebrado nada menos que confiando en que la aseguradora cubrirá, paradójicamente, sus riesgos.

Por eso es mejor en este sentido hablar de riesgos externos a la compañía de seguros, que por supuesto también ponen en juego la responsabilidad civil contractual frente a sus clientes.

En este sentido, muchos de los riesgos provienen de los propios usuarios.

Por un lado, existe un gran desconocimiento sobre si Internet es seguro o no. Esta confusión entre los consumidores dificulta la lucha contra la ciberdelincuencia.

Por otro lado, el apoyo de los usuarios en la educación "tecnológica" y sus riesgos es muy disímil en los distintos países, lo que se traduce en una mayor o menor aversión a los ciber riesgos y, por lo tanto, en una mayor o menor prevención frente a ellos, algo importante porque a veces lo único que puede salvarnos de un ciberataque es la prevención.

Un reciente informe de cxLoyalty (ex AffinionGroup), referente en este tipo de estudios, muestra que los niveles más altos de preocupación se dan en Brasil, con un 87%, y en Estados Unidos, con un 75%. En Europa, Francia, España, Italia y el Reino Unido muestran niveles de preocupación que oscilan entre el 60% y el 70%. Por el contrario, los países nórdicos presentan niveles de preocupación relativamente más bajos, ya que sólo el 40% de los encuestados en Suecia y el 42% en Finlandia dicen estar preocupados por la ciberdelincuencia[6].

La preocupación por la ciberdelincuencia también ha aumentado con el tiempo: los encuestados en el informe, en todos los países analizados, dicen estar más preocupados por todos los tipos de ciberdelincuencia, siendo el robo de identidad el más preocupante. Además, la preocupación por este tipo de ciberdelincuencia es la que más ha crecido en los últimos doce meses.

Para ponerlo en perspectiva, si se compara la ciberdelincuencia con otros delitos más "tradicionales" como el hurto o el robo, las cifras sugieren que, en general, los consumidores están ahora más preocupados por la ciberdelincuencia.

La experiencia personal del usuario–consumidor con la ciberdelincuencia desempeña sin duda un papel fundamental, aumentando la preocupación y manteniendo altos los niveles de concienciación en todos los tipos.

[6] AFFINIONGROUP– CYBERCRIME REPORT – https://www.ciberseguridadpyme.es– Recuperado 30 junio 2022.

Muchas personas han sido víctimas o conocen a alguien que lo ha sido. La concienciación sobre este tipo de delitos es muy alta, siendo el robo de identidad, junto con el pirateo informático, la ciberamenaza más intensamente percibida.

Sin embargo, la preocupación existe pero pocos saben cómo afrontarla y esto genera una importante incertidumbre social.

La investigación reveló que, a pesar de los altos niveles de preocupación, hay una falta de comprensión sobre cómo mantenerse a salvo de las amenazas:

–un tercio de la población mundial –35%– cree erróneamente que una red Wi–Fi pública tiene que ser, por ley, segura;

–más de la mitad –54%– no está segura o no sabe que https:// significa que un sitio web es seguro;

–otro tercio –33%– desconoce que utilizar la misma contraseña en diferentes cuentas aumenta los riesgos de ciberataque.

A pesar de su temor al robo de identidad y otras formas de ciberdelincuencia, muchas personas no han tomado más que las medidas básicas para protegerse en línea.

Sólo el 16% dispone de un sistema para protegerse del robo de identidad. De ellos, un 39% lo tiene porque estaba incluido en otro producto o servicio. Curiosamente, el 38% considera que su inclusión es la principal razón para elegir su actual proveedor.

La investigación también reveló que los encuestados con un gran interés en la tecnología no tienen necesariamente una mayor comprensión o confianza en los riesgos. Parece que la confusión sobre la seguridad trasciende los grupos demográficos y afecta incluso a los que demuestran un gran interés por la tecnología.

Además, los usuarios no suelen saber qué hacer cuando les ocurre un ciberataque, especialmente el robo de identidad que es lo que más les preocupa[7].

Los ciber riesgos más frecuentes que atacan a personas y sobre todo a empresas son:

–*Ransomware*

Busca infiltrarse en los sistemas para codificarlos o dañarlos. Los sistemas pueden ser infectados al exigir un rescate con bitcoins. Suele ocultarse en aplicaciones o software de uso cotidiano; por ejemplo, archivos adjuntos de correos electrónicos, actualizaciones, enlaces en anuncios, entre otros. Actualmente, es común el *Ransomware of Things* (RoT), que afecta a dispositivos conectados a Internet.

–Fuga de información

Estos riesgos cibernéticos pueden implicar sanciones civiles, administrativas y penales. Hacen que las empresas pierdan oportunidades de negocio y también pueden

[7] INSTITUTO NACIONAL DE COMPAÑIAS DE SEGUROS DE ESPAÑA (INESE) “Ciber riesgos y ciber seguros” Ed. INESE, 2019.

dañar seriamente la reputación de la empresa. Implican el robo de algún dispositivo o el acceso a sistemas como las bases de datos. El *malware*, el *rootkit*, la ingeniería social o el backdoor se utilizan para estos fines.

–*Phishing*

La suplantación de identidad de una persona o una página web busca robar información confidencial, como el acceso a cuentas bancarias. El ejemplo más común es un correo electrónico en el que se nos informa de que debemos introducir nuestra contraseña en un enlace de dudosa credibilidad. A nivel personal, se utiliza cuando se demuestra el conocimiento de cierta información de un individuo concreto para acceder a sus cuentas.

–Amenaza Persistente Avanzada (APT)

Estos ciberriesgos atacan a una empresa concreta para infiltrarse en su infraestructura tecnológica, obteniendo así información sensible o dañando procesos. Se trata de un ataque personalizado realizado por grupos supuestamente relacionados con gobiernos.

–Ataque DDoS

Los sistemas de información de una empresa se colapsan artificialmente para evitar que otros usuarios utilicen los mismos. Al saturar estos servicios, el atacante busca posteriormente obtener una remuneración económica para volver al funcionamiento normal.

Estos son algunos de los ciberataques más habituales que pueden afectar a los consumidores. A grandes rasgos, se basan en el mal funcionamiento del sitio web, la extracción de información y la solicitud de acciones que causarán pérdidas. La cobertura del seguro puede ser una herramienta útil para protegerse de estos ataques y ayudar a prevenirlos.

Estamos, por lo tanto, ante una gran oportunidad para las aseguradoras, que pueden marcar una gran diferencia en sus productos si incluyen servicios, suministros, soluciones de ciberprotección, cada vez más demandadas por los consumidores.

Así, las aseguradoras están probando diversas estrategias para responder a los asegurados ante estos riesgos. Estas van desde las advertencias recurrentes hasta la prestación de servicios de prevención, en lugar de indemnizaciones, en la fase previa a los daños. También es clave informar a los clientes, a través de guías, de las mejores prácticas con respecto al manejo de las herramientas de los seguros.

Asimismo, el propio mercado asegurador internacional ha generado protección a través de los llamados “Ciberseguros”, incluso como micro–coberturas para familias y PYMES (pequeñas y medianas empresas).

La cobertura que se ofrece es un seguro de responsabilidad civil, por los daños causados a terceros en caso de que se produzca una violación de la privacidad o de la seguridad de un sistema al que se conecta un tercero, incluso por la actuación de los proveedores de tecnología. En este sentido, podemos hablar de cobertura multimedia, profesional, de privacidad y de seguridad de datos.

El otro tipo de cobertura que otorga el ciberseguro es la de pérdidas, como la pérdida de beneficios o ganancias y los gastos para gestionar las crisis, los riesgos reputacionales, entre otros.

Otra de las coberturas habituales es la de multas y sanciones impuestas en caso de incumplimiento de las leyes y reglamentos de protección de datos personales, que parece superar la extensa discusión doctrinal que históricamente ha provocado la cobertura de multas por parte de las leyes de seguros.

Los seguros cibernéticos se mencionan a menudo como una herramienta para aumentar la resiliencia cibernética –la capacidad de superar situaciones traumáticas–, como un mecanismo de transferencia de riesgos y como una herramienta de evaluación útil para acompañar y ayudar en los cálculos de riesgo de las empresas. Estos seguros se comercializan como un producto independiente o como parte de un paquete de otras coberturas, especialmente de responsabilidad civil, de todo riesgo operacional o del seguro del hogar, si está destinado a la familia.

Pero los ciberseguros tienen sus propias dificultades que superar para ser un seguro fiable.

Por un lado, el riesgo es difícil de medir; el ciber riesgo es un problema global que evoluciona constantemente a medida que el mundo está cada vez más conectado, y vaya si lo está. Además, la falta de datos suficientes sobre los incidentes cibernéticos y el bajo nivel de conocimiento y experiencia del riesgo cibernético son obstáculos que aún no se han abordado[8].

Sin embargo, son obstáculos inherentes a los nuevos riesgos y entiendo que deben ser asumidos con cierta audacia, sobre todo si pensamos en los aspectos preventivos que este tipo de seguros puede aportar a particulares y empresas.

A la vista de lo anterior, es evidente que el seguro es una respuesta válida para abordar la dimensión social de los riesgos cibernéticos y defender a los consumidores y empresarios de este grave peligro que supone el uso de la tecnología.

2.2. Seguros y dimensión funcional

Respecto a la dimensión funcional de los ciber riesgos, refiero en este punto a los riesgos que pueden afectar la funcionalidad de la propia empresa aseguradora y cómo deben ser prevenidos.

Estamos en América Latina en la era del Gobierno Corporativo que implica la gestión de los riesgos empresariales, inspirados en esencia en los "Principios Básicos de Seguros, Normas, Orientaciones y Metodología de Evaluación" de la Asociación Internacional de Supervisores de Seguros, IAIS (www.iaisweb.org)[9].

[8] La cuestión de que los riesgos deben ser medibles es una cuestión que va más allá de los ciber riesgos y se aplica a todos los nuevos riesgos. Así lo afirma claramente el profesor GREENE en su obra ya citada en el capítulo 3 sobre Riesgo y Seguro, pp. 27 y ss.

[9] "Insurance Core Principles, Standards, Guidance and Assessment Methodology" of the International Association of Insurance Supervisors, IAIS (www.iaisweb.org).

El supervisor exige que la aseguradora, como parte de su marco general de gobierno corporativo, cuente con sistemas eficaces de gestión de riesgos y controles internos, incluyendo funciones eficaces de gestión de riesgos, cumplimiento, actuariales y de auditoría interna.

Además de los principios de la IAIS, el otro principio fundamental es el de la sostenibilidad de la empresa como parte de la estrategia global de gestión que persigue los intereses generales.

La sostenibilidad es un término moderno que se utiliza para referirse a la responsabilidad social de las empresas o de los negocios y su alcance y normativa son amplios y tienen un impacto en las prácticas y la gestión de las organizaciones y en el gobierno corporativo. La sostenibilidad exige un interés social en las actividades empresariales, así como una composición especial del órgano de administración, que es esencial en el Gobierno Corporativo, con la participación de asesores independientes, a los que se les confían funciones específicas en aras del interés social colectivo, en lugar del propio interés de la empresa[10].

Siguiendo este camino, incluso los proveedores de servicios se ven influenciados, ya que las empresas les exigen que cumplan los requisitos de sostenibilidad. Es decir, las empresas influyen en el comportamiento de los proveedores tratando de orientar y controlar sus acciones hacia la observancia e integración de criterios de gobernanza ambiental, social y financiera (ASG).

Así, bajo el aura de la sostenibilidad, una compañía de seguros gestiona su tecnología no sólo para evitar riesgos, sino también siguiendo criterios de cuidado del medio ambiente, con criterios verdes –porque no olvidemos que la tecnología también contamina–, al tiempo que exige a los proveedores de tecnología con los que se relaciona la compañía de seguros, que actúen en consecuencia.

En Uruguay, en aplicación de los Principios Básicos de la IAIS, la Superintendencia de Servicios Financieros, organismo de control de la actividad aseguradora, ha establecido estándares mínimos de gestión para las compañías de seguros basados en la evaluación integral y en la denominada metodología CERT.

La Superintendencia de Servicios Financieros ha definido que el proceso de supervisión debe ser integral, proactivo, enfocado al riesgo y sobre una base consolidada.

Una de las herramientas con las que cuenta la supervisión para cumplir con sus tareas es la Evaluación Integral, trabajo que se realiza in situ en la empresa aseguradora. El objetivo de la Evaluación Integral es valorar la calidad de la gestión de las entidades y, si se detectan debilidades, evaluar su impacto en la capacidad de la entidad para mantener los niveles de solvencia prudencial a corto, medio y largo plazo.

[10] Perales Viscasilla M. D. P. "Retos y tendencias actuales en sosteniblidad y gobierno corporativo: una mirada tras el COVID–19" *Revista Española de seguros*, SEAIDA No. 185–186, 2021, pp. 1, 7, 11.

Para sintetizar los resultados de la evaluación, se ha definido una metodología denominada CERT, en la que C significa Gobierno Corporativo, E Evaluación Económico Financiera, R Riesgos y T Tecnología.

La T – Tecnología implica la gestión de los riesgos tecnológicos y la fiabilidad y eficacia de los sistemas de información como herramientas de gestión.

Desde el punto de vista metodológico, el Gobierno Corporativo debe considerarse como el núcleo central del análisis, con el que se interrelacionan los demás componentes del sistema.

Para una mayor transparencia en la aplicación del nuevo sistema y con la idea de orientar a las aseguradoras sobre lo que se espera de ellas, se ha elaborado una serie de estándares mínimos de gestión asociados a los cuatro componentes de la metodología CERT[11]:

Desde el punto de vista del supervisor, se entiende que el incumplimiento de un estándar constituye una debilidad que debe ser tratada con atención prioritaria por la entidad.

Las compañías de seguros adoptan diferentes esquemas y estructuras para llevar a cabo su gestión, teniendo en cuenta la naturaleza, tamaño y complejidad de sus operaciones y su perfil de riesgo. El supervisor lleva a cabo sus procedimientos de supervisión y evaluación teniendo en cuenta estos aspectos.

Como vemos, la tecnología y su gestión constituye nada menos que uno de los cuatro pilares de la metodología CERT, que no la identifica simplemente como un riesgo sino como un verdadero estándar que la empresa debe gestionar como parte central de su negocio.

Los estándares para la evaluación de las áreas de Tecnologías de la Información (TI) se basan en el conjunto de principios conocidos como CobiT, especialmente los relacionados con el dominio de Adquisición e Implementación.

La gestión de las TI (tecnologías de la información) debe tener la capacidad de identificar las necesidades y de desarrollar, adquirir, instalar y mantener las soluciones de TI adecuadas de acuerdo con las necesidades de la entidad.

Queda claro, por tanto, que según estas directrices, los riesgos tecnológicos deben abordarse en un sentido amplio, abarcando tanto los riesgos relacionados directamente con los aspectos informáticos como los relacionados con los recursos humanos, ya que el error humano es a menudo la causa, o la puerta de entrada, de un ciberataque.

Es decir, no sólo la gestión de los aspectos directamente relacionados con la seguridad de los sistemas informáticos como la actualización permanente de los sistemas, la correcta clasificación de la información personal, financiera y comercial, la realización de copias de seguridad periódicas y su custodia en lugares distintos al principal, la eventual restricción de acceso a las redes públicas, el desarrollo de

[11] Regulaciones de la Superintendencia de Servicios Financieros www.bcu.gub.uy.

planes de respuesta a incidentes; sino también la correcta gestión de los recursos humanos con segmentación de accesos y reglas de uso de contraseñas, asegurando la confidencialidad, logrando la capacitación de las áreas de auditoría en la detección de incidentes, entre otros.

Además, teniendo en cuenta lo dicho anteriormente sobre la gestión de riesgos como parte del gobierno corporativo, es evidente que la alta dirección debe entender la protección de datos y la ciberseguridad como un elemento central y clave del negocio.

Debe entender que el origen del riesgo no es sólo externo, que la ciberdelincuencia puede originarse en cualquier posición, conocer la normativa aplicable y las consecuencias de su incumplimiento y crear una política especial y específica de gestión de riesgos que se aplique, documente, actualice y dé a conocer constantemente a la organización, destinando recursos para su implantación.

En definitiva, en la era de la tecnología y el gobierno corporativo, la compañía aseguradora debe abordar la prevención y minimización del ciber riesgo con una gestión de riesgos especializada y prioritaria a nivel general.

Como se desprende del análisis anterior, el seguro no sería la herramienta definitiva para cubrir la dimensión funcional de los ciber riesgos. El enfoque para manejar los riesgos implícitos en esta dimensión debería ser el uso de una gestión tecnológica experta como estándar de calidad a cumplir por las compañías de seguros.

No obstante lo anterior, algunos de los riesgos gestionados por las empresas pueden haber surgido de un evento relacionado con la tecnología y pueden ser cubiertos por el ciberseguro.

Es el caso, por ejemplo, del riesgo reputacional cuando el daño causado a la imagen de la empresa se ha producido por un evento relacionado con la tecnología, como un fraude informático o una violación de la seguridad de los datos o de la privacidad de los usuarios.

2.3. Seguros y dimensión ética

Por último, pero no por ello menos importante, conviene analizar lo que yo llamo la dimensión ética de los riesgos cibernéticos, esta vez vista como otro tipo de riesgo que el entorno o espacio cibernético crea para el ser humano.

Como se expresa en un artículo del Real Instituto El Cano [12]

> "en el ámbito de la ciberseguridad, la IA (Inteligencia Artificial) aporta mejoras significativas a través del análisis algorítmico aplicado a grandes cantidades de información, infiriendo resultados en base al contexto y al aprendizaje adquirido de si-

[12] www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari50–2019–alonsolecuit–implicaciones–uso–inteligencia–artificial–campo ciberseguridad?utm_source=CIBERelcano&utm_medium=email&utm_campaign=44–mayo2019 Autor: ALONSO LECUIT, Javier. ARI 50//2019.

> tuaciones anteriores. Las capacidades de la IA, sus algoritmos, pueden ser aplicados de forma similar –tanto– por quienes crean inseguridad en las sociedades avanzadas y –como– por quienes las protegen".

El enfrentamiento directo entre algoritmos de IA y su escalada puede llevar a un punto en el que la intervención humana podría quedar relegada a un segundo plano. La respuesta a esta situación promueve un debate internacional sobre la necesidad de regular las características y el uso de la IA, principalmente desde el punto de vista ético, pero también desde el punto de vista normativo y de control de su uso, sin limitar los beneficios que aporta la innovación de la IA a la sociedad.

> "Aunque existe unanimidad sobre la necesidad de una regulación internacional, es especialmente difícil establecer una hoja de ruta que establezca los pasos a seguir. La inacción, es decir, dejar que las fuerzas del mercado establezcan las reglas del juego, conduciría a la desprotección de los derechos fundamentales de seguridad de los individuos y las naciones, similar a la que se vive actualmente a nivel mundial en el ámbito de la privacidad. Esto aborda el impacto potencial de la IA, los efectos de su empleo malintencionado y la necesidad de controles y contramedidas que carecen de un marco regulador global".

Esta preocupación no se les ha escapado a las autoridades de la Unión Europea y así es como en abril de 2019 se ha producido la "Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones" sobre "Creación de confianza en la inteligencia artificial centrada en el ser humano"[13].

El documento afirma que la inteligencia artificial (IA) tiene el potencial de transformar nuestro mundo para mejor: puede mejorar la asistencia sanitaria, reducir el consumo de energía, hacer que los vehículos sean más seguros y permitir a los agricultores utilizar el agua y los recursos de forma más eficiente. La IA puede utilizarse para predecir el cambio climático y medioambiental, mejorar la gestión del riesgo financiero y proporcionar las herramientas para fabricar, con menos residuos, productos adaptados a nuestras necesidades.

La IA también puede ayudar a detectar el fraude y las amenazas a la ciberseguridad y permitir a las fuerzas de seguridad luchar contra la delincuencia con mayor eficacia. La IA puede beneficiar a la sociedad y a la economía en su conjunto. Es una tecnología estratégica que se está desarrollando y utilizando a un ritmo rápido en todo el mundo.

Sin embargo, también trae consigo nuevos retos para el futuro del trabajo y plantea cuestiones legales y éticas.

Para hacer frente a estos retos y aprovechar al máximo las oportunidades que ofrece la IA, la Comisión publicó en abril de 2019 una estrategia europea[14].

[13] https://ec.europa.eu/transparency/regdoc/rep/1/2019/ES/COM–2019–168–F1–ES–MAIN–PART–1.PDF. Brussels 8.4.2019.

[14] https://ec.europa.eu/transparency/regdoc/rep/1/2019/ES/COM–2019–168–F1–ES–MAIN–PART–1.PDF. Brussels 8.4.2019.

La estrategia sitúa a la persona en el centro del desarrollo de la IA: es una IA centrada en el ser humano.

Adopta un triple enfoque para potenciar la capacidad tecnológica e industrial de la UE e impulsar la adopción de la IA en todos los ámbitos de la economía, preparar las transformaciones socioeconómicas y garantizar la existencia de un marco ético y jurídico adecuado.

La Estrategia Europea de IA y el plan coordinado en el marco de la misma dejan claro que la confianza es un requisito previo para garantizar un enfoque de la IA centrado en el ser humano: la IA no es un fin en sí misma, sino un medio que debe estar al servicio de las personas con el objetivo último de aumentar su bienestar.

Para ello, debe garantizarse la fiabilidad de la IA. Los valores en los que se basan nuestras sociedades deben integrarse plenamente en la evolución de la IA. Deben respetarse los valores del respeto a la dignidad humana, la libertad, la democracia, la igualdad, el Estado de Derecho y el respeto a los derechos humanos, incluidos los derechos de las personas pertenecientes a minorías.

Estos valores son comunes a las sociedades no sólo de la Unión Europea, sino que pueden extrapolarse a toda América Latina, donde prevalecen el pluralismo, la no discriminación, la tolerancia, la justicia, la solidaridad y la igualdad. Además del respeto a los derechos fundamentales, los derechos individuales, civiles, políticos, económicos y sociales que son la base de nuestras sociedades.

En su informe, la Comisión apoya los siguientes requisitos esenciales para una AI fiable. Anima a las partes interesadas a aplicarlos con el fin de crear el entorno de confianza adecuado para el desarrollo y el uso satisfactorios de la IA.

Los siete requisitos esenciales son los siguientes: –Intervención humana y supervisión –Seguridad y solidez técnica –Privacidad y gobernanza de datos –Transparencia – Diversidad, no discriminación y equidad –Bienestar social y medioambiental – Rendición de cuentas –auditoría–

Adicionalmente, en la Unión Europea, en abril de 2021, se generó un proyecto de resolución para ser aplicado por los miembros, que busca regular la implementación de sistemas basados en Inteligencia Artificial. En efecto, la Comisión Europea propone un "Reglamento del Parlamento Europeo y del Consejo ...para la armonización de las normas sobre Inteligencia Artificial (Ley de Inteligencia Artificial)" que modifica algunas otras leyes de la Unión Europea.[15] La regulación propuesta busca evitar posibles discriminaciones que los algoritmos, incluidos en los sistemas puedan generar, y a su vez preservar derechos esenciales de la persona, como ser la privacidad, la seguridad, el derecho al reclamo, entre varios otros. Esto, en especial, en lo que el proyecto delinea como sistemas de "Alto Riesgo".

[15] https://eur–lex.europa.eu/legal–content/EN/TXT/?uri=CELEX%3A52021PC0206 Recuperado 30 junio 2022.

En la regulación destaca la definición y regulación de sistemas de IA de "Alto Riesgo" caracterizados por la opacidad de la información brindada y de su fuente, la complejidad de sistema, la dependencia de los datos y el aprendizaje autónomo.

En ellos destaca pues, entre otros caracteres, la primacía de los algoritmos de "machine learning" es decir que "aprenden solos", y responden, en base a la sucesiva colecta e intercambio de datos masivos o *Big Data*.

La regulación busca defender los derechos fundamentales del ser humano, básicamente:

–la dignidad humana– el respeto de la privacidad y de los datos– la no discriminación –la igualdad de género y raza– la libertad de expresión–los derechos de los niños– de los discapacitados– la protección del medio ambiente– la garantía del derecho de defensa y de remedio o corrección.

Asimismo, limita el derecho al comercio y el uso de la técnica, si esto es necesario para respetar el derecho del consumidor y proteger los datos personales.

Como puede apreciarse, la preocupación por los aspectos éticos de las nuevas tecnologías y el entorno cibernético merecen que se empiece a hablar de una dimensión ética de los ciber riesgos.

Esta dimensión ética no se resuelve con los seguros. Se resuelve, se mitiga o se previene en general con políticas sociales y gubernamentales que gestionen adecuadamente estos riesgos.

3. CONCLUSIONES

El seguro es una herramienta incuestionable para gestionar los riesgos asegurables.

Las dimensiones que pueden alcanzar los ciber riesgos, tal como hemos analizado, no pueden ni deben ser cubiertas completamente por el seguro. El seguro sólo puede cubrir aquellos riesgos que, de acuerdo con sus bases técnicas, pueden ser cubiertos siguiendo requisitos de solvencia.

Algunos de estos riesgos son inconmensurables o difíciles de medir o delimitar y, por tanto, escapan a los parámetros técnicos en los que se basa el seguro y que precisamente proporcionan su cobertura integral y responsable.

Por lo tanto, y a la luz de lo anterior, la dimensión de los ciber riesgos que puede ser cubierta completamente por el seguro, es la dimensión social, que es precisamente la que afecta principalmente a los consumidores de seguros, así como a los empresarios en general. No obstante, algunos de los riesgos gestionados por las empresas –dimensión funcional de los ciber riesgos– pueden haber surgido de un evento relacionado con la tecnología y pueden ser cubiertos por el ciberseguro. Es el caso, por ejemplo, del riesgo reputacional cuando el daño causado a la imagen de la empresa se ha producido por un evento relacionado con la tecnología.

Así, correctamente dimensionado, el seguro sigue siendo una herramienta estratégica para la debida gestión de los riesgos que afectan a los seres humanos y a la comunidad en general.

4. BIBLIOGRAFÍA

AFFINIONGROUP– CYBERCRIME REPORT – https://www.ciberseguridadpyme.es– Recuperado 29/06/2022.

Alonso Lecuit, Javier. Inteligencia Artificial –ARI 50/2019– Real Instituto El Cano Publication. 2019 –www.realinstitutoelcano.org/wps/portal/rielcano_es/– Retrieved 29/06/2022.

Beer, Stafford. *Cybernetics and Management.* English Universities Press, 1959.

EUROPEAN UNION–COMMUNICATION from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions–Building trust in human–centered artificial intelligencehttps://ec.europa.eu/transparency/regdoc/rep/1/2019/ES/COM–2019–168–F1–ES–MAIN–PART–1.PDF. Brussels 8.4.2019. Recuperado 30/ 06/ 2022.

Greene, Mark. "Risk and Insurance", Ed. MAPFRE, Madrid, 1976.

INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS–Insurance core principles, standards, guidance and assessment methodology – IAIS –www.iaisweb.org. Recuperado 30/06/2022.

INSTITUTO NACIONAL DE COMPAÑÍAS DE SEGUROS DE ESPAÑA (INESE) "Ciber riesgos y ciber seguros" Ed. INESE, 2019.

Junqueira, Thiago. "Tratamento de dados Pessoais e Discriminação Algorítmica nos seguros" Thomson Reuters, São Paolo, 2020.

Perales Viscasilla M. d. P. "Retos y tendencias actuales en sosteniblidad y gobierno corporativo: una mirada tras el COVID-19" *Revista Española de seguros*, SEAIDA No. 185–186, 2021.

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL – Laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts https://eur–lex.europa.eu/legal–content/en/txt/?uri=celex%3a52021pc0206.

REGULACIONES DE LA SUPERINTENDENCIA DE SERVICIOS FINANCIEROS www.bcu.gub.uy.

Sánchez Calero, Fernando. Director–Tirado Suárez; F.J., Tapia Hermida, A, Fernández Rozas, J.C., Fuentes Calderón, V. "Ley de contrato de seguros. Comentarios a la Ley 50/1980 de 8 de octubre y modificativas" Ed. Aranzardi, Madrid 1999.

Signorino, Andrea. "Seguros de responsabilidad civil". Ed. FCU, Montevideo , 2011.

Signorino, Andrea – Ponente por Uruguay– Congreso CILA – Lima 2019.

THURSTON, John B. "Review: Cybernetics by Norbert Wiener". The Saturday Review of Literature: 1949.

WIENER, Norbert "Cybernetics: or Control and Communication in the Animal and the Machine". Hermann &Cie&Camb. Mass. (MIT Press) 1948 2nd ed. 1961.