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

CIBER RIESGOS: SU DIMENSIÓN SOCIAL, FUNCIONAL Y ÉTICA[*]

CYBER RISKS: SOCIAL, FUNCTIONAL AND ETHICAL DIMENSIONS

ANDREA SIGNORINO BARBAT[**]

Fecha de recepción: 18 de septiembre 2019
Fecha de aceptación 30 de octubre 2019
Disponible en línea: 30 de diciembre 2019

Para citar este artículo/To cite this article

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

doi:10.11144/Javeriana.ris51.crsd

[*] Artículo base de la relatoría por Uruguay expuesta por la autora en el Congreso CILA 2019 en Lima, Perú.

[**] Doctora en Derecho y Ciencias Sociales, Traductora Pública, Universidad de la República Oriental del Uruguay. Postgrados en Gerencia, Habilidades gerenciales y Dirección de personas, Universidades ORT, EDU y Católica del Uruguay. Secretaria General de AIDA World (Association Internationale du Droit des Assurances), Secretaria académica internacional AIDA-Uruguay, Presidente Grupo internacional Nuevas Tecnologías, Prevención y Seguros en AIDA, Vicepresidente Grupo internacional Principios generales del contrato de seguros en AIDA-Miembro Comisión Directiva de la Asociación uruguaya de derecho marítimo. Profesora de grado y postgrado en seguros en Argentina, Brasil, Colombia y Uruguay. Directora académica en Universidad de Montevideo. asignorino@netgate.com.uy - www.andreasignorino.com.uy. *https://orcid.org/0000-0001-6857-1537*

RESUMEN

El presente artículo no pretende ser un enfoque tradicional referido a nuevas tecnologías -si podemos referirnos así en un tema relativamente actual-, en el sentido de presentar las tecnologías aplicadas a seguros y sus riesgos, o comentar sus virtudes y defectos, o explicar los tipos de Ciber riesgos existentes, sino que pretende aproximar el tema en forma general al lector y reflexionar sobre los Ciber riesgos en sentido amplio. En esta línea, analizaré este tipo de riesgos clasificados metodológicamente en tres dimensiones que he dado en llamar dimensión social, funcional y ética. La dimensión social refiere a los riesgos que las tecnologías y el mundo cibernético implican para el consumidor-asegurado en el contexto del entramado social-, la dimensión funcional, implica los riesgos que se presentan para las empresas aseguradoras en su gestión interna- y la dimensión ética, -tal vez la más trascedente, refiere a los peligros que el Ciber mundo puede generar para las personas en su individualidad, como seres humanos, si los riesgos implicados no son adecuadamente manejados, regulados o contextualizados-.

PALABRAS CLAVE: Ciber, riesgos, dimensiones, social, funcional, ética.

ABSTRACT

This article does not purport to be a traditional approach referred to new technologies in the sense of introducing technologies applied to insurances and risks thereof, or comment about virtues and flaws thereof, or explain the types of existing Cyber risks. It intends to bring the subject closer to the reader and reflect about Cyber risks in a broad sense, reach and prevention thereof. In this sense, I will analyze the Cyber Risks methodologically classified in three dimensions that I names social, functional and ethical dimensions. The social dimension refers to risks implied by the technologies and cybernetic world to the consumer-user in a social structure context, possible causes and solutions; the functional dimension refers to risks for the actual company. The ethical dimension refers to the dangers the Cyber world may cause to people individually, as human beings, if the risks implied are not properly handled, regulated or contextualized.

KEYWORDS: Cyber, risks, social, functional, ethical, dimensions.

SUMARIO

1. APROXIMACIÓN GENERAL

Para poder comprender mejor estas líneas es indispensable comenzar por un aspecto etimológico, ¿qué significa cibernético?

Como cibernético designamos todo lo relacionado con la tecnología computacional interdisciplinaria usada para la extensión de las capacidades humanas.

La palabra cibernético deriva del griego *kybernetes*, que significa "el arte de manejar un navío". Posteriormente, fue usada por PLATÓN en su obra *La República* para referirse al "arte de dirigir a los hombres" o al "arte de gobernar".

El concepto moderno de lo cibernético, tecnología computacional 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* (Cibernética: o control y comunicación en personas y máquinas)[1].

Hoy en día, lo cibernético se caracteriza por ser todo lo que se relaciona con la tecnología computacional, especialmente, pero no únicamente, con Internet.

Mucho se está hablando en estos momentos por el mundo, de los Ciber Riesgos o *Cyber Risks,* refiriéndose a los riesgos que acechan en el Ciber espacio.

En especial el tema ha sido analizado con respecto al sistema bancario que sufre muchas pérdidas por estos motivos, pero asimismo, se está hablando fuertemente en el mundo del seguro de estos peligros que acechan, dentro y fuera de la empresa aseguradora.

El tema de los Ciber Riesgos va mucho más allá de la acción de un hacker y se relaciona con actividades informáticas ilegales para sustraer, alterar, modificar, manipular, inutilizar o destruir información o activos,

1 https://es.wikipedia.org/wiki/Cibernética. ANTHONY STAFFORD BEER, filósofo de la teoría organizacional y gerencial, de quien el propio Wiener dijo que debía ser considerado como el padre de la cibernética de gestión, define a la cibernética como "la ciencia de la organización efectiva". Según el profesor BEER, la cibernética estudia los flujos de información que rodean un sistema, y la forma en que esta información es usada por el sistema como un valor que le permite controlarse a sí mismo: ocurre tanto para sistemas animados como inanimados indiferentemente. La cibernética es una ciencia interdisciplinar, y está tan ligada a la física como al estudio del cerebro como al estudio de los computadores, y tiene también mucho que ver con los lenguajes formales de la ciencia, proporcionando herramientas con las cuales describir de manera objetiva el comportamiento de todos estos sistemas.

como ser dinero, bonos o bienes inmateriales, información, de las compañías o usuarios afectados, utilizando para dichos propósitos medios electrónicos o dispositivos electrónicos[2].

Para poder comprender su alcance, debe analizarse el riesgo interno, o sea el que se genera o sufre en la propia persona y empresa, y el riesgo externo o respecto de terceros, la responsabilidad que se genera frente a terceros usuarios o vinculados a los sistemas.

En este contexto se habla del fraude informático, que es uno de los más modernos retos para la protección de las personas y empresas tanto de criminales organizados como ocasionales. El fraude va desde el simple robo de información hasta el robo de identidades, de cuentas en redes, con extorsión y terrorismo cibernético, así como el espionaje corporativo y la responsabilidad por manejo de datos.

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

Por supuesto, la actividad aseguradora no está ajena a estos riesgos. Estamos en la era de las nuevas tecnologías, el llamado mundo *Insurtech*, o sea la aplicación de nuevas tecnologías a la actividad aseguradora abre todo un mundo, impensado hace unos años, de nuevas formas de hacer negocios. Este va desde herramientas para la venta de seguros hasta la tecnificación de toda la operativa de suscripción, emisión y hasta el pago de siniestros utilizando la tecnología *blockchain, smart contracts*, algoritmos y otras basadas en la inteligencia artificial.

Pero claro, también abre la puerta a los Ciber riesgos.

En especial proteger la identidad y datos y brindar seguridad a los asegurados es determinante en las estrategias de fidelización del sector asegurador. Los principios que consagran las leyes de protección de datos – legalidad, consentimiento, finalidad, proporcionalidad, claridad, seguridad, protección, recurso… - deben cumplirse aun cuando se trate de un dato utilizado por un medio virtual. Asimismo, se debe proteger al asegurado como consumidor en un contrato de adhesión, pero a su vez en un contexto donde el intercambio de datos es lo natural en la

2 VIVAS, GABRIEL, en su exposición sobre Ciber riesgos en el Curso para APECOSE, Perú, mayo 2019.

sociedad actual. Todo esto constituye la dimensión que llamo social de los Ciber riesgos.

Ahora bien, los Ciber Riesgos también amenazan la propia operativa de las aseguradoras, en su gestión interna, lo cual constituye la que llamo, dimensión funcional de dichos riesgos.

En este sentido es necesario una gestión adecuada para el riesgo tecnológico en sentido amplio lo que va desde la gestión del talento humano hasta el involucramiento de la alta dirección en su gestión.

Finalmente, del eficiente combate a los riesgos cibernéticos depende nada menos que la seguridad de la propia empresa y de los asegurados que son el motivo de su negocio.

Por último, y aunque no menos importante el aspecto ético que implican las nuevas tecnologías y que generan lo que he dado en llamar la dimensión ética de los Ciber riesgos.

Es un enfoque no tradicional de lo que puede considerarse un riesgo del Ciber medio, 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.

2. CIBER RIESGOS Y SU DIMENSIÓN SOCIAL

Cuando mencionamos los Ciber riesgos automáticamente se nos presentan varios aspectos de índole jurídico, en mi visión más amplia de índole social, entre los que destacan la protección de los datos de los usuarios, su identidad y su seguridad.

Si esto lo aplicamos al sector asegurador, es claro que los múltiples usos que las tecnologías más recientes ofrecen para otorgar mejoras en los procedimientos de las aseguradoras, pueden implicar riesgos a terceros y para las propias empresas de seguros.

En cuanto al daño propio, interno, para la empresa nos referiremos a esto al hablar de la dimensión funcional de los Ciber riesgos.

En cuanto al riesgo hacia los terceros, en realidad si referimos al asegurado no es un tercero respecto a la empresa aseguradora, es su cliente con quien tiene un contrato celebrado nada menos que confiando en que el asegurador cubrirá, paradojalmente, sus riesgos. Por esto es mejor en este sentido, hablar de riesgos externos a la empresa de seguros que por

supuesto ponen en juego también la responsabilidad civil contractual frente a sus clientes.

En este sentido muchos de los riesgos nacen en los propios usuarios.

Por un lado, hay un gran desconocimiento sobre si Internet es seguro o no. Esta confusión entre los consumidores hace más difícil la lucha contra la ciberdelincuencia.

Por otro lado, el apoyo al usuario en educación "tecnológica" y sus riesgos es muy disímil en los distintos países lo cual redunda en una mayor o menor aversión a los Ciber riesgos y por ende una mayor o menor prevención frente a ellos, algo importante pues a veces lo único que puede salvarnos ante un ataque cibernético, es prevenir.

Un reciente informe de *Affinion Group*, referente en este tipo de investigaciones, muestra que los niveles más altos de preocupación los presenta Brasil, con un 87%, y EE.UU., con un 75%. En Europa, Francia, España, Italia y el Reino Unido presentan niveles de preocupación que van del 60% al 70%. En cambio, los países nórdicos tienen niveles relativamente más bajos de preocupación donde solo el 40% de los encuestados en Suecia y un 42% en Finlandia afirman estar preocupados por la ciberdelincuencia[3].

La diferencia en los niveles de preocupación podría atribuirse al hecho que Brasil se encuentra constantemente entre los países con mayores niveles de ciberdelincuencia, en especial, en relación con los *botnets*[4], el fraude bancario y el malware financiero. Además, Brasil

3 Informe de Affinion Group https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjA3-X2g5zjAhUbGbkGHUd8BdQQFjAAegQIAhAC&url=https%3A%2F%2Faffinion.es%2Fwp-content%2Fuploads%2Fsites%2F11%2F2016%2F07%2FAFF0350-Affinion-White-Paper-Spanish-v8.pdf&usg=AOvVaw3T5A7OP5jJOCND9yIxotlI

4 *Botnet* es el nombre genérico que denomina a cualquier grupo de PC infectados y controlados por un atacante de forma remota. Generalmente, un hacker o un grupo de ellos crea un botnet usando un malware que infecta a una gran cantidad de máquinas. Los ordenadores son parte del botnet, llamados "bots" o "zombies". No existe un número mínimo de equipos para crear un botnet. Los botnets pequeños pueden incluir cientos de PCs infectados, mientras que los mayores utilizan millones de equipos. Algunos ejemplos de botnets recientes son Conficker, Zeus, Waledac, Mariposa y Kelihos. A menudo, se entiende el botnet como una entidad única, sin embargo los creadores de este malware lo venden a cualquiera que pague por él. Por este motivo, existen docenas de botnets separados usando el mismo malware y operando a la vez. Los usuarios empezaron a conocer este programa malicioso a partir del año 2000 cuando un adolescente de Canadá lanzó una serie de ataques de negación de servicio contra páginas web muy populares. El joven, cuyo apodo era Mafiaboy, atacó Yahoo, ETrade, Dell, eBay, Amazon, entre otros, durante varios días, sobrecargando los sitios web hasta que los servidores se colapsaron. Mafia Boy, o su nombre real Michael Cale, no usó un botnet para su fechoría, pero los expertos en seguridad avisaron, después de este episodio, que los botnets (grandes

también tiene un número significativo de cuentas falsas en las redes sociales, un problema que se ha manifestado recientemente de manera alarmante con el descubrimiento, en un lapso de días, de 12,6 millones de interacciones falsas en Facebook en el periodo previo a las últimas elecciones nacionales.

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

Por ponerlo en perspectiva, al comparar la ciberdelincuencia con delitos más "tradicionales" como el hurto o el robo, las cifras sugieren que, en general, los consumidores están más preocupados ahora por la ciberdelincuencia.

La experiencia personal del usuario-consumidor en relación con la ciberdelincuencia sin duda desempeña un papel fundamental, incrementando la preocupación y manteniendo los niveles de sensibilización altos en todos los tipos.

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

Ahora bien, la preocupación existe pero pocos saben cómo sobrellevarla y esto genera una incertidumbre social muy importante.

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

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

-más de la mitad -54%- no están seguros o no saben que https:// significa que una página web es segura;

-otro tercio -33%- no es consciente de que usar la misma contraseña en diferentes cuentas aumenta los riesgos de sufrir un ciberataque.

redes de ordenadores infectados con una variedad de malware) y los ataques DDoS eran una gran amenaza para la estabilidad e integridad de Internet. Por supuesto, los profesionales no se equivocaron en absoluto. https://www.kaspersky.es/blog/que-es-un-botnet/755/

A pesar de sus temores ante el robo de identidad y otras formas de ciberdelincuencia, muchas personas no han adoptado medidas más allá de las básicas para su protección online.

Solo el 16% cuenta con un sistema que les proteja del robo de identidad. De estos, cerca del 39% cuenta con él porque estaba incluido en otro producto o servicio contratado. Además, como dato interesante, el 38% considera su inclusión la principal razón para haber elegido a su proveedor actual.

La investigación también ha revelado que los encuestados con un elevado interés en la tecnología no presentan necesariamente una mayor comprensión o seguridad en lo que respecta a los riesgos. Parece que la confusión en cuanto a la seguridad trasciende a los grupos demográficos y afecta incluso a aquellos que demuestran un elevado interés en la tecnología

Adicionalmente, los usuarios no suelen saber qué hacer cuando les ocurre un Ciber ataque, en especial el robo de identidad que es lo que como vimos, más les preocupa.

Estamos pues, ante una gran oportunidad para las empresas aseguradoras en nuestro caso, que pueden llegar a marcar una gran diferencia en sus productos si incluyen servicios, insumos, soluciones de ciberprotección, los cuales cada vez cuentan con una demanda mayor entre los consumidores.

Es así que las aseguradoras intentan diversas estrategias para dar respuesta a los asegurados ante estos riesgos. Estas van desde advertencias recurrentes hasta brindar servicios de prevención, antes que el de indemnización, en la fase previa al daño. También es clave informar a clientes, a través de guías, cuáles son las mejores prácticas con respecto al manejo de las herramientas de seguros.

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

Los seguros cibernéticos se suelen mencionar como una herramienta para aumentar la resiliencia - capacidad de superar situaciones traumáticas-cibernética, como un mecanismo de transferencia de riesgos y como una herramienta útil de evaluación para acompañar y ayudar en los cálculos de riesgos de las empresas. Estos seguros se comercializan como un producto independiente o como parte de un paquete de otras

coberturas sobretodo de responsabilidad civil, todo riesgo operativo o seguros de hogar, si se destina a la familia.

Pero claro, los Seguros Cibernéticos tienen sus propios problemas.

Por un lado, el riesgo es difícil de medir, el riesgo cibernético es un problema mundial que evoluciona en forma constante a medida que el mundo se conecta cada vez más, y vaya si lo hace. Asimismo, la falta de datos suficientes sobre los incidentes cibernéticos y el bajo nivel de conocimiento y experiencia sobre el riesgo cibernético, son obstáculos que aún deben abordarse.

No obstante, estos son obstáculos propios de los nuevos riesgos y entiendo deben ser asumidos con un grado de audacia, sobre todo si pensamos en los aspectos preventivos que este tipo de seguros pueden aportar a las personas y empresas.

3. CIBER RIESGOS Y SU DIMENSIÓN FUNCIONAL

Me refiero en este punto a los riesgos que pueden afectar la funcionalidad de la propia empresa de seguros y cómo deberían prevenirse.

Estamos en Latinoamérica en la era del Gobierno Corporativo que implica la gestión de los riesgos empresariales, inspirados en esencia en los "Principios básicos de seguros, estándares, guía y metodología de evaluación" de la Asociación internacional de supervisores de seguros, IAIS (www.iaisweb.org).

En especial sus principios básicos 7 y 8:

PBS 7 Gobierno corporativo

El supervisor requiere que las aseguradoras establezcan e implementen un marco de gobierno corporativo que brinde una administración y supervisión de la actividad de la aseguradora estable y prudente, y que reconozca y proteja de manera adecuada los intereses de los asegurados.

PBS 8 Gestión de riesgos y controles internos

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

En el Uruguay, es así que, en aplicación de estos conceptos, la Superintendencia de Servicios Financieros, órgano de contralor de la actividad aseguradora ha establecido estándares mínimos de gestión para empresas de seguros en base a la evaluación integral y la llamada metodología CERT.

La Superintendencia de Servicios Financieros ha definido que el proceso de supervisión debe estar orientado a ser integral, proactivo, enfocado a riesgos y sobre una base consolidada.

Una de las herramientas con que cuenta la supervisión para cumplir con sus cometidos es la Evaluación Integral, trabajo llevado a cabo *in situ* en la aseguradora. El propósito de la Evaluación Integral es evaluar la calidad de la gestión de las entidades y en caso de detectar debilidades, evaluar su impacto sobre la capacidad de la entidad de mantener niveles prudenciales de solvencia a corto, mediano y largo plazo.

Para sintetizar los resultados de la evaluación, se ha definido una metodología denominada CERT, donde la C corresponde a Gobierno Corporativo, E a Evaluación económica financiera, R a Riesgos y T a Tecnología.

El objetivo del CERT es sintetizar la evaluación por componente y en forma general, de tres aspectos:

- si existe alguna debilidad en uno de los componentes que requiera atención prioritaria por parte de la institución;

- en qué etapa de resolución se encuentra dicha debilidad;

- el impacto potencial de la debilidad encontrada sobre la capacidad de la institución de mantener niveles de solvencia prudenciales en el corto plazo.

Para aplicar la metodología CERT a una entidad, los supervisores analizarán los siguientes componentes:

C. Gobierno Corporativo: es el sistema a través del cual las instituciones son dirigidas, monitoreadas y controladas. Es la forma mediante la cual las instituciones se organizan para llevar a cabo la administración y el control de su gestión.

Está constituido por las estructuras de:

- dirección de la institución (el Directorio o autoridad jerárquica equivalente),

- de gestión (la Alta Gerencia, funcionarios jerárquicos) y
- de control (Comité de Auditoría, Auditoría Interna y Auditoría Externa, entre otros).

Supone un conjunto de prácticas adoptadas para llevar adelante la dirección, monitoreo y control diario del negocio, en el marco de las leyes y regulaciones aplicables.

El gobierno corporativo debe procurar además la adhesión de los funcionarios de la institución a estas prácticas y lograr la eficacia en las prácticas lo cual comporta, entre otros aspectos un adecuado sistema de gestión integral de riesgos.

E. Evaluación Económica Financiera: la situación económica financiera de la institución se analiza haciendo hincapié en el nivel y calidad del patrimonio de la institución y su capacidad de respaldar los riesgos asumidos y proveer protección a los asegurados y beneficiarios.

R. Riesgos: el sistema de gestión de riesgos de la institución y la capacidad de la misma de identificar, controlar, medir y monitorear los siguientes riesgos:

- Riesgo de Seguros
- Riesgo de Crédito
- Riesgo de Mercado
- Riesgo de Liquidez
- Riesgo Operacional
- Riesgo de Lavado de Activos y Financiamiento de Terrorismo
- Riesgo de Reputación
- Riesgo Estratégico

T. Tecnología: es la gestión de los riesgos tecnológicos y confiabilidad y eficacia de los sistemas de información como herramientas de la gestión.

Desde el punto de vista metodológico debe visualizarse el Gobierno Corporativo como el núcleo central del análisis, con el cual se interrelacionan los otros componentes del sistema.

Para mayor transparencia sobre la aplicación del nuevo sistema y con la idea de proveer orientación a las aseguradoras sobre qué se espera de ellas, se ha elaborado una serie de estándares mínimos de gestión asociado a los cuatro componentes de la metodología CERT.

Desde el punto de vista del supervisor se entiende que el no cumplimiento de un estándar constituye una debilidad que debe ser tratada con atención prioritaria por la entidad.

Las empresas de seguros adoptan diferentes esquemas y estructuras para llevar adelante su gestión, tomando en cuenta la naturaleza, tamaño y complejidad de sus operaciones y su perfil de riesgos.

El supervisor lleva adelante sus procedimientos de supervisión y evaluación teniendo en cuenta estos elementos.

Los estándares constituyen prácticas de gestión que el supervisor espera encontrar en las entidades supervisadas.

Como podemos apreciar la tecnología y su gestión constituye nada menos que un de los cuatro pilares de la metodología CERT que no lo identifica simplemente como un riesgo sino como todo un verdadero estándar que la empresa debe gestionar como parte central de su negocio[5].

La Gerencia o responsable de TI (tecnología de la información) debe tener la habilidad para identificar las necesidades y para desarrollar, adquirir, instalar y mantener soluciones de TI apropiadas de acuerdo con las necesidades de la entidad.

Es claro pues, que, bajo estos lineamientos, deben atenderse los riesgos tecnológicos en sentido amplio, abarcando tanto los riesgos directamente relacionados a los aspectos informáticos como los atinentes a los recursos humanos, ya que el error humano suele ser la causa o la puerta, del ataque cibernético.

O sea no sólo la gestión de los aspectos directamente relacionados a la seguridad de los sistemas informáticos como ser la actualización permanente de sistemas, la adecuada clasificación de la información personal, financiera y comercial, la ejecución de *back up* periódico y su custodia en lugares distintos a la ubicación principal, la eventual restricción de acceso a redes públicas, la elaboración de planes de respuesta a incidentes; sino también la debida gestión de los recursos humanos

5 Los estándares para la evaluación de las áreas de Tecnología de Información (TI) tienen como base el conjunto de principios conocido como CobiT, en particular los vinculados al dominio de Adquisición e Implementación.

con segmentación de accesos y reglas de usos de claves, asegurar la confidencialidad, lograr la capacitación de las áreas de auditoría en detección de incidentes, entre otras.

E incluso, por lo antes dicho sobre la gestión de riesgos como parte del Gobierno corporativo, es clara la debida implicancia en la gestión de la alta dirección que debe entender la protección de datos y la ciberseguridad como un elemento central, clave, del negocio.

Debe comprender que la fuente de riesgo no es solo externa, que el delito cibernético puede tener origen en cualquier cargo, ser consciente de las normativas aplicables y las consecuencias de su incumplimiento y crear una política de gestión del riesgo, especial y específica, que sea aplicada en forma constante, documentada, actualizada y puesta en conocimiento de la organización, destinando recursos para su ejecución.

En suma, en la era de la tecnología, del Gobierno corporativo, la empresa aseguradora debería encarar la prevención y minimización del riesgo cibernético con una gerencia de riesgo especializada y prioritaria a nivel general.

4. CIBER RIESGOS Y SU DIMENSIÓN ÉTICA

Por último y no menos importante, cabe analizar lo que llamo la dimensión ética de los Ciber riesgos, esta vez vistos como otro tipo de riesgo que el Ciber medio o espacio crea para los seres humanos.

Como expresa un artículo del Real Instituto El Cano[6] "en el campo de la ciberseguridad, la IA (Inteligencia Artificial) aporta importantes mejoras mediante el análisis algorítmico aplicado a gran cantidad de información, infiriendo resultados basados en el contexto y en el aprendizaje adquirido a partir de situaciones anteriores. Las capacidades de la IA, sus algoritmos, se pueden aplicar de forma similar –tanto– por quienes crean inseguridad en las sociedades avanzadas y –como– por quienes las protegen. La confrontación directa entre algoritmos de IA y su escalada, pueden 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 de ámbito internacional sobre la necesidad

6 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: Javier Alonso Lecuit. ARI 50/2019

de regular las características y el uso de la IA, principalmente desde un plano ético, pero también desde el punto de vista normativo y de control de su empleo, sin por ello limitar los beneficios aportados por la innovación en IA a la sociedad".

"A pesar de existir unanimidad sobre la necesidad de una normativa internacional, resulta particularmente complicado concretar una hoja de ruta que establezca los pasos a seguir. La inacción, es decir, dejar que las fuerzas del mercado establezcan las reglas de juego conduciría a la desprotección de los derechos fundamentales de la seguridad de los individuos y naciones, similar a la experimentada actualmente a escala mundial en materia de la privacidad. Esto se aproxima al impacto potencial de la IA, a los efectos de su empleo malicioso y la necesidad de controles y contramedidas que carecen de un marco regulatorio mundial".

Esta preocupación no ha escapado a las autoridades de la Unión Europea y es así que 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 "Generar confianza en la inteligencia artificial centrada en el ser humano"[7].

En el documento se afirma que la inteligencia artificial (IA) tiene potencial para 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 a la medida de nuestras necesidades.

La IA también puede ayudar a detectar el fraude y las amenazas de ciberseguridad y permite a los organismos encargados de hacer cumplir la ley luchar contra la delincuencia con más 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 buen ritmo en todo el mundo.

No obstante, también trae consigo nuevos retos para el futuro del trabajo y plantea cuestiones jurídicas y éticas.

Para abordar estos retos y aprovechar al máximo las oportunidades que ofrece la IA, en abril de 2018 la Comisión publicó una estrategia europea.

7 https://ec.europa.eu/transparency/regdoc/rep/1/2019/ES/COM-2019-168-F1-ES-MAIN-PART-1.PDF. Bruselas 8.4.2019.

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

Adopta un planteamiento triple para potenciar la capacidad tecnológica e industrial de la Unión Europea e impulsar la adopción de la IA en todos los ámbitos de la economía, prepararse para las transformaciones socioeconómicas y garantizar el establecimiento de un marco ético y jurídico apropiado.

La Estrategia europea de IA y el plan coordinado bajo esta, 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 mismo, sino un medio que debe servir a las personas con el objetivo último de aumentar su bienestar.

Para ello, la fiabilidad de la IA debe estar garantizada. Los valores en los que se basan nuestras sociedades han de estar plenamente integrados en la evolución de la IA. Los valores de respeto de la dignidad humana, la libertad, la democracia, la igualdad, el Estado de Derecho y el respeto de los derechos humanos, incluidos los derechos de las personas pertenecientes a minorías, debe ser respetados.

Estos valores son comunes a las sociedades no solo de la Unión Europea, sino que son extrapolables a toda Latinoamérica, en las que 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 fundamento de nuestras sociedades.

En su informe, la Comisión apoya los siguientes requisitos esenciales para una IA fiable. Anima a las partes interesadas a aplicarlos y a comprobar la lista que los lleva a la práctica con el fin de crear el entorno adecuado de confianza para un desarrollo y un uso provechosos de la IA.

Los siete requisitos esenciales son los siguientes: •Intervención y supervisión humanas •Solidez y seguridad técnicas •Privacidad y gestión de datos •Transparencia •Diversidad, no discriminación y equidad •Bienestar social y medioambiental •Rendición de cuentas

I. Intervención y supervisión humanas. Los sistemas de IA deben ayudar a las personas a elegir mejor y con más conocimiento de causa en función de sus objetivos. Deben actuar como facilitadores de una sociedad floreciente y equitativa, apoyando la intervención humana y los derechos fundamentales, y no disminuir, limitar o desorientar la au-

tonomía humana. El bienestar global del usuario debe ser primordial en la funcionalidad del sistema.

La supervisión humana ayuda a garantizar que un sistema de IA no socave la autonomía humana ni cause otros efectos adversos. Dependiendo del sistema específico de IA y de su ámbito de aplicación, deben garantizarse los grados adecuados de medidas de control, incluida la adaptabilidad, la exactitud y la explicación de los sistemas de IA. La supervisión debe lograrse a través de mecanismos de gobernanza, tales como el enfoque de la participación humana (*human-in-the-loop*), la supervisión humana (*human-on-the-loop*), o el control humano (*human-in-command*).

Asimismo, hay que garantizar que las autoridades tengan la capacidad de ejercer sus competencias de supervisión conforme a sus mandatos. En igualdad de condiciones, cuanto menor sea la supervisión que puede ejercer un ser humano sobre un sistema de IA, más extensas tendrán que ser las pruebas y más estricta la gobernanza.

II. Solidez y seguridad técnicas. La fiabilidad de la IA requiere que los algoritmos sean suficientemente seguros, fiables y sólidos para resolver errores o incoherencias durante todas las fases del ciclo vital del sistema de IA y hacer frente adecuadamente a los resultados erróneos.

Los sistemas de IA deben ser fiables, lo bastante seguros para ser resilientes, tanto frente a los ataques abiertos como a tentativas más sutiles de manipular datos o los propios algoritmos, y deben garantizar un plan de contingencia en caso de problemas. Sus decisiones deben ser acertadas, como mínimo, reflejar su nivel de acierto, y sus resultados, reproducibles. Además, los sistemas de IA deben integrar mecanismos de seguridad y de seguridad desde el diseño para garantizar que sean verificablemente seguros en cada fase, teniendo muy presente la seguridad física y psicológica de todos los afectados. Esto incluye la minimización y, cuando sea posible, la reversibilidad de las consecuencias no deseadas o errores en el funcionamiento del sistema.

Deben instaurarse procesos para aclarar y evaluar los riesgos potenciales asociados al uso de los sistemas de IA, en diversos ámbitos de aplicación.

III. Privacidad y gestión de datos. Deben garantizarse la privacidad y la protección de datos en todas las fases del ciclo vital del sistema de IA.

Los registros digitales del comportamiento humano pueden permitir que los sistemas de IA infieran no solo las preferencias, la edad y el sexo de las personas, sino también su orientación sexual o sus opiniones religiosas o políticas. Para que las personas puedan confiar en el trata-

miento de datos, debe garantizarse que tienen el pleno control sobre sus propios datos, y que los datos que les conciernen no se utilizarán para perjudicarles o discriminarles.

Además de salvaguardar la privacidad y los datos personales, deben cumplirse requisitos en cuanto a garantizar la calidad de los sistemas de IA. La calidad de los conjuntos de datos utilizados es primordial para el funcionamiento de los sistemas de IA cuando se recopilan datos, pueden reflejar sesgos sociales, o contener inexactitudes o errores. Esto debe resolverse antes de entrenar un sistema de IA con un conjunto de datos.

Asimismo, debe garantizarse la integridad de los datos. Los procesos y conjuntos de datos utilizados deben ponerse a prueba y documentarse en cada fase, como la planificación, el entrenamiento, el ensayo y el despliegue. Esto debe aplicarse también a los sistemas de IA que no han sido desarrollados internamente, sino que se han adquirido fuera.

Por último, el acceso a los datos debe estar adecuadamente regulado y controlado.

IV. Transparencia. Debe garantizarse la trazabilidad de los sistemas de IA; es importante registrar y documentar tanto las decisiones tomadas por los sistemas como la totalidad del proceso –incluida una descripción de la recogida y el etiquetado de datos, y una descripción del algoritmo utilizado– que dio lugar a las decisiones.

A este respecto, en la medida de lo posible debe aportarse la explicación del proceso de toma de decisiones algorítmico, adaptada a las personas afectadas. Debe proseguirse la investigación en curso para desarrollar mecanismos de explicación. Además, deben estar disponibles las explicaciones sobre el grado en que un sistema de IA influye y configura el proceso organizativo de toma de decisiones, las opciones de diseño del sistema, así como la justificación de su despliegue –garantizando, por tanto, no solo la transparencia de los datos y del sistema, sino también la transparencia del modelo de negocio–.

Por último, es importante comunicar adecuadamente las capacidades y limitaciones del sistema de IA a las distintas partes interesadas afectadas de una manera adecuada al caso de que se trate.

Por otra parte, los sistemas de IA deben ser identificables como tales, garantizando que los usuarios sepan que están interactuando con un sistema de IA y qué personas son responsables del mismo.

V. Diversidad, **no discriminación y equidad**. Los conjuntos de datos utilizados por los sistemas de IA –tanto para el entrenamiento como

para el funcionamiento– pueden verse afectados por la inclusión de sesgos históricos involuntarios, por no estar completos o por modelos de gobernanza deficientes. La persistencia en estos sesgos podría dar lugar a una discriminación (in)directa. También pueden producirse daños por la explotación intencionada de sesgos del consumidor o por una competencia desleal.

Por otra parte, la forma en la que se desarrollan los sistemas de IA -por ejemplo, la forma en que está escrito el código de programación de un algoritmo- también puede estar sesgada. Estos problemas deben abordarse desde el inicio del desarrollo del sistema.

También puede ayudar a resolver estos problemas establecer equipos de diseño diversificados y crear mecanismos que garanticen la participación, en particular de los ciudadanos, en el desarrollo de la IA. Es conveniente consultar a las partes interesadas que puedan verse afectadas directa o indirectamente por el sistema a lo largo de su ciclo de vida.

Los sistemas de IA deberían tener en cuenta toda la gama de capacidades, habilidades y necesidades humanas y garantizar la accesibilidad mediante un enfoque de diseño universal para tratar de lograr la igualdad de acceso para las personas con discapacidades.

VI. Bienestar social y medioambiental. Para que la IA sea fiable, debe tomarse en cuenta su impacto sobre el medio ambiente y sobre otros seres sensibles. Idealmente, todos los seres humanos, incluso las generaciones futuras, deberían beneficiarse de la biodiversidad y de un entorno habitable.

Debe, por lo tanto, fomentarse la sostenibilidad y la responsabilidad ecológica de los sistemas de IA.

Por otra parte, el impacto de los sistemas de IA debe considerarse no solo desde una perspectiva individual, sino también desde la perspectiva de la sociedad en su conjunto. Debe prestarse especial atención al uso de los sistemas de IA, particularmente en situaciones relacionadas con el proceso democrático, incluida la formación de opinión, la toma de decisiones políticas o en el contexto electoral.

También debe tenerse en cuenta el impacto social de la IA. Si bien los sistemas de IA pueden utilizarse para mejorar las habilidades sociales, de la misma manera pueden contribuir a su deterioro.

VII. Rendición de cuentas. Deben instaurarse mecanismos que garanticen la responsabilidad y la rendición de cuentas de los sistemas de IA y de sus resultados, tanto antes como después de su implementación.

La posibilidad de auditar los sistemas de IA es fundamental, puesto que la evaluación de los sistemas de IA por parte de auditores internos y externos, y la disponibilidad de los informes de evaluación, contribuye en gran medida a la fiabilidad de la tecnología.

La posibilidad de realizar auditorías externas debe garantizarse especialmente en aplicaciones que afecten a los derechos fundamentales, por ejemplo, las aplicaciones críticas para la seguridad.

Los potenciales impactos negativos de los sistemas de IA deben señalarse, evaluarse, documentarse y reducirse al mínimo. El uso de las evaluaciones de impacto facilita este proceso. Estas evaluaciones deben ser proporcionales a la magnitud de los riesgos que plantean los sistemas de IA. Los compromisos entre los requisitos –que a menudo son inevitables– deben abordarse de una manera racional y metodológica, y ser tenidos en cuenta.

Por último, cuando se produzcan efectos adversos injustos, deben estar previstos mecanismos accesibles que garanticen una reparación adecuada.

Como se puede apreciar, la preocupación por los aspectos éticos de las nuevas tecnologías, y el ambiente cibernético, ameritan comenzar a hablar de una dimensión ética de los Ciber riesgos.

CONCLUSIONES

Todos somos rehenes de la tecnología, pero a la vez la disfrutamos y la vivimos.

Esto por supuesto trae luces y sombras, el Ciber espacio puede crear ilusiones falsas, personalidades irreales, perfiles humanos, profesionales y hasta empresariales, que no corresponden a la realidad. Asimismo, nos aleja de la espontaneidad del cara a cara y puede dar lugar a mal entendidos y falta de comunicación genuina y profunda.

Ello nos puede hacer vivir en un mundo paralelo, fantástico e irreal, si no se sabe manejar adecuadamente, con responsabilidad a todos los niveles y si no se regulan los aspectos que sustentan la aplicación y usos de la Inteligencia Artificial, base de esa nueva realidad tecnológica.

Pero, por otra parte, entre otras muchas virtudes, la comunicación de personas entre distintos puntos del planeta, incluso todos a la vez, como si estuvieran conversando en la mesa de un café, es de un valor inconmensurable…

Sin dudas, si el mundo tecnológico, cibernético, no existiera, no conviviera con nosotros, estos riesgos no existirían, pero ¿cómo negarse al avance en tantos aspectos positivos que ellas aportan?

Otra vez como en tantos asuntos de la vida, el equilibrio debería ser la clave.

El lograr el debido equilibrio en el diseño, la aplicación y el uso de las tecnologías, es lo único que puede dar paz al ser humano y a la sociedad toda, resaltando sus bonanzas y no sus debilidades, dentro de la atractiva, apasionante y vertiginosa vorágine, de este mundo cibernético.

BIBLIOGRAFÍA

AFFINION GROUP. Informe sobre ciberdelincuencia - https://www.ciberseguridadpyme.es- Recuperado 10/04/2019.

ASOCIACIÓN INTERNACIONAL DE SUPERVISORES DE SEGUROS. Principios básicos de seguros, estándares, guía y metodología de evaluación - IAIS -www.iaisweb.org. Recuperado 7/06/2019.

BEER, Anthony Satfford. (1959). Cybernetics and Management, English Universities Press.

LECUIT, Javier Alonso. (2019). Inteligencia Artificial - ARI 50/2019- Publicación Real Instituto El Cano. -www.realinstitutoelcano.org/wps/portal/rielcano_es/- Recuperado 12/06/2019.

SIGNORINO, Andrea. (2019). Relatoría por Uruguay- Congreso CILA – Lima.

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

UNIÓN EUROPEA. Comunicación de la Comisión al Parlamento europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones- Generar confianza en la inteligencia artificial centrada en el ser humano https://ec.europa.eu/transparency/regdoc/rep/1/2019/ES/COM-2019-168-F1-ES-MAIN-PART-1.PDF. Bruselas 8.4.2019. Recuperado 5/ 05/ 2019.

VIVAS, Gabriel. (2019). Ponencia en curso APECOSE - Lima.

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