Dos

Ciberriesgo desde la perspectiva de riesgo sistémico

DOI: 10.29236/sistemas.n151a6

"El simple aleteo de las alas de una mariposa puede originar un tsunami al otro lado del mundo". Proverbio Chino

Resumen

"*No importa los riesgos que asumamos, siempre consideramos que el final es demasiado pronto, aunque en la vida, más que nada, la calidad debe ser más importante que la cantidad*"- Alex Honnold. Actualmente la humanidad está enfrentándose a una nueva dinámica social, a unas nuevas formas de convivencias reales no virtuales inmersas en un nuevo espacio de convivencia social que no es territorial ni material, sino un espacio meta-espacial, más que una representación virtual -siendo un ambiente intangible, pero a la vez muy real- (Suñé, 2015). Se trata del ciberespacio, constituido como el quinto entorno estratégico, tras Tierra, Mar, Aire y Espacio (Adams, 2015). Durante el año 2018, el mundo llegó a enfrentar un crecimiento significativo y complejo en los desafíos que trae la "hiperconectividad", enfrentándonos a problemáticas desde el cambio climático, hasta la crisis financiera global. No podemos caer en el error de pensar que exclusivamente las grandes empresas y multinacionales serán las afectadas por este tipo de riesgo, teniendo como referencia que la afectación de cualquier participante de un ecosistema cibernético podrá reflejar su impacto en todos los que en él conviven.

Palabras clave

Riesgo sistémico, ciberriesgo, ciberseguridad, ciberespacio

Introducción

Anualmente el World Economic Forum (WEF) presenta el Global Risks Report (World Economic Forum, 2019), exponiendo para el presente año un contexto de preocupantes tensiones geopolíticas y geoeconómicas. Si no se resuelven, dificultará la capacidad del mundo para enfrentar una gama creciente de desafíos colectivos, desde la evidencia progresiva de la degradación ambiental hasta las crecientes interrupciones y amenazas que ha conllevado el desarrollo de una nueva revolución, donde Klaus Schwab autor del libro "La cuarta revolución industrial", vaticina "*Estamos al borde de una revolución tecnológica que modificará fundamentalmente la forma en que vivimos, trabajamos y nos relacionamos. En su escala, alcance y complejidad, la transformación será distinta a cualquier cosa que el género humano haya experimentado antes*". Son precisamente aquellos países más avanzados los que experimentaron los cambios con mayor rapidez, pero a la vez las economías emergentes las que llegaron a identificar mayores beneficios. Figura 1

La tecnificación y evolución a la interconexión alrededor de las áreas de los sistemas tradicionales de automatización de fabricación continuará ganando impulso; por lo tanto, la convergencia de TI y las tecnologías operativas será un

Figura 1. Resumen Riesgos Top 5 - 2015 a 2019, (WEF, 2019)

punto fuerte de discusión dentro de las organizaciones, enfocando nuevas plataformas y servicios empresariales que potencialmente integrarán diferentes áreas, desde datos empresariales a nivel corporativo, hasta automatización a nivel de campo y proceso. Estas plataformas serán altamente deseables en la búsqueda de la digitalización, ya que ofrecerían mejores diseños, visualizaciones, ergonomía y comodidad de accesibilidad. Sin embargo, estas plataformas presentan el desafío de administrar la privacidad al mismo tiempo que aumentan el área de exposición a las amenazas cibernéticas y, a la vez mantener un nivel similar o superior de seguridad y confiabilidad en torno a las operaciones de estos sistemas interconectados.

Dicha revolución posee la capacidad de incrementar los niveles de ingreso globales y brindar un mejoramiento en la calidad de vida de sociedades y comunidades enteras, apunta Schwab, las mismas que se han beneficiado con la llegada de los diferentes entornos digitales (asignación de parqueaderos en zonas metropolitanas, transporte compartido mediante redes sociales, plataformas de comercio electrónico, servicios financieros, entre otros). Sin embargo, el proceso de transformación sólo beneficiará a quienes sean capaces de innovar y adaptarse.

La interconectividad y la adopción de las nuevas tecnologías traen consigo un incremento en la exposición a una nueva naturaleza de riesgos denominado riesgos cibernéticos, que están demandando por parte de entidades y autoridades esfuerzos importantes para identificarlos y gestionarlos. Uno de los grandes retos de las organizaciones lo constituye la seguridad de la información, en particular, la que reside o se procesa en medios electrónicos, la cual, ahora más que nunca, se encuentra expuesta a las amenazas cibernéticas, dada la naturaleza global de Internet y de los sistemas de información, que no tienen una limitación fronteriza.

Por otro lado, el riesgo sistémico se refiere al riesgo de una avería de todo un sistema en lugar de simplemente la falla de partes individuales. Un ejemplo de ello en un contexto financiero, es el riesgo de una falla en cascada en el sector causada por las interconexiones dentro del sistema financiero, teniendo como resultado una grave recesión económica. Una pregunta clave para los formuladores de estrategias para la gestión de riesgos es cómo limitar la acumulación de riesgo sistémico y contener los eventos de crisis cuando ocurren. Figura 2

Un ecosistema con varios participantes

Podemos entonces decir que el ciberespacio, dentro de su misma definición se podría considerar como un ecosistema cibernético que comprende una variedad de diver-

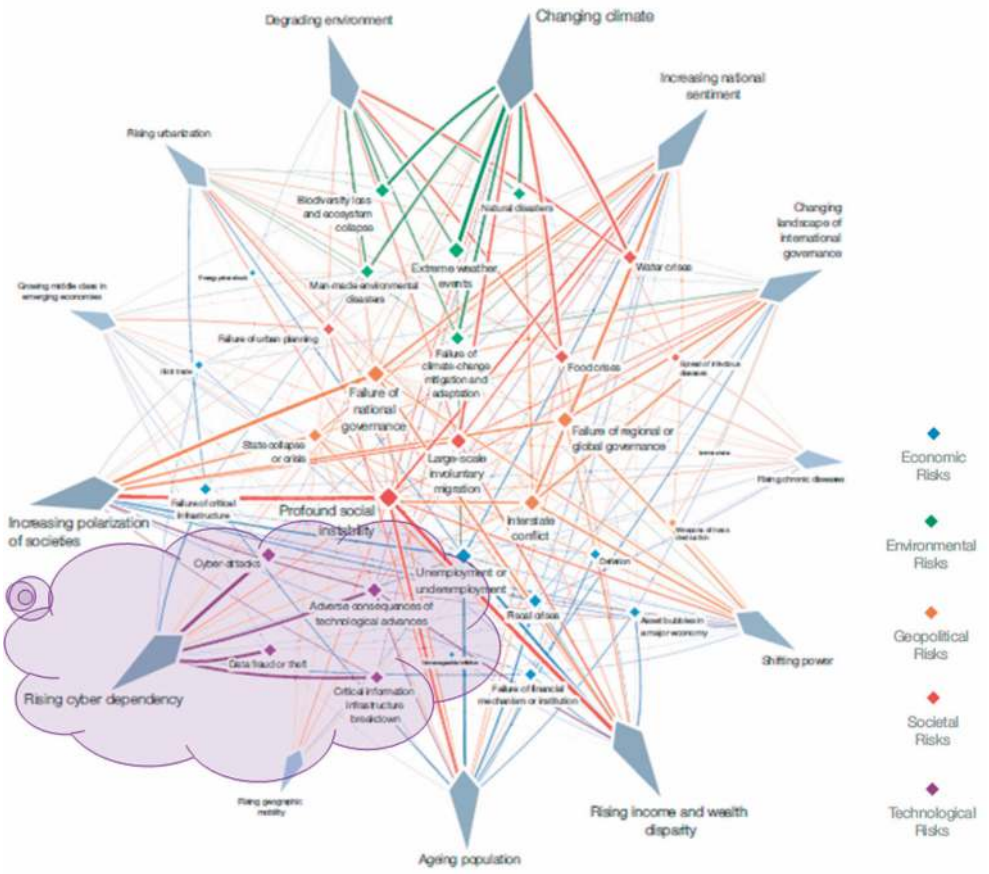

Figura 2. Interdenpencias de los Riesgos, (WEF, 2019)

sos participantes como empresas privadas, organizaciones sin fines de lucro, gobiernos, individuos y dispositivos cibernéticos que interactúan con múltiples propósitos. Son las infraestructuras de TI, que de manera interconectada brindan un sinnúmero de interacciones entre personas, procesos, datos y tecnologías de comunicación junto con el entorno y las condiciones que influyen en esas interacciones.

Las organizaciones de todos los tamaños, tanto en el sector público como en el privado, dependen cada vez más de los activos de información y tecnología, sin embargo, es necesario contar con el apoyo de las personas para ejecutar con éxito procesos de negocios que, a su vez, respaldan la prestación de servicios. La falla de estos activos tiene un impacto directo y negativo en los procesos de negocios que soportan. Esto, además, puede convertirse en una incapacidad para la prestación de los servicios, lo que finalmente afecta la misión de la organización. Dadas estas relaciones, la gestión de los riesgos para estos activos es un factor clave para posicionar la organización para el éxito. Aun cuando se pueda caer

en la falla que la identificación de riesgos cibernéticos aplica única y exclusivamente a las organizaciones de TI, nuestra vida diaria, vitalidad económica y seguridad nacional dependen de un ciberespacio estable, seguro y resistente que se encuentra comprendido por diferentes sectores e industrias.

El ciberespacio y su infraestructura subyacente son vulnerables a una amplia gama de riesgos derivados de amenazas y peligros tanto físicos como cibernéticos. Los sofisticados actores y los estados nacionales explotan las vulnerabilidades para robar información y dinero y están desarrollando capacidades para interrumpir, destruir o amenazar la prestación de servicios esenciales.

En 2017, la firma Deloitte informó que la industria de la energía era el segundo objetivo más popular para los ataques cibernéticos en 2016. Casi tres cuartos de las compañías de petróleo y gas de los Estados Unidos, según la consultora, tuvieron un incidente cibernético en dicho año; no obstante, sólo una pequeña mayoría citaron el riesgo como una de las principales preocupaciones en sus informes anuales. Estas compañías al día de hoy tienen miles de dispositivos conectados y esto conlleva a una situación muy preocupante de ciberriesgo en el petróleo y el gas.

Se espera que el mercado de IoT (internet de las cosas por sus siglas en inglés) para la industria del petróleo y el gas crezca a una tasa del 82% entre 2017 y 2022.

En los últimos años, la industria global del petróleo y el gas ha sido testigo de desafíos como la caída de los precios, la poca demanda y las preocupaciones ambientales. IoT permite monitorear las instalaciones de forma remota y obtener conocimiento sobre los inventarios diarios y las condiciones de los equipos que soportan la operación. El creciente número de compañías de petróleo y gas está invirtiendo en sistemas de control, software y análisis mejorados para optimizar sus operaciones y darles una ventaja competitiva.

Según *MarketsandMarket*, hasta el año 2022 se espera que el mercado general de tecnología operacional (OT) se valúe en USD 42 mil millones, con un crecimiento anual del 6,7%. Los factores que impulsan el crecimiento de este mercado es la creciente demanda de industrialización en economías emergentes; evolución de IIoT (internet de las cosas en el sector industrial), y aumento de las máquinas de comunicación y monitoreo; junto a la creciente demanda de soluciones de automatización inteligente.

Con el sector del petróleo y el gas, adoptar IoT para mejorar sus procesos es parte de su futuro, pero su primer objetivo es aprender cómo implementar la seguridad en su infraestructura e identificar clara-

mente que los ciberriesgos presentes podrán llegar a verse reflejados en otros sectores o hasta en la misma sociedad. Las amenazas cibernéticas para las compañías de petróleo y gas son una realidad en incremento exponencial. El objetivo de un atacante no sólo contempla equipos de campo, sino subcontratistas y bufetes de abogados que trabajan para varias de estas compañías. En junio de 2017, el virus informático NotPetya afectó a muchas compañías en todo el mundo, incluido el gigante ruso Rosneft.

Basado en ello, gobiernos como el de Estados Unidos vienen trabajando en estrategias que proporcionan al Departamento de Seguridad Nacional un marco para identificar las responsabilidades de seguridad cibernética durante los próximos cinco años. De esta manera buscan mantener el ritmo del panorama de riesgo cibernético en evolución, mediante la reducción de las vulnerabilidades y la creación del concepto de ciberresiliencia; contrarrestar a los actores maliciosos en el ciberespacio; responder a incidentes, además de que el ecosistema cibernético sea más seguro y resistente.

Contextualización del riesgo sistémico

Los riesgos generalmente son abordados de manera individual por una organización dentro de la gestión para sus procesos de negocio. Uno de los aspectos relevantes es la identificación y diferenciación de lo que es un riesgo sistémico y un riesgo sistemático. Al referirnos al primero se enfoca al reconocimiento de un sistema, como un conjunto de diferentes elementos que se encuentran relacionados entre sí, teniendo una o varias interdependencias con un objetivo en común; ejemplo de ello es un equipo de futbol, donde cada uno de los integrantes del equipo cumple una función para el objetivo común. El riesgo sistemático, por su parte, se refiere a la metodología de hacer las cosas, donde se debe identificar y analizar el problema antes de realizar cualquier acción, formular múltiples opciones, definir y establecer los criterios de selección, como también elegir y ejecutar la decisión final. Cuando se habla de riesgos sistémicos, el contexto es importante. Un riesgo que parece generalizado cuando se observa desde un país puede parecer diferente al de otro. Por ejemplo, durante la recesión de 2008 a 2010, las economías que para ese momento se encontraban en desarrollo como India y China obtuvieron mejores resultados que el resto de naciones. El impacto de la recesión fue mínimo para estos países.

La identificación de un marco de referencia es importante para juzgar si un riesgo tiene la naturaleza de ser sistemático o no. Pongamos por caso la existencia de dos países que tienen relaciones comerciales con la Unión Europea. El primero, completamente dependiente

(basado en exportaciones) y el segundo con una sola exposición parcial a los mercados de la Unión.

Adicional a esto, contemplemos la hipótesis de que dentro del plan de desarrollo de la Unión Europea se lleguen a realizar algunas modificaciones en el ámbito jurídico legal para disminuir las relaciones del mercado de exportación con ambos países, estableciendo un alto impuesto a las importaciones, lo cual afecta negativamente las exportaciones de cualquiera de los dos países, en donde el riesgo relativo se fundamenta en el marco de referencia. Para el primero, el riesgo tiene una naturaleza sistémica, pero, para el segundo país sólo representará una afectación para una pequeña cantidad de compañías. Por lo tanto, desde la perspectiva del segundo país, el riesgo puede llegar a no ser considerado sistémico.

Si no está seguro de la naturaleza del riesgo, definiendo si es sistémico o no, simplemente hágase esta pregunta, ¿es posible eliminar o equilibrar los impactos negativos sin llegar afectar a terceros o llegar a generar agentes de masificación de nuevos riesgos? Si la respuesta es afirmativa, ese riesgo no es sistémico.

El riesgo sistémico aplicado a las finanzas tiene muchas analogías con el análisis de riesgos que otros sistemas (no financieros) pueden exhibir. Fundamentalmente, el estudio del riesgo sistémico (financiero) se deriva de la constatación de que los sistemas financieros son frágiles. Hay cuatro elementos fundamentales para un mejor entendimiento del riesgo sistémico (Danielsson, 2016):

Riesgo endógeno
Se considera aquel riesgo creado por y dentro del propio ecosistema, en lugar de un resultado a un evento devastador fuera del sistema.

Mecanismos de amplificación
El origen de las crisis sistémicas generalmente se desencadena por un pequeño evento, cuyo impacto se magnifica por los vínculos dentro del ecosistema. En otras palabras, existen elementos que llegan a potencializar el impacto producido, viéndose reflejado en consecuencias a otros dentro del ecosistema.

Identificación de riesgos
Más allá de los factores comunes generados dentro de la identificación de riesgo es necesario establecer variables como la afectación de diferentes elementos del entorno, como el comportamiento de la materialización del riesgo y su magnificación, teniendo como focos las interdependencias que la organización posea en el ecosistema.

Creación de políticas
Los entes reguladores deben centrarse en iniciativas que reduzcan el riesgo sistémico y evitar aquellas

que, incluso con buenas intenciones, conduzcan realmente a la creación de nuevos y mayores riesgos.

Presencia del ciberriesgo en el sector financiero

Las entidades financieras en Colombia están comenzando a usar conceptos como blockchain para el registro y aseguramiento de las transacciones; big data y data analitics para el almacenamiento de grandes volúmenes de información y la toma de decisiones; *machine learning* para el otorgamiento de créditos, reconocimiento de siniestros y prevención del fraude; *algorithmic trading* para la compra y venta de valores en los mercados electrónicos; *cloud computing* para el desarrollo, pruebas y operación de aplicaciones administrativas y misionales; *artifitial intelligence* para manejar portafolios financieros; *biometrics* para el reconocimiento y autenticación de los clientes; IoT o internet de las cosas para lograr una tarifación adecuada de las pólizas de seguros; *smart contracts* o contratos inteligentes, en operaciones de comercio electrónico; APIs y *web services* para proveer información a otras organizaciones sin depender de elementos computacionales particulares. Estas tecnologías ya se han consolidado, están al alcance de personas y entidades de todo tipo y tamaño y su aplicación en diferentes sectores y actividades sólo está limitada por la creatividad.

El sector financiero ha estado durante mucho tiempo a la vanguardia de la ciberseguridad y el intercambio de información y cooperación en toda la industria. Aun así, los ataques cibernéticos a las diferentes instituciones financieras alrededor del mundo y las infraestructuras de los mercados financieros se han vuelto más frecuentes y sofisticados, lo que ha provocado inversiones de seguridad cada vez mayores y un mayor enfoque en la mitigación y gestión del riesgo cibernético. Paralelamente a estos esfuerzos, el sector financiero, los reguladores y los gobiernos nacionales han estado trabajando para mejorar la resistencia y la estabilidad en general con la esperanza de evitar una repetición de pánicos como la crisis financiera hace una década.

Otros ejemplos incluyen las intrusiones norcoreanas en el banco central de Bangladesh para intentar robar USD 951 millones a través del sistema de mensajes de pago global SWIFT (The New York Times, 2017) y el ataque al Banco de Chile, el banco más grande de dicho país, que “denegó el servicio a más de 9,000 computadoras y más de 500 servidores, para acceder a los sistemas conectados a la red SWIFT local del banco y realizar transacciones internacionales" (Cimpanu, 2018). A continuación, una breve reseña de los últimos 7 años que muestran algunos ciberataques significativos.

Figura 3

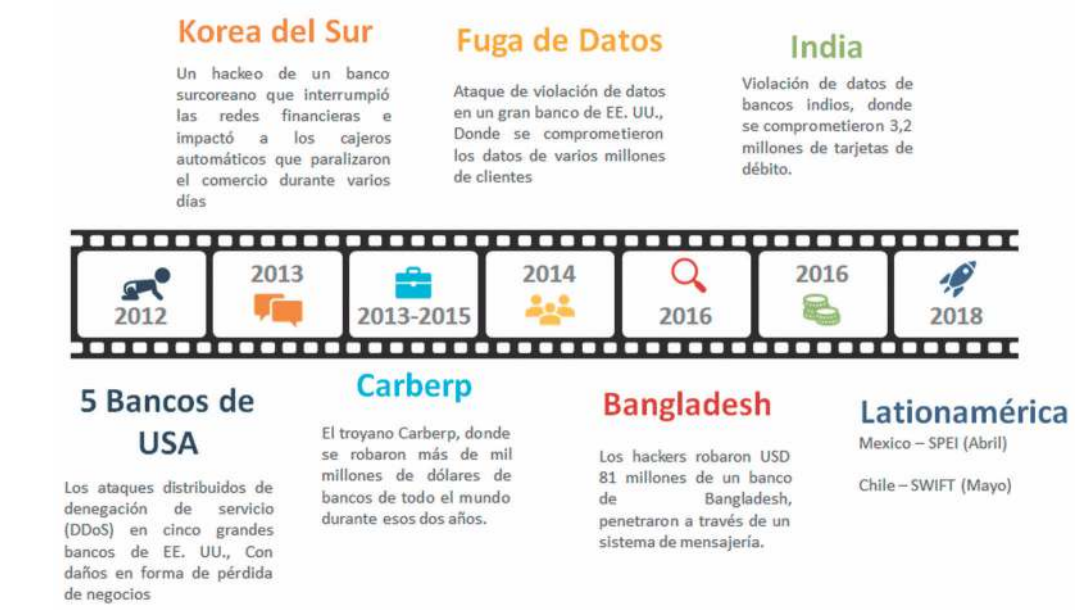

Figura 3. Reseña ataques cibernéticos 2012 - 2018. Adaptación del autor

Entonces surge la duda de, ¿cómo podrían los riesgos cibernéticos y los riesgos financieros interactuar para causar crisis sistémicas?, ¿hay algo fundamentalmente nuevo o diferente acerca de los riesgos cibernéticos?, ¿cómo deberían los economistas, reguladores, legisladores y bancos centrales enfocados en la estabilidad financiera incorporar los riesgos cibernéticos en sus modelos y pensamiento?

Algunas de las iniciativas más directas sobre estas preguntas comenzaron en 2013, luego de que una Orden Ejecutiva de la Casa Blanca instruyera al Departamento de Seguridad Nacional, en consulta con el Departamento del Tesoro, a identificar aquellas instituciones financieras para las cuales “(...) un incidente cibernético tendría un impacto de gran alcance, en seguridad económica regional o nacional" (Casa Blanca, 2014). En respuesta, ocho instituciones financieras líderes crearon el Centro de Análisis y Resiliencia Sistémica Financiera (FSARC) en 2016, concentrando los esfuerzos del sector en el "riesgo sistémico para el sistema financiero de los Estados Unidos, la seguridad cibernética actual y las amenazas emergentes" (FS-ISAC,2016).

Convergencia hacia una ciberresiliencia

La gestión del riesgo cibernético no es fundamentalmente diferente de la gestión del riesgo. Sin embargo, hay aspectos de los ecosistemas cibernéticos que hacen que la gestión del riesgo sea un desafío. La principal característica es el uso del ciberespacio. Las tecnologías de la

información y el ciberespacio han traído mejoras significativas para los individuos, las empresas y la sociedad en general en numerosas áreas, que incluyen la vida social, los servicios públicos, el comercio y la economía, el entretenimiento y las infraestructuras críticas. Al mismo tiempo, el uso y la dependencia del ciberespacio han introducido una serie de nuevas amenazas y vulnerabilidades. La ciberresiliencia se entiende como la capacidad de los sistemas para anticipar y adaptarse al potencial de sorpresa y falla, debiendo considerarse en el contexto de sistemas complejos que comprenden no sólo los dominios físicos y de información, sino también los dominios cognitivos y sociales, garantizando que la recuperación del sistema ocurra al considerar el *hardware*, el *software* y los componentes de detección interconectados de la infraestructura cibernética (Kott & Linkov, 2019).

Otro desafío importante con respecto a la gestión del ciberriesgo es que el ciberespacio evoluciona rápidamente y con frecuencia de una manera que es difícil de predecir. Los sistemas que hacen presencia en este ambiente meta espacial deben ser capaces de hacer frente a esta evolución. De hecho, se ven obligados a evolucionar en respuesta a la evolución del ciberespacio. Esto requiere un mayor enfoque en el monitoreo y la evaluación de riesgos en tiempo real como parte de la gestión general del riesgo cibernético.

Aunque los sistemas cibernéticos suponen un desafío desde el punto de vista de la gestión de riesgos, también existen características que podemos aprovechar y que tienen un efecto simplificador. El hecho de que estén hiperconectados en gran medida es beneficioso cuando se trata de la recopilación de datos, por lo que hemos enfatizado el uso de técnicas como el monitoreo y las pruebas. Además, la recolección de datos puede reducir la incertidumbre en la evaluación de riesgos con el uso de tecnologías emergentes como lo es Data Analytics y Big Data.

Finalmente es necesario la aceptación que el mundo en el cual vivimos ahora posee una dependencia tecnológica que obliga a desarrollar capacidades y metodologías que ofrezcan una identificación clara de aquellos riesgos cibernéticos teniendo como precedente que dichos riesgos tienden a ser sistémicos debido a su naturaleza la cual atenta contra más de un elemento dentro del ecosistema que representa el ciberespacio.

Día a día, nos enteramos de más ataques cibernéticos en nuestro país y en todo el mundo. Nuestra dependencia tecnológica hace que estos ataques lleguen a poseer el potencial de destruir nuestra seguridad militar y económica y, quizás, impactar el proceso que usamos para elegir a nuestros líderes.

Referencias

Adams, J. (2015). Cyber blackout (1st ed., pp. 15-21). Victoria, BC, Canada, FriesenPress.

Casa Blanca. (2014). *3 CFR 13636* - Executive Order *13636* (p. Sec. 7). Washington D.C.

Cimpanu, C. (2018). Hackers Crashed a Bank's Computers While Attempting a SWIFT Hack. Recuperado de: https://www.bleepingcomputer.com/news/security/hackers-crashed-a-bank-s-computers-while-attempting-a-swift-hack/

Danielsson, J. Fouché, M. & Macrae, R. (2016). Cyber risk as systemic risk. Recuperado de: https://voxeu.org/article/cyber-risk-systemic-risk

FS-ISAC Announces the Formation of the Financial Systemic Analysis & Resilience Center (FSARC) | FS-ISAC: Financial Services - Information Sharing and Analysis Center. (2016). Recuperado de: https://www.fsisac.com/article/fs-isac-announces-formation-financial-systemic-analysis-resilience-center-fsarc

Kott, A., & Linkov, I. (2019). *Cyber Resilience of Systems and Networks*. [S.l.]: Springer Nature (1st ed., pp. 4-7).

The New York Times (2017). North Korea Said to Be Target of Inquiry Over $81 Million Cyberheist. Recuperado de: https://www.nytimes.com/2017/03/22/business/dealbook/north-korea-said-to-be-target-of-inquiry-over-81-million-cyberheist.html

Refsdal, A., Bjørnar, S., & Stølen, K. (2015). *Cyber-risk management* [Cham]: Springer. (pp. 4, 9-25,26).

Suñé Llinás, E. (2015). La constitución del ciberespacio (1st ed.). Madrid: Porrúa México.

Ventre, D. (2014). Chinese cybersecurity and defense (1st ed., p. 46). London: ISTE. Edward

Griffor (2017) *Handbook of System Safety and Security: Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems.* Cambridge, MA. USA: Singress.

World Economic Forum. (2019). *The Global Risks Report 2019* (pp. 5-8). Geneva: World Economic Forum. Recuperado de: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

Joshsua J. González Díaz, M.Sc. *Ingeniero de Sistemas de la Pontificia Universidad Javeriana, especialista en seguridad de la información de la Universidad de los Andes, Especialista en Derecho Informático de la Universidad Externado de Colombia y Magister en Seguridad de la Información de la Universidad de los Andes. Actualmente se desempeña como profesor catedrático e investigador de la maestría en Seguridad de la Información de los Andes y la Pontificia Universidad Javeriana. Líder del grupo de competencia en CTF Av3ng3rs 1n1t14t1v3 y CEO de la empresa de consultoría Stark Industries SAS.*