Ciberriesgo

DOI: 10.29236/sistemas.n151a5

Aprendizaje de un riesgo sistémico, emergente y disruptivo.

Resumen

En una sociedad digitalmente modificada como la actual, el aumento de la conectividad da lugar a la aparición de un nuevo tipo de riesgos denominados ciberriesgos o riesgos cibernéticos, los cuales surgen de la convergencia tecnológica entre el mundo físico y el lógico, apalancada por la densidad digital que lo rodea, es decir, de las nuevas conexiones e interfases que generan datos sobre la condición particular del objeto. Estos riesgos, en su naturaleza diferentes a los tecnológicos, establecen un nuevo paradigma de gestión, que demanda una vista interdisciplinar y sistémica para comprender los retos de las tensiones a las cuales se ven sometidas las organizaciones en un escenario global. En consecuencia, este artículo plantea algunas reflexiones conceptuales y prácticas que permitan retar y desconectar algunos saberes previos sobre la gestión de riesgos y explorar nuevas apuestas de comprensión y análisis en escenario volátil, incierto, complejo y ambiguo.

Palabras clave

Ciberriesgo, pensamiento sistémico, interdisciplinar, emergente, disruptivo

Jeimy J. Cano M.

Introducción

La evolución acelerada de la tecnología, los cambios e implicaciones geopolíticas actuales y la insistente demanda de las personas por experiencias cada vez más novedosas y personalizadas, establece un escenario inestable para las organizaciones y la sociedad, que exige reconocer la convergencia de diferentes campos de conocimiento, sus distintas posturas disciplinares y la incorporación de tecnologías emergentes, con el fin de encontrar formas inéditas que desconecten y

reten lo conocido, identifiquen relaciones poco visibles y creen nuevos vínculos entre objetos y las ideas para cambiar el *status quo* vigente.

Esta nueva realidad, más allá de superar las diferentes perspectivas de las disciplinas tradicionales, establece retos para los profesionales en todas las áreas, como quiera que su visión del contexto ahora responde a múltiples relaciones entre los objetos, para tratar de encontrar certezas en medio de las volatilidades propias de las condiciones actuales. Lo anterior, revela comportamientos del entorno que se manifiestan como rarezas, inconsistencias y contradicciones (Charan, 2015), las cuales deben ser identificadas y leídas, como insumo para avanzar y proponer alternativas que hagan del "incierto", una oportunidad para crear incentivos y motivaciones, que quiebren el estándar actual y revelen aquello que no era posible ver previamente.

Por lo anterior, el nuevo contexto digital en el que los objetos son cada vez más digitalmente densos (Zamora, 2017), configura una vista sistémica tanto de los negocios como de la sociedad. La conectividad como habilitador de nuevas formas de encuentro, como facilitador de novedosos flujos de información y la conexión entre mundos u objetos antes aislados, funda una mirada enriquecida de la dinámica global actual, que cuestiona la manera mecanicista y determinista de entender el mundo. Este paradigma sistémico, reconoce en la complejidad, entendida como esa capacidad del observador para distinguir características de los objetos del mundo y sus interacciones, una oportunidad para cambiar las estructuras existentes y las relaciones con su entorno, como un vehículo para "ver" y "darse cuenta" que es posible desafiar y cambiar las reglas.

Por consiguiente, al desarrollar nuevas propuestas disruptivas, generalmente basadas en iniciativas digitales, se introducen distinciones que tensionan el estado del arte de la técnica y la práctica en los diferentes negocios, configurando experiencias inéditas que capturan la atención de los clientes, pero al mismo tiempo, desarrollan zonas de incertidumbre, ambigüedad y complejidad, que pueden crear situaciones o eventos en los que se ponen en juego las expectativas y necesidades humanas, y cuyos resultados son aún desconocidos.

En consecuencia, explorar y analizar el ciberriesgo o riesgo cibernético, como esa nueva gama emergente de riesgos en las organizaciones, abre un ámbito de participación activa de los diferentes actores empresariales, no sólo para aceptar, mitigar o transferir la gestión de su tratamiento, sino para configurar una visión pedagógica corporativa que prepare la corporación para entender, aprender y

responder a los retos de la inevitabilidad de la falla y así mismo, anticipe las acciones necesarias y suficientes para dar cuenta de los estados de incertidumbre que implica estar inmersos en un mundo digitalmente modificado.

Luego, desde una lectura sistémica, este artículo plantea la emergencia de un nuevo tipo de riesgo en un contexto digital, como lo es el ciberriesgo, que busca ilustrar cómo las situaciones inciertas y volátiles se convierten en oportunidades y retos para comprender las inestabilidades de las nuevas relaciones generadas por la convergencia tecnológica, y responder a las amenazas emergentes que nacen de los intereses encontrados de los distintos actores participantes de la dinámica social y digital.

Perspectiva sistémica del ciberriesgo: aumento de la densidad digital

Para comprender la nueva realidad del ciberriesgo, es necesario reconocer que tenemos un incremento de la conectividad en los objetos físicos, generando datos sobre la condición del mismo, los cuales son transmitidos a sistemas conocidos en las organizaciones, como también a infraestructuras en la nube, en donde cada vez más se pierde su control.

Este incremento de interfases en los objetos físicos, introduce el concepto de densidad digital (Zamora, 2017), como una propuesta inédita hacia nuevas experiencias de las personas con los objetos de la realidad, de tal manera que es posible una mayor conectividad e información en tiempo real, que puede ser (y será) utilizada para superar las expectativas de los clientes. Esta nueva condición de objetos "inteligentes" revela originales propuestas de valor que las organizaciones están dispuestas a explorar y explotar para crear nuevos activos digitales (Porter & Heppelmann, 2014).

Al incrementarse la conectividad y la caracterización de novedosos objetos o dispositivos inteligentes, se define un nuevo tejido de conexiones en el marco de relaciones conocidas y desconocidas que transforman la manera de hacer las cosas y, que terminan cambiando la realidad de los clientes. En este sentido, si bien se habilitan espacios para lograr experiencias distintas, de igual forma se configuran posibilidades que pueden motivar usos no autorizados, como quiera que es la información personal la que ahora se moviliza en estas nuevas interfases.

En perspectiva sistémica de la construcción social, podemos indicar como anota Luhmann (1998), que el sujeto deja de ser el centro del análisis, para centrarse en los sistemas y sus relaciones con el entorno. Esto es, que una persona efectúa nuevas indicaciones y distinciones (Brown, 1979) de la reali-

dad interconectada para advertir nuevas propiedades emergentes del sistema que analiza y que, en el escenario de la densidad digital, es habilitado por la conectividad y las expectativas de los diferentes participantes de la sociedad.

En lectura de una vista de ecosistema, es posible entender la densidad digital como el habilitador de una red de fenómenos interconectados e interdependientes, donde las actuaciones y actividades de los participantes son relevantes para darle sentido a la dinámica del sistema interrelacionado. En este contexto, se entiende que una mayor conectividad enfatiza los valores y principios de la cooperación, la creatividad, la síntesis, la asociación y la experiencia de vida, con fines superiores para actuar de esta misma forma (Capra, 2003), sin perjuicio de la canalización de estos mismos principios y valores, para concretar acciones abiertamente contrarias a la ética digital de los datos y en favor de intereses particulares, que afecten el interés general sobre el cual evoluciona el ecosistema.

Por consiguiente, la actual omnipresencia de las tecnologías de información y el aumento de la dependencia de la conectividad para el desarrollo de los negocios a nivel internacional, hacen que cualquier evento de inestabilidad, fallo o interrupción genere impactos globales con afectaciones en la estabilidad de las economías, las dinámicas sociales, las tensiones políticas, las innovaciones tecnológicas y hasta impactos de nivel ecológico, cuando artefactos tecnológicos son los responsables del monitoreo de condiciones particulares del ambiente y sus relaciones (WEF, 2019).

Ciberriesgo: una realidad emergente

Al entender el ciberriesgo como una realidad sistémica de las organizaciones, es necesario comprender en perspectiva relacional la forma de pensar y concebir el mundo. La vista mecanicista basada en causa-efecto, en la homogeneidad de los resultados y la predictibilidad de los procesos deja de ser funcional, como quiera que efectos de borde o no documentados, se pueden presentar sin explicación aparente.

El ciberriesgo, como una propiedad emergente de las relaciones digitalmente modificadas de la realidad, establece un reto cognitivo y social, que demanda romper con los paradigmas disciplinares, para encontrar respuestas o mejores preguntas en escenarios cada vez más inestables e inciertos, fruto de una mayor densidad digital en la dinámica de los elementos sociales. En este sentido, el ciberriesgo se configura como una apuesta relacional entretejida en la conectividad de los objetos físicos y las realidades sociales, que cambia la manera como se percibe el mundo y crea escena-

rios inéditos que retan las prácticas de gestión de riesgos actuales.

En consecuencia, el ciberriesgo desarrolla una serie de características que lo configuran como una realidad emergente, la cual demanda una vista interdisciplinar, para tratar de comprender sus movimientos en el contexto organizacional y establecer patrones que puedan ser de interés para los objetivos estratégicos de las empresas. A continuación, se detallan siete (7) características claves que revelan la presencia del ciberriesgo en las corporaciones modernas (Fahrenthold, P. et al, 2010).

- *Alta incertidumbre*: la frecuencia y el potencial de impacto son difíciles de valorar. Es necesario comprender la dinámica del todo y sus relaciones con el entorno para tratar de leer la inestabilidad del sistema y la asimetría de la información disponible.

- *Sin consenso*: tanto analistas como ejecutivos no alcanzan acuerdo sobre la forma de enfrentar o reconocer los inciertos que se presentan en un entorno digitalmente modificado.

- *Relevancia incierta*: existe poca guía o información sobre situaciones planteadas, que pueden sonar futuristas o poco creíbles.

- *Difícil de comunicar*: existe bajo entendimiento y, en tal sentido, no se les presta atención, dando lugar a puntos ciegos en la organización que pasan desapercibidos dentro de la dinámica empresarial.

- *Sin dueño concreto*: comprender el ciberriesgo implica superar la visión disciplinar y salir al encuentro de las diferentes formas de ver la realidad, para comprender sus alcances e impactos. No es el ejercicio de un área, sino la construcción colectiva de diferentes actores.

- *Tiene carácter sistémico*: son riesgos que sólo se manifiestan en relación con otros. Se entiende la densidad digital como el tejido que habilita esta nueva comprensión de la realidad.

- *Tendencias imperceptibles*: se manifiestan en rarezas, inconsistencias y contradicciones en el entorno. Son revelaciones de señales y eventos que para muchos pueden ser imperceptibles y para otros, la identificación de realidades que pueden llegar a ser relevantes para el negocio.

Al ser el ciberriesgo un riesgo emergente es necesario reinventar la práctica de la gestión de riesgos, desde el pensamiento sistémico, de tal forma que no sólo prime la vista de las probabilidades asociadas con los riesgos conocidos, sino que se incorpore la dinámica de las posibilidades, en las que se perciben y entienden los riesgos latentes y emergentes (Cano, 2017). Por

tanto, movilizar los esfuerzos en el tratamiento de los ciberriesgos significa comprender que el entorno es cambiante y demanda superar las cegueras cognitivas (Meyer & Kunreuther, 2017) propias de los saberes previos y las exigencias de certezas de los ejecutivos actuales.

Ciberriesgo: un escenario disruptivo para las empresas

Si entendemos que un escenario disruptivo es aquel proceso a través del cual una empresa pequeña con menos recursos, es capaz de desafiar las empresas ya establecidas, concentrándose con éxito en segmentos olvidados, ganando terreno mediante la entrega de una funcionalidad más adecuada, a menudo a un precio más bajo (Christensen, Raynor & McDonald, 2015), se ingresa en terrenos donde la convergencia tecnológica y la densidad digital, habilitan nuevas posibilidades para crear distinciones inexistentes.

Esto es, que la disrupción surge de la incorporación y desarrollo de nuevas relaciones entre los negocios existentes, la conectividad, el aumento de la densidad digital de los objetos físicos y la mayor dependencia de los terceros de confianza, donde se apalancan las capacidades requeridas para enriquecer la experiencia diferenciadora que esperan los clientes. En este sentido, se advierte una acelerada disrupción digital, en la que las empresas deben transformar rápidamente su modelo operativo y de negocio, además de las experiencias del cliente, con el fin de mantener su posición estratégica vigente y repensar la forma como genera valor dentro y fuera de su segmento de negocio (Kane, Nguyen, Copulsky & Andrus, 2019).

Así las cosas, el ciberriesgo se advierte como una realidad emergente, ahora en un ecosistema digital, en el que los diferentes participantes cooperan entre sí, intercambian conocimientos, desarrollan tecnologías abiertas y adaptables; proponen modelos de negocios novedosos que buscan encontrar patrones diferenciadores para que los clientes puedan explorar los límites de sus expectativas (Jimeno, 2017). En efecto, al aumentar la interacción y flujo de datos, generalmente personales, se crean contextos digitales enriquecidos para los individuos, de manera de dar respuesta a situaciones particulares y alimentar un escenario de vulnerabilidades emergentes, cuya naturaleza y efectos pueden ser desconocidos, y requieren un gobierno y gestión diferentes.

En una realidad como la actual, digital y tecnológicamente modificada es necesario desarrollar un nuevo paradigma de confianza, para que tanto las empresas como las personas establezcan relaciones de confiabilidad, sobre la base de la vulnerabilidad por defecto. Es decir que, a pesar de los esfuerzos y acciones adelantadas para evitar un evento no deseado, se tendrán

acuerdos concretos de acción y respuesta, cuando se materialice la inevitabilidad de la falla (Cano, 2017b).

Bajo esta perspectiva, las organizaciones deberán estar preparadas para enfrentar la materialización de un ciberriesgo, de escalas locales o de proporciones internacionales, como lo puede ser un ciberataque coordinado y desplegado desde diferentes lugares, con capacidad de infección viral sobre diferentes tipos de dispositivos de escritorio o móviles y secuestro de la información allí contenida (Daffron, Ruffle, Andrew, Copic, Quantrill, Smith & Leverett, 2019). De esta forma, la gestión de incidentes deberá ser la capacidad más relevante que deberán desarrollar las empresas frente al reto de la materialización de un riesgo cibernético.

Retos de la gestión del riesgo cibernético

Un reciente estudio de Deloitte (2018) revela algunos aspectos claves de la gestión del riesgo cibernético, los cuales advierten la necesidad de una visión holística por parte de las organizaciones, inversiones requeridas para configurar visiones prospectivas de las amenazas y contratación de talento especializado para reinventarse frente a la volatilidad del entorno. A continuación, se detallan algunas reflexiones alrededor de tres (3) de los elementos que mayor puntuación tuvieron en el estudio en mención.

El primer elemento, no hace referencia a aspectos técnicos o tácticos de la organización, sino a consideraciones estratégicas como "estar adelante en los cambios de las necesidades del negocio", parafraseado como "**anticipar escenarios emergentes para la organización**". Este primer punto, establece una declaración clave para las empresas y sus ejecutivos; no se trata de repetir aquello que se conoce o generalmente se lleva para presentar en la junta, sino crear un espacio para retar aquello que se hace a la fecha y tratar de imaginar cómo se puede afectar el modelo de generación de valor de la empresa.

Lo anterior, significa revisar y comprender el riesgo cibernético como una malla de implicaciones técnicas, sociales, económicas y políticas que ubica a la empresa en un ecosistema tecnológico dinámico, espacio en el que se reconocen actores relevantes de su entorno, incluidos sus aliados y competidores estratégicos, para identificar las interacciones de interés, y así crear zonas de ventajas competitivas (OECD, 2015), las cuales deben protegerla de las amenazas digitales naturales, que contemplan actores conocidos y desconocidos, los cuales hacen parte del nuevo paisaje digital.

El segundo aspecto clave identificado en el estudio se refiere a "hacer frente a las amenazas de actores sofisticados", que pudiésemos

configurar como "**enfrentar las amenazas de actores desconocidos**".

Cuando se entiende que en la actualidad una organización se encuentra ubicada en un espacio en el que existe una confrontación de intereses por activos digitales estratégicos, se quiebra el marco general de prácticas asociadas con los riesgos informáticos, dedicado a proteger y asegurar, para inaugurar la incorporación de las capacidades críticas como defender y anticipar.

Mientras en los estándares tradicionales de seguridad se busca alcanzar certezas sobre el incierto que puede producir un ataque, en el escenario del riesgo cibernético, no solamente hay que considerar lo anterior, sino reconocer el territorio de acción de los adversarios, sus recursos, sus posibilidades, capacidades e impactos con el fin de modelar acciones en diferentes aspectos: técnico, políticos, económicos y sociales, de tal forma, que enfrentar las amenazas digitales actuales, no responde a un ejercicio de los "técnicos", sino a una visión estratégica del negocio, que da cuenta de comportamientos y movimientos coordinados para demorar, interrumpir, contener o anticipar los efectos de una ciberoperación deliberada para afectar los intereses claves de la compañía (Donaldson, Siegel, Williams & Aslam, 2015).

Un tercer elemento es "incorporar talento especializado en ciberseguridad", frase que se puede adaptar como "**incorporar analistas de ciberriesgos especializados**". Los nuevos profesionales especializados en riesgos cibernéticos, no sólo deben demostrar competencia técnica básica en los aspectos de seguridad de la información, sino exponer capacidades analíticas de inteligencia, análisis y correlación de eventos, reflexiones y formación geopolítica e infopolítica, cooperación interorganizacional y gubernamental, reconocimiento de patrones de amenazas emergentes y suficiencia en el diseño, análisis y simulación de escenarios.

Este profesional, ya no tiene una visión disciplinar de un dominio de conocimiento específico, sino la construcción de saberes interdisciplinares, que configuran marcos de trabajo agregados, que revisan una realidad inestable e incierta, para dar respuesta a las propuesta de los atacantes, que no vacilan en proponer retos complejos a las organizaciones, los cuales van desde el secuestro de datos, pasando por las noticias y videos falsos, las agresiones a las marcas, las afectaciones a la infraestructura tecnológica, hasta la creación de amenazas digitales desconocidas basadas en la inteligencia artificial.

De modo que, adelantar la gestión del riesgo cibernético, no será viable si no se entiende desde la perspectiva sistémica de las relaciones entre los objetos. Esto es, entender el entorno

como un todo que evoluciona y se transforma conforme sus diferentes actores toman posiciones respecto a temas específicos, las cuales, terminan afectando la dinámica de una sociedad digital y tecnológicamente modificada que demanda mayores y mejores experiencias en sus productos y servicios (Saran, 2017).

Reflexiones finales

Al tener en la base de su fundamentación una visión mecanicista y los saberes de la seguridad de la información, el riesgo cibernético ha heredado una gestión de riesgos, por lo general, desconocidos. En este sentido, cuando se incorpora una vista sistémica extendida de la organización para comprender cómo los efectos de la materialización de los ciberataques pueden comprometer la promesa de valor de la empresa, se cruzan los límites de los estándares tradiciones de gestión de riesgos, para darle paso a una revisión amplia de las amenazas que pueden ser conocidas, latentes y emergentes (Cano, 2017).

Por tanto, en un entorno de "disrupción digital", entendida ésta como "un efecto que cambia las expectativas fundamentales y comportamientos en una cultura, mercado, industria o proceso causada por, o expresada a través de, capacidades digitales, canales o activos" (Yockelson & Smith, 2018), es necesario mantener una monitorización del ambiente, identificando aquellas anomalías, rarezas y contradicciones, que adviertan patrones no conocidos, los cuales marcan las nuevas capacidades y habilidades de los adversarios (Charan, 2015), con el fin de anticipar sus movimientos y crear acciones de defensa tanto activas como pasivas, que permitan, no evitar ser atacados exitosamente, sino prevenir, demorar, distraer o interrumpir sus acciones bajo condiciones inciertas.

De esta forma, las organizaciones siguiendo las reflexiones de Schoemaker & Day (2017) deberán desarrollar una **mentalidad de experimentación permanente** para anticipar los efectos adversos de los atacantes, contar con **equipos de trabajo con personal calificado** en el riesgo cibernético, que al experimentar y simular, puedan codificar, compartir y aplicar los nuevos conocimientos y patrones identificados, y finalmente, **mirar más allá de sus fronteras organizaciones y de mercado** buscando puntos de vista distintos, que reten sus saberes previos, no sólo para aprender/desaprender, sino para obtener una ventaja estratégica competitiva en un mundo turbulento que a menudo paraliza a los demás.

Finalmente, vale la pena recordar que los ciberriesgos definen una forma distinta de entender la dinámica de las organizaciones y que sus impactos, frente a hechos materializados, pueden tener conse-

cuencias globales, muchas de ellas no conocidas. En consecuencia, es necesario tener presente que los riesgos cibernéticos:

- No son retos aislados, son un resultado de la lectura sistémica de sus componentes (personas, procesos, tecnología y regulaciones).
- Son desafíos complejos en los que no tenemos la variedad requerida para poderlos comprender y atender.
- Son desafíos que generan tensiones socioeconómicas globales y asimetrías de información.
- Son emergentes, fruto de las relaciones entre los diferentes elementos y actores de los nuevos ecosistemas digitales, los cuales generalmente son puntos ciegos para la gestión tradicional de riesgos.
- Son interdisciplinares y demanda el desarrollo de lenguajes alternativos entre las disciplinas actuales, para darle forma y sentido a los efectos e impactos de su posible materialización.

Referencias

Brown, S. (1979). *Laws of Form*. New York, USA: E.P. Dutton

Cano, J. (2017). La ventana de AREM. Una estrategia para anticipar los riesgos y amenazas en ciberseguridad empresarial. *ISACA Journal*. vol. 5. Recuperado de: https://www.isaca.org/Journal/archives/2017/Volume-5/Pages/the-arem-window-spanish.aspx

Cano, J. (2017b). Riesgo y seguridad. Un continuo de confianza imperfecta. En Dams, A., Pagola, H., Sánchez, L. y Ramio, J. (eds) (2017) *Actas IX Congreso Iberoamericano de Seguridad de la Información*. Universidad de Buenos Aires - Universidad Politécnica de Madrid. 34-39

Capra, F. (2003). *Las conexiones ocultas: implicaciones sociales, medioambientales, económicas y biológicas de una nueva visión del mundo*. Barcelona, España: Anagrama.

Charan, R. (2015). *The attacker's advantage. Turning uncertainty into breakthrough opportunities*. New York, USA: Perseus Books Groups.

Christensen, C., Raynor, M. & McDonald, R. (2015) What is disruptive innovation? *Harvard Business Review*. December. 44-53

Daffron, J., Ruffle, S., Andrew, C., Copic, J., Quantrill, K., Smith. A. & Leverett, E. (2019). Bashe Attack: Global Infection by Contagious Malware. Cambridge Centre for Risk Studies. *Research Report*. Recuperado de: https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/bashe-attack

Deloitte (2018). Global Risk Management Survey, 11 edition. *Deloitte Insights*. Recuperado de: https://www2.deloitte.com/content/dam/insights/us/articles/4222_Global-risk-management-survey/DI_global-risk-management-survey.pdf

Donaldson, S., Siegel, S., Williams, C. & Aslam, A. (2015). *Enterprise cybersecurity. How to build a successful cyber-defense program against advanced threats*. New York, USA: Apress.

Fahrenthold, P. et al (2010). Emerging risk and Enterprise risk management. *RIMS Executive Report*. Recuperado de: https://www.rims.org/resources/ERM/Documents/EmergingRisk_ERMweb.pdf

Jimeno, J. (2017). *La responsabilidad civil en el ámbito de los ciberriesgos*. Madrid, España: Fundación MAPFRE.

Kane, G., Nguyen, A., Copulsky, J. & Andrus, G. (2019). *The technology falacy. How people are the real key to digital transformation*. Cambridge, MA. USA: MIT Press.

Luhmann, N. (1998). *Complejidad y modernidad. De la unidad a la diferencia*. Madrid, España: Trotta.

Meyer, R. & Kunreuther, H. (2017). *The ostrich paradox. Why we underprepare for disasters*. Philadelphia, PA. USA: Wharton Digital Press.

OECD (2015). Digital Security Risk Management for Economic and Social Prosperity: *OECD Recommendation and Companion Document*, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en

Porter, M. & Heppelmann, J. (2014). How Smart, connected products are transforming competition. *Harvard Business Review*. Noviembre.

Saran, S. (2017). Time to face up to cyber threats. *Observer research foundation*. Recuperado de: https://www.orfonline.org/research/time-to-face-up-to-cyber-threats/

Schoemaker, P. & Day, G. (2018). Strategic actions in the face of uncertainty. *Revista Brasileira de Marketing – ReMark*. Special Issue. 17(5). 700-712

WEF (2019). The Global Risks Report 2019. 14th Edition. *Insight Report*. World Economic Forum. Recuperado de: https://www.weforum.org/reports/the-global-risks-report-2019

Yockelson, D. & Smith, D. (2018). Willful Disruption — Scaling, Operating and Changing the Digital Game: A Gartner Trend Insight Report. *Gartner Research*.

Zamora, J. (2017). ¿Es posible programar modelos de negocio? *IESE Insight*. II Trimestre de 2017.

Jeimy J. Cano M., Ph.D, CFE, CICA. *Ingeniero y Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes. Especialista en Derecho Disciplinario por la Universidad Externado de Colombia. Ph.D en Business Administration por Newport University, CA. USA. y Ph.D en Educación por la Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista Sistemas de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*