Retos de seguridad/ciberseguridad en el 2030

DOI: 10.29236/sistemas.n154a7

Reflexión sobre un ejercicio prospectivo incompleto.

Resumen

Establecer una mirada prospectiva sobre la seguridad/ciberseguridad es un ejercicio retador e incierto en el contexto de una sociedad líquida, basada en volatilidades y cambios permanentes, de ahí que sea una apuesta incompleta e inestable. Por tanto, más que un pronóstico, este artículo plantea una reflexión conceptual con el fin de integrar las tendencias globales identificadas, los cambios de paradigmas de pensamiento y los desafíos que deben asumir los profesionales de seguridad/ciberseguridad frente a un adversario que se nutre y evoluciona con la incertidumbre del entorno.

Palabras clave

Ciberseguridad, pronósticos, prospectiva, seguridad, tendencias.

Introducción

Cumplida una década de cambios y transformaciones surgen dos ejercicios en todos los espacios que conforman la sociedad: uno de carácter retrospectivo y otro prospectivo, los dos en procura de explorar los retos y las oportunidades hacia el futuro.

En tal escenario, queda en medio el "presente", lugar común desde donde se establece una tribuna privilegiada para lanzarse a colonizar nuevos territorios y descubrir aquellas tendencias que cambiarán la manera de hacer las cosas en la actualidad. Para lograrlo, es necesario transformar la forma de pensar, los paradigmas aceptados hasta hoy, además de realizar una mirada diferente para romper la inercia que genera lo que sabemos, conocemos y manejamos.

En consecuencia, tratar de pronosticar los movimientos y transformaciones en diez años, es un ejercicio que busca tomar una foto en movimiento, en la que el cambio de velocidad, del tiempo y del lugar, serán la constante y la probabilidad de error estará por demás asegurada. Aun así, aparecen diferentes apuestas conceptuales, analíticas, cognitivas y prácticas para buscar los mejores antecedentes (si es que existen) y tratar de reconocer y explorar lo que podría llamarse las "memorias del futuro" (De Geus, 2011).

En tal sentido, realizar un ejercicio prospectivo sobre la seguridad/ciberseguridad para el 2030, exige no solo encontrar algunos referentes y signos visibles (o invisibles) en el entorno, sino cambiar el marco de trabajo vigente basado en la imagen mecánica del mundo, para tratar de desconectar las "verdades" parciales e integrarlas con las novedades, tendencias, rarezas y contradicciones disponibles (Charan, 2015), para abrir nuevas ventanas de aprendizaje.

En consecuencia, este documento plantea una revisión conceptual flexible, que no busca dar recetas o apreciaciones definitivas sobre las dinámicas de los temas de seguridad, control y protección de datos, sino plantear un mapa incompleto e inexacto del territorio, para ofrecer a los lectores algunas pistas de lo que puede ocurrir en la siguiente década, de manera que cada uno pueda construir una cartografía individual para navegar en medio de los cambios e inestabilidades propias de la realidad líquida (Bauman, 2017) actual y futura.

Tendencias en el mundo para el 2030

Durante la última década se han producido diferentes documentos

de prospectiva (que algunos señalan como predictivos) con el fin de observar un camino de transformación de la humanidad en 10, 20 o 30 años. Si visualizar o explorar lo que puede pasar en 10 años es un reto de marca mayor, qué decir de quienes plantean cómo será el mundo en el 2070.

El reporte global de riesgos publicado recientemente por el Foro Económico Mundial, muestra desafiantes realidades para la humanidad, además de revelar los 'secretos a voces' sobre las acciones y posturas de los seres humanos con consecuencias adversas en todos los ámbitos de carácter político, económico, social, tecnológico, legal y ecológico.

Los ciberataques y el cambio climático, unido a la inestabilidad geopolítica global que afecta el comercio y las economías globales, ponen el punto de referencia desde donde se plantean las diferentes reflexiones para los líderes mundiales y los retos que se deben asumir como comunidad global (WEF, 2020).

Considerando este panorama y revisando recientes documentos sobre cómo podría ser el mundo en diez años (Ricart & Berrone, 2020; Lesser, Reeves, Whitaker & Hutchinson, 2018; Ray, 2018), se presentan a continuación algunas apuestas de escenarios que como sociedad demandarán otras prácticas y acciones para evolucionar a un nuevo nivel de conocimiento, en el que nada estará aislado, sino interconectado e interdependiente lo uno de lo otro.

El reto será escribir la historia desde un paradigma distinto, evitando caer en la trampa de la escasez y la diferencia, para ir más allá de lo avanzado, no con la promesa de éxito, sino con la apertura y humildad para aprender.

La tendencias emergentes al 2030 son:

- **Ecosistemas digitales**: se desdibujan las fronteras entre competidores y colaboradores.
- **Tensiones geopolíticas**: mayores efectos adversos de los conflictos comerciales y la desinformación.
- **Naturaleza del trabajo**: la tecnología repiensa la relación entre empresa, individuo y cliente.
- **Dinero digital**: aumenta la tensión social y comercial por el uso de criptoactivos.
- **Convergencia tecnológica**: basada en inteligencia artificial, computación en la nube y analítica de datos.
- **Ciberconflictos, cibercrimen y ciberataques**: crearán mayor desestabilización e impacto en una sociedad digital.
- **Descarbonización de la economía**: se acelera el uso de energías alternativas y menos dependencia de los hidrocarburos.
- **Inteligencia colectiva**: mayor colaboración e innovación em-

presarial para el desarrollo de capacidades conjuntas.
- **Educación 4.0**: reivindicación del error como fundamento del aprendizaje y la innovación.
- **Riesgos líquidos**: tensiones cambiantes y emergentes que retan los estándares y las buenas prácticas.
- **Liderazgo resiliente**: actuar, de saprender, priorizar y despertar. El reto no es competir, sino conectar, compartir, construir y colaborar.

Estas tendencias planteadas demandan una manera distinta de entender el mundo. Superar la pedagogía del éxito, en la que el error o la diferencia pueden ser sancionadas, para abrirle paso a nuevas ventanas de aprendizaje, en procura de puntos de conexión para identificar patrones que faciliten una visión distinta (De la Torre, 2004). Esto es, en palabras de Mlodinow (2019) desarrollar ideas que representen una forma original y fructífera de entender o de abordar un problema, en la que es posible reconocer al otro como verdadero otro.

Tecnologías emergentes al 2030

Tratar de darle forma a varias de las tendencias enumeradas previamente implica reconocer en la tecnología avances fundamentales que cambian la manera de hacer las cosas, que quiebran el *status quo* vigente y obligan a todos los participantes de la sociedad a reconocer un nuevo tipo de derechos humanos en el contexto digital, en el que la información fluye y las innovaciones plantean retos que van más allá de las reflexiones hasta ahora planteadas (Jones, 2019).

Lo anterior supone comprender que para el 2030 habrá una saturación digital que llevará a entender a los clientes y sus retos con mayor granularidad. Cada interacción de los individuos proporcionará una lectura y huella digital con la capacidad de crear un potencial de convergencia en el que participan clientes, empleados, socios de negocio y terceros de confianza. La realidad conectada y aumentada estará en el marco de la interacción digital, lo cual advierte sobre los retos de privacidad, seguridad y respeto de los derechos individuales en un escenario antes desconocido (Accenture, 2019).

Considerando las reflexiones de un reciente estudio realizado por Accenture (2019), las propuestas tecnológicas más relevantes para los próximos 10 años tendrán varias características claves que se deben tener en cuenta:

- Estarán basadas en computación en la nube, inteligencia artificial y analítica de datos.
- Tendrán un componente aumentado para enriquecer la experiencia y expectativas del cliente.
- Representarán sus activos reales en libros mayores distribuidos (“tokenización”) como estra-

tegia para conceptualizar su valor y registro en el tiempo.
- Articularán y desarrollarán capacidades basadas en terceros de confianza para crear múltiples ecosistemas conectados.
- Demandarán mayor capacidad de procesamiento en menor tiempo, para responder a los retos del mercado.
- Buscarán apoyarse en las nuevas fronteras que revela la computación cuántica.

En estas condiciones, los referentes actuales del desarrollo de soluciones para las empresas y naciones basadas en la computación en la nube, la analítica de datos, la computación móvil y las redes sociales, se convertirán en los *commodities* básicos para manejar y articular el nuevo escenario de transformación y cambio que trae la nueva década.

La tecnología de libro mayor distribuido (representada en la cadena de bloques o *blockchain*), la inteligencia artificial, la realidad virtual (aumentada y asistida) y la computación cuántica, llevarán a la humanidad a una nueva frontera de conocimiento y expansión que habilitará un proceso de transición y cambio más acelerado que el actual. Este salto permitirá pasar de las experiencias digitales, a las propuestas cognitivas y las manifestaciones cuánticas.

Si lo anterior es correcto, los fundamentos de lo que conocemos sobre ciencias de la computación deberán ser replanteados, para lo cual será necesario habilitar la convergencia de saberes disciplinares tradicionales y una mayor apertura por parte de los diferentes participantes de la dinámica social, en procura de construir soluciones conjuntas para entender la complejidad creciente planteada por este nuevo ecosistema cuántico e inteligente, en el que no es suficiente tener un punto de vista y todos los retos no tienen respuestas definitivas.

En consecuencia, es necesario balancear las oportunidades que este escenario futuro plantea, con sus desafíos y tensiones sobre los derechos humanos en el contexto digital (el dato como la representación de un individuo), habida cuenta de no ser proclives al síndrome de la modernidad que empieza a desdibujar los avances de la ciencia y la tecnología como logros compartidos al servicio de la humanidad, y se cambian por impulsos e inclinaciones que erosionan los valores inherentes a la vida y la construcción de relaciones sociales sanas y presentes (Korff, 2014).

Nuevos paradigmas y referentes para pensar en el 2030

Con la revisión de las tendencias y las tecnologías para los próximos diez años queda claro que lo aprendido para llegar al año 2020, no será suficiente para alcanzar los retos y transformaciones previstas para

ese año. En este sentido, todos aquellos que piensan desde sus propias islas, procurando dar respuestas desde su archipiélago de certezas, tendrán que buscar interconectarse con otros en el mar de incertidumbres, para descubrir y analizar las propuestas emergentes que estarán sobre la mesa en los próximos años.

En este contexto, se hace necesario pasar de los saberes disciplinares tradicionales y mecanicistas, basados en respuestas conocidas, problemas resueltos y fundamentos conceptuales referenciados y probados, a un escenario de construcción interdisciplinar, basado en el pensamiento complejo, crítico y sistémico, que busque nuevas respuestas a problemas no resueltos, para de esta manera fundar nuevas bases conceptuales enriquecidas, donde el error es parte del proceso de aprendizaje, la experimentación y simulación es la norma base para descubrir y explorar las posibilidades que se presentan en las nuevas dinámicas de una sociedad digital y tecnológicamente modificada (Luengo, 2018).

El conocimiento generado desde la perspectiva interdisciplinar busca compartir argumentos, procedimientos e interpretaciones para darle sentido al reto novedoso planteado por la realidad frente a los cambios y disrupciones que la tecnología ofrece en el contexto actual y futuro. En este sentido, es importante actualizar los métodos de trabajo que se nutren desde las diferentes aproximaciones de las disciplinas, para fundar nuevas opciones sobre el objeto de estudio y así plantear propuestas inéditas (o inusuales) que lleven a resultados imprevistos y enriquecidos (Nicolescu, 2014).

Desarrollar este tipo de conocimiento demanda una serie de características en los profesionales, que implica salir de su zona cómoda, en la que la seguridad de sus conceptos y aprendizajes los protegen del incierto provocado por la posibilidad del error. Por tanto, los nuevos universitarios y profesores que deseen abordar la experiencia evolutiva de la construcción de un saber interdisciplinar deberán tener motivaciones y habilidades distintas encaminadas a abandonar sus propias certezas, para abrirse a la aventura de deconstruir el mundo desde nuevas miradas.

Siguiendo los resultados de los estudios realizados por Guimarães, Pohl, Bina y Varanda (2019) las siguientes son las motivaciones, actitudes y habilidades de los individuos que caminan por los senderos de las reflexiones inter y transdisciplinares.

Si bien esta investigación se circunscribe a un conjunto de investigadores que han venido trabajando desde esta perspectiva, sus conclusiones son relevantes y orientadoras para motivar una ruta en esta nueva postura epistemológica.

Motivaciones:

- *Ética*: la ética individual, el deseo de mejorar la sociedad y contribuir al avance del bien común.
- *Recompensa*: motivación extrínseca para las recompensas o anticipación de beneficios.
- *Problemas del mundo real*: compromiso con la comprensión de la dinámica del reto que se plantea que no surge necesariamente del discurso académico exclusivamente.
- *Realización*: basada en la experiencia y la posibilidad de hacer una diferencia en la vida del investigador y en la de los demás.

Actitudes y habilidades:

- *Apertura*: reconocimiento de la existencia de diferentes niveles de realidad regida por diferentes tipos de lógica.
- *Tolerancia*: capacidad de construir redes dentro de un contexto "desconocido".
- *Reflexividad*: rigor en la discusión. Capacidad de autorreflexión disciplinada.
- *Modestia*: capacidad de admitir que es imposible resolver o entender completamente un problema.
- *Creatividad*: eliminar las restricciones autoimpuestas y experimentar los efectos de haber prescindido de ellas.
- *Curiosidad*: indagación e inquietud permanente.
- *Facilitador*: compromiso, conexión, buena comunicación y habilidades de escucha, flexibilidad, adaptabilidad, capacidad para construir puentes.
- *Integrador*: capacidad de localizar y trabajar con información pertinente, comparar y contrastar diferentes métodos y enfoques, aclarar cómo las diferencias y las similitudes se relacionan con una tarea designada, y generan una síntesis, marco integrador, o más holístico de comprensión para un tema, pregunta o problema.

Retos y desafíos de la seguridad/ciberseguridad en el 2030

Luego de hacer un recorrido por una visión de lo que podría ser el mundo en el 2030, los temas de seguridad y control encuentran un lugar preferente en la agenda no sólo de las empresas, sino en el ejercicio de la gobernabilidad y defensa de las naciones en el contexto digital.

Teniendo en cuenta que la ciberseguridad es una disciplina interdisciplinar naciente, requiere una contextualización y empuje, para salir de la zona disciplinar en la que en muchas ocasiones se encuentra atrapada, para buscar nuevos lugares comunes construidos desde diferentes perspectivas y saberes vinculados con disciplinas antes ignoradas como las ciencias políticas, la economía, el derecho, las ciencias biológicas y médicas, la visión actuarial y de los seguros, entre otras, de tal forma que se pueda

caracterizar como un bien común, con visión transversal e implicaciones globales (Ramírez, 2017).

Si en seguridad de la información el reto es asegurar la triada basada en confidencialidad, integridad y disponibilidad, temática que es la base de cualquier ejercicio de ciberseguridad, en el contexto ciber, en el que se habilita una convergencia de tecnologías, saberes y realidades de la sociedad, es necesario ir más allá para comprender la dinámica de los ciberriesgos, como esa tensión "relacional entretejida en la conectividad de los objetos físicos y las realidades sociales, que cambia la manera como se percibe el mundo y crea escenarios inéditos que retan las prácticas de gestión de riesgos actuales" (Cano, 2019, p.66-67).

Lo anterior demanda el desarrollo de una postura interdisciplinar, que inicialmente reconozca los límites propios de las disciplinas, experiencias y saberes previos, para abordar una realidad emergente e inestable, y así, explorar los márgenes de las nuevas interdependencias que plantea el nuevo escenario digital, construyendo propuestas conjuntas y enriquecidas que respondan a la complejidad inherente de los riesgos escondidos en el tejido digital habilitado por las disrupciones tecnológicas y las tendencias expuestas previamente.

El profesional o investigador en ciberseguridad se enfrentará a la lectura de los "riesgos líquidos", aquellos que se "van entre los dedos", cuyo cambio, volatilidad y fluidez no permiten entenderlos con facilidad y que le exigen propuestas y reflexiones que vayan más allá de los marcos conocidos o probados (Ray, 2018). Deberá encontrar en el atacante su inspiración, pero no su imitación, con el fin de deconstruir la forma como ve el mundo y conectarse desde su propio territorio para identificar algunos archipiélagos de certezas (Cano, 2019 b).

El especialista en ciberseguridad no sólo deberá priorizar los ciberriesgos basados en los impactos en las actividades más críticas del negocio o nación, seleccionar los controles que mitiguen de la manera más eficiente los ciberriesgos identificados, validar la efectividad de los controles y desarrollar planes de remediación conectada con las actividades claves del negocio (Parenty & Domet, 2020), sino plantear zonas de experimentación y simulación orientadas a defender y anticipar las estrategias de sus adversarios. Mientras mayor sea la capacidad de exploración y pruebas, mayores espacios de acción y resiliencia se podrán desarrollar.

En este mismo sentido, la tecnología de seguridad y control deberá evolucionar, para conectar las necesidades y experiencias extendidas requeridas para construir la seguridad digital imperfecta (Cano, 2019c) que serán demandadas en

las organizaciones y naciones. En esta línea, las apuestas de los proveedores deberán motivar y promover soluciones ajustadas en tiempo real, que construyan y proyecten propuestas basadas en patrones y aprendizajes, para comprender la necesidad de actuar sobre la misma base que usa el adversario con su víctima: la incertidumbre, lo que hoy se denomina tecnologías de engaño (en inglés *deception technologies*) (Sadowski & Kaur, 2019).

De esta manera, es posible equilibrar un poco el tablero de juego, en el que las estrategias tanto de un lado como del otro encuentren un lugar común para ser ejecutadas, y dependerá de las habilidades y capacidades de cada una de las partes, de su tolerancia al error, de su apertura, de su creatividad e integración, obtener victorias parciales para el analista, las cuales se transforman inmediatamente en nuevos retos para el agresor, o tener triunfos de los atacantes, que terminan en las lecciones aprendidas de los analistas.

Reflexiones finales

Mientras la seguridad/ciberseguridad continúe atada a sus conceptos, ideas y marcos tradicionales de control, poco margen de avance y efectividad podrá tener en un mundo con aumento creciente de la densidad digital. Cada vez que un objeto físico se nutre de conectividad, se habilita con flujo de datos y se potencia con las capacidades de un tercero de confianza, es evidente una nueva realidad de seguridad y control que responde a los retos de los ciberriesgos (Sieber & Zamora, 2018).
En este sentido, las tendencias del mundo presentadas a 2030 ilustran cómo la conectividad habilitará posibilidades y presentará nuevas amenazas que están más allá de los límites naturales y tradicionales de los estándares y buenas prácticas de seguridad y control. En consecuencia, la formación de los especialistas en ciberseguridad/seguridad deberá responder a una postura interdisciplinar, comoquiera que es posible desde esta perspectiva, construir una nueva narrativa de ciberriesgos en la que se integre, no solamente la actividad del negocio o nación, los sistemas de soporte, los ciberataques y sus consecuencias y el adversario (Parenty & Domet, 2020), sino la realidad colindante y emergente que está en la visión sistémica lograda cuando se conectan y desconectan los referentes políticos, económicos, sociales, tecnológicos, legales y ecológicos.

Por tanto, el pronóstico de la seguridad/ciberseguridad al 2030 seguirá siendo reservado y lleno de sorpresas que todavía no podemos distinguir, para lo cual será necesario cambiar la conversación actual en torno a las prácticas de seguridad y control, motivar una colaboración y consenso desde las diferentes perspectivas y lugares de

las empresas y naciones, así como generar un nuevo lenguaje que conecte la realidad de los datos y la información de las personas y empresas, desde una mirada de múltiples partes interesadas, cuidando ahora no sólo la información, sino los derechos digitales y las experiencias que como sociedad se van a demandar y consolidar.

Pensar la seguridad de la información y la ciberseguridad en el 2030 es un ejercicio de Yin y Yang (Vincent & Hitch, 2019). *Yin* asociado con los aspectos internos de la organización o nación, ese delicado tejido humano basado en la textura de los comportamientos de los individuos que configura la cultura organizacional de seguridad de la información. Esa conexión clara y fluida que declara la información como activo relevante y se confirma con el liderazgo visible de los ejecutivos. Y por otro lado, el *yang*, como la comprensión de las relaciones y los tejidos interconectados de la empresa o nación con su entorno, que define la manera como la organización se mueve y se prepara para asumir y continuar a pesar de la inevitabilidad de la falla y el marco de incertidumbre propuesto por sus adversarios.

La visión de la seguridad/ciberseguridad para los próximos diez años no podrá ser ajena al pensamiento flexible, a la explotación deliberada del incierto y la desinformación, a la moderna cultura líquida de discontinuidad, olvido y desvinculación, a las tensiones geopolíticas de las naciones, al ego y la vergüenza de los éxitos de los adversarios, al derecho a la desconexión digital, a la autodeterminación informática, al uso generalizado de los dispositivos inteligentes, al uso indiscriminado e ilegal de los libros contables distribuidos, a los usos no autorizados de herramientas de inteligencia y monitorización, en general a las posibilidades de crear momentos de verdad, que algunas veces serán gratificantes y en otras ocasiones, oportunidades y retos para deconstruir y desaprender sobre la inevitabilidad de la falla.

Referencias

Accenture (2019). The Post-Digital Era is Upon Us. Are you ready for what's next? Accenture Technology Vision 2019. *Research Report*. Recuperado de: https://www.accenture.com/_acnmedia/PDF-94/Accenture-TechVision-2019-Tech-Trends-Report.pdf

Bauman, Z. (2017). *Vida líquida*. Bogotá, Colombia: Editorial Planeta

Cano, J. (2019). Ciberriesgo. Aprendizaje de un riesgo sistémico, emergente y disruptivo. *Revista SISTEMAS*. Asociación Colombiana de Ingenieros de Sistemas. 63-73. Doi: 10.29236/sistemas.n151a5

Cano, J. (2019b). Analyst and Adversary. Deconstructing the “Imaginary” of Security and Cybersecurity Professionals. *ISACA Journal*. 4. 48-53

Cano, J. (2019c). Confianza digital imperfecta: Un reto de simetría, reciprocidad y sinceridad. *Linkedin*. Recuperado de:

https://www.linkedin.com/pulse/confianza-digital-imperfecta-un-reto-de-simetría-y-cano-ph-d-cfe/

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

De Geus, A. (2011). *La empresa viviente. Hábitos para sobrevivir en un ambiente de negocios turbulento*. Buenos Aires, Argentina: Gránica.

De la Torre, S. (2004). *Aprender de los errores. El tratamiento didáctico de los errores como estrategia de innovación*. Buenos Aires, Argentina: Editorial Magisterio del Río de la Plata.

Guimarães, M. H., Pohl, C., Bina, O. & Varanda, M. (2019). Who is doing inter- and transdisciplinary research, and why? An empirical study of motivations, attitudes, skills, and behaviours. *Futures*. 112. 1-15. Doi: 10.1016/j.futures.2019.102441

Jones, K. (2019). Online Disinformation and Political Discourse. Applying a Human Rights Framework. *Research Paper*. Chatham House. London, UK. Recuperado de: https://www.chathamhouse.org/publication/online-disinformation-and-political-discourse-applying-human-rights-framework

Korff, D. (2014). The rule of law on the Internet and in the wider digital world. Council of Europe. Commissioner For Human Rights. *Issue Paper*. Recuperado de: https://book.coe.int/en/commissioner-for-human-rights/7321-pdf-the-rule-of-law-on-the-internet-and-in-the-wider-digital-world.html

Lesser, R., Reeves, M., Whitaker, K. & Hutchinson, R. (2018). A Leadership Agenda for the Next Decade. *BCG Report*. Recuperado de: https://www.bcg.com/publications/2018/winning-the-20s-leadership-agenda-for-next-decade.aspx

Luengo, E. (2018). *Las vertientes de la complejidad. Pensamiento sistémico, ciencias de la complejidad, pensamiento complejo, paradigma ecológico y enfoques holistas*. Guadalajara, México: ITESO. Recuperado de: https://rei.iteso.mx/handle/11117/5421

Mlodinow, L. (2019). *Elástico. El poder del pensamiento flexible*. Bogotá, Colombia: Editorial Planeta.

Nicolescu, B. (2014). Methodology of transdisciplinarity. *World Futures*. 70: 186–199. Doi: 10.1080/02604027.2014.934631

Parenty, T. & Domet, J. (2020). *A leader's guide to cybersecurity. Why boards need to lead and how to do it*. Boston, MA. USA: Harvard Business Review Press.

Ramírez, R. (2017). *Making cyber security interdisciplinary : recommendations for a novel curriculum and terminology harmonization*. (Tesis de Maestría) Massachusetts Institute of Technology, School of Engineering, Institute for Data, Systems, and Society, Technology and Policy Program. Recuperado de: https://dspace.mit.edu/handle/1721.1/111232

Ray, A. (2018). Riesgos líquidos y los nuevos retos de la seguridad. Recuperado de: https://www.linkedin.com/pulse/riesgos-líquidos-y-los-nuevos-retos-de-la-seguridad-alberto-ray/

Ricart, J. & Berrone, P. (2020). Cuenta para atrás 2030. *IESE Insights*. Recuperado de: https://insightreports.iese.edu/ods/

Sadowski, G. & Kaur, R. (2019). Improve Your Threat Detection Function With Deception Technologies. *Research Report*. Gartner. Recuperado de: https://www.gartner.com/doc/reprints?id=1-6GXJYOW&ct=190402&st=sb

Saydjari, O. (2018). *Engineering trustworthy systems: get cybersecurity design right the first time*. New York, USA.: McGraw Hill

Sieber, S. & Zamora, J. (2018). The Cybersecurity Challenge in a High Digital Density World. *European Business Review*. November. Recuperado de: https://www.europeanbusinessreview.com/the-cybersecurity-challenge-in-a-high-digital-density-world/

Vincent, J. & Hitch, J. (2019). *Winning not fighting*. UK: Penguin Random House

WEF (2020). The Global risk report 2020. *World Economic Forum.* Recuperado de: https://www.weforum.org/reports/the-global-risks-report-2020

***Jeimy J. Cano M., Ph.D, CFE, CICA**. Ingeniero y Magíster en Ingeniería de Sistemas y Computación, Universidad de Los Andes. Especialista en Derecho Disciplinario, Universidad Externado de Colombia. Ph.D en Business Administration, Newport University, CA. USA. y Ph.D en Educación, 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–.*