Ciberdefensa basada en datos

Un modelo conceptual para su desarrollo e implementación.

DOI: 10.29236/sistemas.n170a6

Resumen
Los retos inherentes de un mundo cada vez más interconectado y mediado por ecosistemas digitales, establecen un escenario con mayores oportunidades para crear experiencias novedosas e igualmente un tejido digital de riesgos cibernéticos latentes y emergentes. En este contexto, tanto organizaciones como Estados deben entender, explorar y visualizar su postura de seguridad y control más allá de los territorios conocidos, y establecer nuevas posibilidades de acción que permitan articular el ejercicio de defensa ahora en el ciberespacio. Por lo tanto, este artículo desarrolla un concepto base de ciberdefensa, que más allá de la perspectiva militar, establece un reconocimiento de las capacidades ofensivas del adversario, las capacidades defensivas de las organizaciones y la articulación de estas perspectivas desde cuatro culturas: basada en preguntas, basada en retos, basada en datos y basada en aprendizaje, en un modelo base de defensa cibernética donde la información y los datos son los vínculos que nutren y despliegan la dinámica de la defensa cibernética en empresas y naciones.

Palabras clave
Capacidades defensivas, capacidades ofensivas, ciberdefensa, ciberoperaciones, riesgo cibernético

Introducción

La dinámica global de la sociedad actual establece múltiples retos de tensiones e inestabilidades, que hacen cada vez más desafiante establecer patrones o espacios de planeación a largo plazo y por lo tanto, la materialización de un ejercicio permanente de actualización y cambio que compromete los mejores pronósticos de analistas y especialistas en los diferentes temas (Colomina, 2023). En este contexto, tanto las organizaciones como los Estados se ven envueltos en diferentes perspectivas para priorizar sus actividades, y es allí, donde los adversarios toman ventaja para desarrollar y situar sus acciones en momentos y contextos específicos, con el fin de tomar posiciones estratégicas generalmente en la opacidad de los eventos cotidianos, como una forma invisible de operar a "plena luz del día" y por debajo de los radares de los mecanismos de protección.

En este sentido, las capacidades ofensivas de los adversarios revelan las posibilidades que poco a poco han incorporado en su caja de herramientas, con el fin de lograr el mayor daño, el mayor incierto y el mayor sigilo, comoquiera que sus actividades no siempre están orientadas a producir directamente un efecto nocivo, sino a mantenerlo de forma encubierta por largos periodos de tiempo, buscando deteriorar la capacidad de respuesta del objetivo, sin que éste se percate de dicha situación, y así crear un autoengaño creíble, donde el afectado piensa que puede defender o proteger una posición específica (Gartzke & Lindsay, 2015)

Los escenarios de ciberseguridad empresarial y nacional actual, ahora están imbricados en la realidad geopolítica de los países, en el entorno dinámico de las relaciones internacionales y sus apuestas de operaciones cibernéticas en el ciberespacio. De esta forma, más allá de las prácticas de seguridad y control que se desarrollen en las organizaciones y los gobiernos, se hace necesario avanzar en una consolidación de una visión de protección y defensa que permita maniobrar a las organizaciones en medio de las acechanzas cibernéticas de los países y las agendas desestabilizadoras que se plantean con ocasión de lograr influencia y mayor control en algunas naciones (WEF, 2024).

De esta forma, el concepto de defensa, ahora aplicado en el contexto cibernético con la calificación de ciberdefensa, deja de ser una palabra restringida para uso del contexto del Estado en su derecho natural y constitucional que busca mantener y fortalecer la soberanía de la nación en los diferentes dominios de la guerra: tierra, mar, aire y espacio, para extenderse en nuevas capacidades que deben incorporar

las empresas y alinear con las instituciones estatales, para lograr una mayor presencia en un nuevo dominio denominado ciberespacio. Así las cosas, si bien las organizaciones deben mantener y fortalecer una postura defensiva, de inteligencia, disuasiva y posiblemente diplomática frente a eventos cibernéticos adversos de alcance nacional, son las Fuerzas Militares y sus comandos conjuntos cibernéticos, los que deben coordinar las acciones de defensa necesarias para neutralizar las amenazas y responder si es del caso (Kolini & Janczewski, 2015).

Por lo tanto, este artículo busca comprender las nueva dinámica de la ciberdefensa en el escenario empresarial para lo cual los datos se convierten en el elemento fundamental de su actuación y desarrollo, habida cuenta que, el concepto de seguridad o protección estará relacionado con las amenazas y riesgos conocidos, mientras la defensa y anticipación se fundará desde las amenazas latentes y emergentes, allí donde el adversario quiere crear el reto de inestabilidad y concretar la agenda prevista para inhabilitar las capacidades de amortiguación, flexibilidad y respuesta que las organizaciones tienen dispuestas frente a la inevitabilidad de la falla.

Capacidades ofensivas del adversario

Las capacidades ofensivas del adversario, no sólo están en sus técnicas, tácticas y procedimientos para lograr sus fines, sino en la configuración de una estructura de trabajo que le permita articular sus acciones para lograr una misión. Esto es, una encomienda concreta establecida por un liderazgo particular o colectivo que ordene una serie de actividades, despliegue un conjunto de operaciones y asegure diversas victorias tempranas, que le permitan lograr aquello que es parte fundamental de la agenda trazada por gobierno de los agentes agresores (Arquilla, 2021).

Lo anterior significa que debe existir una estrategia racionalizada que cuente con personas, “exploits”, herramientas, infraestructura y estructura organizacional que articuladas alrededor de los intereses generales de la organización adversarial, es capaz de ubicar operaciones cibernéticas particulares para concretar parte de los planes previstos por los atacantes (Smeets, 2022). Esta estrategia debe privilegiar la potencialización de la creatividad e innovación necesaria para operar en medio de las tensiones geopolíticas vigentes, bien como “proxies” (intermediarios de otros, generalmente Estados), o como actores no-estatales particulares que quieren lograr propósitos y misiones específicas.

El primer elemento son las *personas* las cuales cuentas con habilidades especiales que bien se pueden “arrendar” en medio de las redes oscuras, o incorporar como

parte del cuerpo base de operaciones alineado con un credo o ideal particular (Smeets, 2022). Estas personas pueden jugar diferentes roles como analistas de vulnerabilidades, cazadores de fallos, operadores, equipos de pruebas, analistas de inteligencia y contrainteligencia entre otros, los cuales son capaces de construir capacidades de ataque alrededor de la información recabada por diferentes roles y establecer así el fundamento de las actividades previstas por la organización agresora.

Los "*exploits*" son programas diseñados para aprovechar las vulnerabilidades identificadas en un sistema, para ganar, escalar y mantener acceso en plataformas objetivo.

Para ello, de acuerdo con Smeets (2022) se tienen al menos tres tipos de estos "exploits": los de día cero, la vulnerabilidad no parchada hace N días y la vulnerabilidad corregida hace N días no aplicada.

Los de día cero, que son aquellos que se aprovechan de vulnerabilidades no conocidas por el proveedor del producto, las cuales requieren un estudio particular, o muchas veces se encuentra por interacciones no estándar que se tiene con el producto o servicio. La vulnerabilidad no parchada hace N días, es aquella que responde a una vulnerabilidad conocida por el proveedor, pero este no ha generado el parche para remediarla. La vulnerabilidad corregida hace N días no aplicada, es aquella que cuenta con un parche disponible corregir la falla y no se ha aplicado por la organización. Cualquiera de ellas puede ser utilizada para lograr los objetivos de desestabilización o distracción para motivar acciones adversas de alto impacto (Smeets, 2022).

Las *herramientas* se refieren al conjunto de programas informáticos usados para crear, depurar, mantener o soportar otros programas o aplicaciones, para realizar las operaciones cibernéticas (Smeets, 2022). Estas herramientas se relacionan directamente con los tipos de "exploits" que son capaces de desarrollar y desplegar en las organizaciones o Estados.

Aquellos que se especializan en los de "día cero" tendrán mayor capacidad para generar daños, inestabilidad y caos, comoquiera que se advierte habilidades avanzadas, para producir los efectos específicos que se requieren.

La *infraestructura* responde a los procesos, estructuras e instalaciones que articulan la estrategia que se formula para desarrollar las operaciones. Esto es, contar con los dominios requeridos para concretar el *phishing*, las cuentas de correo electrónico requeridas para los engaños, la infraestructura de equipos para el proceso de comando y control, así como los mecanismos de cifrado de las comunicaciones requeridos para mantener la confi-

dencialidad de las transferencias de los archivos comprometidos. De igual forma, tener las máquinas de prueba y simulación disponibles que permita afinar las fases de la operación y aumentar las probabilidades de éxito, sobremanera mantener el anonimato y la invisibilidad de las acciones (Smeets, 2022).

La *estructura organizacional* que están asociados con características y procesos interorganizacionales: relaciones con otros grupos no-estatales y estados, e intraorganizacionales: cómo las personas efectivamente colaboran y se comunican (Smeets, 2022). Los primeros buscan crear sinergias de fines y objetivos con otros actores o Estados que persiguen misiones semejantes a los disponibles en su agenda, mientras los segundos establecen los marcos de trabajo y autonomía de los participantes de la organización que les permite orientar sus actividades para potenciar la creatividad, innovación y posibles efectos colaterales que se puedan presentar que puedan generar ventajas estratégicas y tácticas para el desarrollo de su misión.

La articulación de estos cinco componentes permite concretar las operaciones cibernéticas claves por parte de los adversarios, los cuales más que iniciativas individuales y con sentido de logro, son estructuras organizadas que cuentan con agendas específicas o conjuntas con Estados u otros agentes no-estatales para lograr sus objetivos destinados a crear inestabilidad, incierto y caos, generalmente basados en misiones concretas que particularmente están fundadas en ciberespionaje o cibersabotaje (Steffens, 2020).

Capacidades defensivas de la organización

Así como los agentes agresores se encuentran organizados, las capacidades defensivas, tanto de las organizaciones como de los Estados, deben responder de la misma forma para enfrentar las asimetrías que generan los atacantes:
(Smeets, 2022)

- *Asimetría de la información*: El adversario tiene un mayor nivel de conocimiento de la infraestructura tecnológica objetivo que la organización.
- *Asimetría de capacidades*: El adversario conoce mejor que la organización el tiempo y los recursos necesarios para acceder al objetivo (y realizar actividades de seguimiento).
- *Asimetría de riesgos*: El adversario conoce mejor que la organización el riesgo que conlleva la realización de determinadas operaciones cibernéticas.
- *Asimetría de oportunidades*: El adversario tiene un mayor nivel de comprensión de la información que puede adquirir y/o de la capacidad de disrupción, negación, degradación y destrucción en comparación con la organización.

En este sentido, el reto de la defensa está en distinguir de forma anticipada posibles señales débiles, amenazas latentes y emergentes con el fin de establecer cinco capacidades básicas claves: (Cano, 2023)

- *Detectar*: Alertas tempranas basadas en la identificación de señales débiles.
- *Disuadir*: Incorporación de tecnología de objetivos móviles o engaño para deteriorar la inteligencia previa del adversario.
- *Demorar*: Crear zonas de distracción para el adversario.
- *Confundir*: Cambiar dinámicamente la configuración de la infraestructura.
- *Anticipar*: Establecer la trayectoria y el movimiento del adversario en la infraestructura, habilitando así un espacio concreto para interceptarle antes de que tenga éxito.

Concretar estas capacidades demanda un ejercicio previo de inteligencia y captura de información del entorno y de la infraestructura tecnológica disponible, de tal forma que alineada con los objetivos estratégicos de la información, se puedan establecer acciones concretas que inviertan la ecuación de las asimetrías previamente planteadas y ofrezcan un espacio de acción y respuesta que sorprenda al atacante en su propio territorio.

Por lo tanto, el ejercicio de defensa se adelanta en el territorio de la incertidumbre que plantea del atacante, un espacio para explorar nuevas estrategias del adversario y crear espacios de confrontación y respuesta que permitan mayor sorpresa en la ecuación de riesgos del agresor, así como mejores capacidades de revelación de patrones emergentes e inusuales que funden ventajas estratégicas para los analistas.

Las defensas tradicionales asociadas con niveles o anillos de seguridad, denominada defensa en profundidad, seguirán siendo válidas y necesarias, como elementos claves para revelar las acciones de los agresores dentro de la infraestructura, lo que implica la generación de alertas y datos que alimenten la inteligencia y la analítica necesaria para darle forma a los patrones que se revelan al procesar los datos (Martin, 2019). Estos resultados, son insumo fundamental para los aprendizajes que se deben tener e incorporar en tiempo real para responder y disuadir al atacante de sus acciones sobre las plataformas de la organización.

Al final, la mejor defensa es: (Adaptado de Donaldson et al., 2015, p.150)
"*aquella que interrumpe los ataques para disuadir a los agresores con menos determinación, detecta aquellos que están en curso, retrasa a los atacantes antes que tengan éxito, vulnera a su contraparte y en el mejor de los casos, supera e infiltra a su adversario*".

Modelo base de ciberdefensa

Considerando los elementos previos relacionados con las capacidades ofensivas del adversario y los retos propios de las capacidades defensivas de las organizaciones, se articula en esta sección una propuesta académica y práctica de ciberdefensa, que entiende el ciberespacio como un escenario de explotación de capacidades estratégicas ofensivas para impactar la dinámica de organizaciones y Estados, siguiendo una agenda geopolítica que busca alcanzar mayor nivel de influencia y poder a través del espacio cibernético (Fischerkeller et al., 2022)

La propuesta está basada en cuatro componentes que se refuerzan entre sí para concretar la definición de defensa establecida en el aparte anterior. Los componentes son: inteligencia de ciberamenazas, escenarios y simulaciones, gobierno y gestión de la ciberdefensa y resiliencia cibernética.

La *inteligencia de ciberamenazas* hace referencia a la información recopilada de diversas fuentes sobre ataques actuales o potenciales de eventos de amenazas cibernéticas contra las organizaciones o naciones. El objetivo principal es hacer visibles y defendibles los diversos riesgos cibernéticos que pueden enfrentar las empresas o Estados (Möller, 2023). Este componente está fundamentado en una *cultura basada en preguntas* que piensa en posibilidades más que en probabilidades, cuestiona y reta el "status quo" y reconoce que la defensa se centra en la postura de "vulnerabilidad por defecto", es decir tarde o temprano el adversario encontrará la ruta para llegar y tener éxito.

Los *escenarios y la simulaciones* son ejercicios que se adelantan para sacar fuera de la zona cómoda a la organización o Estado, con el fin de establecer situaciones de crisis cibernéticas posibles y reales, para validar la capacidad de respuesta y el nivel de preparación de la entidad o nación, para enfrentar la realidad de un evento que genere confusión, inestabilidad y caos.

Este tipo de actividades demanda una participación interdisciplinaria que sume desde diversos puntos de vista y contextos, con el fin de crear conocimiento y advertir nuevas capacidades para enfrentar a los adversarios. Para lograr los resultados esperados, es necesario motivar y desarrollar una *cultura basada en retos*, en situaciones que ponen a prueba el saber previo de los participantes.

La *gestión y gobierno de la ciberdefensa* opera como la torre de control que articular los esfuerzos de los diversos componentes del modelo. Para ello se requiere una *cultura basada en datos*, que permita cuantificar la incertidumbre de los ejecutivos sobre las capacidades e intenciones de los adversarios, desarrollar pruebas de concepto sobre las iniciativas digitales

que se tienen en la organización y sobre el panorama de amenazas emergente y latentes, que permitan establecer una toma de decisiones informada y articulada que se enfoque en: (Grimes, 2019, p.150)

- Las causas y eventos que más daño le producen a la organización.
- La capacidad de respuesta y amortiguación disponible frente a eventos exitosos.
- El nivel de capacidades de defensa disponibles en la organización: detectar, disuadir, demorar, confundir y anticipar.
- El tiempo medio de respuesta entre el compromiso exitoso del atacante y la puesta en operación del sistema comprometido.
- El estado de resistencia de las personas a los engaños de los adversarios.

La *resiliencia cibernética* se entiende como la capacidad amortiguamiento, flexibilidad y respuesta que debe tener la organización al enfrentarse al deterioro de su estado de estabilidad actual, para lo cual, tanto las organizaciones como las empresas, deben estar dispuestas a tomar riesgos en territorios desconocidos que plantean los atacantes, motivar las ideas e inquietudes por parte de los diferentes actores organizacionales y estatales sin temor a represalias en medio de las inestabilidades con el fin de habilitar una *cultura basada en aprendizajes* y mejoramiento discontinuos. Lo anterior supone entender el evento adverso, en un entorno psicológicamente seguro, que desde la pedagogía del error, reconoce en cada escenario condiciones particulares que se presentan (y hasta ahora desconocidas), que permite movilizar acciones de respuesta coordinadas y no centrarse exclusivamente en el resultado que ya se sabe crea inestabilidad y efectos inesperados.

Así las cosas, el accionar integrado de estos componentes deberá orientar tanto a la organización como al Estado para darle forma a cinco preguntas claves que permitan afinar y desplegar las capacidades de ciberdefensa en escenarios generalmente adversos, agrestes y por demás inexplorados: (Recorded Future, 2022)

- Sector de industria o nación: *¿Afecta la amenaza a otras organizaciones del sector u otra nación?*
- Tecnología: *¿La amenaza compromete el software, el hardware u otras tecnologías utilizadas en la empresa o país?*
- Geografía: *¿La amenaza se mueve hacia instalaciones en regiones donde se tienen operaciones o aliados estratégicos?*
- Adversario: *¿Es posible conocer el adversario(s) y sus intenciones que están ocasionando la amenaza?*
- Métodos de ataque: *¿Es posible identificar las capacidades y métodos utilizados de forma exitosa por el adversario?*

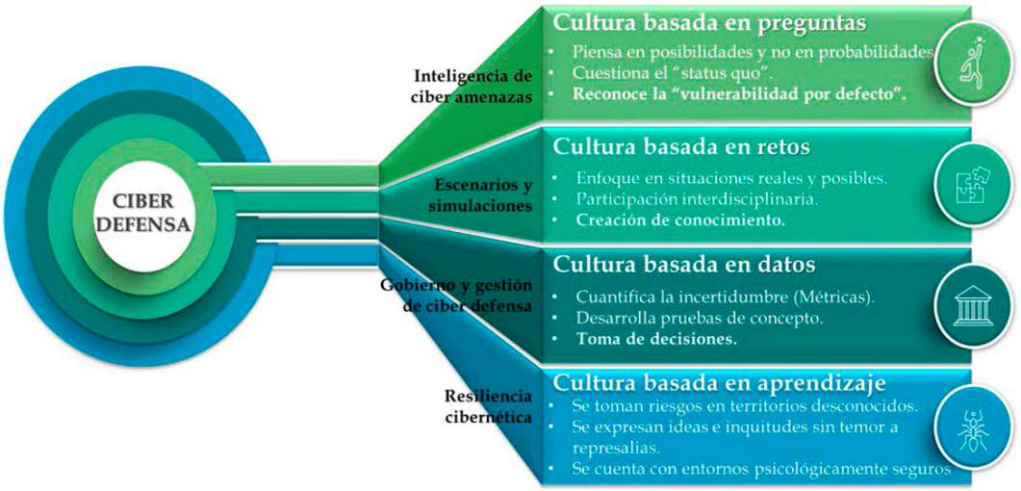

Figura 1. Modelo base de ciberdefensa (Elaboración propia)

Una vista resumen del modelo se presenta en la figura 1.

Reflexiones finales

De acuerdo con Mckinsey (2022) una organización habilitada por los datos o basada en datos debe contar con las siguientes características:

- Los datos están integrados en cada decisión, interacción y proceso,
- Los datos se procesan y entregan en tiempo real,
- Los almacenes de datos flexibles permiten integrar datos listos para su uso,
- El modelo operativo de datos los trata como un producto,
- El papel del director de datos se amplía para generar valor,
- Los miembros del ecosistema de datos son la norma,
- La gestión de datos se prioriza y automatiza para favorecer la privacidad, la seguridad y la resiliencia.

Cada una de estas características aplicadas al modelo de ciberdefensa, particularmente desde su componente de gobierno y gestión, permite incorporar y desarrollar rápidamente las capacidades necesarias que aumenten la visibilidad de la organización de su entorno, ofreciendo una actualización permanente de las variantes del estado de exposición y vulnerabilidad que tiene la empresa en un momento específico. Nótese que es el desarrollo cultural en cada uno de los componentes del modelo el que motiva y transforma el ejercicio de defensa, no como una respuesta a una novedad en el

entorno, sino como una unidad de acción y mando, que se sabe vulnerable y por lo tanto, vigilante para seguir los pasos de sus posibles adversarios.

Por tanto, el modelo de ciberdefensa presentado en este artículo inicia con las *preguntas*, como referente natural de la defensa que indaga en el reto de tratar de anticipar al adversario en su propio terreno como lo es la incertidumbre. Adelantar esta acción establece *retos* que cuestionan lo que tanto el Estado como la organización han aprendido hasta la fecha, con el fin de situar el saber actual y dejarse interrogar por las nuevas condiciones del entorno para visualizar aquello que los sesgos propios hacen invisible.

Enfrentar los retos, implica recolectar *datos* de diferentes fuentes y sensores disponibles para luego procesarlos en el contexto actual asistidos con inteligencia artificial mediante algoritmos supervisados, algoritmos no supervisados o algoritmos de refuerzo, con el fin de filtrar los resultados basados en conocimiento técnico, aprendizajes previos y bases de datos especializadas, para revelar anomalías, eventos inusuales, alertas tempranas y señales débiles, las cuales den sentido a las decisiones de la organización frente a las amenazas latentes y emergentes.

Toda esta información debe llevar al desarrollo *aprendizajes* en la organización, esto es, tener la capacidad de sorprenderse y encontrar situaciones novedosas que cambian la forma de entender al atacante y por tanto, actualizar las prácticas y estrategias que las organización o Estado ha tomado hasta el momento. Lograr lo anterior, requiere un ejercicio de madurez en la defensa y anticipación de las amenazas que se traduce en un marco de trabajo de preparación para el futuro que implica: (Rorhbeck & Kum, 2018)

- adaptar las capacidades actuales frente a los cambios disruptivos,
- aumentar la resiliencia cibernética frente a los eventos adversos, y
- transformar la estrategia de defensa.

El modelo de ciberdefensa propuesto en este documento no responde a una doctrina militar específica, ni es ajeno a la dinámica de las organizaciones actuales, sino que busca integrar la esencia del reto de la defensa en el ciberespacio como un imperativo cultural de las organizaciones y los Estados del siglo XXI. Una capacidad estratégica de las naciones y las empresas que se transforma y nutre desde las preguntas, hasta habilitar espacios de aprendizaje concretos y específicos, semejantes al entrenamiento que el adversario adelanta en su propio ecosistema, para hacer del ejercicio de la defensa un escenario de construcción colecti-

va y respuesta conjunta, no sólo tácito sino estratégico.

En palabras de Sun Tzu:
"*La estrategia sin táctica es el camino más lento hacia la victoria. La táctica sin estrategia es el ruido que precede a la derrota*".

Referencias

Arquilla, J. (2021). Bitskrieg. The new challenge of cyberwarfare. Cambridge, UK: Polity Press.

Cano, J. (2023). Security Risk Management and Cybersecurity: From the Victim or from the Adversary?. En: Jahankhani, H. (eds) Cybersecurity in the Age of Smart Societies. Advanced Sciences and Technologies for Security Applications. Springer, Cham. 1-8. https://doi.org/10.1007/978-3-031-20160-8_1. ISBN:978-3-031-20159-2

Colomina, C. (editora) (2023). El mundo en 2024: diez temas que marcarán la agenda internacional. CIDOB Notes Internationals 299. https://shorturl.at/fiW48

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

Fischerkeller, M., Goldman, E. & Harknett, R. (2022). Cyber persistence theory. Redifining national security in cyberspace. New York, NY. USA: Oxford University Press.

Gartzke, E. & Lindsay, J. (2015). Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. Security Studies. 24. 316–348. doi: 10.1080/09636412.2015.1038188

Grimes, R. (2019). A data-driven computer defense. A way to improve any computer defense. Lexington, KY. USA.

Kolini, F. & Janczewski, L. (2015). Cyber Defense Capability Model: A Foundation Taxonomy. CONF-IRM 2015 Proceedings. 32. https://aisel.aisnet.org/confirm2015/32

Martin, P. (2019). The rules of security. Staying safe in a risky world. Oxford, UK.: Oxford Press.

Mckinsey (2022). The data-driven enterprise of 2025. Insights. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-data-driven-enterprise-of-2025

Möller, D. (2023). Guide to Cyber security in Digital Transformation. Trends, Methods, Technologies, Applications and Best Practices. Cham, Switzerland: Springer Verlag

Recorded Future (2022). The Threat Intelligence Buyer's Guide. Everything you should know about threat intelligence before you buy. https://go.recordedfuture.com/hubfs/white-papers/intelligence-buyers-guide.pdf

Rorhbeck, R. & Kum, M. (2018). Corporate foresight and its impact on firm performance: A longitudinal analysis. Technological Forecasting and Social Change. 129. 105-116. https://shorturl.at/vIJK0

Smeets, M. (2022). No shortcuts. Why states struggle to develop a military cyber-force. New York, NY. USA: Oxford University Press.

Steffens, T. (2020). Attribution of Advanced Persistent Threats. How to Identify the Actors Behind Cyber-Espionage. Alemania: Springer Verlag

WEF (2024). Global Risk Report 2024. Global Risk Report 2024. 19th Edition. Insight Report. https://www.weforum.org/publications/global-risks-report-2024/

***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–.*