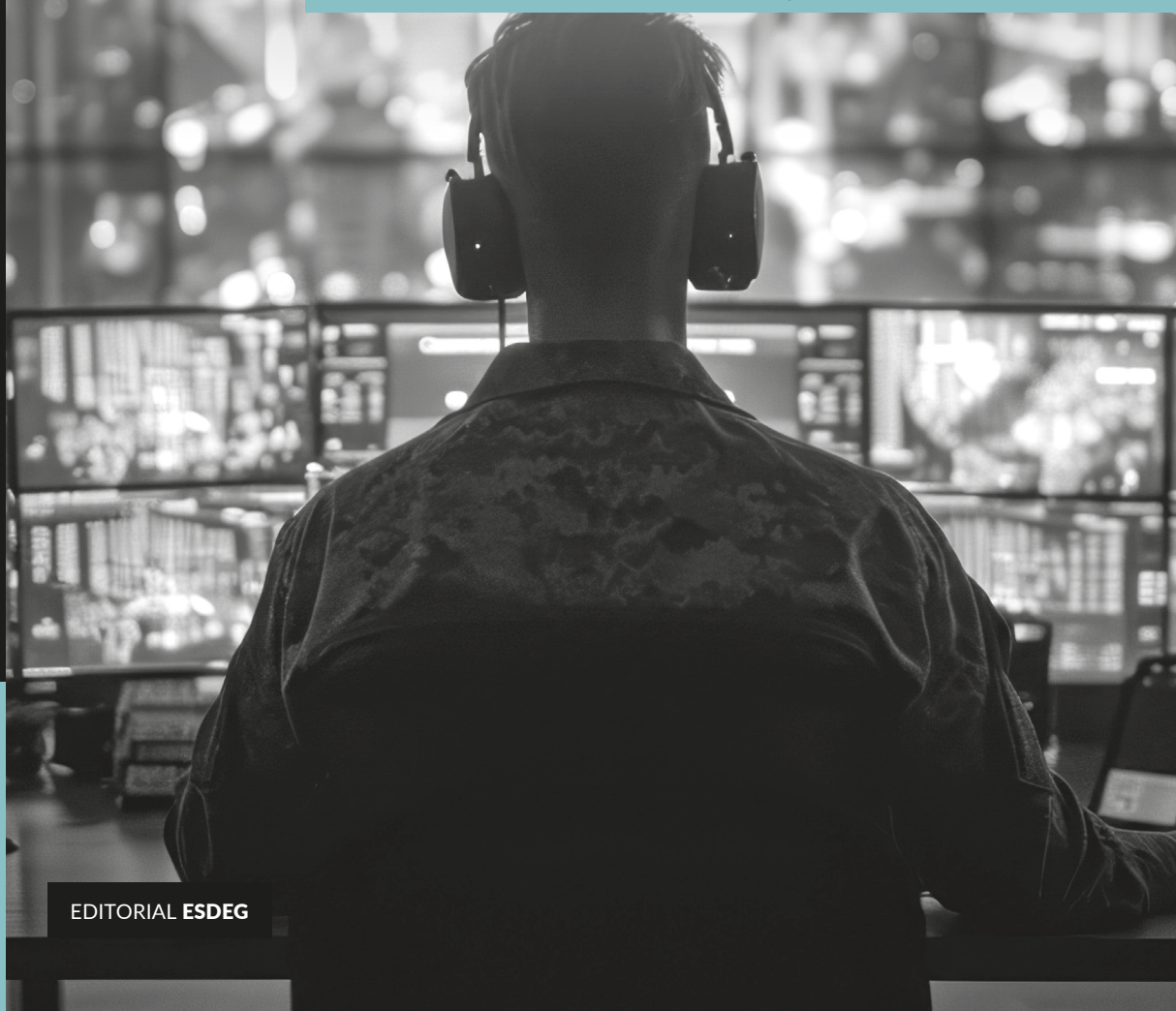
Tecnologías disruptivas, logística, seguridad y defensa en el ciberespacio

Milena Elizabeth Realpe Díaz
Angélica María González González
(Editoras)

Colección Ciberseguridad y Ciberdefensa



EDITORIAL **ESDEG**

Tecnologías disruptivas, logística, seguridad y defensa nacional en el ciberespacio

Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Colombia

Colección Ciberseguridad y Ciberdefensa
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Tecnologías disruptivas, logística, seguridad y defensa nacional en el ciberespacio

Milena Elizabeth Realpe Díaz
Angélica María González González
(Editoras)

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., 2024

Catalogación en la publicación – Escuela Superior de Guerra "General Rafael Reyes Prieto"

Tecnologías disruptivas, logística, seguridad y defensa nacional en el ciberespacio / editores Milena Elizabeth Realpe Díaz y Angélica María González González -- Bogotá: Editorial ESDEG, 2024.

166 páginas : ilustraciones, tablas, mapas y gráficos; 24 cm.
Incluye referencias bibliográficas al final de cada capítulo

ISBN impreso: 978-628-7602-69-4
E- ISBN: 978-628-7602-70-0

(Colección Ciberseguridad y Ciberdefensa)

1.Ciberespacio 2.Seguridad informática -- Aspectos políticos -- Colombia 3.Colombia -- Defensa nacional i.Alonso Galindo, Jaime, Brigadier General (prólogo) ii.Realpe Díaz, Milena Elizabeth, Teniente Coronel (editora - autora) iii.González González, Angélica María (editora - autora) iv.Giraldo Ríos, Lucas Adolfo (autor) v.Ospina Navas, Jaider (autor) vi.Barrios Torres, Sergio, Coronel (RA) (autor) vii.Maldonado, Carlos Eduardo (autor) viii.Colombia. Escuela Superior de Guerra "General Rafael Reyes Prieto (ESDEG)

HF5548.37 T43 2024 Registro Catalográfico SIBFuP 991297812607231
658.478 23

Archivo descargable en formato MARC en: https://tinyurl.com/esdeg991297812607231

Tecnologías disruptivas, logística, seguridad y defensa nacional en el ciberespacio
Primera edición, 2024

Editoras:
Milena Elizabeth Realpe Díaz
Angélica María González González

Cubierta:
Raquel Arianne Alvarado Candela con base en imágenes de Adobe Stock

Colección Ciberseguridad y Ciberdefensa

ISBN impreso: 978-628-7602-69-4
ISBN digital: 978-628-7602-70-0
DOI: https://doi.org/10.25062/9786287602700

Libro electrónico publicado a través de la plataforma Open Monograph Press.
Tiraje de 100 ejemplares
Impreso en Colombia

Libro resultado de investigación de la Escuela Superior de Guerra "General Rafael Reyes Prieto".

Contenido

Prefacio

Brigadier General Jaime Alonso Galindo
Director Escuela Superior de Guerra "General Rafael Reyes Prieto"

Vivimos una era definida por la acelerada evolución de las tecnologías disruptivas, fenómeno que trasciende las formas tradicionales de entender y abordar la seguridad y defensa nacional en el ciberespacio. En este contexto, dinámico y desafiante, es mandatorio realizar una constante revisión académica sobre cambios tan drásticos para mejorar la toma de decisiones y las capacidades de organizaciones, entidades públicas y Fuerzas Militares con miras a enfrentarlos de la manera más efectiva.

El propósito de este libro es esclarecer las particularidades inherentes a las tecnologías disruptivas, destacando su impacto específico en el ámbito de la seguridad y defensa nacional en el ciberespacio. A medida que estas innovaciones emergen y transforman nuestras realidades, su influencia se extiende más allá de las esferas tecnológicas, afectando de manera significativa los intereses nacionales y la seguridad de las naciones.

La obra desarrolla un análisis profundo de las tendencias actuales, desentrañando el entramado de amenazas y ataques que se gestan en las redes, invisibles, pero potencialmente devastadoras. Las tecnologías disruptivas, al reemplazar rápidamente las infraestructuras existentes, plantean desafíos cruciales para la ciberseguridad y ciberdefensa nacional. ¿Cuál es el impacto de las tecnologías disruptivas y la logística global en el mantenimiento de la seguridad y defensa nacional en el ciberespacio?

En este recorrido intelectual, exploraremos la distinción esencial entre ciberseguridad y ciberdefensa, dos pilares para abordar las amenazas en el ciberespacio. La ciberseguridad se erige como la primera línea de defensa, enfocada en proteger sistemas y datos de las amenazas cibernéticas. Sin embargo, para salvaguardar la integridad nacional, debemos ir más allá, abarcar la ciberdefensa

con estrategias y políticas que blinden a una nación contra ataques cibernéticos que podrían comprometer su seguridad y estabilidad.

La necesidad imperante de analizar, prevenir y tomar decisiones prospectivas ante las tecnologías disruptivas resalta la importancia de la sinergia entre la ciberseguridad y la ciberdefensa. En este contexto, el presente libro presenta estas interrelaciones cruciales, consolidándose como un recurso esencial para aquellos que buscan comprender y enfrentar los desafíos emergentes en el ciberespacio.

Preparémonos para explorar un terreno donde la innovación y la seguridad convergen y el conocimiento se convierte en la mejor herramienta contra las amenazas invisibles que acechan en el mundo digital.

Introducción

Milena Elizabeth Realpe Díaz
Angélica María González González
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Con la transición de la Era Industrial, a finales del siglo XX, y el surgimiento de la Era de la Información con la Cuarta Revolución Industrial, a principios del siglo XXI, se ha experimentado un cambio radical en el panorama de la globalización. En este nuevo paradigma, la internet ha logrado interconectar a todos los individuos, configurando el ciberespacio como un dominio único que desafía y redefine los conceptos tradicionales de seguridad y defensa de los Estados.

En contraste con los conflictos convencionales, caracterizados por contar con regulaciones y doctrinas específicas, los ciberconflictos y las amenazas que se originan en el mundo cibernético, impulsados por el constante aumento de la densidad digital, generan una zona gris marcada por la inestabilidad y la incertidumbre. Este escenario se caracteriza por la ausencia de regulaciones específicas y condiciones de acción claramente definidas, lo cual abre las puertas a actividades de difícil interpretación y sujeción a las reglas existentes.

Con la aparición de las tecnologías disruptivas, definidas como "una innovación que ayuda a crear una nueva red de valor y que eventualmente interrumpe el mercado actual (en unos pocos años o décadas), desplazando una tecnología anterior" (Dabirian & Loza, 2015, p. 30) consolidan nuevos relatos por medio de los cuales la sociedad se relaciona y se desarrolla.

El presente libro, *Tecnologías disruptivas, logística y seguridad y defensa nacional en el ciberespacio,* examina, desde diversas perspectivas académicas, el impacto que las tecnologías disruptivas y la logística ejercen en el mantenimiento de la seguridad y defensa nacional. Tal examen se fundamenta en el desarrollo científico y tecnológico, la logística, la administración y la seguridad digital, a fin de comprender los cambios en entornos caracterizados por su volatilidad, incertidumbre, complejidad y ambigüedad (VICA) y facilitar procesos de toma de decisiones más informados para la seguridad y defensa nacional en el ciberespacio.

El capítulo 1, "Definición e impacto de la transformación digital en la ciberseguridad", analiza la previsión y la prospectiva estratégicas; señala que la previsión estratégica implica la anticipación de posibles escenarios futuros, mientras que la prospectiva estratégica busca identificar tendencias emergentes; resalta la necesidad de estrategias que promuevan la sensibilización y concienciación en ciberseguridad para una cultura organizacional sólida en seguridad de la información, y concluye que al fomentar dicha cultura, se fortalece la resiliencia organizacional ante amenazas cibernéticas.

El capítulo 2, "*Blockchain* y ciberseguridad: fortalecimiento de la confianza digital", explora el estado del arte de esta tecnología disruptiva, con miras a identificar su papel en la construcción de un ecosistema digital seguro. Para ello precisa los aspectos que caracterizan la cadena de bloques como la descentralización, la inmutabilidad y el consenso; discute sus ventajas en términos de seguridad, transparencia y resistencia a la manipulación; analiza los diferentes tipos de ataques en materia de inmutabilidad que se reconocen a la fecha; describe los diferentes tipos de aplicaciones en que se emplea *blockchain*, y presenta los desafíos y limitaciones actuales, proporcionando una visión holística de las posibilidades y obstáculos en este campo en evolución.

El capítulo 3, "Ejército Nacional de Colombia: cadena logística, ciberseguridad y ciberdefensa", examina el interés estratégico de la Fuerza por los estudios sobre la relación ciberseguridad, ciberdefensa y logística militar; destaca la necesidad de ampliar el conocimiento en este ámbito, tanto en la academia como en la actualización de la doctrina militar, para fortalecer la seguridad nacional; indica posibles rezagos conceptuales y de acción que podrían convertirse en debilidades operativas, y sugiere reflexiones como base para futuras investigaciones y desarrollos doctrinales, con el objetivo de mejorar y proteger la cadena logística militar del EJC desde una perspectiva emergente de ciberseguridad.

El capítulo 4, "Ciencias de punta y tecnologías disruptivas en el ciberespacio como marco y condición para la ciberdefensa de Colombia", problematiza la importancia de las ciencias de la complejidad, sus ejes, temas y problemas en el marco de la digitalización del mundo y de la sociedad y, en consecuencia, respecto de la seguridad y defensa nacional; sostiene que las ciencias de la complejidad son ciencias de la vida que se ocupan exactamente de todo aquello de lo cual la ciencia normal se desentiende; señala que existe, asimismo, una tensión esencial entre ciencia y tecnologías, a saber, la ciencia tradicionalmente comporta un principio de democracia, mientras que, por su parte, la historia de la tecnología

fue siempre la de tecnologías *prima facie* militar, y concluye que las ciencias de la complejidad permiten superar o resolver esta tensión.

Finalmente, el capítulo 5, "El poder en la era digital: perspectivas sobre el ciberpoder", analiza las dinámicas que tienen lugar en el ciberespacio; expone cómo empieza a hablarse de ciberpoder en el ámbito general del poder; examina las acepciones del término de acuerdo con diferentes perspectivas regionales y en el entendido de que se define según como se comprenda y dónde se localice; describe el poder desde la perspectiva militar de EE. UU. y desde la óptica de la Unión Europea, y amplía la comprensión del ciberpoder, a partir de su localización, todo lo cual apunta a establecer estimaciones adecuadas de este objeto de estudio.

Se espera que, con esta obra, el lector se sienta inspirado a llevar a cabo un análisis propio sobre estas nuevas dinámicas, contribuyendo así a la discusión académica y técnica en los campos de la ciberseguridad y la ciberdefensa.

Referencias

Dabirian, R., & Loza Matovelle, D. (2015). Introducción a la tecnología disruptiva y su implementación en equipos científicos. Revista Politécnica, 36(3), 1-4. https://n9.cl/su68o

Capítulo 1

Definición e impacto en la transformación digital y la ciberseguridad*

DOI: https://doi.org/10.25062/9786287602700.01

Lucas Adolfo Giraldo Ríos
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este capítulo analiza la previsión y la prospectiva estratégicas; señala que la previsión estratégica implica la anticipación de posibles escenarios futuros, mientras que la prospectiva estratégica busca identificar tendencias emergentes; resalta la necesidad de estrategias que promuevan la sensibilización y concienciación en ciberseguridad para una cultura organizacional sólida en seguridad de la información, y concluye que al fomentar dicha cultura, se fortalece la resiliencia organizacional ante amenazas cibernéticas.

Palabras clave: ciberseguridad; concienciación; cultura organizacional; estrategia; previsión; prospectiva.

* Capítulo de libro resultado del proyecto de investigación "*Tecnologías disruptivas, logística y seguridad y defensa nacional en el ciberespacio*", del grupo de investigación *"Ciberespacio Tecnología e Innovación"*, de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado C por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) y registrado con el código COL0181179. Los puntos de vista y los resultados de este capítulo pertenecen a los autores y no necesariamente reflejan los de las instituciones participantes

Lucas Adolfo Giraldo Ríos
Candidato a doctor en Ingeniería, Industria y Organizaciones, Universidad Nacional de Colombia. Magíster en Administración de Empresas de Base Tecnológica, Universidad Antonio de Nebrija, España. Magíster en Innovación, Universidad EAN, Colombia. Especialista en Gestión Financiera Empresarial, Universidad de Medellín, Colombia. Administrador de Empresas, Universidad de Antioquia, Colombia.
https://orcid.org/signin - Contacto: **lucas.giraldo@esdeg.edu.co**

Citación APA: Giraldo Ríos, L. A. (2024). Definición e impacto en la transformación digital y la ciberseguridad. En M. E. Realpe Díaz, & A. M. González González (Eds.), *Tecnologías disruptivas, logística y seguridad y defensa nacional en el ciberespacio* (pp. 15-46). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602700.01

TECNOLOGÍAS DISRUPTIVAS, LOGÍSTICA Y SEGURIDAD Y DEFENSA NACIONAL EN EL CIBERESPACIO
ISBN impreso: 978-628-7602-69-4
ISBN digital: 978-628-7602-70-0
DOI: https://doi.org/10.25062/9786287602700

Colección Ciberseguridad y Ciberdefensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2024

Introducción

La convergencia tecnológica, donde los flujos de información son cada día más frecuentes, marca el advenimiento de la revolución digital, debido al mundo interconectado en que nos encontramos, con información instantánea, permanente y actualizada, todo lo cual ha generado un cambio en los sistemas informáticos y en la exigencia de la seguridad como un reto al cual se enfrentan día a día las organizaciones y los individuos.

La protección de la información es una de las mayores preocupaciones que tienen hoy las organizaciones. Debido a la globalización y al internet de las cosas (IoT), cada vez más las entidades, tanto públicas como privadas, se enfrentan a nuevas amenazas y riesgos. Por esto, no basta con las políticas de seguridad implementadas o la inversión tecnológica que hacen las empresas para contrarrestar este flagelo, sino que debe tenerse en cuenta el personal que labora en las instituciones y que representa el eslabón más débil en la seguridad de la información.

En este sentido, las organizaciones deben asumir una postura resiliente frente a los problemas de ciberseguridad. Es decir, anticiparse a las amenazas y riesgos que se presentan, ya que cada día son más variados y se masifican exponencialmente, dificultando la protección de los activos de información y generando en las organizaciones un cambio de perspectiva frente a la forma de actuar en este mundo dinámico e incierto.

La seguridad de la información debe operar en el diseño de estrategias corporativas y en la articulación de planes tácticos que entiendan el modelo de negocio en que se encuentra la organización para que, mediante este entendimiento, pueda anticiparse a los principales desafíos futuros y brinde apoyo para la toma de decisiones frente a los problemas de ciberseguridad.

Este artículo, en tal sentido, ofrece una visión general de los conceptos e ideas clave sobre la previsión y prospectiva estratégica, la importancia de la sensibilización y concienciación en ciberseguridad en las organizaciones y el uso de la perspectiva para alcanzar una cultura organizacional en ciberseguridad.

Previsión y prospectiva estratégica

Durante mucho tiempo, la previsión se ha utilizado para describir la preparación y la forma como se abordan los problemas a largo plazo por parte de los Gobiernos. El término *prospectiva tecnológica* se empezó a utilizar en los años 1990 en Europa, aunque luego otros países empezaron abordarlo como política relativa a los sistemas de ciencia, tecnología e innovación (Miles, 2010).

Los estudios de Irvine y Martin destacaron la palabra *previsión* como la forma popular de describir amplios programas de estudios de investigación y de innovación para futuros desarrollos (Miles, 2010). En muchos casos, la previsión se lleva a cabo para anticiparse a los principales desafíos sociales y futuros, logrando brindar apoyo en la toma de decisiones, no solo porque permite identificar los cambios tecnológicos, sino porque involucra a las partes interesadas relevantes que van a generar conocimiento e innovación.

Según Könnölä et al. (2010), las actividades de previsión han tendido a cambiar, centradas en las tecnologías positivistas y racionalistas hacia el reconocimiento de preocupaciones más amplias que abarcan todo el sistema de innovación, teniendo en cuenta enfoques sociales, como la sostenibilidad, la seguridad y la sociedad de la información.

La prospectiva, por su parte, juega un papel definitivo en la toma de decisiones de las organizaciones, ya que es función crucial que les permite a las organizaciones prepararse para el futuro, no solo identificando vías tecnológicas prometedores, sino también, diferentes actores interesados en el proceso de anticipación y creación de acciones comunes que conlleven la preparación y confrontación de lo que se viene (Könnölä et al., 2010).

La prospectiva, por lo anterior, se reconoce como un proceso sistemático, participativo y de construcción de ideas que puedan enfrentarse a largo plazo para la toma de decisiones, tanto actual como futura, y que permitan construir esa planeación estratégica que responda a los objetivos de las organizaciones.

Debido a los desafíos sociales que se presentan día a día por la convergencia tecnológica, por el IoT y por la economía digital, entre otros, existe la necesidad de

basarse en los resultados de investigación con miras a apoyar situaciones específicas en la toma de decisiones. Por lo anterior, es necesario tener en cuenta los datos y estudios realizados, los cuales sirven de guía y preparan para el futuro, a fin de poder enfrentar los desafíos en cuanto a ciencia, tecnología e innovación y, con ellos, poder tomar mejores decisiones (Könnölä et al., 2010, p. 3).

La experiencia en el uso de la prospectiva y la perspectiva en países como Japón, Holanda, EE. UU. , España y Reino Unido demuestra que la sistemática incorporación de estas en los procesos de ciencia y tecnología ha permitido mejorar las estrategias y servido de guía para la toma de decisiones en la implementación de políticas en las entidades tanto públicas como privadas. Lo anterior revela la importancia que tiene la prospectiva para una organización, ya que a partir de los estudios sobre ella se logran minimizar muchos riesgos que traen la tecnología y la digitalización y, en general, se obtiene la seguridad de la información que es uno de los retos de todas las organizaciones (Miles, 2010, pp. 7-8).

En cuanto a la sensibilización en ciberseguridad, se exige la implementación de la prospectiva, no solo como predicción del futuro, ya que cada día se presentan nuevos riesgos y amenazas, sino como herramienta que les permita a las organizaciones tener una postura resiliente frente a los desafíos e implementar mejores estrategias.

De igual forma, la inseguridad de la información seguirá siendo un problema inminente para los Gobiernos debido a la conectividad y a la necesidad de estar informados permanentemente, por lo que los desafíos seguirán siendo grandes para los investigadores y encargados de la seguridad de los activos de información.

Prospectiva estratégica: importancia para el futuro de las organizaciones

La prospectiva estratégica es utilizada cada vez más por las organizaciones, porque les da una visión de futuro y les permite una mejora continua en los procesos para contrarrestar los riesgos y amenazas que pueden generarse por la falta de previsión.

Las empresas deben considerar la estrategia como un todo y empezar a implementarla o corregirla gradualmente, según su ritmo de adaptación. Según Mintzberg et al. (1998), en diez escuelas, la estrategia se categoriza en tres grupos principales. El primero, conocido como *prescriptivo,* se centra en la formulación de

estrategias antes de considerar su concepción. El segundo grupo, compuesto por seis escuelas, se enfoca en la descripción de los procedimientos, dando prioridad al contenido y al posicionamiento, lo que transforma la estrategia en algo distinto, sistemático y formal. Por último, surge la escuela del conocimiento, que busca utilizar las herramientas de la psicología cognitiva para comprender la mente del estratega.

Uno de los principales objetivos de la estrategia es resolver los grandes desafíos y problemas que pueden presentarse a futuro en las organizaciones. Esto no quiere decir que al implementar o modificar una estrategia ya estamos exentos de una amenaza o peligro, sino que, con esto, se minimizan muchos riesgos que pueden acaecer. Se acuerdo con Mintzberg et al. (1998), "una estrategia modera la capacidad de respuesta frente a los cambios y modificaciones del entorno, es decir, que es un elemento fundamental que lo obliga a ir derecho y no le permite desviar la mirada" (p. 4).

Para implementar una buena estrategia, debemos, no obstante, revisar su importancia para las organizaciones. Por esto, Mintzberg et al. (1998) describen el papel de la estrategia y sus ventajas en cuatro puntos: 1) como orientación, ya que sirve como brújula a una organización; 2) como concentración de esfuerzos, ya que permite la concentración de actividades; 3) como sentido a la organización, ya que la distingue de las demás, y 4) como fuente de coherencia, ya que ayuda a comprender el entorno y con esto la implementación de acciones que responden a este.

Por lo anterior, al implementar estrategias, las organizaciones deben tomarlas como un todo y no como a su conveniencia o como mejor se le acomode a la organización. Para la escuela de la cultura y del espíritu, las estrategias son únicas perspectivas del punto de vista de una persona o de la cultura organizacional y, por lo tanto, cada una es diferente, es decir, no se pueden comparar con otras estrategias, ya que estas se derivan y nacen del fruto de procesos personales de adaptación y son el resultado de esfuerzos individuales de creación (Mintzberg et al., 1998).

Estrategias para una cultura en seguridad de la información

En este apartado, nos sumergimos en la esencia misma de la ciberseguridad y la transformación digital: la cultura organizacional en torno de la seguridad de la información. Según Beaver (2018), la seguridad efectiva no es simplemente una

cuestión de herramientas y tecnología, sino también de actitudes, comportamientos y conciencia dentro de la organización. Es aquí donde las estrategias para fomentar una cultura de seguridad se vuelven cruciales (Spafford, 2006).

La cultura organizacional de seguridad de la información (COSI) es un asunto relevante que permite aumentar la resistencia de las empresas a los ataques cibernéticos. Aunque se trata de un tema que debe estudiarse, las empresas tanto públicas como privadas infortunadamente todavía no le han dado la relevancia que requiere (Cano, 2016).

La cultura organizacional trabaja en pro de la protección de la información, la cual deja de ser un recurso más de las empresas y pasa a ser un activo estratégico muy importante para la toma de decisiones. La ciberseguridad es un problema de gestión de riesgos y debe abordarse desde una perspectiva estratégica, económica y reactiva, la cual debe involucrar a todos los miembros de las organizaciones y tomarse como un proceso transversal para todas las áreas de la entidad. "Proteger los activos de las entidades de delitos cibernéticos nos es una opción, sino un elemento clave para el desarrollo de una organización" (Organization of American States [OAS], 2017, s.p.).

Según Sechin (citado por Cano, 2015), "una cultura organizacional se construye a partir de lo que la gente cree, lo que las personas hacen y lo que los individuos ven" (s.p.). Es decir, que para construir una cultura en seguridad de la información es necesario estudiar el comportamiento de las personas, ya que este refleja la forma como actúan frente a los temas de seguridad, la responsabilidad como la afrontan y en muchos casos se puede llegar a observar el nivel de conocimiento que estas tienen frente al tema de ciberseguridad. Este análisis busca articular la relación de las personas frente a la información y la responsabilidad que cada uno tiene desde el rol que desempeña frente a este activo y el valor que tiene para el cumplimiento estratégico y misional de cada entidad, buscando no solo el cumplimiento de estrategias y normas implementadas por la empresa, sino también la apropiación para la protección de la información.

Es sabido que cuando se implementan estrategias de prospectiva para una organización en temas de seguridad de la información, estas no pueden abordarse en un 100 %, ya que cada día surgen nuevas amenazas y riesgos debido a la evolución tecnológica y la convergencia de la mismas; aquí es donde los gerentes en seguridad de la información empiezan a evaluar cuáles "riesgos se pueden evitar, cuáles aceptar y cuáles mitigar o transferir mediante un seguro, así como los planes específicos asociados a cada enfoque" (OAS, 2017). Es bueno tomar esta

decisión una vez se evalúen estos aspectos con el costo y el beneficio que pueden generar para la empresa. A partir de lo anterior, se describen algunas estrategias que apoyan la cultura de la ciberseguridad de la información.

Importancia de la seguridad de la información

La seguridad de la información es fundamental en cualquier organización para garantizar la protección de los datos confidenciales y evitar posibles pérdidas financieras o daños reputacionales. En la era digital, cuando la información se encuentra expuesta a diversos riesgos y amenazas como el robo de datos o ciberataques, es crucial tener estrategias y medidas de seguridad adecuadas. La información es un activo valioso que puede brindar ventajas competitivas, por lo que su protección se convierte en una prioridad para garantizar la continuidad del negocio. La implementación de políticas y procedimientos de seguridad, así como la capacitación y concienciación del personal, son aspectos clave para lograr una cultura en seguridad de la información efectiva. Además, es importante evaluar y mejorar de forma continua el sistema de seguridad para adaptarse a los cambios tecnológicos y a las nuevas amenazas que puedan surgir.

Identificación de riesgos y vulnerabilidades

La identificación de riesgos y vulnerabilidades es un paso fundamental para alcanzar una cultura en seguridad de la información efectiva. Este proceso nos permite identificar los posibles peligros a los que está expuesta nuestra organización, así como las debilidades en nuestros sistemas y procesos que podrían ser aprovechadas por los actores maliciosos. Para llevar a cabo esta tarea, se deben realizar evaluaciones de riesgo, tanto internas como externas, para detectar posibles amenazas y vulnerabilidades. Además, se pueden utilizar herramientas y técnicas de análisis de seguridad, como pruebas de penetración y escaneos de vulnerabilidades, que nos ayudarán a identificar las posibles brechas en nuestros sistemas. Una vez identificados los riesgos y vulnerabilidades, se podrán implementar las medidas necesarias para mitigarlos y garantizar la protección de la información de la organización (Cando, 2024; Castillo, 2023).

Desarrollo de políticas y procedimientos de seguridad

El desarrollo de políticas y procedimientos de seguridad es fundamental para establecer una cultura sólida de seguridad de la información en una organización. Estas

políticas deben ser diseñadas de manera integral y considerar todos los aspectos relevantes, como la clasificación de la información, el acceso y la protección de los activos, la gestión de contraseñas y la seguridad en el uso de dispositivos móviles, entre otros. Además, es importante que los procedimientos sean claros y detallados, especificando las medidas técnicas y operativas necesarias para garantizar la seguridad de la información. Estos documentos deben ser comunicados y distribuidos a todos los miembros de la organización, quienes deben comprometerse a cumplir con las políticas y procedimientos establecidos. Además, debe establecerse un proceso de revisión y actualización periódica de estas políticas y procedimientos, para garantizar que estén alineados con las nuevas amenazas y los cambios en el entorno de seguridad (Muñoz, 2021; Montalbán et al., 2020; Valencia, 2021).

Capacitación y concienciación del personal

La capacitación y la concienciación del personal son aspectos fundamentales para alcanzar una cultura en seguridad de la información. Es vital brindar a todos los empleados una formación adecuada en temas de seguridad informática, incluyendo conceptos básicos de protección de datos, manejo seguro de contraseñas, prevención de ataques cibernéticos y buenas prácticas en el uso de los sistemas y recursos tecnológicos. Además, es importante concienciar sobre los derechos y responsabilidades del personal en relación con la seguridad de la información, promoviendo la importancia de mantener la confidencialidad, integridad y disponibilidad de los datos. Para asegurar el cumplimiento de estas medidas, se deben llevar a cabo programas de capacitación regulares y actualizados, que incluyan evaluaciones periódicas para medir el nivel de conocimiento y promover la mejora continua en la cultura de seguridad. (Fong & Bayona, 2022; Barcia, 2023; Arpi & Cajamarca, 2023).

Evaluación y mejora continua del sistema de seguridad

La evaluación y mejora continua del sistema de seguridad de la información es fundamental para garantizar su efectividad y eficiencia a lo largo del tiempo. Para ello, es necesario realizar auditorías periódicas que permitan identificar posibles fallos o debilidades en el sistema. Estas auditorías deben ser realizadas tanto de forma interna como externa, por profesionales con experiencia en seguridad de la información. Deben seguirse estándares reconocidos internacionalmente, como ISO 27001, para evaluar el grado de cumplimiento de los controles y medidas de seguridad implementados. Además, es importante tener en cuenta las nuevas

amenazas y vulnerabilidades que van surgiendo y adaptar el sistema de seguridad en consecuencia. Para lograr una mejora continua, deben establecerse indicadores y métricas que permitan medir la eficacia del sistema y realizar acciones correctivas cuando se detecten desviaciones. Es recomendable también llevar a cabo simulacros y pruebas de seguridad de forma regular, para evaluar la capacidad de respuesta y detectar posibles áreas de mejora. En resumen, la evaluación y mejora continua del sistema de seguridad de la información es un proceso esencial para mantener la protección de los activos y garantizar la confidencialidad, integridad y disponibilidad de la información (Sepúlveda & Medina, 2024; Sánchez et al., 2023; Bedoya & Patiño, 2023).

Por último, los individuos son fundamentales para que tengan éxito los programas de cultura organizacional en seguridad, ya que desde el rol que cada uno desempeña le aporta de manera positiva o negativa a la organización; por esto los programas de concienciación y sensibilización son importantes para las empresas, ya que con estos se reducen los riesgos y vulnerabilidades que pueden llegar a sufrir las entidades.

Filosofía del ciberdelito

El ciberdelito se define como una actividad delictiva que se lleva a cabo en el ámbito digital, utilizando las tecnologías de la información y las comunicaciones como herramientas para cometer delitos (Saín, 2018). Estos delitos pueden incluir el robo de datos personales o financieros, la falsificación de identidades, el acceso no autorizado a sistemas informáticos y la difusión de contenido ilegal, entre otros. El cibercrimen se caracteriza por su naturaleza global, ya que puede ser perpetrado desde cualquier lugar del mundo, y por su capacidad de causar daños a gran escala tanto a nivel individual, como en la sociedad en su conjunto.

El cibercrimen presenta diversas características que lo distinguen de otros tipos de delitos. En primer lugar, se lleva a cabo de forma encubierta, aprovechando la relativa anonimidad que proporciona internet. Además, el cibercrimen es altamente sofisticado, ya que requiere conocimientos especializados en tecnología de la información y habilidades técnicas avanzadas. Asimismo, el ciberdelito es un fenómeno en constante evolución, con los ciberdelincuentes que adaptan sus métodos y técnicas para eludir las medidas de seguridad. Por último, el cibercrimen puede tener un alcance global casi ilimitado, ya que internet permite a los delincuentes operar en diferentes países y afectar a personas de todo el mundo (Incibe-Cert, 2020).

El ciberdelito tiene un impacto significativo en la sociedad en múltiples niveles. A nivel individual, puede causar la pérdida de datos personales y financieros, así como el deterioro de la privacidad y la seguridad en línea. A nivel empresarial, el cibercrimen puede resultar en brechas de seguridad, pérdida de clientes y daños a la reputación de las organizaciones. A nivel societal, el ciberdelito puede afectar la confianza en las instituciones, socavar la economía digital y generar costos significativos tanto para los Gobiernos, como para los ciudadanos (Cano, 2011). Además, el cibercrimen puede contribuir a la propagación de la desinformación, el aumento de la brecha digital y la exacerbación de la desigualdad. Por lo tanto, es importante abordar el cibercrimen de manera efectiva para proteger a los individuos y salvaguardar el bienestar de la sociedad en su conjunto.

La filosofía del ciberdelito se encarga de analizar y reflexionar sobre los aspectos fundamentales relacionados con este fenómeno delictivo. Se abordan diferentes aspectos como el origen y la evolución del cibercrimen, las motivaciones de los ciberdelincuentes, la ética y moral involucradas en estas prácticas y las implicaciones filosóficas que surgen a raíz de este tipo de delito (Creese et al., 2020). Con un enfoque crítico y reflexivo, se busca comprender las dimensiones éticas, morales y filosóficas que están presentes en el ciberdelito y su influencia en la sociedad actual (Sáinz, 2016).

La lucha contra el ciberdelito enfrenta constantes retos y desafíos debido al rápido avance tecnológico y a la sofisticación de las técnicas utilizadas por los ciberdelincuentes. El aumento de la conectividad y la digitalización de diversos ámbitos de la sociedad brindan nuevas oportunidades para la comisión de delitos en línea. Los ciberdelincuentes se adaptan constantemente, mejorando sus técnicas y aprovechando vulnerabilidades emergentes. Además, el anonimato y la falta de una jurisdicción única dificultan la persecución y captura de los responsables (Saín, 2018). Otros desafíos incluyen la falta de conciencia y capacitación en seguridad cibernética en diversos sectores, la escasez de expertos en ciberseguridad y la necesidad de recursos financieros para combatir eficazmente el cibercrimen. Superar estos retos requiere de una respuesta colectiva y una constante adaptación a las nuevas amenazas y escenarios para combatirlo.

Con el desarrollo de internet, se han creado condiciones favorables para quienes persiguen intereses personales a expensas de los usuarios de la red. Los efectos resultantes tienen características comunes, como un entorno de asesino en serie y bajos niveles de acoso. El delito se puede cometer en cualquier parte del mundo con acceso a internet y puede afectar a organizaciones o individuos en cualquier lugar, otorgando a los delincuentes un nivel de riesgo, eficiencia y eficacia

de alto impacto, fácil de implementar y anónimo. En algunos casos, no es necesario un conocimiento profundo del autor para cometer un delito cibernético, en tal sentido, el Foro Económico Mundial enumera los principales fallos de infraestructura, los ciberataques y el fraude o robo de datos (que implica el robo de datos personales), como las diez principales amenazas globales (World Economic Forum [WEF], 2013).

Retos en materia de ciberseguridad

En la actualidad, las amenazas cibernéticas están en constante evolución y representan un desafío cada vez mayor para la seguridad digital. Las técnicas de ataque utilizadas por los ciberdelincuentes son cada vez más sofisticadas y pueden afectar tanto a individuos como a organizaciones (Incibe-Cert, 2020). Algunas de las amenazas cibernéticas más comunes incluyen el *phishing,* el *malware*, el *ransomware* y los ataques de denegación de servicio. Estos ataques pueden tener consecuencias devastadoras, como la pérdida de datos confidenciales, el robo de información personal o financiera y el daño a la reputación de una empresa. Para hacer frente a estas amenazas, es fundamental contar con medidas de seguridad adecuadas, como el uso de *software* antivirus, la autenticación de dos factores y la educación en ciberseguridad para garantizar la protección de los sistemas y datos digitales (Mijares, 2020).

Las vulnerabilidades en las infraestructuras digitales representan un desafío significativo en materia de ciberseguridad. Estas vulnerabilidades pueden surgir debido a diversas razones, como el uso de sistemas obsoletos o desactualizados, la falta de parches de seguridad, la implementación inadecuada de medidas de protección y la falta de concienciación sobre las amenazas cibernéticas. Además, las infraestructuras digitales a menudo están interconectadas, lo que significa que la vulnerabilidad de un sistema puede afectar otros sistemas. Esto resalta la importancia de implementar medidas de seguridad sólidas y actualizadas en todas las capas de la infraestructura digital, desde los servidores y la red hasta los dispositivos finales (Pérez et al., 2012). Asimismo, es crucial hacer evaluaciones periódicas de vulnerabilidades y realizar las correcciones necesarias para mitigar los riesgos y fortalecer la seguridad en las infraestructuras digitales.

Las estrategias de protección de datos juegan un papel fundamental en la ciberseguridad. Para garantizar la seguridad de la información, es imprescindible implementar medidas como el cifrado de datos, el uso de *firewalls* y sistemas de

detección de intrusiones y aplicar políticas robustas de contraseñas. Además, es importante realizar copias de seguridad periódicas y contar con un plan de respuesta a incidentes que permita actuar de manera rápida y efectiva ante cualquier eventualidad. Otras estrategias incluyen la segmentación de redes, la autenticación de dos factores y el monitoreo constante de la actividad de los usuarios. Asimismo, la implementación de herramientas de gestión de identidad y acceso puede ayudar a prevenir el acceso no autorizado a los sistemas. En resumen, contar con una estrategia integral de protección de datos es esencial para mitigar los riesgos y proteger la información frente a posibles ciberataques (IT Trends, 2019).

El rol de los Gobiernos en la ciberseguridad es fundamental para proteger y garantizar la seguridad de los ciudadanos y las organizaciones frente a las amenazas cibernéticas. Los Gobiernos tienen la responsabilidad de establecer y hacer cumplir leyes y regulaciones que promuevan la protección de los sistemas de información y la privacidad de los datos. Además, deben promover la cooperación y colaboración entre los sectores público y privado, facilitando el intercambio de información y el desarrollo de buenas prácticas en ciberseguridad (Ibarra & Igartua, 2018). Asimismo, los Gobiernos deben invertir en la formación y capacitación de profesionales en ciberseguridad, para estar preparados frente a los nuevos desafíos tecnológicos. Además, es importante que los Gobiernos promuevan la investigación y desarrollo de tecnologías y herramientas avanzadas que puedan ayudar a prevenir y detectar ataques cibernéticos. En resumen, el rol de los Gobiernos en la ciberseguridad es esencial para proteger a la sociedad y fomentar un entorno digital seguro y confiable (Evans & Farrell, 2020).

La educación y la concienciación sobre ciberseguridad desempeñan un papel fundamental en la protección de individuos y organizaciones ante las amenazas cibernéticas. Mediante programas educativos y campañas de concienciación, se busca informar a las personas acerca de las diversas formas en que pueden ser víctimas de ciberataques y cómo pueden prevenirlos. Estos programas incluyen la enseñanza de prácticas seguras en el uso de internet, el correo electrónico y las redes sociales, así como la promoción de la importancia de mantener actualizados los sistemas operativos y el *software* de seguridad. Además, se destacan los riesgos asociados con el uso de contraseñas débiles y la compartición de información personal en línea. La concienciación sobre ciberseguridad también se extiende a las empresas, fomentando la implementación de políticas internas de seguridad, la capacitación del personal y la creación de una cultura organizacional que priorice la protección de la información digital (Deloitte et al., 2013). Algunos ejemplos frente a estos retos son:

Avances y políticas en Estados Unidos

En EE. UU., se han implementado diversas iniciativas y legislaciones para abordar los desafíos en materia de ciberseguridad. Un ejemplo destacado es la Ley de Modernización de la Infraestructura de Investigación e Innovación (MIIRIA, por sus siglas en inglés), que incluye disposiciones para fortalecer la ciberseguridad en instituciones de investigación y desarrollo financiadas por el gobierno federal. Además, la Estrategia Nacional de Ciberseguridad, lanzada en 2018, establece un marco integral para proteger la infraestructura crítica y fortalecer la resiliencia cibernética del país.

Avances y políticas en la Unión Europea

En la UE, se ha adoptado un enfoque coordinado para mejorar la ciberseguridad en toda la región. El Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés), implementado en 2018, establece estándares rigurosos para la protección de datos personales y obliga a las organizaciones a tomar medidas proactivas para garantizar la seguridad de la información. Además, la Estrategia de Ciberseguridad de la Unión Europea, lanzada en 2013 y actualizada en 2020, promueve la cooperación entre los Estados miembro y el sector privado para abordar las amenazas cibernéticas de manera efectiva.

Avances y políticas en China

China ha establecido una serie de regulaciones y leyes para fortalecer su postura en ciberseguridad. Por ejemplo, la Ley de Seguridad Cibernética de China, implementada en 2017, establece requisitos para proteger la infraestructura crítica y regular el manejo de datos personales. Además, el Plan de Acción para la Seguridad de la Información Nacional de China, lanzado en 2019, establece objetivos y medidas para mejorar la seguridad cibernética en el país.

Avances y políticas en Japón

Japón ha desarrollado una serie de iniciativas para fortalecer su capacidad en ciberseguridad. La Estrategia de Ciberseguridad de Japón, lanzada en 2015 y actualizada en 2020, establece objetivos y medidas para proteger la infraestructura crítica y promover la colaboración entre el Gobierno, el sector privado y la academia. Además, la Ley de Protección de la Información Personal de Japón, implementada en 2005 y enmendada en 2015, establece estándares para el manejo seguro de datos personales.

Avances y políticas en Australia

Australia ha desarrollado una serie de iniciativas para fortalecer su capacidad en ciberseguridad. Por ejemplo, el Gobierno australiano lanzó la Estrategia de Ciberseguridad de Australia en 2020, que incluye inversiones significativas en infraestructura de ciberseguridad y capacidades de defensa cibernética. Además, la Ley de Notificación de Brechas de Seguridad de Datos de Australia, implementada en 2018, requiere que las organizaciones notifiquen a las autoridades y a los individuos afectados en caso de una violación de seguridad de datos.

Eslabones débiles

En la actualidad, la ciberseguridad se ha convertido en un tema de vital importancia para las organizaciones. Además de proteger la información confidencial de la empresa y los datos de los clientes, la ciberseguridad también juega un papel fundamental en la protección contra amenazas externas. La creciente dependencia de la tecnología en el entorno empresarial ha aumentado la vulnerabilidad de las organizaciones a ataques cibernéticos, lo que resalta la necesidad de implementar medidas de seguridad adecuadas. La falta de ciberseguridad puede tener consecuencias devastadoras, como el robo de información sensible, la interrupción de los procesos comerciales y la pérdida de la confianza de los clientes. Por lo tanto, es fundamental que las organizaciones reconozcan la importancia de invertir en la ciberseguridad para proteger sus activos y mantener la continuidad del negocio.

Las organizaciones enfrentan diversas amenazas comunes en materia de ciberseguridad. Una de ellas es el *phishing,* en que los atacantes intentan obtener información confidencial haciéndose pasar por entidades de confianza. También están los ataques de *malware,* que pueden infectar los sistemas de la organización y comprometer la integridad de los datos. Otro tipo de amenaza es el *ransomware*, con que los ciberdelincuentes bloquean el acceso a los archivos y exigen un rescate para su liberación. Además, los ataques de fuerza bruta son frecuentes, utilizando programas que intentan adivinar contraseñas para acceder a sistemas o cuentas. Por último, las organizaciones también deben preocuparse por los ataques de denegación de servicio, donde se intenta sobrecargar un sitio web o servicio para que no sea accesible para los usuarios legítimos. Es esencial que las organizaciones estén preparadas y tomen medidas preventivas para mitigar estas amenazas y proteger sus sistemas y datos.

Existen varios factores que pueden debilitar la ciberseguridad en las organizaciones. Uno de ellos es la falta de conciencia y formación en seguridad cibernética por parte de los empleados. Muchas veces, los trabajadores desconocen las buenas prácticas de seguridad o caen en trampas de *phishing* y otros ataques. Otro factor es la falta de actualización de los sistemas y aplicaciones utilizadas. Si las organizaciones no instalan los últimos parches y actualizaciones de seguridad, están dejando vulnerabilidades abiertas a los ataques. Además, la falta de políticas y procedimientos de seguridad claros y aplicados de manera consistente puede debilitar la protección cibernética de una organización. Es necesario establecer reglas y políticas de seguridad y garantizar su cumplimiento para evitar brechas en la seguridad. En resumen, el desconocimiento, la falta de actualización y la falta de políticas claras son factores que debilitan la ciberseguridad en las organizaciones.

Los eslabones débiles en ciberseguridad en las organizaciones pueden tener graves consecuencias. Una de las principales repercusiones es el riesgo de sufrir un ciberataque. Los *hackers* pueden aprovechar estos puntos vulnerables para infiltrarse en el sistema y acceder a información confidencial. Esto puede resultar en el robo de datos, como contraseñas, números de tarjetas de crédito o información personal de clientes y empleados. Además, los eslabones débiles también pueden facilitar la propagación de *malware*, lo que puede afectar el rendimiento de los sistemas y causar daños financieros. Por otro lado, las organizaciones que no gestionan adecuadamente la seguridad de la información pueden enfrentar graves consecuencias legales y daños a su reputación en caso de filtraciones de datos. En resumen, los eslabones débiles en ciberseguridad son una amenaza seria que puede tener repercusiones financieras, legales y de reputación para las organizaciones.

Para mejorar la ciberseguridad en las organizaciones, es fundamental adoptar una serie de medidas y soluciones. En primer lugar, se recomienda implementar un sistema de monitoreo continuo de la red, que permita detectar cualquier actividad sospechosa o intento de intrusión. Asimismo, es importante contar con un programa de educación y concienciación sobre ciberseguridad, brindando capacitación a todos los miembros de la organización para que estén al tanto de las amenazas y sepan cómo actuar frente a ellas. Además, es necesario establecer políticas claras y rigurosas de gestión de contraseñas, fomentando el uso de contraseñas robustas y periódicamente actualizadas. Otra medida importante es la implementación de sistemas de autenticación de dos factores, que brinden una capa adicional de protección. Por último, se debe contar con un plan de respuesta ante incidentes de seguridad, que permita una rápida y eficiente reacción ante posibles ataques o

brechas de seguridad. Estas mejoras y soluciones son fundamentales para fortalecer la ciberseguridad en las organizaciones y proteger la integridad de los datos y sistemas.

Ciberresiliencia y concienciación en ciberseguridad

En el mundo actual, donde la tecnología y la interconectividad juegan un papel cada vez más importante en nuestra sociedad, *ciberresiliencia* y *concienciación* en ciberseguridad son dos conceptos fundamentales. En este capítulo, se analizan en detalle ambos términos, explorando su importancia y las estrategias que pueden implementarse para fortalecer la seguridad en el entorno digital. Además, se examinan las herramientas y tecnologías disponibles que pueden contribuir a la ciberresiliencia, así como las conclusiones alcanzadas tras el estudio. Este trabajo tiene como objetivo brindar un conocimiento sólido sobre temas tan relevantes y fomentar una mayor conciencia en materia de seguridad cibernética.

Importancia de la ciberresiliencia

La ciberresiliencia es un aspecto fundamental en la ciberseguridad actual. Se refiere a la capacidad de una organización para resistir, adaptarse y recuperarse frente a incidentes y ataques cibernéticos. Es indispensable para asegurar la continuidad del negocio y proteger la información confidencial. La importancia de la ciberresiliencia radica en que permite reducir los riesgos y mitigar las posibles consecuencias negativas de un ciberataque. Además, garantiza la capacidad de respuesta rápida y eficiente ante posibles incidentes, minimizando así el impacto en la organización. La implementación de estrategias de ciberresiliencia ayuda a fortalecer la seguridad de los sistemas y a mantener la confianza de los clientes y socios comerciales.

Estrategias de concienciación en ciberseguridad

Las estrategias de concienciación en ciberseguridad son fundamentales para educar y sensibilizar a las personas sobre los riesgos y amenazas que existen en el mundo digital. Una de las estrategias más efectivas es la realización de programas de formación y capacitación que brinden conocimientos prácticos sobre buenas prácticas de seguridad informática. Estos programas pueden incluir charlas,

talleres y cursos en los que se aborden temas como el uso seguro de contraseñas, la identificación de correos electrónicos y enlaces sospechosos y la protección de información personal. Otra estrategia importante es la creación de campañas de concienciación que lleguen a un público amplio por medios de comunicación, redes sociales y otros canales de difusión. Estas campañas pueden utilizar mensajes claros y directos para informar sobre los riesgos y promover el uso responsable de la tecnología. Además, se pueden implementar simulaciones de ataques cibernéticos para evaluar la capacidad de respuesta y concienciar sobre la importancia de mantenerse alerta ante posibles amenazas. En suma, las estrategias de concienciación en ciberseguridad son esenciales para fomentar una cultura de seguridad en la sociedad y reducir la incidencia de ataques cibernéticos.

En conclusión, la ciberresiliencia es de vital importancia en el mundo actual, donde los ciberataques son cada vez más frecuentes y sofisticados. Contar con estrategias de concienciación en ciberseguridad es fundamental para proteger las organizaciones de posibles amenazas y minimizar los riesgos. Además, el uso de herramientas y tecnologías adecuadas para fortalecer la ciberresiliencia es crucial. Estas herramientas pueden incluir sistemas de detección y prevención de intrusiones, cifrado de datos y sistemas de respaldo y recuperación, entre otros. Es necesario que las organizaciones inviertan en capacitación y actualización constante para estar preparadas ante cualquier eventualidad. La ciberresiliencia no solo se trata de resistir y recuperarse de los ataques, sino también de aprender de ellos y mejorar la seguridad en el futuro.

Cooperación público/privada en ciberseguridad y cultura

La cooperación entre el sector público y privado en ciberseguridad es de vital importancia debido a los crecientes desafíos relacionados con la protección de la información y los sistemas digitales. Ambos sectores poseen conocimientos y recursos únicos que, al combinarse, pueden fortalecer significativamente las defensas de ciberseguridad. El sector público cuenta con expertos en políticas y marcos regulatorios, mientras que el sector privado aporta experiencia en tecnología y adaptabilidad. Además, la colaboración permite el intercambio oportuno de información sobre amenazas y vulnerabilidades, lo que facilita la detección y respuesta temprana a incidentes de seguridad. Al trabajar juntos, el sector público y el privado pueden abordar eficazmente los desafíos de la ciberseguridad y asegurar la protección de los datos y sistemas críticos.

La colaboración entre el sector público y el privado en ciberseguridad tiene numerosos beneficios. En primer lugar, combina la experiencia y conocimientos de ambos sectores, lo que permite abordar de manera más efectiva los desafíos en materia de seguridad informática. Además, esta colaboración promueve la interoperabilidad y el intercambio de información entre las organizaciones, permitiendo una respuesta más rápida y coordinada ante amenazas cibernéticas. Asimismo, la colaboración pública-privada en ciberseguridad contribuye a fortalecer la protección de infraestructuras críticas, al poner en común recursos, tecnologías y buenas prácticas. Por último, esta colaboración también puede impulsar el desarrollo económico, al fomentar la innovación y la creación de empleo en el ámbito de la ciberseguridad.

Uno de los principales desafíos en la cooperación en ciberseguridad es la falta de confianza mutua entre el sector público y el privado. Existe una reticencia por parte de las empresas privadas a compartir información sensible con las autoridades gubernamentales por temor a la filtración de datos o a que se utilicen en su contra. Por otro lado, las instituciones públicas pueden verse limitadas en su capacidad de actuar debido a restricciones legales y burocráticas. Además, la falta de estándares y protocolos comunes dificulta la comunicación y colaboración efectiva entre ambos sectores. Asimismo, la rápida evolución de las tecnologías de la información y comunicación presenta un desafío constante, ya que las amenazas y vulnerabilidades cibernéticas evolucionan de manera rápida y compleja. Por lo tanto, es necesario superar estos desafíos y promover nuevas formas de cooperación en ciberseguridad que permitan una respuesta efectiva y coordinada ante las amenazas digitales.

La promoción de una cultura de ciberseguridad es fundamental para proteger la información y mantener la seguridad en el ámbito digital. Para lograrlo, es necesario concienciar a las personas sobre los riesgos y las buenas prácticas en materia de ciberseguridad. Esto implica proporcionar capacitación y educación en ciberseguridad, tanto a nivel individual como organizacional. Las organizaciones deben implementar programas de concienciación que incluyan la importancia de contraseñas seguras, la detección y prevención de *phishing* y la protección adecuada de datos sensibles. Además, es esencial fomentar una cultura de ciberseguridad en la sociedad en general, promoviendo la responsabilidad y el uso seguro de las tecnologías digitales.

Para fomentar la cooperación y cultura de ciberseguridad, es fundamental establecer una serie de medidas. En primer lugar, es necesario promover la formación y capacitación en ciberseguridad tanto para el sector público como para el

privado, con el objetivo de contar con personal especializado y consciente de los riesgos. Asimismo, se deben establecer programas de sensibilización y concienciación dirigidos a la sociedad en general, para que los ciudadanos estén informados y adopten prácticas seguras en su vida digital. Además, es importante facilitar la colaboración y el intercambio de información entre ambas partes, mediante la creación de plataformas y redes de cooperación. Estas plataformas permitirán compartir buenas prácticas, conocimientos y alertas de seguridad de manera ágil y efectiva. Por último, se deben establecer incentivos y reconocimientos para aquellas organizaciones y empresas que demuestren un compromiso significativo con la ciberseguridad y fomenten una cultura de protección de la información. En definitiva, estas medidas contribuirán a fortalecer la cooperación y cultura de ciberseguridad en el ámbito público y privado.

Experiencias y prácticas adecuadas

En esta sección, se presentan diversas experiencias exitosas en el ámbito de la ciberseguridad. Se abordan casos reales en que empresas e instituciones han implementado medidas efectivas para proteger su infraestructura digital y salvaguardar la confidencialidad, integridad y disponibilidad de sus datos. Se analiza cómo estas organizaciones han logrado hacer frente a las amenazas cibernéticas y fortalecer su seguridad mediante la adopción de tecnologías avanzadas, la implementación de políticas de seguridad robustas, la capacitación del personal y la colaboración con expertos en ciberseguridad. Además, se destacan los beneficios obtenidos a partir de estas experiencias exitosas, tanto a nivel de protección de información como a nivel de reputación y confianza de los clientes. Asimismo, se exploran los desafíos y obstáculos enfrentados durante el proceso de implementación, así como las lecciones aprendidas que pueden ser útiles para otras organizaciones interesadas en mejorar su seguridad digital (Goundar et al., 2021; Pérez et al., 2018; Vial, 2019).

En el ámbito de la transformación digital, es vital seguir una serie de prácticas recomendadas para asegurar el éxito y maximizar los beneficios de este proceso. En primer lugar, es fundamental establecer una estrategia clara y definida que defina los objetivos y metas que se desean alcanzar con la transformación digital. Además, es esencial contar con el apoyo y liderazgo del equipo directivo para asegurar la implicación de todos los miembros de la organización (Schmitt, 2018). Otro aspecto importante es realizar un análisis exhaustivo de los procesos y sistemas existentes, identificando las áreas de mejora y los posibles obstáculos

que pueden surgir durante el proceso de transformación. Es recomendable también utilizar herramientas tecnológicas y soluciones innovadoras que faciliten la automatización y optimización de los procesos. Por último, es crucial contar con un plan de capacitación y formación en nuevas tecnologías y habilidades digitales para garantizar que todos los miembros de la organización estén preparados para adaptarse a los cambios y aprovechar al máximo las oportunidades que ofrece la transformación digital (Patiño, 2018; Teslia et al., 2016).

La implementación de ciberseguridad presenta una serie de desafíos y riesgos que es importante tener en cuenta. En primer lugar, uno de los principales desafíos se relaciona con la adaptabilidad y actualización constante de las medidas de seguridad. Los avances tecnológicos y las nuevas amenazas cibernéticas demandan que las organizaciones estén constantemente al tanto de los cambios y actualicen sus sistemas de seguridad de manera efectiva. Otro desafío se relaciona con la falta de conciencia y educación en ciberseguridad. Muchos empleados carecen de conocimientos básicos sobre cómo reconocer y evitar ataques cibernéticos, lo que puede poner en riesgo la seguridad de la empresa. Además, la implementación de ciberseguridad también puede enfrentar desafíos técnicos, como la integración de diferentes sistemas y la gestión de datos de manera segura. Es fundamental abordar estos desafíos y riesgos con estrategias efectivas y priorizar la protección de la infraestructura digital de las organizaciones.

Tecnologías comerciales para la ciberseguridad

En el mundo digital actual, la ciberseguridad se ha convertido en una prioridad ineludible para empresas y Gobiernos. Con el aumento de los ataques cibernéticos, la demanda de tecnologías avanzadas y soluciones robustas para proteger los sistemas y los datos es más alta que nunca. Entre las tecnologías comerciales empleadas hoy en ciberseguridad, según Palo Alto Networks (2023), figuran:

Autenticación y gestión de identidades

Tecnologías utilizadas

Autenticación Multifactor (MFA): tecnología esencial que añade capas adicionales de seguridad requiriendo múltiples formas de verificación antes de conceder

acceso al usuario. Ejemplo de uso: las instituciones financieras utilizan MFA para proteger las cuentas de usuario, combinando contraseñas con un código temporal enviado a un dispositivo móvil del usuario.

Gestión de Identidad y Acceso (IAM): soluciones como Okta o Microsoft Azure Active Directory que permiten a las organizaciones gestionar y monitorear identidades de usuario y sus accesos a diferentes recursos corporativos. Ejemplo de uso: las empresas implementan IAM para asegurar que solo los empleados autorizados puedan acceder a sistemas críticos y datos sensibles.

Cifrado

Tecnologías utilizadas

Cifrado de datos en reposo y en tránsito: utilización de algoritmos como AES y RSA para cifrar datos, asegurando que la información sea inaccesible durante la transferencia o almacenamiento. Ejemplo de uso: los servicios de almacenamiento en la nube utilizan cifrado para proteger los datos de los usuarios almacenados en sus servidores.

Seguridad de red

Tecnologías utilizadas

Firewalls de próxima generación y sistemas de prevención de intrusiones (IPS): herramientas como Cisco Firepower o Palo Alto Networks que monitorean el tráfico de red y bloquean actividades sospechosas. Ejemplo de uso: las organizaciones utilizan IPS para detectar y prevenir ataques automatizados y otras amenazas de red.

Red privada virtual (VPN): permite a los usuarios establecer una conexión segura y cifrada a una red corporativa desde una ubicación remota. Ejemplo de uso: durante el trabajo remoto, los empleados utilizan VPN para acceder a recursos internos de la empresa de manera segura.

Análisis de seguridad y respuesta a incidentes

Tecnologías utilizadas

Herramientas de detección y respuesta extendida (XDR): plataformas como SentinelOne o CrowdStrike que proporcionan visibilidad completa mediante los *endpoints*, red y servidores, facilitando la detección rápida de amenazas y la respuesta

automatizada. Ejemplo de uso: las empresas de tecnología implementan XDR para detectar comportamientos anómalos en tiempo real y responder a incidentes de seguridad de manera automatizada.

Tecnologías emergentes: su impacto en la ciberseguridad para la transformación digital

Inteligencia artificial en ciberseguridad

La inteligencia artificial (IA) está transformando la ciberseguridad, ofreciendo nuevas formas de detectar y responder a amenazas en tiempo real. La IA puede analizar grandes volúmenes de datos para identificar patrones y comportamientos sospechosos, lo que permite una detección de amenazas más rápida y precisa que los métodos tradicionales. Además, los sistemas de IA se utilizan para automatizar respuestas a incidentes de seguridad, lo que reduce la carga sobre los equipos de ciberseguridad y mejora la eficacia de las respuestas (Morgan, 2021).

Internet de las cosas

La internet de las Cosas (IoT, por sus siglas en inglés) representa un desafío significativo para la ciberseguridad debido a la gran cantidad y diversidad de dispositivos conectados, muchos de los cuales no diseñados con la seguridad como prioridad. Esto aumenta la superficie de ataque y presenta vulnerabilidades únicas en redes corporativas y de consumidores. Las tecnologías de ciberseguridad para IoT deben abordar desde la seguridad del dispositivo hasta la protección de la red y los datos transmitidos, asegurando la integridad de sistemas cada vez más interconectados (Weber, 2023).

Computación en la nube

La computación en la nube ha permitido a las empresas escalar recursos y mejorar la eficiencia, pero también ha introducido nuevos riesgos de ciberseguridad, como la configuración incorrecta de los entornos en la nube que pueden exponer datos sensibles. Las soluciones de seguridad en la nube, como los *firewalls* de aplicaciones web y las herramientas de gestión de identidad y acceso, son cruciales para proteger los datos alojados en servicios en la nube (Jackson, 2022).

Big data y ciberseguridad

Big data (macrodatos) ofrece oportunidades significativas para mejorar la ciberseguridad mediante el análisis de enormes conjuntos de datos para detectar anomalías y tendencias de ataques. Sin embargo, también plantea desafíos en términos de proteger y gestionar estos grandes volúmenes de datos. Las tecnologías emergentes en macrodatos requieren robustas medidas de seguridad, incluyendo el cifrado avanzado y soluciones específicas para la protección de datos a gran escala (Thompson, 2023).

Para ilustrar los conceptos descritos, se presentan los diagramas que explican cada tecnología emergente mencionada y su impacto en la ciberseguridad para la transformación digital. Estos diagramas incluyen detalles sobre IA, IoT, computación en la nube y *big data,* cada uno resaltando cómo estas tecnologías se utilizan para fortalecer la seguridad en un entorno digital. La descripción y uso de cada uno se presenta en la Tabla 1.

Tabla 1. *Descripción y uso de tecnologías emergentes en la transformación digital*

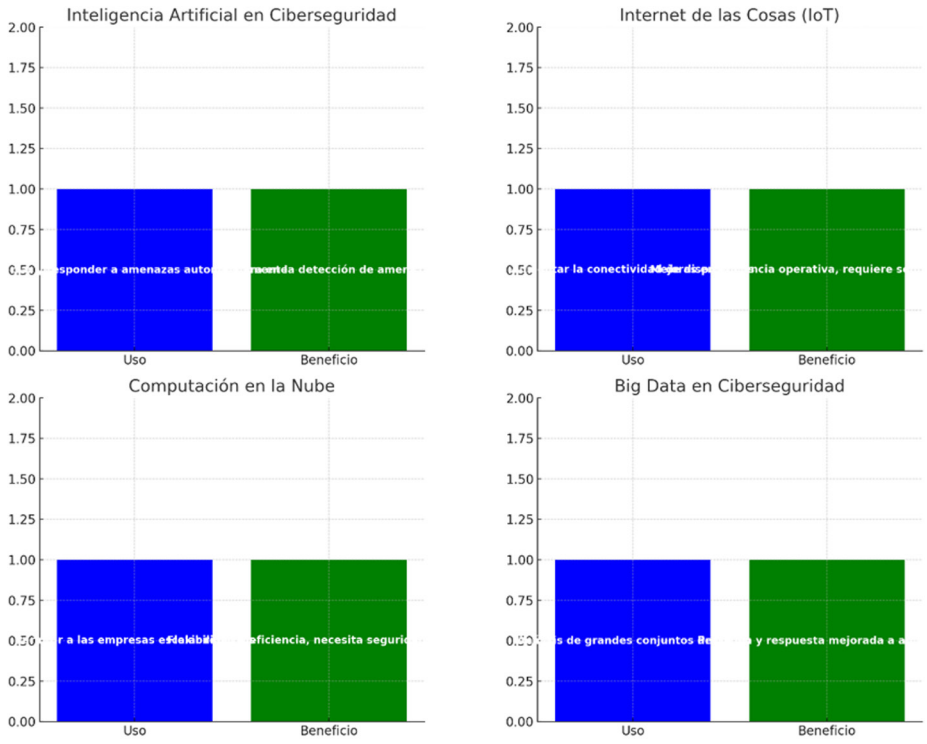
Tecnología	Uso	Beneficio
IA en ciberseguridad	Detectar y responder a amenazas automáticamente mediante el análisis de grandes volúmenes de datos para identificar patrones de comportamiento anómalo.	Mejora la velocidad y la precisión en la detección de amenazas.
IoT	Aumentar la conectividad de dispositivos, pero incrementa la superficie de ataque debido a la diversidad y cantidad de dispositivos conectados.	Mejora la eficiencia operativa, pero requiere robustas medidas de seguridad para proteger redes corporativas y de consumidores.
Computación en la nube	Permite a las empresas escalar recursos y mejorar eficiencias, pero introduce nuevos riesgos como la configuración inadecuada que puede exponer datos sensibles.	Flexibilidad y eficiencia con la necesidad de implementar soluciones de seguridad específicas para la nube.
Big data	Análisis de grandes conjuntos de datos para detectar amenazas y anomalías, enfrentando desafíos para proteger y gestionar esos datos.	Capacidad mejorada para prever y responder a amenazas cibernéticas mediante la identificación de tendencias a partir de grandes volúmenes de información.

Fuente: elaboración propia.

La figura 1 muestra el impacto de las tecnologías emergentes en ciberseguridad para la transformación digital. Cada diagrama destaca la aplicación y el

beneficio principal de las siguientes tecnologías: 1) IA en ciberseguridad: utilizada para detectar y responder automáticamente a amenazas, mejorando la velocidad y precisión en la detección; 2) IoT: aumenta la conectividad de dispositivos, lo que requiere robustas medidas de seguridad para proteger redes ampliadas; 3) computación en la nube: permite a las empresas escalar recursos, necesitando soluciones de seguridad específicas para proteger datos en entornos en la nube, y 4) *Big data* en ciberseguridad: utiliza el análisis de grandes volúmenes de datos para detectar tendencias y amenazas, mejorando la capacidad de previsión y respuesta.

Figura 1. *Diagramas de impacto de las tecnologías emergentes en ciberseguridad*



Fuente: elaboración propia.

En los diagramas de la Figura 1 se utilizan barras para representar dos categorías principales: "uso" y "beneficio" de cada tecnología. Enseguida, la función de cada eje en los diagramas:

Eje X (horizontal): representa las categorías comparadas para cada tecnología. En este caso, el eje X tiene dos categorías etiquetadas como "uso" y "beneficio".

Estas categorías se utilizan para describir cómo se usa cada tecnología en ciberseguridad y qué beneficio principal aporta.

Eje Y (vertical): muestra una escala de medición para los valores comparados. En los diagramas proporcionados, el eje Y no representa una escala cuantitativa tradicional, sino que se usa más como un método para organizar visualmente la información. Las barras tienen la misma altura, ya que el objetivo es destacar la información textual dentro de ellas, no medir cantidades.

Cada barra en el diagrama tiene un color diferente para distinguir entre el uso y el beneficio de cada tecnología. La información en las barras proporciona detalles específicos sobre cómo cada tecnología se aplica en el contexto de ciberseguridad y los beneficios que ofrece. Esto ayuda a entender visualmente la contribución de cada tecnología a la seguridad digital en la era de la transformación digital.

Conclusiones

Los estudios de prospectiva son fundamentales para la generación de políticas y estrategias que permitan minimizar los riesgos que pueden presentarse en las organizaciones y que permitan a futuro tomar mejores decisiones. Para que esto se logre, debe darse un trabajo interactivo en el cual se involucren todos los interesados, se logren construir proyectos futuristas y se mejoren los procesos existentes.

La sensibilización sobre la ciberseguridad es una actividad continua que debe comenzar en el nivel de educación primaria e involucrar a todos los ciudadanos. Sin duda, esto beneficiará claramente a las personas y al lugar de trabajo y, en última instancia, conducirá a una nación ciberresiliente.

La utilización de la prospectiva estratégica es la mejor opción para que las entidades estén preparadas para los cambios futuros, tanto sociales como políticos y económicos y que puedan responder a estos. Es decir, la generación de planes estratégicos permite a las empresas tener una respuesta resiliente frente a los posibles cambios que se puedan presentar. Lo anterior no quiere decir que al generar prospectiva estratégica se va a solucionar el futuro, pero esta sí va a permitir minimizar muchos riesgos y amenazas que puede sufrir una organización.

Es aquí donde la generación de conocimiento e innovación juega un papel importante en la previsión en la ciberseguridad y la integración de todos los actores involucrados, para que la generación de esta planeación conlleve mejoras en los procesos y, en el caso de la ciberseguridad, sirva de guía para minimizar los riesgos y amenazas que traen consigo las tecnologías emergentes.

La construcción de un ente con estas particularidades presenta desafíos evidentes. En primer lugar, requiere que la administración proporcione recursos especializados en diversas áreas, tales como comunicación pública, ciberseguridad y asesoría legal. En segundo lugar, requiere establecer acuerdos y llevarlos a la práctica. Por último, requiere una inversión adecuada para garantizar el éxito de esta compañía.

A pesar de los retos que conlleva, los beneficios a largo plazo de esta iniciativa son evidentes. Un ejemplo de esto es el enfoque adoptado por la Unión Europea para impulsar la inversión en I+D+i dentro del marco de Horizonte 2020. Existen varias asociaciones público-privadas (PPP), especialmente en el ámbito de la ciberseguridad, con el objetivo de orientar la inversión hacia los intereses y necesidades de los sectores productivos.

No obstante, el conocimiento individual sobre ciberseguridad no es suficiente. Es imperativo que las personas se comprometan de manera efectiva con sus empresas y naciones. En el ámbito laboral, las empresas y organizaciones deben brindar a los empleados un sentido de pertenencia, seguridad laboral, identidad grupal e incluso un propósito compartido, además de ofrecer valores agregados más allá de la remuneración económica directa. A nivel nacional, es fundamental informar a los ciudadanos de que su seguridad cibernética personal contribuye a la seguridad nacional.

En conclusión, para mejorar nuestra cultura global de ciberseguridad, es esencial: 1) tener en cuenta el factor humano; 2) disponer del respaldo institucional y los recursos necesarios para implementar los planes requeridos y coordinarlos con los intereses estatales, y 3) reunir a todos los interesados en una asociación público-privada para definir las estrategias de trabajo más adecuadas que garanticen el éxito.

La transformación digital y la ciberseguridad continuarán evolucionando en el futuro a medida que las tecnologías avanzan y las amenazas cibernéticas se vuelven más sofisticadas. Las organizaciones deberán adaptarse a nuevas tendencias y desafíos para proteger su infraestructura digital. Dos áreas clave en esta evolución son la inteligencia artificial (IA) y el *machine learning* (ML) en la seguridad digital. La IA y el ML permiten a las soluciones de ciberseguridad ser más proactivas y eficientes al detectar y mitigar amenazas en tiempo real. Estas tecnologías pueden analizar grandes cantidades de datos de forma automatizada, identificando patrones y anomalías para anticiparse a futuros ataques. Su aplicación en la seguridad digital será fundamental en la lucha contra los ciberdelincuentes.

Inteligencia artificial y *machine learning* en la seguridad digital

La inteligencia artificial (IA) y el machine learning (ML) están revolucionando la seguridad digital. Estas tecnologías permiten a los sistemas de ciberseguridad aprender y adaptarse de forma autónoma, sin necesidad de intervención humana constante. La IA y el ML analizan datos en tiempo real, identifican patrones y comportamientos anómalos y generan alertas ante posibles amenazas. Además, pueden predecir y anticiparse a futuros ataques, brindando una mayor protección en un entorno cibernético en constante evolución. Estas capacidades avanzadas hacen que la IA y el ML sean herramientas esenciales para la seguridad digital, permitiendo una detección temprana y una respuesta rápida a las amenazas.

Internet de las cosas y su impacto en la ciberseguridad

La IoT es una tendencia en la transformación digital que está generando un gran impacto en la ciberseguridad. Con la creciente interconexión de dispositivos y sistemas, surge la necesidad de proteger no solo los equipos informáticos, sino también los objetos cotidianos que forman parte de la vida diaria. Los dispositivos IoT están expuestos a amenazas cibernéticas, como el acceso no autorizado, la interceptación de datos o la manipulación remota. Para mitigar estos riesgos, se deben implementar medidas de seguridad adecuadas, como el cifrado de datos, la autenticación fuerte y la segmentación de redes. Además, el monitoreo y la gestión de la seguridad de los dispositivos IoT se vuelven fundamentales para garantizar una transformación digital segura y confiable en un entorno conectado.

Las tecnologías de ciberseguridad discutidas son fundamentales para proteger las infraestructuras críticas y los datos valiosos en el entorno digital actual. Su implementación adecuada puede significar la diferencia entre la seguridad y la vulnerabilidad en el panorama de amenazas en constante evolución.

Referencias

Arpi-Saquipay, W. A., & Cajamarca-Criollo, O. A. (2023). Análisis de riesgos de seguridad de la información en una Institución de Educación Superior en Ecuador, basado en la Norma ISO 27002 Anexo A dominio 7. *MQRInvestigar, 7*(3), 2793-2808. https://doi.org/10.56048/MQR20225.7.3.2023.2793-2808

Banco Interamericano de Desarrollo. (2020). *Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe*. Banco Interamericano de Desarrollo; Organización de Estados Americanos. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Barcia Baque, G. A. (2023). *Implementación del estándar ISO/IEC 27001 para la seguridad de la información en la Unidad Educativa Fiscal Cultura Machalilla* [Tesis de pregrado, Universidad Estatal del Sur de Manabí]. Repositorio UNESUM. https://repositorio.unesum.edu.ec/bitstream/53000/5917/1/BARCIA%20BAQUE%20GABRIEL%20ALEXANDER.pdf

Bedoya Velásquez, J. E., & Patiño Castrillón, J. I. (2023). *Plan estratégico para la identificación de riesgos y vulnerabilidades en la seguridad de la información de los datos personales en una empresa* [Tesis de pregrado, Tecnológico de Antioquia]. Repositorio TDEA. https://n9.cl/25ntkg

Cando Cando, E. D. (2024). *Propuesta de mejora de seguridad de la información digital a desarrollarse en el centro de mediación Online Dispute Resolution Quito-Rumipamba, Ecuador* [Tesis de maestría, Escuela de Posgrados Newman]. Repositorio EPNEWMAN. https://repositorio.epnewman.edu.pe/bitstream/handle/20.500.12892/929/rev_trabajo_obtencion_de_grado_edwin_daniel_cando_cando_epnewman_invest_aplicada.pdf?sequence=1&isAllowed=y

Cano, J. (2011). Ciberseguridad y ciberdefensa: Dos tendencias emergentes en un contexto global. *Sistemas,* (119), 4-7. https://acis.org.co/archivos/Revista/119/Editorial.pdf

Cano, J. (2015, 13 de diciembre). Cultura organizacional de seguridad de la información. Más allá de las implementaciones tecnológicas. https://insecurityit.blogspot.com/2015/12/cultura-organizacional-de-seguridad-de.html

Cano. J. (2016). Modelo de madurez de cultura organizacional de seguridad de la información: Una visión desde el pensamiento sistémico. En P. Ll. Ferrer Gomila & M. F. Hinarejos Campos, *Actas de la XIV Reunión Española sobre Criptología y Seguridad de la Información* (pp. 24-29). https://www.researchgate.net/publication/309717795_Modelo_de_madurez_de_cultura_organizacional_de_seguridad_de_la_informacion_Una_vision_desde_el_pensamiento_sistemico-cibernetico

Castillo Accarapi, W. (2023). *Sistema de gestión de la seguridad de la información utilizando la metodología Magerit en las redes informáticas de la Empresa Electronic Mihaba* [Tesis de pregrado, Universidad Andina Néstor Cáceres Velásquez]. Repositorio UANCV. https://repositorio.uancv.edu.pe/server/api/core/bitstreams/3142acc5-a69d-4fb8-8109-8705189e6ec0/content

Cisco. (2023). *Cisco Firepower.* https://www.cisco.com/

Evans, M., & Farrell, P. (2020). Barriers to integrating Building Information Modelling (BIM) and lean construction practices on construction mega-projects: A Delphi study. *Benchmarking: An International Journal, 28*(2), 652-669. https://doi.org/10.1108/BIJ-04-2020-0169

Fong, N., & Bayona-Oré, S. (2022). Consideraciones para el cumplimiento de la política de seguridad de la información. *Revista Ibérica de Sistemas e Tecnologias de Informação,* (E51), 528-539.

Fundación Telefónica. (2016). *Ciberseguridad, la protección de la información en un mundo digital.* Planeta.

Goundar, S., Avanija, J., Sunitha, G., Madhavi, K. R., & Bhushan, S. B. (2021). *Innovations in the Industrial Internet of Things (IIoT) and Smart Factory.* IGI Global.

Ibarra, D., Ganzarain, J., & Igartua, J. I. (2018). Business model innovation through industry 4.0: A review. *Procedia Manufacturing,* (22), 4-10. https://doi.org/10.1016/j.promfg.2018.03.002

Instituto Nacional de Ciberseguridad [INCIBE-CERT]. (2020). Incibe-Cert. https://www.incibe-cert.es/

itTrends. (2019, 29 de marzo). Crecen los ataques cibernéticos, especialmente los destinados a Lot. IT. https://www.ittrends.es/seguridad/2019/03/crecen-los-ataques-ciberneticos-especialmente-los-destinados-a-io

Könnölä, T., Scapolo, F., Desruelle, P., & Mu, R. (2010). Foresight tackling societal challenges and implications on policy-making. *Futures, 43*(3), 252-264. https://doi.org/10.1016/j.futures.2010.11.004

Microsoft. (2023). *Azure Active Directory*. https://azure.microsoft.com/en-us/services/active-directory/

Mijares, V. M. (2020). Filling the structural gap: Geopolitical links explaining the South American Defense Council. *Colombia Internacional,* (101), 3-28. https://journals.openedition.org/colombiaint/4185

Miles, I. (2010). The development of technology foresight: A review. *Technological Forecasting and Social Change, 77*(9), 1448-1456. https://doi.org/10.1016/j.techfore.2010.07.016

Mintzberg, J. L., Lampel, J., & Ahlstrand, B. (1998). La estrategia y el elefante: una síntesis de las más célebres escuelas de estrategia, concebida para aplicar lo mejor de cada una. *Gestión, 3*(4), 24-34. http://planuba.orientaronline.com.ar/wp-content/uploads/2009/09/02b-mintzberg-la-estrategia-y-el-elefante.pdf

Mitrovic, Z., Taylor, W., Mymoena, S., Claassen, W., & Wesso, H. (2013). E-social Astuteness skills for ICT-supported equitable prosperity and a capable developmental state in South Africa. *International Journal of Education and Development Using Information and Communication Technology, 9*(3), 103-123. https://files.eric.ed.gov/fulltext/EJ1071374.pdf

Muñoz Campuzano, P. S. (2021). Modelos de seguridad para prevenir riesgos de ataques informáticos: Una revisión sistemática. [Tesis de pregrado, Universidad Politécnica Salesiana]. Repositorio UPS. https://dspace.ups.edu.ec/bitstream/123456789/20932/1/UPS-GT003373.pdf

Observatorio de la Seguridad de la Información [INTECO]. (2012). *Estudio sobre la seguridad de los sistemas de monitorización y control de procesos e infraestructuras* (SCADA). INTECO. https://www.aguasresiduales.info/revista/libros/estudio-sobre-la-seguridad-de-los-sistemas-de-monitorizacion-y-control-de-procesos-e-infraestructuras-scada

Okta. (2023). Okta Identity Cloud. https://www.okta.com

Organización de Estados Americanos [OEA]. (2017). Why a cyber-risk oversight? En *Cyber-Risk oversight handbook for corporate boards* (p. 4). OEA. https://www.oas.org/en/sms/cicte/docs/ENG-Cyber-Risk-Oversight-Handbook-for-Corporate-Boards.pdf

Palo Alto Networks. (2023). Next-Generation Firewalls. https://www.paloaltonetworks.com/

Patiño Mazo, E. (2018). Planeación estratégica de mercadeo y relaciones de transferencia en el ecosistema digital. *Espacios, 39*(50), 13-27. https://www.revistaespacios.com/a18v39n50/a18v39n50p13.pdf

Pérez Zúñiga, R., Mercado Lozano, P., Martínez García, M., Mena Hernández, E., & Partida Ibarra, J. A. (2018). La sociedad del conocimiento y la sociedad de la información como la piedra angular en la innovación tecnológica educativa. *Revista Iberoamericana para la Investigación y el Desarrollo Educativo, 8*(16), 847-70. https://www.scielo.org.mx/scielo.php?pid=S2007-74672018000100847&script=sci_arttext

Rosales Montalbán, E. A., Martelo Gómez, R. J., & Franco Borré, D. A. (2020). Diseño de un sistema de gestión de seguridad de la información para el proceso administrativo de la infraestructura tecnológica de instituciones académicas basado en Magerit. *Aglala, 11*(1), 227-245. https://revistas.uninunez.edu.co/index.php/aglala/article/view/1579

Sain, G. (2018). La estrategia gubernamental frente al cibercrimen: La importancia de las políticas preventivas. En *Cibercrimen y delitos informáticos: Los nuevos tipos penales en la era de internet* (pp. 7-32). Erreius. https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

Sáinz Peña, R. M. (2016). Ciberseguridad, la protección de la información en un mundo digital. *Revista TELOS.* https://n9.cl/n5bry

Sánchez Holguín, A. del M., Imán Sánchez, A. N. K., Chocan Sosa, E. A., Barreto Espinoza, K. L., & Torres Ruiz, M. I. (2023). *Propuesta de mejora de los servicios del taller R&T a través de un análisis de procesos aplicando metodologías de mejora continua* [Trabajo final de curso, Universidad de Piura]. Repositorio UDEP. https://pirhua.udep.edu.pe/backend/api/core/bitstreams/b2a30486-9b67-46dc-b341-3499a699d2d3/content

Schmitt, U. (2018). Rationalizing a personalized conceptualization for the digital transition and sustainability of knowledge management using the SVIDT Method. *Sustainability, 10*(3), 839. https://doi.org/10.3390/su10030839

Sepúlveda Marciales, C. M., & Medina Ulloa, O. L. (2024). *Desarrollo de un sistema tutorial inteligente para la implementación del modelo de medición de madurez y territorios inteligentes para Colombia (MMMCTIC)* [Tesis de grado]. Universidad Santo Tomás. https://n9.cl/4udig

Teslia, I., Yehorchenkov, N., Iegorchenkov, O., Kataieva, Y. (2016). Enterprise information planning - A new class of systems in information technologies of higher educational institutions of Ukraine. *Eastern-European Journal of Enterprise Technologies, 4*(2), 11-23. https://journals.uran.ua/eejet/article/view/74857

Valencia Duque, F. J. (2021). *Sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000.* Universidad Nacional de Colombia. https://repositorio.unal.edu.co/bitstream/handle/unal/80158/9789587946017.pdf?sequence=2&isAllowed=y

Vial, Gregory. (2019). Understanding digital transformation: A review and a research agenda. *Journal of Strategic Information Systems, 28*(2), 118-44. https://n9.cl/3rlun

World Economic Forum. (2013). *Global Risks 2013* (8.a ed.). World Economic Forum. http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf

Capítulo 2

Blockchain y ciberseguridad: fortaleciendo la confianza digital*

DOI: https://doi.org/10.25062/9786287602700.02

Jaider Ospina Navas
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este capítulo explora el estado del arte de la tecnología *blockchain,* con miras a identificar su papel en la construcción de un ecosistema digital seguro. Para ello precisa los aspectos que caracterizan la cadena de bloques como la descentralización, la inmutabilidad y el consenso; discute sus ventajas en términos de seguridad, transparencia y resistencia a la manipulación; analiza los diferentes tipos de ataques en materia de inmutabilidad que se reconocen a la fecha; describe los diferentes tipos de aplicaciones en que se emplea *blockchain,* y presenta los desafíos y limitaciones actuales, proporcionando una visión holística de las posibilidades y obstáculos en este campo en evolución.

Palabras clave: *blockchain;* confianza digital; descentralización; ecosistema digital; inmutabilidad; transparencia.

* Capítulo de libro resultado del proyecto de investigación *"Tecnologías disruptivas, logística y seguridad y defensa nacional en el ciberespacio"*, del grupo de investigación *"Ciberespacio Tecnología e Innovación"*, de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado C por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) y registrado con el código COL0181179. Los puntos de vista y los resultados de este capítulo pertenecen a los autores y no necesariamente reflejan los de las instituciones participantes

Jaider Ospina Navas
Doctorando en Sistemas de Información. Magíster en Ciencias de la Información y las Comunicaciones e ingeniero electrónico, Universidad Distrital Francisco José de Caldas, Colombia. Consultor en ciberseguridad y arquitecto en soluciones en la nube.
https://orcid.org/0000-3251-3017 - Contacto: **jaider.ospina@esdeg.edu.co**

Citación APA: Ospina Navas, J. (2024). Blockchain y ciberseguridad: fortaleciendo la confianza digital. En M. E. Realpe Díaz, & A. M. González González (Eds.), *Tecnologías disruptivas, logística y seguridad y defensa nacional en el ciberespacio* (pp. 47-76). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602700.02

TECNOLOGÍAS DISRUPTIVAS, LOGÍSTICA Y SEGURIDAD Y DEFENSA NACIONAL EN EL CIBERESPACIO
ISBN impreso: 978-628-7602-69-4
ISBN digital: 978-628-7602-70-0
DOI: https://doi.org/10.25062/9786287602700

Colección Ciberseguridad y Ciberdefensa
Sello Editorial ESDEG
Escuela Superior de Guerra “General Rafael Reyes Prieto”
Bogotá D.C., Colombia
2024

Introducción

Este capítulo explora el estado del arte de la tecnología cadena de bloques (*blockchain*), con miras a identificar su papel en la construcción de un ecosistema digital seguro. Como objetivo general se busca precisar las características que permiten construir un ecosistema digital confiable, mediante agentes habilitadores que garanticen la privacidad, confidencialidad y disponibilidad de los datos, así como una visión de las principales limitaciones para su adopción. Para esto se revisan: artículos orientados a la evaluación de aspectos propios de la ciberseguridad, documentación de aplicaciones o iniciativas tendientes a la mejora de la confianza digital y estudios en que se realiza una revisión sistemática de literatura.

Nacimiento de las cadenas de bloque

Si bien el origen de la *blockchain* (BC) se asocia a la publicación del *whitepaper* "*Bitcoin: A Peer-to-Peer Electronic Cash System*", en realidad debe atribuirse al trabajo de Stuart Haber y W. Scott Stornetta, quienes en su artículo "*How to Time-Stamp a Digital Document*", publicado en el *Journal of Criptology*, en 1991, presentaron un sistema de sellado de tiempo digital para certificar la fecha de creación o modificación de un documento electrónico, sin depender del medio físico, mediante el uso de *hash* criptográficos para generar resúmenes únicos de los documentos y su almacenamiento en una cadena de bloques (Haber & Scott, 1991).

Posteriormente, el 1.o de noviembre de 2008, Satoshi Nakamoto, seudónimo empleado por la persona o grupo que creó el concepto y la tecnología subyacente de bitcoin, envía un mensaje a la lista de correos especializado en criptografía metzdowd, en el que anunciaba un nuevo sistema de dinero electrónico basado en

redes *Peer-to-Peer* (P2P). Este documento sentó las bases teóricas y técnicas de la tecnología *blockchain* y expuso de manera concisa los aspectos técnicos que proponía una nueva moneda digital, así como el objeto principal de su creación: prescindir de terceros de confianza.

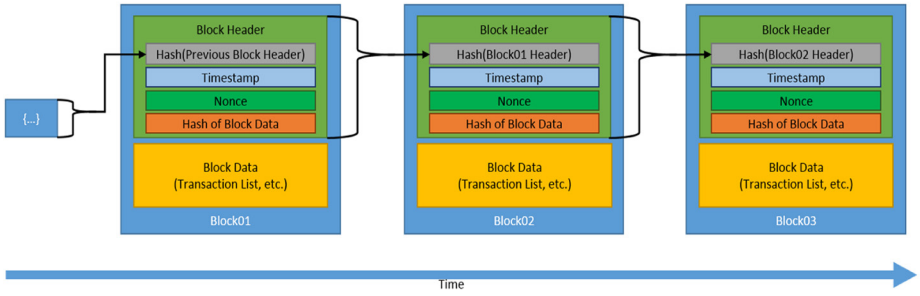
"Lo que se necesita es un sistema de pago electrónico basado en pruebas criptográficas en lugar de confianza, permitiendo así que dos partes interesadas realicen transacciones directamente sin necesidad de una tercera parte de confianza" (Nakamoto, 2008, s.p.).

De esta manera, nace la más reconocida moneda digital, el bitcoin; y se propone una solución a uno de los mayores problemas de este tipo de divisa: el doble gasto. Mediante el uso de una cadena de bloques descentralizada y un consenso distribuido para validar y registrar las transacciones de forma segura y transparente, características estas heredadas por diferentes sistemas y aplicaciones para generar protección de los datos y generar un ecosistema digital confiable.

Fundamentos de la tecnología *blockchain*

La cadena de bloques se define como una base de datos distribuida y segura que ha revolucionado la forma en que se almacenan y verifican los datos (Xu et al., 2019). Cada bloque de la cadena contiene un *hash* criptográfico del bloque anterior entrelazado mediante un *hash* garantizando una "firma digital" 1 que garantiza su integridad y eventual manipulación, una marca de tiempo y datos de la transacción efectuadas (Figura 1).

Figura 1. *Cadena de bloques genérica*



Fuente: NISTIR 8202 (2018).

En términos generales, BC puede ser concebida como una tecnología de registro de datos descentralizada y segura, que ha emergido como un componente fundamental en la era digital. Según Nakamoto (2008), *blockchain* se define como un "registro público de transacciones" que almacena información de manera inmutable y transparente. La fortaleza de BC radica en su naturaleza descentralizada, donde múltiples nodos de la red verifican y validan las transacciones, eliminando la necesidad de un intermediario central de confianza (Swan, 2015). Esto garantiza la seguridad y la integridad de los datos almacenados, ya que cualquier intento de alteración requeriría el consenso de la mayoría de los participantes, lo que lo hace altamente resistente a la manipulación y a los ataques cibernéticos (Mougayar, 2016; Krichen et al., 2022; Yli-Huumo et al., 2016). Como ya se mencionó, la estructura única de BC la hace resistente a la manipulación, ya que cualquier cambio en un bloque requeriría cambios en todos los bloques siguientes para mantener la coherencia de la cadena (Popchev et al., 2021).

Hablando específicamente del protocolo bitcoin descrito originalmente por Nakamoto, este se apoya sobre la pila de protocolos TCP/IP a partir del cual se construye una red de nodos superpuesta a internet. En ella, los nodos conforman una red P2P donde todos los nodos proveen y consumen servicios simultáneamente mientras colaboran vía un servicio de consenso Vamsi_Cz5cgo y Vamsi_Cz5cgo (2020).

Blockchain y Distributed Ledger Technology

Tecnología de libro distribuido (DLT)

Estrictamente hablando, BC es un tipo específico de DLT y, a su vez, DLT es un caso particular de base de datos distribuida, caracterizada por su proceso de validación consensuado (Romero, 2018). DLT se caracteriza por hacer uso de tres elementos tecnológicos articulados para conformar su arquitectura, ellos son las redes P2P, criptografía asimétrica y algoritmos de consenso. Una diferencia significativa entre DLT y BC radica en su estructura y funcionamiento. Mientras que la DLT puede tener diferentes grados de descentralización y puede ser pública o privada, la BC es completamente descentralizada y generalmente pública (Hurtado, 2021). Algunos ejemplos de plataformas que hacen uso de DLT son Hyperledger Fabric, Corda y Quorum por citar algunas de las más representativas. Estas tecnologías pueden

ser públicas o privadas y customizadas para adaptarse a las necesidades específicas de una aplicación o industria.

Tipos de blockchain

Existen varios tipos de BC, cada uno con sus propias características y capacidades que se adaptan a diferentes necesidades.

Blockchain públicas

Redes a las que cualquier persona puede unirse, verificar transacciones y participar en la validación de bloques. En general, los usuarios son anónimos y ningún participante tiene más derechos que los demás, por lo cual no hay administradores de la red. Son consideradas impulsoras de las tecnologías de contabilidad distribuida DLT y el uso de redes P2P para la distribución de datos (Haleem et al., 2021). Las redes públicas más conocidas son Bitcoin, Bitcoin Cash, Ethereum y Litecoin.

Blockchain privadas

Redes donde el acceso está restringido a un grupo específico de entidades. Suelen ser utilizadas por empresas que desean aprovechar las ventajas de la tecnología BC, pero manteniendo el control sobre quién puede participar en la red y todas las labores de gestión como la creación y aceptación de bloques.

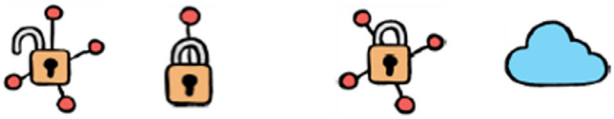
Blockchain federadas o de consorcio

Implementación híbrida de las anteriores. El control no recae en una sola entidad, sino en un grupo, lo que permite que se mantenga cierto nivel de privacidad al tiempo que se aprovecha la seguridad y transparencia de la tecnología BC.

Blockchain como un servicio (BaaS)

Productos que permiten a los usuarios crear sus propias redes sin tener que preocuparse por la infraestructura subyacente, permitiendo a los usuarios centrarse en desarrollar sus aplicaciones sin tener que preocuparse por aspectos técnicos. Finalmente se recogen algunas particularidades de los diferentes tipos de BC en la Figura 2.

Figura 2. *Tipos de redes blockchain*



	Públicos Bitcoin, Ethereum, Litecoin	**Privados** Hyperledger, Corda, Quorum	**Federados** Hyperledger, Corda, Quorum	***Blockchain as a Service*** IBM, Microsoft, Amazon
Cualquiera puede participar	✓	✗	✗	NA
Los participantes actúan, en general, como nodos	✓	✗	✗	NA
Transparencia	✓	~	~	NA
Hay un único administrador	✗	✓	✗	NA
Hay más de un administrador	✗	✗	✓	NA
No hay administradores	✓	✗	✗	NA
Ningún participante tiene más derechos que los demás	✓	✗	✗	NA
Se pueden implementar Smart *Contracts*	✓	✓	✓	NA
Existe recompensa por minado de bloques	~	✗	✗	NA
Soluciona problema de falta de confianza	✓	✗	~	NA
Seguridad basada en protocolos de consenso	✓	✗	~	NA
Seguridad basada en funciones *hash*	✓	~	~	NA
Provee servicios en la nube	NA	NA	NA	✓

✓ Sí ✗ No ~ A veces **NA** No Aplica

Fuente: López (2018).

Generaciones de *blockchain*

En el artículo *"Evolution of Industry and Blockchain Era: Monitoring Price Hike and Corruption Using BIoT for Smart Government and Industry 4.0"*, Hasan et al. (2022) identifican cinco generaciones de BC desde su aparición: 1.a generación: se centra en la creación de bitcoin por Satoshi Nakamoto en 2008, moneda digital descentralizada que permite transacciones P2P sin necesidad de un intermediario; 2.a generación: introduce la idea de los contratos inteligentes (*Smart Contracts*), programas que se ejecutan automáticamente cuando se cumplen ciertas condiciones. Ethereum es el ejemplo más conocido; 3.a generación: se centra en resolver los problemas de escalabilidad e interoperabilidad que enfrentan las generaciones anteriores. Proyectos como Cardano y Polkadot están trabajando en soluciones para permitir que diferentes BC interactúen entre sí y para manejar un mayor número de transacciones, pasando de 6 transacciones por segundo (TPS) a 100.000 TPS. Esta generación introdujo las aplicaciones descentralizadas (dApps); 4.a generación: se enfoca en la integración de sistemas empresariales y gubernamentales existentes, proporcionando soluciones para problemas de interoperabilidad, privacidad y seguridad (Banafa, 2022). Ya se alcanza un nivel de 300.000 TPS y aumenta el abanico de aplicaciones a campos como la cadena de suministro, el voto electrónico y Smart Grid, y 5.a generación: la actual y en pleno proceso de gestación, que surge según los expertos con la aparición de proyectos como Relictum Pro (Bitcoin.es, 2020). Se distingue por el uso de máquinas inteligentes y analítica de datos para la automatización de procesos de aplicaciones inteligentes (Choi & Siqin, 2022).

Rasgos distintivos de la tecnología *blockchain*

Algunas características de la BC, y que se convierten en elementos potencializadores de estrategias de ciberseguridad, son la descentralización, la inmutabilidad, la transparencia y el consenso. Estos pilares han transformado la confiabilidad y la seguridad en las operaciones en línea, y su comprensión es esencial para apreciar el potencial de esta tecnología.

Descentralización

En palabras de Tapscott y Tapscott, (2016), la descentralización significa que no existe una autoridad central que controle la red. En lugar de depender de una

entidad centralizada como un banco o un Gobierno, las transacciones se verifican y registran en una red distribuida de nodos que trabajan juntos de manera colaborativa. La eliminación de intermediarios genera confianza y reduce los puntos únicos de fallo, lo que hace que la red sea altamente resistente a la censura y a eventuales ataques que comprometan los datos. La descentralización tiene varias ventajas:

- Proporciona un entorno sin confianza: en una red BC descentralizada, nadie tiene que conocer o confiar en alguien más. Cada miembro posee una copia exacta de los mismos datos en forma de un libro de contabilidad distribuido.
- Mejora la reconciliación de datos: todos los nodos tienen acceso a una vista compartida y en tiempo real de los datos.
- Reduce puntos de debilidad: la descentralización puede reducir los puntos de debilidad en sistemas donde exista dependencia de actores específicos. Un punto de debilidad puede deberse a dependencia de recursos específicos como capacidad de almacenamiento o cómputo.
- Optimiza la distribución de recursos: se optimiza la distribución de recursos, mejorando rendimiento y consistencia de red mediante estrategias como mejora en los tiempos de entrega de contenido.

Inmutabilidad

La inmutabilidad, según Mougayar (2016), es un principio que se refiere a la incapacidad de cambiar o borrar una vez que se ha registrado una transacción en la cadena de bloques. Cada bloque de datos en la cadena se vincula criptográficamente al anterior, lo que hace que sea extremadamente difícil, si no imposible, modificar el contenido de un bloque sin modificar todos los siguientes. Ello asegura que las transacciones registradas sean permanentes y confiables, lo que es esencial en aplicaciones donde la integridad de los datos es crucial, como la atención médica y la gestión de identidades.

Transparencia

En una red BC, todas las transacciones son visibles para todos los participantes de la red, lo que proporciona un alto nivel de transparencia. Es de aclarar que esta transparencia puede presentar desafíos, especialmente cuando se trata de datos sensibles.

Según Sedlmeir et al. (2022), la transparencia establece desafíos en empresas y el sector público relacionados con un grado excesivo de esta. Se señala cómo los tipos de datos sensibles involucrados en diferentes patrones de casos de uso de *blockchain* y se argumenta que las implicaciones de la exposición de información de las BC causada por el almacenamiento y ejecución de transacciones replicadas van más allá de los conflictos a menudo mencionados con el "derecho al olvido" del GDPR y pueden ser más problemáticos de lo previsto. Los autores presentan el equilibrio entre proteger información sensible y aumentar la eficiencia del proceso mediante contratos inteligentes. También exploran hasta qué punto las *blockchain* con permisos y las nuevas aplicaciones de tecnologías criptográficas como las identidades autónomas y las pruebas de conocimiento cero pueden ayudar a superar el desafío de la transparencia y, por lo tanto, actuar como catalizadores para la adopción y difusión de BC en las organizaciones.

Como se acaba de mencionar, una de las maneras propuestas de atacar esta problemática es mediante el empleo de prueba de conocimiento cero o *zero-knowledge proof* (ZKP), técnica criptográfica que puede utilizarse en el entorno de *blockchain* para verificar si el probador tiene suficiente cantidad de transacciones sin filtrar ningún dato privado de transacciones (Konkin & Zapechnikov, 2023).

De manera similar, Sun et al. (2021) realiza un estudio sobre ZKP en el entorno de *blockchain* con el objetivo de resaltar los problemas de seguridad y sus desafíos y discuten un marco, los modelos y las aplicaciones de ZKP. A manera de conclusión, ZKP resulta una herramienta valiosa para mejorar la privacidad y la seguridad en las transacciones de *blockchain*, permitiendo la verificación de las transacciones sin revelar detalles sensibles.

Consenso

El consenso se logra mediante algoritmos gracias a los cuales la "red va tomando decisiones consensuadas, valida la información y asigna las tareas a cada uno de los nodos que la componen" (Criptodemy, n.d.). Este concepto fue expuesto originalmente por Adam Back en mayo de 1997 y buscaba regular el abuso desmedido de recursos de internet, como correos electrónicos y *remailers* anónimos (Back, 2002).

En palabras de Narayanan et al. (2016), el consenso puede ser definido como un proceso mediante el cual los nodos llegan a un acuerdo sobre la validez de una transacción antes de agregarla a la cadena de bloques. El ejemplo más significativo de este tipo de protocolos de consenso se puede hallar en la prueba de trabajo

(PoW), empleada por la criptomoneda bitcoin. Dicho protocolo implica que los mineros compitan para resolver complejos problemas matemáticos y el primero en hacerlo tiene el derecho de agregar un nuevo bloque. Este mecanismo garantiza que todas las partes de la red estén de acuerdo en el estado de la cadena de bloques y que las transacciones sean válidas y seguras.

Algoritmos de consenso

Existen diversos protocolos y algoritmos de consenso para garantizar la seguridad y la confiabilidad de la red; cada uno define sus propias características y ventajas. Algunos son:

Prueba de trabajo (*Proof of Work, PoW*)

PoW es el protocolo de consenso más conocido, asociado principalmente con bitcoin y Ethereum, aunque se utiliza en otras criptomonedas y redes *blockchain.* En esencia, la prueba de trabajo requiere que los nodos de la red realicen un cálculo computacional intensivo para demostrar que han invertido tiempo y recursos en la verificación de transacciones. Este proceso se conoce como *minería* y los participantes se denominan *mineros,* y se repite continuamente para mantener la cadena de bloques segura y distribuida.

Según Narayanan et al. (2016), la prueba de trabajo es esencialmente un rompecabezas matemático complejo que requiere una gran cantidad de poder de cómputo para su resolución. Los mineros compiten para resolver este rompecabezas, y el primero en hacerlo tiene el derecho de agregar un nuevo bloque a la cadena y es recompensado con nuevas monedas (por ejemplo, bitcoins) y tarifas de transacción.

Nakamoto (2008) introdujo por primera vez el concepto de *prueba de trabajo* en el contexto de bitcoin y proporcionó los fundamentos teóricos de su funcionamiento. Su adopción se asemeja, según las propias palabras de Nakamoto, a la presentada por Back (2006) Hashcash, algoritmo que inicialmente se utilizó para abordar el *spam* por correo electrónico y los ataques DDoS, y en la actualidad se utiliza para fines de verificación de transacciones.

PoW, como protocolo de consenso, ha demostrado ser efectivo en la prevención de ataques maliciosos y en la creación de un registro seguro y confiable de transacciones en la red *blockchain.* Aunque su mayor debilidad es su poca capacidad

de escalamiento y rendimiento limitado en términos de transacciones por segundo (TPS). Este protocolo es quizás uno de los mayores aportes de Nakamoto a la creación de la BC, y al mismo tiempo, ha proporcionado una solución a uno de los problemas más desafiantes en el campo de la informática, conocido como el problema de los generales bizantinos. Ventajas: seguridad comprobada, alta resistencia a ataques del 51 %. Desventajas: consumo energético elevado, centralización en minería.

Prueba de participación (*Proof of Stake, PoS*)

En PoS, los validadores bloquean una cierta cantidad de criptomonedas como garantía, y la probabilidad de ser seleccionados para validar un bloque se basa en la cantidad de monedas en juego. Ethereum ha migrado PoS con Ethereum 2.0. Este tipo de consenso se introdujo como una alternativa más eficiente y menos costosa a (PoW). En lugar de requerir que los mineros realicen cálculos computacionales intensos, PoS permite a los participantes de la red crear bloques y validar transacciones en función de la cantidad de monedas que poseen y están dispuestos a "apostar" para el consenso (Ge et al., 2022).

Existe una gran variedad de algoritmos de consenso derivados de PoS, entre ellos DPoS, Snow White, Sleepy Consensus, Ouroboros, Ouroboros Praos, Ouroboros Genesis, Ouroboros Crypsinous, EOS, Improvement of DPoS, entre otros (Ge et al., 2022).

Ventajas: eficiencia energética, menos centralización, incentiva a los poseedores de monedas. Menor barrera de entrada (la red acepta participantes sin necesidad de comprar y configurar hardware costoso). Transacciones más rápidas en comparación con las redes PoW. Desventajas: posible centralización en función de la riqueza, ya que aquellos con más monedas tienen más oportunidades de crear bloques. Problema del "nada en juego", en PoS, no hay un costo real asociado con la validación de bloques incorrectos, lo que puede llevar a problemas de seguridad.

Prueba de participación delegada (*Delegated Proof of Stake, DPoS*)

Se trata de una variante de PoS donde un grupo seleccionado de validadores, elegidos por la comunidad, es responsable de validar las transacciones. EOS es un ejemplo de una cadena de bloques que utiliza DPoS. Ventajas: alta escalabilidad, rapidez en la confirmación de transacciones. Desventajas: menos descentralización, poder concentrado en los nodos elegidos.

Proof of Authority (PoA)

Algoritmo basado en la reputación, donde los validadores no arriesgan criptodivisas sino su reputación, en consecuencia, estos son elegidos de manera arbitraria al considerárseles confiables. Su uso se da principalmente en redes privadas; entre ellas, se distingue su uso en logística, donde se le considera una solución eficiente y razonable, ya que su naturaleza permite aprovechar las características de BC manteniendo la privacidad de los participantes. Ventajas: eficiencia energética, alta velocidad en comparación con PoW y PoS, incentivos monetarios. Desventajas: menor descentralización, ya que se basa en un número limitado de validadores de bloque. Vulnerable a la colusión, pues se confía en un número limitado de validadores, existiendo el riesgo de que estos puedan coludir para actuar malintencionadamente.

Proof of Space and Time (PoST)

Se trata de un nuevo primitivo criptográfico que permite a un probador convencer a un verificador de que ha gastado un recurso de "espacio-tiempo". En palabras de Ortega (2023), "…en el algoritmo de Proof of Space and Time, los nodos de la red deben demostrar que están almacenando una cantidad específica de datos mediante un proceso denominado agricultura" (s.p.). Ventajas: eficiencia energética, llegando incluso a ser posible minar con este algoritmo en dispositivos comunes. Accesible para más participantes. Descentralización del proceso. Desventajas: crecimiento permanente debido que a medida que se añaden más mineros a la red, se requiere más espacio de almacenamiento (Moran & Orlov, 2019).

Round Robin

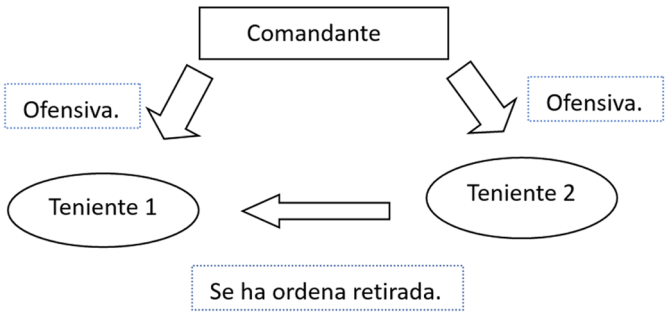
Round Robin en BC ha sido estudiado en varios artículos científicos. Una propuesta de su uso se presenta en Raikwar y Gligoroski (2021), quienes proponen el protocolo de consenso R3V. Este selecciona un conjunto de candidatos a líder de manera rotativa según su antigüedad. Luego, estos compiten para ser el líder del bloque resolviendo un rompecabezas basado en una Función de Retardo Verificable (VDF) (Raikwar & Gligoroski, 2021). Ventajas: mayor resistencia contra la mayoría de los ataques comunes en los protocolos PoS, además de menor consumo de energía, menos complejidad de comunicación y una mayor equidad. Para finalizar, otros algoritmos existentes de menor difusión son prueba de peso (PoW), la prueba de importancia (PoI), la prueba de cobertura (PoC) y gráficos acíclicos dirigidos (DAG).

El problema de los generales bizantinos: una mirada militar

El problema de los generales bizantinos fue anunciado por Robert Shostak y desarrollado con Leslie Lamport y Marshall Pease en 1982 en el centro de investigación científica y tecnológica SRI International (BBC News Mundo, 2020). Y, sin duda, recoge la esencia de la problemática de un consenso en una red en la que existen agentes no confiables. En ella, desde la perspectiva de la teoría de juegos, se proporciona una descripción de la medida en que las partes descentralizadas experimentan dificultades para llegar a un consenso sin que exista un agente central de confianza.

En esencia, se plantea un escenario de guerra donde existe un grupo de generales bizantinos asediando una ciudad desde varios puntos y debe ser acordado si atacar o retirarse de manera coordinada. Entre los generales, solo uno puede impartir la orden a toda la fuerza, pues es el comandante. Al resto de generales se les considera tenientes. Los tenientes se comunican entre sí cuando reciben las órdenes del comandante, y las dos órdenes posibles del comandante son "atacar" y "retirarse". Se conoce que uno o más generales pueden ser traidores. El objetivo es que todos los generales leales NO estén de acuerdo. Para ello, pueden proporcionar información incorrecta. Por ejemplo, si el comandante es un traidor, puede enviar órdenes contradictorias a diferentes tenientes. Si su lugarteniente es un traidor, puede mostrárselo a los demás lugartenientes, para confundirlos y hacerles creer que el traidor es el comandante, que el comandante les envió órdenes contrarias a las órdenes que realmente les envió (Soto, 2020). Una solución acertada en el campo de batalla debe llevar a uno de dos objetivos: 1) todos los tenientes leales toman la misma decisión, y 2) si el comandante es leal, todos los tenientes cumplirán fielmente sus órdenes. La Figura 3 ilustra el caso en que el "teniente 2" es un traidor.

Figura 3. *Teniente 2 es un traidor*



Fuente: Lamport et al. (1982).

Este tipo de problemas son asociados a la necesidad de consenso y la posibilidad de que existan actores poco confiables en el sistema. Un sistema informático confiable debe lidiar con componentes que funcionan mal y que brindan información contradictoria a varias partes del sistema. El problema es encontrar un algoritmo que garantice que los generales leales lleguen a un acuerdo. Se demostró que, utilizando únicamente mensajes verbales, este problema podría resolverse si y solo si más de dos tercios (2/3) de los generales fueran leales. Un traidor puede confundir a dos generales leales. Esta problemática se traslada al mundo de *blockchain* cuando se requiere agregar un nuevo bloque a la cadena, donde cada nodo debe estar de acuerdo en el estado del sistema antes de que este pase a ser parte de esta. Claramente en el contexto que nos atañe, la "lealtad" es un aspecto constitutivo de la confianza.

Amenazas en una red *blockchain*

El aspecto más sobresaliente en la construcción de un sistema seguro que ofrece BC es su inmutabilidad. No obstante, esta no tiene garantía del 100 % de ser invulnerable. BC puede ser comprometida bajo ciertas circunstancias. Algunos de estos posibles escenarios son:

- Ataque del 51% (51% Attack): este tipo de ataque se debe a la posibilidad de que un grupo de mineros controle más del 50 % del poder de cómputo de la red, pudiendo con ello cambiar y reorganizar la cadena de bloques (afectando su integridad), invalidando transacciones anteriores y creando una cadena alternativa. Sin embargo, realizar un ataque del 51 % en una red con una gran cantidad de mineros es extremadamente costoso, aunque se han identificado ataques de este tipo (Sayeed & Marco-Gisbert, 2019).
- Ataque Sybil: recibe su nombre del libro *Sybil* (Schreiber, 1973) y del relato de una mujer diagnosticada con trastorno disociativo. El ataque se caracteriza por corromper redes P2P mediante la creación de identidades falsas. La vulnerabilidad de una red BC a este ataque dependerá del costo de generar identidades, el grado en que el sistema de reputación acepta nuevas identidades, y si el sistema de reputación trata a todas las entidades de manera idéntica. Mohaisen y Kim (2013) identifican tres principales estrategias de defensa: 1) entidades certificadoras de confianza; 2) pruebas

de recursos (pruebas de IP, coordenadas de red y resolución de algoritmos entre otros), y 3) redes sociales (Mohaisen y Kim, 2013).

- Ataques de doble gasto: aunque la mayoría de las cadenas de bloques están diseñadas para prevenir el doble gasto, en ciertas circunstancias, un atacante podría intentar gastar la misma criptomoneda dos veces antes de que la red actualice su estado. Este riesgo se da en cadenas con confirmaciones de transacciones lentas. Existen diferentes tipos de ataques de doble gasto, entre ellos un estudio reciente presenta un tipo de ataque bautizado Adaptive Double-Spending Attack (Adaptive DSA) como un ataque avanzado de doble gasto en BC basadas en PoW. En este, el atacante duplica una transacción válida en la red y se convierte en un proceso de decisión de Márkov (PDM) y mediante la explotación focalizada en programación dinámica estocástica (SDP), se explotan estrategias optimizadas de ataque Adaptive DSA (Zheng et al., 2023).
- Presencia de vulnerabilidades del protocolo: los errores o vulnerabilidades en el *software* o el protocolo de una cadena de bloques pueden ser explotados para comprometer la inmutabilidad. Por ejemplo, errores en la implementación del código pueden permitir que un atacante realice transacciones inválidas o altere el estado de la cadena.
- *Forks* y actualizaciones del protocolo: a veces, una cadena de bloques puede experimentar una bifurcación (*fork*) o una actualización del protocolo que podría afectar la inmutabilidad. Si una comunidad no está de acuerdo sobre los cambios en el protocolo, podría dar lugar a dos cadenas separadas (*hard fork*), lo que podría tener implicaciones para la inmutabilidad y la continuidad de la cadena.

Blockchain, tecnología disruptiva

La tecnología BC es una de las mayores innovaciones del siglo XXI, con un impacto significativo en sectores que van desde el financiero, manufactura, votaciones electrónicas y educación, por citar algunos. Esta sección recoge algunas revisiones sistemáticas realizadas por terceros en los que se ha evaluado el impacto de BC en diferentes áreas, buscando con ello validar la hipótesis de cómo la implementación de la tecnología *blockchain* puede incrementar significativamente la confianza digital al proporcionar un sistema descentralizado y transparente que garantiza la integridad y la inmutabilidad de los datos, lo que podría redundar en

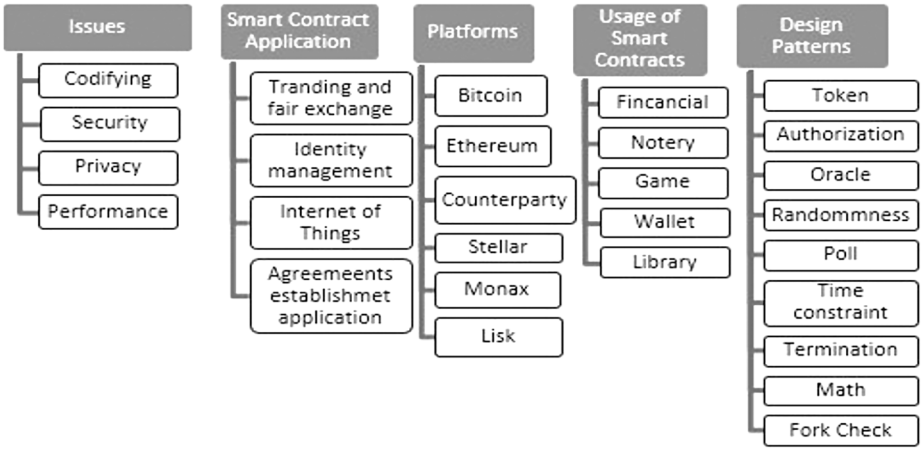
una mayor adopción de servicios digitales, una reducción en el fraude y una mejora en la eficiencia de las transacciones digitales.

Trabajos como el de Baena y García (2022) permiten, tras una rigurosa revisión bibliográfica, establecer un consenso respecto de los beneficios de seguridad, transparencia, trazabilidad, confianza, autenticidad y privacidad y la reducción de costes en las cadenas de suministro, mediante el uso de la cadena de bloques.

Por su parte, Xu et al. (2019) realizan un estudio de 756 artículos, los cuales fueron decantados a 119 bajo los criterios de economía y negocios y destacan el potencial impacto en áreas como el *crowdfunding* y la gestión contable, el almacenamiento y compartición de datos, la administración de las cadenas de suministro y el comercio inteligente para beneficiarse de las características de BC (Xu et al., 2019).

El estudio de Leka evalúa 292 *papers* extraídos de bases de datos como IEEE, ACM, Science Direct y Springer; centrando su diagnóstico final en 28 y se centra en el uso de BC en *smart contratcs,* identificando como sus principales vulnerabilidades los errores de código, los ataques maliciosos y las explotaciones de los mineros y los usuarios. También revisa algunas herramientas y métodos para verificar y auditar los contratos inteligentes. En la figura 4 se aprecia un esquema de clasificación que resulta interesante, toda vez que se aprecia qué aspectos como la codificación, la seguridad, la privacidad y el desempeño son trasversales a cualquier tipo de aplicación y campo donde se haga uso de BC, por lo que conviene asumir su enfoque taxonómico para evaluar casos particulares de uso (Leka et al., 2019).

Figura 3. *Esquema de clasificación de smart contracts*



Fuente: Leka et al. (2019).

Romero (2018) resalta el uso de la tecnología de registro distribuido (DLT) en transacciones financieras, identificando ventajas como la aceleración del proceso de liquidación de transacciones financieras, la reducción del número de intermediarios y la mejora de la eficiencia del proceso de reconciliación. Además, se vislumbra cómo puede mejorar la transparencia y la trazabilidad de las transacciones, aspecto especialmente útil en el comercio internacional, donde hay muchos actores y facilita la negociación y posnegociación de valores, el cumplimiento regulatorio y la gestión de la identidad digital. Reforzando este aspecto, resulta clara la tendencia hacia una total digitalización de la economía. Aspectos como la transformación digital cimentada sobre la cuarta Revolución Industrial, lleva a una economía considerada como digital (Bogdanov et al., 2021), donde BC se esgrime como elemento habilitador tecnológico.

A esta altura, resulta evidente que el impacto de BC se ha expandido más allá de su uso en criptomonedas. BC se ha convertido en un pilar en diversos campos, como la cadena de suministro, la atención médica y la protección de la propiedad intelectual. Según Tapscott y Tapscott (2016), *blockchain* proporciona una mayor visibilidad y trazabilidad en la cadena de suministro, permitiendo el seguimiento en tiempo real de productos desde su origen hasta su destino. En el sector de la salud, Griggs et al. (2018) señalan que *blockchain* garantiza la seguridad y la privacidad de los registros médicos electrónicos, facilitando el intercambio seguro de información entre médicos y pacientes. Además, en el ámbito de los derechos de autor y la propiedad intelectual, *blockchain* ofrece un registro inmutable de la autoría y la propiedad de contenido digital, lo que puede ser fundamental para la protección de los derechos de los creadores (Lorenzo, 2020).

En general, BC puede ayudar a mejorar la confianza y la colaboración entre diferentes partes en sectores como la industria 4.0. Así lo presenta Haleem et al. (2012; 2022), quien destaca varios aspectos habilitadores de BC en campos como las *smart cities, smart factories,* productos inteligentes y cadena de suministro.

A nivel de responsabilidad social, resulta interesante la propuesta del uso de BC como instrumento de auditoría y modelo de operación (Martínez et al., 2020). Esto gracias al uso del modelo de registro de datos que se puede llevar a cabo en las billeteras (*wallets*).

Autores como Haleem et al. (2021) identifican una amplia gama de aplicaciones y funcionalidades de BC, como la contabilidad distribuida que permite la transmisión segura y auditada de registros médicos de pacientes y la gestión de la cadena de suministro de medicamentos; aunque se identifica como principal obstáculo la poca experiencia que se tiene en el medio de las aplicaciones que hacen

uso de la tecnología BC. Otra ejemplificación de uso de BC, se da en la cadena de suministro de medicamentos (Casino et al., 2019).

De otra parte, escenarios arquitecturales en los que se emplea BC como solución a problemáticas en la centralización de recursos en redes IoT permiten en lugar de almacenar datos de sensores centralizadamente, realizarlo sobre la base distribuida de BC donde los datos de los sensores pueden ser gestionados de manera similar a la filosofía *blockchain* (Conoscenti et al., 2017).

Blockchain y ciberseguridad

Si bien ya se han mencionado algunas características que convierten a BC en agente dinamizador de la ciberseguridad, algunos aspectos que vienen a reforzar son:

Ventajas y beneficios

- Mayor seguridad y protección de datos debido a su estructura inmutable.
- Mejora de la transparencia y la integridad de los datos mediante la auditoría y verificación distribuida.
- Arquitecturas con alta disponibilidad y resilientes.
- Reducción de los puntos de vulnerabilidad y riesgo mediante la descentralización y la resistencia a ataques cibernéticos.

Aplicaciones prácticas de *blockchain* en la ciberseguridad

- Protección de identidad y autenticación mediante sistemas IDMS (identity management systems). Estos permiten administrar, la autenticación, autorización y compartición de archivos.
- Registro y verificación de eventos de seguridad para la detección de intrusiones y análisis forense.
- Gestión de acceso y control de datos mediante contratos inteligentes.
- Contabilidad distribuida, transparencia operacional.
- Arquitecturas redundantes y resilientes.

Desafíos y consideraciones en el uso de *blockchain* en la ciberseguridad

- Escalabilidad y rendimiento.
- Privacidad y protección de datos personales en entornos BC transparentes.

- Actualización y mantenimiento de la infraestructura BC para garantizar la seguridad a largo plazo.
- Colaboración y desarrollo de estándares BC orientados en ciberseguridad.
- Colaboración entre los actores involucrados, como desarrolladores, investigadores y usuarios finales.
- Declaración de buenas prácticas de implementación BC en entornos ciberseguros.

Construcción de un ecosistema de confianza digital

Son numerosos y diversos los campos de uso de la tecnología *blockchain* y sus potencialidades de construcción de confianza digital. Pero esta, como toda tecnología, no representa una panacea y su adopción es un proceso que debe ser construido día a día y con la participación de todos los interesados (*stakeholders*) y sobre todo garantizar su uso como un medio y no como un fin. *A priori,* BC concibe una seguridad por diseño cimentada en sus características de inmutabilidad, integridad y transparencia. Una vez las transacciones se confirman, los datos se almacenan permanentemente en el libro mayor, a prueba de manipulaciones, y se salvaguardan estas transacciones. En términos de diseño, la tecnología BC incluye criptografía y consenso distribuido como mecanismos preventivos para reducir los riesgos de ciberataques y una arquitectura distribuida sin requerimientos de entidades centrales de "confianza". Sin intermediarios confiables, la confianza dentro de una red BC es posible gracias a cuatro características clave: 1) libro mayor (*ledger*): proporciona trazabilidad transaccional. A diferencia de las bases de datos tradicionales, las transacciones en BC no se eliminan; 2) seguridad: los datos se consideran criptográficamente seguros, garantizando la no manipulación; 3) compartido: el libro mayor es compartido entre varios participantes, lo que provee transparencia, y 4) carácter distribuido: permite escalar el número de nodos de una red BC para hacerla más resistente a eventuales ciberataques y optimizar la entrega y consumo de contenido.

De esta manera, aunado a pilares clave de la seguridad de la información (inmutabilidad-integridad, disponibilidad-redes distribuidas y redundantes, trasparencia-auditoria distribuida) aunado en la construcción y adopción de prácticas y estrategias en ciberseguridad, a la postre, permiten construir un ecosistema digital confiable.

En el plano nacional, es de resaltar que el Ministerio de Tecnologías de la Información y las Comunicaciones, de manera expresa, manifiesta la potencialidad en generación de confianza digital:

> La clave en DLT/*Blockchain* es generar "Confianza" en las transacciones que se realicen en la red, al punto que no se requieran ni documentos físicos (Papeles) o entidades centralizadas (Bancos o Notarios) para poseer un título que represente valor social o económico. (MinTIC, 2022, s.p.)

En el contexto nacional es importante resaltar la integración entre el gobierno y el Banco Interamericano de Deasarrollo (BID) para el impulso de BC mediante iniciativas como el espacio de experimentación de proyectos con BC en el sector público, que nace mediante la firma de un memorando de entendimiento con BID Lab, el laboratorio de innovación del BID.

Así mismo, el MinTIC publicó la "Guía de referencia para la adopción e implementación de proyectos con tecnología *blockchain* para el Estado colombiano". Esta facilita el acercamiento del Estado a esta tecnología y promueve un enfoque ético y de cumplimiento, proporciona además un enfoque de gobernanza, presenta lineamientos para el desarrollo de proyectos en entidades gubernamentales y brinda herramientas para que los proyectos sean diseñados y operados organizada, escalonada y estructuradamente.

Discusión

No obstante, lo prometedor de BC como tecnología de alto impacto en diferentes campos y sus potencialidades para garantizar prácticas de ciberseguridad deben abordarse responsablemente sus desafíos. Problemáticas como la limitación en escalabilidad derivada del tamaño que puede llegar a tener BC, se solucionaría mediante la implementación de algoritmos de poda de cadena, lo que implica que "transacciones antiguas podrían ser eliminadas, guardando de ellas solo su hash, para preservar la integridad de la cadena" (Pérez & Joancomartí, 2014).

Los desafíos a que se enfrenta la BC en entornos descentralizados pueden ser superados mediane el empleo de protocolos de red como Named Data Networking (NDN). Esto puede contribuir al impulso de BC en aspectos como la entrega efectiva de contenido, gracias al uso de enrutamiento basado en nombres y almacenamiento en caché en la red, permitiendo la entrega eficiente de contenido y mejorar

la entrega de datos, especialmente en redes descentralizadas donde la eficiencia es crucial (Guo et al., 2019; Kharjana et al., 2023). No obstante, es de aclarar que NDN no presenta compactibilidad directa con BC, ya que las aplicaciones de BC (sin permisos) generalmente requieren la transmisión de transacciones y bloques en tiempo real, lo cual no es compatible con el diseño *"pull"* de NDN.

Es bajo esta premisa que BoNDN (BC sobre NDN) se presenta como alternativa de integración. Este se basa en un diseño central de NDN y trata cada tipo de datos que necesita ser transmitido individualmente (Guo et al., 2019). BoNDN, además, propone un enfoque de suscripción-push para soportar la transmisión de bloques, en el cual cada minero realiza una suscripción, y una vez que se genera un bloque, el minero suscrito recibirá el bloque (Benmoussa et al., 2023).

En el campo del desarrollo de aplicaciones, el surgimiento de patrones arquitecturales propios para BC es ya una realidad que presagia la evolución de la tecnología en cuestión. Alzhrani et al. (2023) describen doce patrones aplicables a 400 aplicaciones existentes en la actualidad.

En esta misma línea, se halla el desarrollo de algoritmos y librerías tolerantes a fallas bizantinas BFT. Castro y Liskov (2001) describen un nuevo algoritmo BFT de replicación, concebido para el diseño de sistemas altamente disponibles que toleren fallos bizantinos. El algoritmo es empleado en entornos asíncronos como internet, incorpora mecanismos que previene nodos defectuosos y permite una rápida recuperación de réplicas de forma proactiva. Su tolerancia a fallos se garantiza siempre que menos de 1/3 de las réplicas presenten fallos en la ventana de falla. Castro y Liskov (2001) también presentan una implementación del algoritmo como una biblioteca genérica y su aplicación para construir el primer sistema de archivos NFS tolerante a fallos bizantinos.

Ahora bien, alternativas de autenticación diferentes a las tradicionales, como el uso de encriptación basada en atributos (ABE), garantizan que solo aquellos que poseen ciertos atributos pueden acceder a la información puede ser una solución efectiva para el control de acceso y la compartición de datos encriptados (Hong et al., 2022). ABE puede dividir generalmente en dos patrones: ABE de política de texto cifrado (CP-ABE) y ABE de política de clave (KP-ABE). La política de acceso se incorpora en los textos cifrados y la clave privada del usuario se asocia con una colección de atributos como la ubicación, rango de edad, direcciones de correo entra otros. No obstante, ABE puede ser vulnerable a ataques como el abuso y la custodia de claves (Arshad et al., 2023). En resumen, ABE es una herramienta poderosa

para el control de acceso y la compartición de datos, pero presenta desafíos que deben abordarse para su implementación efectiva.

En términos de confianza, las llamadas redes BC sin permiso, brindan capacidades de confianza entre partes sin conocimiento previo entre sí. Este principio puede permitir efectuar transacciones directamente, lo que resulta en que las transacciones se entreguen más rápido y con costos más bajos. Por otro lado, una red BC que controle más estrictamente el acceso, llamada redes con permiso y donde existe cierto nivel de confianza entre las partes, presenta capacidades que ayudan a reforzar esa confianza.

Otro aspecto fundamental es el desempeño que resulta de la alta relevancia para permitir la evolución de una tecnología; esto es prometedor dado el aumento de transacciones por segundo (TPS) al pasar de 4-6 TPS desde la primera generación BC a 100.000-300.000 TPS en la cuarta y las potenciales que se alcanzará en una quinta generación con la adopción de tecnologías como 6G (Hasan et al., 2022).

No podría faltar en este discernimiento la disponibilidad de las redes BC. El interactuar permanente con el ciberespacio ha creado una fuerte dependencia de las aplicaciones y espacios de interacción que constituyen un ecosistema "vital". En este contexto, es determinante la construcción de una alta disponibilidad de los recursos, garantizando un servicio sin fallos y sin interrupciones (Castro & Liskov, 2001).

Bien es sabido que la primera estrategia en disponibilidad la constituye la replicación. Gracias a esta se logra redundancia en aprovisionamiento de recursos que eventualmente puedan presentar falla, y la "toma de posta" por los recursos redundantes. En BC la replicación y el empleo de algoritmos tolerantes a fallos como BFT (Byzantine-fault-tolerant) permiten la construcción de estructuras jerárquicas que optimizan el uso de recursos y aumentan la escalabilidad (Rahulamathavan et al., 2017).

Este último aspecto puede resultar no deseable en dispositivos con baja capacidad de almacenamiento, con lo que se evidencia que BC debe tener la capacidad de adaptación a diferentes escenarios, sabiendo "explotar" características particulares a necesidades específicas. De esta manera, la ventaja que puede representar el resguardo total y acumulativo de data sobre la cadena de bloques puede no ser deseable en otros escenarios.

El almacenaje de la cadena de bloques se lleva a cabo con mucha redundancia: todos los nodos completos de la red contienen una copia entera de la BC (y

sus transacciones). Esto permite a estos nodos validar de manera correcta cada nueva transacción. Tener que mantener una copia completa de la cadena puede suponer un problema para los nodos que operan en dispositivos ligeros como los dispositivos móviles (Pérez & Joancomartí, 2014).

Para finalizar, vale la pena reflexionar sobre si BC se trata de "magia" capaz de resolver toda problemática moderna, como se ha pretendido o infiere de la gran cantidad de artículos que así lo sugieren y que como bien lo anunció en su tercera "ley" Clarke (1962), "Cualquier tecnología lo suficientemente avanzada es totalmente indistinguible de la magia". La respuesta es no. Esta debe ser asumida a la par con el desarrollo de una cultura de seguridad de la información y tras el estudio de su conveniencia ingenieril en el campo de exploración.

Conclusiones

Blockchain introduce aspectos disruptivos en la construcción de sistemas de información y aplicaciones que preserven inmutabilidad y registro de transacciones. Aspectos como la descentralización, la inmutabilidad y el consenso son conceptos fundamentales en BC que han revolucionado la forma en que manejamos y confiamos en los datos digitales. La descentralización elimina la necesidad de intermediarios; la inmutabilidad garantiza la integridad de los datos, y el consenso asegura que todas las partes lleguen a acuerdos confiables en una red distribuida. Estos principios son la base de la seguridad y la confianza en las aplicaciones basadas en BC y tienen el potencial de transformar numerosos sectores.

Aunque la transparencia es una de las principales ventajas de la tecnología *blockchain,* también puede presentar desafíos, especialmente cuando se trata de proteger datos sensibles y cumplir con las regulaciones de privacidad. Aspectos como este, al lado del alto consumo energético y el crecimiento de tamaño de los nodos pueden llegar a limitar la adaptación de BC como tecnología, aunque en este trabajo se han documentado varias estrategias para su superación.

De esta manera, combinaciones como el uso de NDN y BoNDN para enfrentar problemas de conectividad con la característica de libro mayor distribuido inmutable y confiable de BC pueden ser garantía de que los datos intercambiados sean confiables y menos susceptibles a pérdidas de paquetes y sufrir ataques cibernéticos.

Blockchain no es una solución en sí misma. BC es una herramienta tecnológica que ha de ser rodeada de un plan estratégico que entienda las necesidades

del proyecto, identifique el grado de transparencia y descentralización, determine los miembros que actuarán como nodos y establezca la estructura de *blockchain* adecuada, definiendo cómo van a ser las transacciones o los Smart Contracts por ejecutar (MinTIC, 2020).

Esta revisión crítica recoge aspectos sobre las diferentes consideraciones para el desarrollo de soluciones que, mediante el uso de BC, brinden garantías en ciberseguridad y con ello la construcción de un ecosistema digital confiable.

Referencias

Ali, R., Clarke, D., & McCorry, P. (2017). Towards developing a blockchain-based approach for the secure storage of patient records. En *IEEE International Conference on E-Health Networking, Applications and Services* (pp. 400-406). IEEE.

Alzhrani, F., Saeedi, K., & Zhao, L. (2023). Architectural patterns for blockchain systems and application design. *Applied Sciences, 13*(20), 11533. https://doi.org/10.3390/app132011533

Amazon Web Services. (s. f.). What is decentralization? https://aws.amazon.com/es/blockchain/decentralization-in-blockchain/

Arshad, H., Picazo-Sanchez, P., Johansen, C., & Schneider, G. (2023). Attribute-based encryption with enforceable obligations. *Journal of Cryptographic Engineering,* (13), 343-371. https://doi.org/10.1007/s13389-023-00317-1

Back. A. (2002). Hashcash - A denial of service counter-measure [Technical report]. http://www.hashcash.org/papers/hashcash.pdf

Baena-Luna, P., & García-Río, E. (2022). Tecnología Blockchain: Desafíos presentes y futuros en su aplicación. *Revista Conocimento Online,* (2), 258-273. https://doi.org/10.25112/rco.v2.2859

Banafa, A. (2022, 22 de diciembre). Blockchain 4.0. https://www.bbvaopenmind.com/tecnologia/mundo-digital/blockchain-4-0/

Benmoussa, A., Kerrache, C. A., Calafate, C. T., & Lagraa, N. (2023). NDN-BDA: A Blockchain-Based decentralized data authentication mechanism for vehicular named data networking. *Future Internet, 15*(5), 167. https://doi.org/10.3390/fi15050167

Bitcoin.es. (2020, 17 de noviembre). Vamos por la 5ta generación de la Blockchain ¿Cuáles son? https://bitcoin.es/actualidad/vamos-por-la-5ta-generacion-de-la-blockchain-cuales-son/

Brooks, D. (2020, 9 de febrero). Criptomonedas: Qué es el "problema de los generales bizantinos" y por qué explica el origen del bitcoin. https://www.bbc.com/mundo/noticias-51380491

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification, and open issues. *Telematics and informatics*, (36), 55-81. https://doi.org/10.1016/j.tele.2018.11.006

Castro, M., & Liskov. B. (2001). Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems*, (20)4, 398-461. https://doi.org/10.1145/571637.571640

Choi., T.-M., & Siqin., T. (2022). Blockchain in logistics and production from Blockchain 1.0 to Blockchain 5.0: An intra-inter-organizational framework. *Transportation Research Part E: Logistics and Transportation Review,* (160), 102653. https://doi.org/10.1016/j.tre.2022.102653

Conoscenti, M., Vetrò, A., & De Martin, J. C. (2017). Peer to peer for privacy and decentralization in the internet of things. En *2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C), Buenos Aires, Argentina* (pp. 288-290). https://doi.org/10.1109/ICSE-C.2017.60

Criptodemy. (2023, 20 de enero). Guía sobre algoritmos de consenso Blockchain. Criptodemy ®. https://criptodemy.com/guia-algoritmos-consenso-blockchain/

Guo, J., Wang, M., Chen, B., Yu, S., Zhang, H., & Zhang, Y. (2019). Enabling Blockchain applications over named data networking. En *2019 IEEE International Conference on Communications (ICC), Shanghai, China* (pp. 1-6). IEEE. https://doi.org/10.1109/ICC.2019.8761919

Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. En A. J. Menezes & S. A. Vanstone (Eds.), Advances in Cryptology-CRYPTO' 90 (pp. 437-455). Springer. https://doi.org/10.1007/3-540-38424-3_32

Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain technology applications in healthcare: An overview. I*nternational Journal of Intelligent Networks,* (2), 130-139. https://doi.org/10.1016/j.ijin.2021.09.005

Hasan, M. K., Akhtaruzzaman, Md., Kabir, S. R., Gadekallu, T. R., Islam, S., Magalingam, P., Hassan, R., Alazab, M., & Alazab, M. A. (2022). Evolution of industry and Blockchain era: Monitoring price hike and corruption using BIoT for smart government and industry 4.0. *IEEE Transactions on Industrial Informatics, 18*(12), 9153-9161. https://doi.org/10.1109/tii.2022.3164066

Hong, L., Zhang, K., Gong, J., & Qian, H. (2022). A practical and efficient blockchain-assisted attribute-based encryption scheme for access control and data sharing. *Security and Communication Networks*, (2022), 4978802. https://doi.org/10.1155/2022/4978802

Hurtado, J. S. (2021, 1 de julio). Qué son las DLT y en qué se diferencian de Blockchain. https://www.iebschool.com/blog/que-son-las-dlt-y-en-que-se-diferencian-de-blockchain-digital-business/

Kharjana, M., Pohrmen, F. H., Sahana, S. C., & Saha, G. K. (2023). Blockchain-based key management system in named data networking: A survey. *Journal of Network and Computer Applications,* (220), 103732. https://doi.org/10.1016/j.jnca.2023.103732

Konkin, A., & Zapechnikov, S. (2023). Zero knowledge proof and ZK-SNARK for private blockchains. *Journal of Computer Virology and Hacking Techniques,* (19), 443-449. https://doi.org/10.1007/s11416-023-00466-1

Krichen, M., Ammi, M., Mihoub, A., & Almutiq, M. (2022). Blockchain for modern applications: A survey. *Sensors, 22*(14), 5274. https://doi.org/10.3390/s22145274

Leka, E., Selimi, B., & Lamani, L. (2019). Systematic literature review of blockchain applications: Smart contracts. En *2019 International Conference on Information Technologies (InfoTech)* (pp. 1-3). IEEE. https://doi.org/10.1109/InfoTech.2019.8860872

Lorenzo, C. (2020). Blockchain for copyright and intellectual property protection. En *Handbook of research on emerging business models and managerial strategies in the nonprofit sector* (pp. 180-198). IGI Global.

Martínez-Ríos, F. O., Marmolejo-Saucedo, J. A., & Abascal-Olascoaga, G. (2020). A new protocol based on blockchain technology for transparent operation of corporate social responsibility. En S. García-Álvarez & C. Atristain-Suárez (Eds.), *Strategy, power, and CSR: Practices and challenges in organizational management* (pp. 205–233). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83867-973-620201012

Ministerio de Tecnologías de la Información y Comunicaciones [Mintic]. (2022). *Guía de referencia de Blockchain para la adopción e implementación de proyectos en el Estado colombiano.* Mintic. https://gobiernodigital.mintic.gov.co/692/articles-161810_Ley_2052_2020.pdf

Mohaisen, A., & Kim, J. (2013, 22 de diciembre). The Sybil attacks and defenses: A survey. https://arxiv.org/abs/1312.6349

Moran, T., & Orlov, I. (2019). Simple proofs of space-time and rational proofs of storage. En A. Boldyreva & D. Micciancio (Eds.), *Advances in Cryptology–CRYPTO 2019* (pp. 381-409). Springer International Publishing. https://eprint.iacr.org/2016/035.pdf

Mougayar, W. (2016). *The business Blockchain: Promise, practice, and application of the next internet technology.* Wiley.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction.* Princeton University Press.

Ortega Llorente, P. O. (2023). Estudio comparativo de algoritmos de consenso para una Blockchain orientado al consumo de energía [Tesis de pregrado, Universidad Politécnica de Madrid]. Repositorio UPM. https://oa.upm.es/75158/1/TFG_PABLO_ORTEGA_LLORENTE.pdf

Pérez Solà, C., & Joancomartí, J. (2014). Bitcoins y el problema de los generales bizantinos. En R. Álvarez Sánchez, J.-J. Climent Coloma, F. Ferrández Agulló, F. Martínez Pérez, L. Tortosa Grau, J. F. Vicent Francés, A. Zamora Gómez (Coords.), *Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información RECSI XIII: Alicante, 2-5 de septiembre de 2014* (pp. 241-246). https://rua.ua.es/dspace/handle/10045/40461

Popchev, I., Radeva, I., & Velichkova, V. (2021). Blockchains in enterprise global risk management. En *2021 International Conference Automatics and Informatics (ICAI)* (pp. 282-287). IEEE. https://doi.org/10.1109/ICAI52893.2021.9639500

Raikwar, M., & Gligoroski, D. (2021). R3V: Robust round robin VDF-based consensus. En *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)* (pp. 81-88). IEEE. https://doi.org/10.1109/BRAINS52497.2021.9569781

Relictum Pro. (s. f.). Is blockchain 5.0 of the latest generation. https://relictum.pro/

Romero Ugarte, J. L. (2018). Distributed ledger technology (DLT): Introduction. *Economic Bulletin,* (4) 2-11. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3269731

Sayeed, S., & Marco-Gisbert, H. (2019). Assessing Blockchain consensus and security mechanisms against the 51% attack. *Applied Sciences, 9*(9), 1788. https://doi.org/10.3390/app9091788

Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations. *Electron Markets,* (32), 1779-179. https://doi.org/10.1007/s12525-022-00536-0

Soto, M. G. (2018, 6 de agosto). El problema de los generales bizantinos (PGB). https://marvin-soto.medium.com/el-problema-de-los-generales-bizantinos-pgb-e0cb8c4279c2

Sun, X., Yu, F. R., Zhang, P., Sun, Z., Xie, W., & Peng, X. (2021). A survey on zero-knowledge proof in blockchain. *IEEE Network, 35*(4), 198-205. https://doi.org/10.1109/MNET.011.2000473

Swan, M. (2015). *Blockchain: Blueprint for a New Economy* (1st. ed.). O'Reilly Media, Inc.

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the Technology behind Bitcoin Is Changing Money, Business, and the World.* Penguin.

Vamsi_Cz5cgo. (2016, enero 28). The Architecture of Blockchain (4/5). https://www.vamsitalkstech.com/blockchain/the-architecture-of-blockchain-45/

Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. *Financial Innovation, 5*, 27. https://doi.org/10.1186/s40854-019-0147-z

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain Technology? A systematic review. *PLoS ONE, 11*(10), e0163477. https://doi.org/10.1371/journal.pone.0163477

Zheng, J., Huang, H., Zheng, Z., & Guo, S. (2023). Adaptive double-spending attacks on PoW-based Blockchains. En *IEEE Transactions on Dependable and Secure Computing* (pp. 1-13). IEEE. https://doi.org/10.1109/TDSC.2023.3268668

Capítulo 3

La cadena logística del Ejército Nacional de Colombia y ciberseguridad y ciberdefensa: atención a la academia*

DOI: https://doi.org/10.25062/9786287602700.03

Sergio Barrios Torres
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este capítulo examina el interés estratégico del Ejercito Nacional de Colombia por los estudios en que se vincula la relación entre la ciberseguridad, la ciberdefensa y la logística militar; destaca la necesidad imperiosa de ampliar el conocimiento en este ámbito, tanto en la academia como en la actualización de la doctrina militar, para fortalecer la seguridad nacional; señala que las capacidades logísticas en apoyo de las operaciones militares son de gran importancia estratégica; indica posibles rezagos conceptuales y de acción que podrían convertirse en debilidades operativas, y sugiere reflexiones como base para futuras investigaciones y desarrollos doctrinales, con el objetivo de mejorar y proteger la cadena logística militar del EJC desde una perspectiva emergente de ciberseguridad.

Palabras clave: cadena de suministro; cadena logística; ciberdefensa; ciberseguridad; estrategia; logística militar.

* Capítulo de libro resultado del proyecto de investigación *"Tecnologías disruptivas, logística, seguridad y defensa nacional en el ciberespacio"*, del grupo de investigación *"Ciberespacio Tecnología e Innovación"*, de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado C por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) y registrado con el código COL0181179. Los puntos de vista y los resultados de este capítulo pertenecen a los autores y no necesariamente reflejan los de las instituciones participantes.

Sergio Barrios Torres
Magíster en Logística Integral, Universidad Militar Nueva Granada, Colombia. Especialista en Seguridad y Defensa Nacional y especialista y diplomado en Comando y Estado Mayor, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia.
https://orcid.org/my-orcid?orcid=0000-0001-7207-4605 - Contacto: **sergio.barrios@esdeg.edu.co**

Citación APA: Barrios Torres, S. (2024). La cadena logística del Ejército Nacional de Colombia y ciberseguridad y ciberdefensa: atención a la academia. En M. E. Realpe Díaz, & A. M. González González (Eds.), *Tecnologías disruptivas, logística y seguridad y defensa nacional en el ciberespacio* (pp. 77-110). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602700.03

TECNOLOGÍAS DISRUPTIVAS, LOGÍSTICA Y SEGURIDAD Y DEFENSA NACIONAL EN EL CIBERESPACIO
ISBN impreso: 978-628-7602-69-4
ISBN digital: 978-628-7602-70-0
DOI: https://doi.org/10.25062/9786287602700

Colección Ciberseguridad y Ciberdefensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2024

Introducción

La logística militar es un elemento sensible y del más alto impacto en el sistema de seguridad y defensa del Estado. Esta importancia se interpreta en la intención de la actualización doctrinal del Ejército Nacional de Colombia que la destaca como una función que congrega la aplicación de la estrategia militar y la agrupación de labores y sistemas unidos por un propósito común expresados a manera de objetivos militares y tareas de apoyo a las operaciones militares terrestres y de defensa nacional. En dicha actualización doctrinal, se han destacado las funciones de conducción de la guerra, entre ellas la de sostenimiento, a la cual se atribuye el empleo de sistemas representados en personal, conocimiento, labores e infraestructura que proporciona apoyo y servicios destinados al cumplimiento de objetivos operacionales que proveen al comandante militar de todo nivel el ostentar "libertad de acción, extender el alcance operacional, y prolongación de la resistencia" ante los embates de las amenazas o el enemigo (Fuerzas Militares de Colombia, 2018, p. 66).

Sumado a lo anterior, el concepto de ciberespacio aborda y reúne tanto la ciberseguridad, como la ciberdefensa, de suerte que el ciberespacio es definido como un espacio compuesto y originado con el cual se vinculan el libre flujo de datos ubicado y transmitido por redes informáticas, que se fundó inicialmente para empleo de Fuerzas Militares (FF. MM.) y que posteriormente se trasladó y desarrolló al ámbito de empleo de las sociedades en general, de tal manera que exige interpretar en el mundo globalizado actual, las vulnerabilidades que se representan en los sistemas de información militar y no militar que pueden llegar a filtrar, corromper o destruir datos en beneficio político e igualmente militar, especialmente dando lugar a debilidades o falta de control a través acceder a cierta información o dar cuenta de conocimiento sobre información sensible, motivando incluso intervención,

alcance de certeza de acceso de capacidades y hasta influir en el comportamiento social mediante la tergiversación de narrativas o de la misma información (OTAN, 2020, pp. 1-2).

La importancia conceptual de la ciberdefensa se aprecia en lo expuesto por Sánchez (2020), quien, citando conceptos emanados de la Comisión de Regulación de Comunicaciones CARI, 2009, concibe la ciberseguridad como:

> conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos y usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. (p. 35)

En consecuencia, se destaca el desempeño de lo que es la ciberseguridad, adicionando que esta corresponde a

> […] todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas, lo anterior, según lo que se ha considerado desde el Parlamento Europeo (2019) y el Consejo de la Unión Europea, bajo la labor de la Agencia de la Unión Europea para la Ciberseguridad. (p.32)

Este capítulo examina el interés estratégico del Ejercito Nacional de Colombia por los estudios en que se vincula la relación entre la ciberseguridad, la ciberdefensa y la logística militar, abarcando, además, la función de conducción de la guerra de sostenimiento, por lo que esta investigación se propone formular razones que den cuenta de la importancia de la promoción del conocimiento, ante la sociedad académica vinculada para aumentar los aspectos temáticos específicos.

En el ciberespacio se han generado transformaciones que impactan directamente en la seguridad de la información, como lo evidencia el incremento de medidas preventivas contra ataques cibernéticos, la asignación de recursos, la adquisición de equipos y el desarrollo de conocimientos especializados, es decir, se observa una mayor dependencia tecnológica que incrementa las amenazas en el ámbito digital. Es fundamental, por lo tanto, que la academia focalice sus esfuerzos en fortalecer mecanismos de ciberdefensa y ciberseguridad, especialmente en lo que respecta a la seguridad de la cadena de logística militar de sostenimiento.

Esto implica ampliar el conocimiento sobre posibles amenazas que puedan comprometer las capacidades, ventajas y desventajas del sistema de apoyo operacional del Ejército Nacional de Colombia, el cual constituye un pilar en la defensa y seguridad del Estado.

Ante esta preocupación, los procesos de planeamiento y conducción de operaciones requieren de adaptabilidad, por lo cual es importante generar estrategias militares de superioridad en tiempo real sobre las diversas amenazas que afecten el desempeño normal del factor logístico militar, a causa de no entender las posibles afectaciones de cadenas de suministro del sector Defensa en Colombia.

Ciberseguridad, ciberdefensa y logística militar del Ejército Nacional de Colombia

Muchas funciones y desempeño de la logística militar dependen hoy del apoyo de redes informáticas y del uso de información y flujos de bienes, cuyo funcionamiento estriba en un entorno complejo que incluye el manejo de capital humano, infraestructuras, sistemas de entrenamiento, sostenimiento de capacidades, sistemas de adquisición y administración de *stocks,* así como de los modos y medios de suministro y abastecimientos de diversas clases, que requieren administrarse por estar ubicados de manera estratégica, adaptados a entornos definidos por capacidades propias y por el ambiente operacional.

Por lo tanto, al realizar las acciones militares de defensa y de seguridad por parte del Ejército Nacional, se ha desarrollado una cadena logística en constante evolución, pasando de acciones de simple adquisición de suministro de bienes y servicios, hasta lograr un mejoramiento productivo, administrativo y operacional táctico como apoyo estratégico. Hoy la logística militar del EJC acuña parte de su desempeño sobre el acceso a las tecnologías de la información. Por lo anterior y no siendo ajena la dependencia tecnológica, se establece una creciente necesidad de resistir ante todo tipo de arremetidas informáticas o de ciberataques que favorecen latentemente la acción de las amenazas o de adversarios sobre la obtención de información sensible representada en activos estratégicos y que permitirían evidenciar las capacidades de apoyo logístico y de sostenimiento propio.

¿Qué tanto puede afectar la falta de desarrollo académico y doctrinal sobre la relación *logística militar, ciberseguridad y ciberseguridad* en apoyo de las operaciones del Ejército Nacional de Colombia? Ante este interrogante, el presente capítulo analiza la necesidad de aumentar el enfoque investigativo y académico en apoyo

a la doctrina que aborde la relación entre la logística militar, la ciberseguridad y la ciberdefensa.

En respuesta a la problemática planteada y al interrogante central, se establece un objetivo general que servirá como eje conductor de la investigación. Este objetivo se alcanzará mediante análisis intermedios específicos para promover un desarrollo óptimo de la propuesta de investigación. Se emprenderá un camino destinado a resaltar la importancia de ampliar el conocimiento académico sobre la relación entre ciberseguridad, ciberdefensa y logística militar, tanto en el ámbito académico, como en el doctrinal y operacional del EJC.

En complemento, se da lugar a alcance de análisis u objetivos intermedios, por lo cual se estima inicialmente: conceptuar y establecer la importancia de la relación ciberdefensa, ciberseguridad y cadena logística del EJC como factor determinante de su cadena de suministro y fortalecer el desempeño de la función de conducción de la guerra (FCG) sostenimiento.

En una segunda instancia, se da lugar a determinar y justiciar la adopción o consideración del abordaje interpuesto por diferentes medios y conceptos, sobre los cuales se sustenta la importancia de orientar a la academia en la investigación y mayor desarrollo del conocimiento puesto sobre la relación entre la cadena logística del EJC y la ciberseguridad, como factor de mejoramiento sobre el desempeño de la cadena de suministro, el desempeño del sistema integrado de gestión logística y, obviamente, la FCG sostenimiento.

Además, y como último propósito intermedio y específico, se pretende formular un análisis que establezca fortalezas, debilidades, oportunidades y amenazas sobre la cadena logística del EJC, su cadena de suministro, a partir del aumento del desarrollo de la investigación y estudio vinculado a la relación ciberseguridad, ciberdefensa y cadena logística del EJC, para obtener una herramienta de apoyo al desempeño de su cadena de suministro.

Métodos

Esta investigación, de enfoque cualitativo, se basa en un área del conocimiento en temas específicos: la logística, la logística militar, la ciberseguridad y la ciberdefensa, por lo que, según Hernández et al. (2014)

> La inmersión inicial en el campo significa sensibilizarse con el ambiente o entorno en el cual se llevará a cabo el estudio, identificar informantes que aporten

> datos y guíen al investigador por el lugar, adentrarse y compenetrarse con la situación de investigación, además de verificar la factibilidad del estudio. (p. 8)

De ahí que el presente análisis implique un proceso inductivo para explorar diferentes perspectivas conceptuales y teóricas. Se recopilan datos, teorías y opiniones diversas para analizar el problema central y responder a la pregunta problema destacada, siguiendo los objetivos intermedios planteados. Además, se consideran la experiencia y las opiniones del autor, así como la contribución conceptos y opiniones relevantes. De esta manera

> postula que la "realidad" se define mediante las interpretaciones de los participantes en la investigación respecto de sus propias realidades. De este modo, convergen varias "realidades", por lo menos la de los participantes, la del investigador y la que se produce en la interacción de todos los actores. (Hernández et al., 2014, pp. 8-9)

A partir de la recolección de datos estructurados en fuentes abiertas, como artículos de investigación y publicaciones especializadas, relacionadas con la logística militar, la ciberseguridad y la ciberdefensa, se formula un enfoque desde la visión del autor especialista en logística militar, que identifica información destacada utilizada como base de exploración que sirve además como antecedente del tema propuesto.

Además, se utilizan dos técnicas adicionales: análisis bibliográfico-documental y análisis histórico-lógico. El análisis bibliográfico consiste en seleccionar y recopilar información de diversas fuentes, como bibliotecas y centros de documentación, para luego analizar y presentar resultados, contribuyendo así a la construcción de conocimiento (Matos, 2020, párr. 8).

Por otro lado, Rodríguez & Pérez (2017) plantean que el análisis histórico-lógico es un método o destreza donde

> lo histórico y lo lógico están estrechamente vinculados. Lo lógico para descubrir la esencia del objeto requiere los datos que le proporciona lo histórico […] lo lógico debe reproducir la esencia y no limitarse a describir los hechos y datos históricos. Estas ideas se resumen en que lo lógico es lo histórico liberado de la forma histórica […] El análisis de la práctica investigativa posibilita afirmar que este método se emplea comúnmente cuando se buscan los antecedentes del problema científico y durante la elaboración de los fundamentos teóricos y metodológicos de la propuesta de solución al problema […] su

> finalidad es la búsqueda de información como parte del momento de la red de indagaciones. (pp.189-190)

Por lo tanto, ante la acumulación y apropiación de datos y gestión documental de obtención de información considerada como relevante se pretende una evaluación a partir de consideraciones de valoración de información basada en principios como los establecidos por (Hitzler & Honer, 2016):

> Las técnicas fundamentales de la recopilación de datos cualitativa consisten en observar los acontecimientos, conseguir documentos […] La observación sirve para obtener impresiones sensoriales, hacer experiencias y registrar fenómenos. Los enfoques de la observación se deberían dar durante el proceso de investigación, formando las teorías, y esto con una tendencia ascendente: las observaciones se precisan y sistematizan en forma de embudo. (p. 63)

De esta manera, se revisaron más de ochenta fuentes, como artículos científicos, documentos académicos y oficiales, que abordan los temas de ciberseguridad, ciberdefensa y logística militar. Se seleccionaron las más relevantes para este documento y se incluyen en la bibliografía.

Se procura hacer una correlación entre la información recolectada y los objetivos trazados, lo cual se enuncia como lo aborda Martínez et al. (2023), un enfoque metodológico donde: "el analista toma un conjunto de decisiones para construir conocimiento ya que, se propone una secuencia sistemática y lógica […] Se aporta solidez en el proceso, en la robustez de la evidencia científica y en las competencias del investigador" (p. 79), lo anterior se orienta al cumplimiento del primer objetivo específico.

Se propone destacar la importancia de desarrollar un enfoque conceptual que explore la relación entre los temas principales. Se emplea un enfoque comparativo para evaluar cómo la ciberseguridad y la ciberdefensa afectan el desempeño de la logística militar y la cadena de suministro del EJC, analizando sus contribuciones científicas y sus similitudes y diferencias de aplicación, "lo que supone una operación mental como lo es observar, analizar e interpretar elementos que posteriormente permiten generar significados y producir conocimiento" (Jiménez, 2021, p. 181).

Se comparan factores de poder con multiplicadores en teorías y prácticas de ciberseguridad. Estas aplicaciones conceptuales y consideraciones generan el

establecimiento del objetivo mediante un enfoque constructivista y un método observacional para recopilar información simple y analizar variables. Esto ayuda al investigador a enriquecer el documento encontrando diferencias e interpretaciones personales (O´leary, 2014, citado por Rodríguez, s.f., pp. 33-35), dando lugar al porqué de proponer mayor aproximación y preocupación de llevar la ciberdefensa sobre la cadena de suministro en el sistema integrado de gestión logística, mediante ampliación doctrinal e investigación.

Consecuentemente, a fin de lograr el tercer asunto por destacar de la presente indagación y análisis, se aborda de una manera reflexiva, mediante un análisis FODA. Lo que permite establecer sobre el eje temático y profundizar en la academia la relación ciberseguridad, ciberdefensa y logística militar, una comprensión sobre debilidades, oportunidades, fortalezas y amenazas, en este caso para las FF. MM. y el conjunto, lo que representa para la estrategia militar y la seguridad y defensa nacional, como aborda Ponce (2007, pp. 114-117), quien estima una evaluación de los factores fuertes y débiles que diagnostican la situación interna de una organización o propósito, muestra de evaluar oportunidades y amenazas. El modelo por emplear se evidencia en la Figura 1.

Figura 1. *Matriz análisis FODA*

ANÁLISIS FODA	**Fortalezas** Anotar elementos propios a destacar	**Debilidades** Anotar elementos que deben revisarse/ mejorarse
Oportunidades Anotar elementos externos que pueden significar oportunidad	**Estrategias SO** Uso de fortalezas para tomar avance de las oportunidades	**Estrategias DO** Superar debilidades para tomar ventaja de las oportunidades
Amenazas Anotar elementos representan una ventaja externa y que pueda afectar intereses	**Estrategias FA** Uso de fortalezas para reducir amenazas	**Estrategias DA** Minimizar debilidades y evitar amenazas

Fuente: elaboración propia con base en AMCES (2023).

Relación logística, ciberseguridad y ciberdefensa

Logística y logística militar

El vaivén, la dinámica y la transformación de los conflictos, la guerra y las amenazas exigen hoy mantener una evolución constante debido al devenir de un mundo en constante movimiento. El ritmo frenético que la evolución de la tecnología influye el impulso de nuevas nociones, ordenamientos, métodos y medios, que se colocan a disposición de la logística a manera de instrumentos en procura del mejor sistema de apoyo a estructuras militares en su encargo estatal de proveer seguridad y defensa.

El origen de la logística integral y empresarial se dio por la preocupación de pulir movimientos de tropa, alojamiento y sostenimiento de estas a gran escala, y aprovisionamiento de pertrechos requeridos en empeños militares. De ahí que el barón de Jomini, al servicio de Napoleón I y del zar de Rusia sobre el siglo XIX, consideró la logística entre las tres estructuras por destacar al arte de la guerra, además de la táctica y la estrategia (Montanyá, 2021), por lo tanto, la logística militar se puede definir como

> parte de la ciencia y arte de la guerra, y como ella, ha sido parte de la historia de la humanidad, con la cual ha evolucionado, y se ha refinado hasta convertirse en una ciencia de aplicación a diferentes procesos de apoyo a las fuerzas operativas. La logística militar se define como "la parte del arte de la guerra que tiene por objeto proporcionar a las Fuerzas Armadas los medios necesarios para satisfacer adecuadamente las exigencias de la guerra". (FAC, 2016, p. 2)

La constante evolución de la logística luego de incorporarse al mundo empresarial impone conceptos novedosos y creación de entidades del orden mundial enfocadas en su estudio como el Council of Supply Chain Management Professionals, CSCMP, (2023) que en la actualidad propone unión de esfuerzos entre profesionales en gestión de la cadena de suministro en el mundo estudiando y aumentando el aumento de educación y desarrollo apropiados en logística.

La actualización doctrinal del Ejercito Nacional de Colombia formula que, si bien la logística militar como concepto no desaparece, sí agrega de manera destacada y evolutiva un actuar orientado en mayor dimensión sobre la aplicación y

desempeño de la logística en el campo militar; tal es el caso de organizaciones como el EJC, donde la logística se considera como

> el planeamiento y ejecución del movimiento y el apoyo de las fuerzas. Implica tanto el arte militar como la ciencia, saber cuándo y cómo aceptar el riesgo, priorizar una mirada de requerimientos y equilibrar recursos limitados, todo requiere arte militar, mientras que la comprensión de las capacidades del equipo incorpora la ciencia militar. (EJC, 2016, p. 8)

Es de enfatizar que la logística militar ha sido ampliamente definida y constituye todo el poder de soporte estructural operacional para dar lugar a lo que puede ser posible en el planeamiento estratégico y táctico de las operaciones militares, hasta el punto de considerar que casi todo es factible por desarrollarse en el campo de la táctica militar, pero solo la logística permite en gran proporción que sea posible hacerlo y hasta donde se llega.

> La actualidad de las áreas de manejo de la logística militar y el soporte que se surte mediante ella acumula responsabilidades basadas en el planeamiento y conducción de operaciones de sostenimiento que involucran producción, logística inversa, adquisición, apoyo general de ingenieros, almacenamiento, servicios en campaña, transporte, entrega, y mantenimiento. (EJC, 2018, p. 28)

Lo que indica que este amplio espectro de integración de funciones y responsabilidades se orienta a suplir necesidades complejas, para lo cual la logística es responsable de la obtención y administración de flujos de información sensible que exigen máxima seguridad tanto de sí, como de sus procesos y procedimientos. Sobre esta información y manejo de sus infraestructuras recae el peso que debe considerarse de uso crítico, por lo que el conocimiento de esta información da lugar a una conducción y manejo amparado bajo el dominio de la ciberseguridad, dadas las condiciones de ventaja que deben destacar y de su celo, ante las amenazas y capacidades que representan o conocimiento que se estima de su funcionamiento, o del denominado sistema integrado de gestión logística, denominación empleada dentro del EJC y sobre el que se especifican los flujos transversales del ejercicio sobre el que fluye su estructura.

Ciberseguridad y cadena de suministro

En cumplimiento de la estructura del presente documento, se establece que existe la realidad de colocación del ciberespacio como el quinto dominio de la seguridad.

Dicha categoría ha traído consigo la necesidad de asegurarlo, intención que se dinamiza ante la exigencia de variadas modalidades de irrupción del mismo ciberespacio. Además, se ha afianzado como concepto de poder y de defensa, a lo que se suma el uso de novedosas tecnologías evidenciando recursos al alcance de diversos actores que hacen parte del sistema internacional a manera de herramienta del equilibrio del poder, por lo tanto

> es una práctica cada vez más necesaria en un mundo cada vez más digitalizado y, por ende, más desprotegido ante los ataques informáticos, tanto internos como externos. Esto lo convierte en una actividad cada vez más atractiva para las organizaciones cibercriminales por los grandes beneficios que reporta. (UNIR, 2022, s.p.)

Así, organizaciones de todo tipo aplican medidas para dar cara y anticipadamente, ante embates, pero sobre todo para fortalecer acciones de detección y corrección que generen confianza y libre desempeño de acciones y actividades propias de la organización. Análogamente, crear un escenario diseñado desde el ámbito militar da cuenta de su relación de la ciberseguridad a partir de combatir riesgos y amenazas diversas, motivadas por enemigos a la paz, el equilibrio de las regiones, la proliferación del terrorismo y varias capacidades de dañar estructuras criminales trasnacionales, que pretenden encausar brechas sobre las capacidades militares de los Estados y alianzas estratégicas. Ante lo anterior

> La alta dependencia tecnológica de nuestra sociedad es una realidad constatable, siendo imprescindible para el buen funcionamiento de los Estados, sus fuerzas y cuerpos de seguridad y sus infraestructuras. Esta dependencia seguirá aumentando en el futuro. Las tecnologías de la información hacen posible casi todo lo que nuestras FAS necesitan: apoyo logístico, mando y control de sus fuerzas, información de inteligencia en tiempo real y un largo etcétera. (Díaz, 2011, p. 220)

El ciberespacio debe ser considerado, entonces, como una dimensión sobre la cual se trasladan los conflictos y las guerras restringiendo los límites de acción de las amenazas, y este uno de los principales motivos que requieren de toda la atención de los estrategas militares, y que pueden ser determinantes ante la intención de doblegar al contendiente o enemigo. Caso contrario la carencia o desestimación del empleo del ciberespacio en contra de las acciones de la fuerzas de defensa y seguridad de los estados, pueden suponer una amenaza significativa

autoconstruida debido a los bajos costos requeridos para causar daños a partir del empleo y uso de hábiles programadores que estén en capacidad de encontrar las más sensibles vulnerabilidades de todos tipo de sistema de defensa, de armas y, sobre todo, de los sistemas destacados para el apoyo logístico, que pueden dar lugar a poner en evidencia ubicaciones estratégicas logísticas, y hasta información relacionada con la disposición de entrenamiento de sostenimiento y las formas de hacerlo.

En su recopilación de elementos y eventos introductorios a un estudio a manera de estado del arte sobre ciberseguridad, Joyanes (2011) destaca la relación entre la ciberseguridad y el sector militar, mencionando, entre otros aspectos, que el ciberespacio y la ciberdefensa obedecen a un campo de batalla, actuando como activo nacional estratégico, que obliga a la toma de decisiones encausadas a defender las redes militares, que incluyen dominios de aire -tierra-mar-espacio y ciberespacio en lo relativo a la guerra, y subordinados a la seguridad nacional (p. 31).

De la misma manera, se hace una aproximación a situaciones consideradas como catastróficas generadas a partir de la carencia de estrategias y mal entendimiento tras ataques cibernéticos, sobre los cuales se relacionan con secretos militares logísticos y nucleares y donde además se encierran accesos a informaciones de logística militar no considerada inicialmente como clasificada, que dan apertura al conocimiento de asuntos sensibles que incluyen sistemas económicos y de adquisición y da lugar al acomodo de términos como el de las ciberarmas, haciendo alusión a equipos utilizados en complemento a las armas convencionales propias de los teatros de operaciones (p. 34), en intentos de controlar ciberataques de alto impacto.

Ciberdefensa y cadena de suministro

Ante lo ya destacado, existe la intención de desarrollar componentes que alerten e intervengan bajo detección anticipada y reactiva de intrusiones aisladas o no a las redes de flujo de información reservadas y prevenir potenciales ataques cibernéticos de organizaciones u otras naciones del orden foráneo.

Así las cosas, el concepto de *ciberdefensa* se establece como una medida ante un ciberataque, por lo tanto y en términos prácticos simples, corresponde a una renuencia sobre una acción deliberada para causar perjuicio o una consecuencia sobre algún considerado adversario orientado a obtener efectos a favor en el ámbito de las operaciones militares propia o particularmente dicho. IBM (s.f.) establece que "los ciberataques son intentos no deseados de robar, exponer,

alterar, inhabilitar o destruir información mediante el acceso no autorizado a los sistemas". Ahora bien, y en apoyo a lo anterior, la Junta Interamericana de Defensa, mediante Ganuza (2020) establece que la ciberdefensa es capacidad organizada y preparada para combatir en el ciberespacio. Comprende actividades defensivas, ofensivas y de inteligencia. (p. 14), y la ciberdefensa militar, como la unidad que aproxima: la ciberdefensa al arte militar del empleo del ciberespacio y a las operaciones militares en el ciberespacio (ciberoperaciones) y propone una taxonomía de los diferentes tipos de ciberoperaciones (p. 8).

Para la Unión Internacional de Comunicaciones (UTI), la ciberseguridad es "el conjunto de herramientas políticas, guías de acción, abordajes de gestión, acciones, mejores prácticas y tecnologías empleados para proteger la disponibilidad integridad y confiabilidad de activos en las infraestructuras interconectadas" (UTI, 2018, p. 13).

La relación entre ciberdefensa y ciberseguridad, de manera específica para el ámbito militar debe entenderse como la primera, en función de actuar mediante entidades estatales, orientadas bajo políticas que interactúan organizadamente para luchar en el ciberespacio, bajo acciones de defensa, acciones operacionales ofensivas dentro de la inteligencia militar. La segunda es, en consecuencia, las medidas formuladas y acogidas dese la estrategia militar operativa y táctica, establecidas y destinadas a la prevención o mitigar hasta la manera mínima posible afectaciones sobre los sistemas de manejo de información sensible y no sensible que permita el conocimiento detallado de los medios militares (equipos, infraestructura, manejo de personal y capacidades) de un nación o Estado empleados para su defensa y seguridad. Todo lo anterior, entendido y relacionado con las acciones provistas desde la logística militar para administrar los recursos de todo orden requerido para adelantar cualquier plan u operación militar empleando una capacidad bélica ostentada.

Logística militar, ciberdefensa y ciberseguridad

Sobre este particular, se otorga alcance a las menciones del Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE, 2023), que coloca de presente la importancia dentro de la alianza, en torno a

> el ciberespacio como un ámbito de operaciones en el que la OTAN debe defenderse con tanta eficacia como lo hace en el aire, la tierra y el mar […] que arrojan más luz sobre las implicaciones prácticas, una disuasión y defensa

> más amplias [...] la integración en la planificación operativa y las operaciones y misiones de la Alianza [...] organización más eficaz de la ciberdefensa de la OTAN y mejor gestión de recursos, habilidades y capacidades. (s.p.)

De ahí que, así como para organizaciones tan poderosas, y que asumen el aspecto de las amenazas inmersas en el ciberespacio, dan cuenta del entorno del desempeño en operaciones militares, y la influencia de la seguridad en las mismas sumado al gran desafío puesto sobre la amplia gama de actores, intereses, medios y capacidades conjuntas. Es en esta proporción en que se debe asumir la máxima seguridad sobre la información enfilando el interés en el cumplimiento de la misión y ejercer control para cumplir los propósitos deseados.

La preparación en ciberdefensa y ciberseguridad militar requiere decisión, con base en los preceptos emanados del concepto nacional de lo que debe ser la ciberdefensa nacional y, por lo tanto, debe apoyarse en otros campos de acción del Estado, como el económico y el de la logística nacional en sustento de la logística militar y de sostenimiento, primero como medio de financiamiento y segundo por ser parte de la estrategia de movilización nacional (integración de los campos del poder del Estado para enfrentar una guerra) en caso de requerirse.

La anterior discusión orienta la necesidad de asociar la ciberdefensa y la ciberseguridad con la logística militar, logrando unión de esfuerzos conceptuales, organizacionales y destacados para aumentar el desempeño de las operaciones de defensa y seguridad. De esta manera, deben fluir las ciberoperaciones militares[1] fundadas en la misión del EJC pensando en causar efectos que aporten a los objetivos de la misión logística de sostenimiento. Así, se correlacionan las ciberoperaciones con un eje articulador a partir de capacidades técnicas, logísticas y administrativas requeridas en beneficio redundante para planeamiento y conducción de operaciones militares partiendo de la premisa de fortalecer la seguridad de redes y sistemas de apoyo, causando sorpresa e iniciativa y obstaculizando intenciones de amenazas y enemigos que intenten dar cuenta de los conocimientos en ventajas logísticas y su soporte propio.

La relación entre logística militar y ciberseguridad se alcanza bajo la siguiente condición: la logística militar asume técnicas que enmarcan la planeación, realización y vigilancia de flujos de todo tipo de suministros y pertrechos, recursos físicos y financieros, además de personal especializado en satisfacer elementos

[1] Las ciber operaciones son operaciones militares que se desarrollan en el ciberespacio con los mismos objetivos que las que se producen en las dimensiones clásicas del teatro de operaciones: adquirir ventaja, conservarla, situar al enemigo en desventaja y explotarla (Real Instituto Elcano, 2014).

esenciales y que soportan necesidades de las operaciones militares. Es esta disciplina considerada entonces como eslabón primordial que garantiza el buen desempeño y fluidez de equipos críticos y comunes, sus suministros y máximo grado de disponibilidad en el instante y terreno apropiado. En la actualidad y en la era digital, la logística militar igualmente se afecta a causa de ciberataques, donde estos estriban en influencia de tecnologías de la información y comunicación (TIC), que le permiten gestión y coordinación de sus medios apropiados, de ahí la importancia de resguardarlos impidiendo que sean vulnerables ante ataques cibernéticos y robo o conocimiento de su información.

Lo anterior conlleva peligrosos efectos para el desarrollo de las operaciones militares, ya que los ciberataques destinados a las redes de información logística y en general a todos sus sistemas podrían obstaculizar o inutilizar los flujos de información y de bienes, con sus respectivos elementos, servicios, suministros, mantenimiento y especial funcionamiento, lo que implicaría una baja de la certeza operativa y la capacidad de alistamiento y respuesta efectiva requerida por la táctica militar operativa.

De ahí que adoptar medidas de ciberseguridad para los sistemas de cadena logística del EJC y su cadena de suministro involucra diseñar medidas a fin de preservar los sistemas de información y comunicación utilizados en los sistemas integrados de gestión logística militar. Lo anterior debe incluir canales de diseño de identificación de riesgos, protocolos de verificación, capacitación del talento humano destacado en logística para lograr una mejora y resiliencia frente a estos posibles efectos cibernéticos.

En síntesis, la logística militar y la ciberseguridad viven interrelacionadas debido a la gradual dependencia de sistemas de información y comunicación y su importancia en las operaciones militares. Añadiendo que, sin sistemas de logística integrales en apoyo a las operaciones, será considerada baja la capacidad de éxito y cumplimiento de la misión.

Diseño de la cadena de suministro del Ejército Nacional de Colombia

Es necesario esbozar cómo está diseñada la cadena de suministro del EJC, lo que permite distinguir su funcionamiento y poner de presente sus intervinientes, flujos y apoyos de relación recursos, planeamiento, adquisición, conducción logística y

máximo canal de distribución. Definida dicha cadena como "la interacción de tres procesos que integran el macroproceso de gestión logística de la Fuerza: planeamiento logístico; adquisición bienes y servicios, y operación logística" (EJC, 2023, s.p.).

Tabla 1. *Diseño de la cadena de suministro del Ejército Nacional de Colombia*

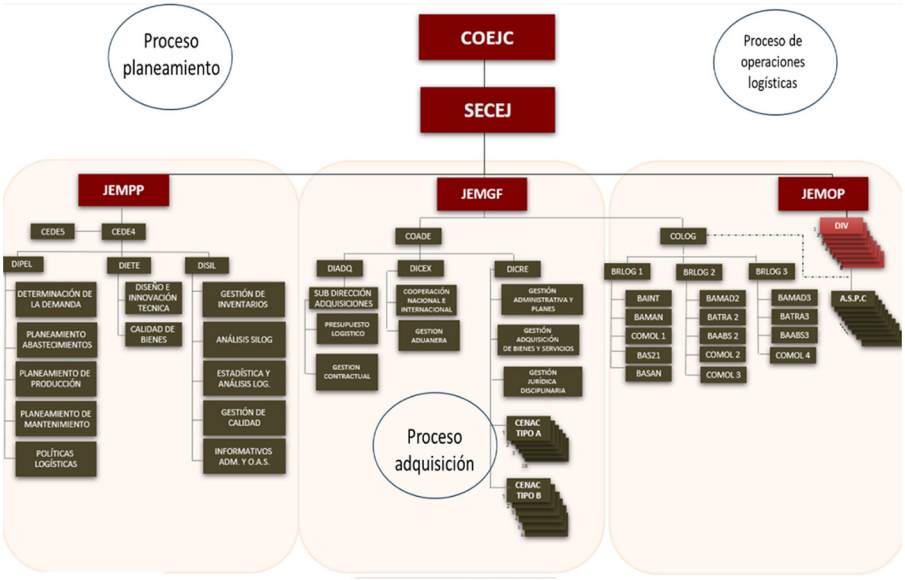
Proceso	Función	Objetivos	Gestión de procesos
Planeamiento logístico	Direccionar la logística mediante la creación de estrategias y su alineamiento en la organización.	Controlar y medir la gestión logística producción, abastecimiento, mantenimiento, servicios técnicos y transporte	Almacenamiento. Auditoría y confrontación de cargos. Contratación unidades ejecutores de presupuesto y centrales administrativas. Control de calidad productos de intendencia. Diseño, investigación y desarrollo productos de intendencia. Entrega. Exportación. Mantenimiento de maquinaria de producción. Mantenimiento de tercer nivel de armamento. Mantenimiento de tercer nivel cascos blindados. Mantenimiento segundo nivel armamento vehículos tácticos y optrónicos unidades móviles de mantenimiento. Mantenimiento tercer nivel optrónicos. Mantenimiento tercer nivel vehículos tácticos. Nacionalización. Planeación de producción. Producción material intendencia. Recepción. Registro y certificado de matrícula de una aeronave. Rehabilitación funcional. Trámite *loa's* y enmiendas. Transportes.
Adquisición de bienes y servicios	Identificación de las necesidades, selección de modalidad de compra, y todas las fases de la administración de la vida útil del bien o servicio, logrando dar sostenibilidad al Ejército.	Adquirir bienes y servicios que requiere la Fuerza mediante procesos, empleando buenas prácticas logísticas, que satisfagan las necesidades permitiendo el sostenimiento, proyección y soporte oportuno de la Fuerza.	
Operación logística	Parte de la cadena de suministro que consiste en calcular, preparar, disponer, organizar, entregar y vigilar el material, los bienes y servicios desde el punto de origen hasta el punto de consumo y satisfacer las necesidades para el funcionamiento de un Ejército y sus operaciones militares.	Garantizar la optimización de la cadena de suministro en las cantidades, el lugar, el tiempo y las condiciones exigidas por los hombres y unidades del Ejército para el sostenimiento de las operaciones miliares y la rehabilitación funcional del personal herido en combate.	Adquisición. Mantenimiento. Producción. Logística inversa. Ingenieros en apoyo general. Almacenamiento. Servicios en campaña. Transporte. Entrega.

***** Según los procesos, función y objetivos del sistema integrado de gestión logística del EJC.

****LOA:** Letter of Offer and Acceptance (Carta de oferta y aceptación).

Fuente: Sistema Integrado de Gestión Logística del EJC (2023).

Figura 2. *Sistema integrado de gestión logística, cadena de suministro del EJC y sus procesos*



Fuente: elaboración propia con base en Sistema Integrado de Gestión Logística del EJC (2023).

La Figura 2 muestra los procesos, funciones y objetivos vistos desde la organización y sus responsables, estableciendo gráficamente los tres momentos esenciales sobre los cuales se genera: planeación, adquisición y puesta en marcha de la logística militar y el sostenimiento propiamente dicho. Desde su diseño estructural, da lugar a formalizar la similitud conceptual establecida a partir de la diferencia entre la cadena de suministro y la cadena de abastecimiento.

Tabla 2. *Diferencias entre cadena de suministro y cadena de abastecimiento*

	Cadena de suministro	**Cadena de abastecimiento**
Alcance	Abarca todas las actividades involucradas en la producción, manejo y distribución de bienes y servicios.	Se enfoca específicamente en el movimiento y almacenamiento de bienes.
Objetivos	Garantizar que los productos correctos estén disponibles en el momento y lugar correctos.	Garantizar la entrega oportuna y eficiente de bienes y servicios a los clientes.
Actividades	Abastecimiento, la fabricación y la distribución.	Transporte, el almacenamiento y la gestión de pedidos.

Fuente: ISIL (2023).

Así las cosas, y dando alcance al significado de la FCG sostenimiento, en las operaciones logísticas, la producción sitúa la cadena de suministro por encima de la cadena de abastecimiento. Por lo tanto, es importante resaltar en este punto, la influencia del apoyo tecnológico que permite dar dominio fundado sobre la cadena de suministro y su manejo de información logística en el EJC, lo que implica manejo no solo de la información, sino además la administración de recursos medios y bienes. El Ministerio de Defensa Nacional, MDN, (2023) destaca al Sistema de Información Logística (SILOG) como:

> un sistema informático integrado que agrupa en tiempo real todas las funciones de la administración organizacional, trabaja en la integración de los departamentos logísticos de todas las Fuerzas con el fin de optimizar los bienes y recursos, para hacer más eficiente el abastecimiento de tropas, el mantenimiento de equipos y la compra de insumos […] implementado un sistema de información tipo ERP donde se gestiona en una misma plataforma, todos los procesos logísticos y financieros, convirtiéndose en una herramienta indispensable de soporte para la planeación, el control y fiscalización del sector. (párr.1)

En términos de su función, el SILOG

> desarrolla, integra e implementa los procesos administrativos, logísticos y financieros del sector Defensa en un sistema de información integrado, utilizando mejores prácticas y tecnología moderna para el control y administración óptima de los recursos, encaminados al apoyo efectivo de las operaciones que adelanta la fuerza pública. (párr. 3)

Tabla 3. *Manejo de Información logística SILOG*

Módulo Logístico	**Módulo de Mantenimiento**	**Módulo Financiero**
Debe subir a la plataforma SAP todos los procesos logísticos de las FF. MM., para controlar y verificar, en cada paso, desde el momento de la contratación hasta la llegada de elementos al cliente final.	El módulo de mantenimiento establece procedimientos para el mejoramiento y sostenimiento de las aeronaves de la fuerza pública y el armamento liviano.	Gestión financiera en los movimientos de los módulos Logístico y de Mantenimiento. Igualmente, se procesa la información financiera ingresada en el sistema y se evalúa el cumplimiento de normas contables y fiscales.

• Compras • Gestión de inventarios • Producción • Ventas • Plan de Compras • Calidad	• Aeronáutico • Naval • Terrestre • Biomédico • Armamento • Comunicaciones • Recursos Humanos	• Activos Fijos • Contabilidad • Presupuesto • Costos • Tesorería
Módulo Técnico Tiene como fin proveer el direccionamiento tecnológico, el mantenimiento de las aplicaciones, garantizando la seguridad y disponibilidad de la plataforma sobre la cual se opera el sistema de información. **Módulo de Seguridades y Control de Accesos** Tiene como fin realizar la gestion de los usuarios del Sistema de Informacion Logistica garantizando de esta manera la confidencialidad de la infromacion dando acceso solo al personal autorizado. **Módulo de Formacion para el trabajo** Tiene como misión facilitar el cambio organizacional que implica la implementación del sistema SAP en la fuerza pública. Tiene tres ejes: Capacitación Presencial, Capacitación Semipresencial y Sensibilización.		

Fuente: elaboración propia con base en MDN (2023).

La tabla 3 evidencia la calidad y magnitud de la información acumulada sobre la plataforma SAP, parte integral de la administración de bienes, recursos y *stock* de almacén representados en varias clases de abastecimientos, que incluyen información que da cuanta de las dimensiones de capacidades en áreas varias, y que se encuentran en forma de datos sensibles en la cadena de suministro de toda la organización del sector Defensa, las FF. MM. y el Ejército Nacional de Colombia. Sumado a lo anterior y desde la infraestructura logística del EJC y sus unidades tácticas y técnicas que manejan las operaciones logísticas se complementa la información indicando que actualmente la Fuerza cuanta con 46 unidades (batallones) de Apoyo de Servicios Para el Combate con capacidades individuales que soportan de manera regional en concordancia con la asignación territorios de la divisiones, brigadas y más sobre los comandos conjuntos, constituyéndose en una amplia red que vinculan capacidades sobre las que se generan y se nutren las fases del planeamiento de operaciones militares ofensivas, defensivas y de apoyo de la defensa a la autoridad civil.

Esta organización requiere igualmente que, a su nivel, se dé un manejo de información en aspectos administrativos que involucran, equipos de transporte, cantidades y consumo de combustible, sistemas de mantenimiento de equipos, personal destacado en labores de logística, almacenamiento y *stock* de inventarios de abastecimiento varios, elementos de apoyo de sanidad igualmente de comunicaciones, sumando capacidades de distribución entrega y suministro en cada una

de sus áreas de responsabilidad. Por lo anterior, una vez se establece y formaliza el relacionamiento entre la logística militar, la ciberseguridad y la ciberdefensa que crean un vínculo de manejo de la información que amerita ser orientado bajo la lupa y un mayor interés desde la academia y su generación de doctrina que ampare la seguridad de esta información valiosa.

Ataques cibernéticos a la cadena de suministro del EJC

La logística integral[2] y el ciberespacio[3] pueden ser considerados factores de poder y multiplicadores de eficiencia en el sostenimiento de la logística militar de varias maneras y sobre las cuales se cimenta el proponer amplitud de la academia y la doctrina a fin de fomentar el estudio de la ciberseguridad de la logística militar y de sus sistemas de gestión y de flujo de información:

Seguridad y manejo óptimo de recursos

La logística militar involucra la gestión eficaz de recursos en procura de la adquisición de medios, suministros, mantenimiento de equipos y preparación de personal. Los sistemas cibernéticos y herramientas empleados para el cumplimiento de estas funciones facilitan el seguimiento y rastreo en tiempo real de tales recursos; el correcto funcionamiento de sistemas logísticos da cuenta de tomar decisiones a partir de pronósticos de demanda orientados al sistema logístico militar, lo que admite una alta gestión y administración de los recursos. Además, los sistemas cibernéticos ayudan a anunciar y evadir inconvenientes logísticos, como la inexactitud de provisiones o el sostenimiento de equipos, mejorando así el uso de los recursos.

Dado lo anterior y sobre el sector Defensa en Colombia, es importante destacar la manera en que se ha dado importancia en este aspecto mediante la adopción de la estrategia sectorial establecida como Guía metodológica de planeamiento por capacidades (MDN, 2018)

---

2 Nuevo modelo de organización y gestión mediante el cual todos los procesos y departamentos están coordinados para redirigir los esfuerzos en una misma dirección (Esnova, s.f.).

3 Mundo no físico, sin límites, donde cualquier persona puede estar interconectada únicamente con una conexión a la red de tal manera que pueda interactuar con el mundo entero sin barreras.

> En respuesta a hacer que la estructura de Fuerza para el cumplimiento de su misión constitucional de brindar seguridad y defensa […] La proyección y desarrollo de la Estructura de Fuerza busca garantizar que la Fuerza Pública sea sostenible y eficiente en el presente y futuro. (p. 4)

Sin embargo, entidades u organizaciones como el Ejercito Nacional y, en general, las FF. MM. pueden ser foco de atención de ataques a sus cadenas de suministro, utilizando varios canales. Tal es el caso de utilización de información proveniente de proveedores externos que a su vez sea vulnerable a ataques sobre su información; ante eventos como este, se estima que existan tres ataques principales o clases de eventos:

> 1) amenazas físicas a la cadena de suministro: suelen requerir la cooperación con fabricantes y proveedores; 2) amenazas a la cadena de suministro digital: para reducir el tiempo de desarrollo, los desarrolladores de *software* utilizan una biblioteca común de terceros para realizar una función en su aplicación sobre información y acceso a las herramientas dígales, y 3) comprometer información de correos electrónicos empresariales con información financiera o destacada de negocio vinculante. (Proofpoint, 2023, párr. 7)

Se agrega, a manera de ejemplo, la ocurrencia de situaciones presentadas como la perpetrada al Sistema de Gestión de la Cadena de Suministro en 2018, y un asalto cibernético intensivo encaminado al sistema de gestión de la cadena de suministro manejado por el Departamento de Defensa de EE. UU. , complicando la seguridad de los datos afines a provisores y sus vínculos logísticos, poniendo en peligro las cadenas de suministro de las FF. MM., hecho referenciado como el ciberataque a SolarWinds. (BBC News Mundo, 2020, párr. 1).

Automatización como factor de seguridad del sistema de gestión logística

Los adelantos en tecnologías cibernéticas y automatización de técnicas agilizan y optimizan operaciones logísticas militares de sostenimiento. Ejecutan trabajos administrativos de forma expedita liberando ejecutores humanos, logrando desempeños transcendentales y de manejo más complejo. A manera de ejemplo, se ilustra el empleo de satélites militares en la eficiencia de las operaciones de la cadena de suministro.

> los satélites militares brindan una plataforma para una mayor automatización del proceso de gestión de la logística y la cadena de suministro. Mediante

> el uso de inteligencia artificial, los satélites militares pueden proporcionar un análisis automatizado de datos, lo que permite a los administradores de la cadena de suministro tomar mejores decisiones en una fracción del tiempo […] están revolucionando la logística y la gestión de la cadena de suministro, proporcionando una mejor comunicación, seguimiento de activos y automatización. Al permitir una mejor toma de decisiones. (Frąckiewicz, 2023, pp. 8-10)

Lo anterior formula la orientación a futuro del desarrollo que se establece en la dependencia del uso de tecnologías en apoyo a las cadenas de suministro dentro de la logística militar de sostenimiento, que, si bien requiere de asignación de recursos, permite evidenciar las fortalezas que ameritan mayor atención de la academia en procura de afianzar la aproximación entre la ciberseguridad, la ciberdefensa y la logística militar. A mayor avance y apoyo tecnológico en logística militar, mayor dependencia, mayor atención a la ciberseguridad orientada fortalecer la seguridad de los sistemas logísticos militares.

Sistemas de comunicación y coordinación logística

La logística militar requiere herramientas que provean en muchos y destacados casos comunicación vertiginosa entre estructuras y niveles de mando. Los sistemas logísticos apoyados en tecnologías de la información deben asegurar la toma de decisiones mediante canales seguros, logrando eficacia y máxima precisión de situación respecto de materiales y suministros propios de la cadena de suministro del sistema de gestión logística militar otorgando rapidez en la respuesta logística de sostenimiento de operaciones militares.

La cadena de suministro no ha sido ajena al impacto de las tecnologías, influyendo positivamente en su funcionamiento; este aporte también se formaliza en la administración de la logística militar, siempre con el horizonte de analizar información oportuna y detallada propendiendo por calidad de apoyo logístico, influyendo en asuntos tales como reducción de costos, reducción de tiempos de espera y mejorando la administración en asuntos de flujos de abastecimientos de diversas clases. Simchi-Levi (citado por Correa, 2008) relaciona los objetivos de las tecnologías en la administración de las cadenas de suministro:

> 1) proporcionar información disponible y visible; 2) tener en un solo punto el acceso a los datos; 3) facilitar la toma de decisiones basadas en el hecho que se tiene información de toda la cadena de suministro, y 4) permitir la colaboración entre los actores de la cadena de suministro. (p. 40)

Lo anterior permite referenciar la importancia de procesos que den cuanta del mejoramiento adaptativo establecido a partir de implementación de métodos y modelos de administración de la información en procura de evidenciar con ellos la formalización de sus deficiencias posibles o de las amenazas o riesgos del manejo de dicha información a favor de la implementación de la ciberdefensa en la logística militar y las maneras estratégicas de hacer las cosas en su sistema integral de funcionamiento.

Estrategias de seguridad y protección del sistema integrado de la logística militar

El ciberespacio libra un papel decisivo en la seguridad y amparo de la logística militar. Los sistemas de ciberseguridad consiguen revelar y advertir de ciberataques, al sistema logístico militar resguardando así los procedimientos y la información considerada crítica de la logística militar. Conjuntamente, los métodos cibernéticos de seguridad logran robustecer la seguridad en la cadena de suministro, certificando la legitimidad y la realidad de los bienes, y materiales empleados para el funcionamiento del sistema de logística y funcionamiento de las FF. MM.

Pero más allá de la estrategia para lograr objetivos militares en sí, puede llegar a ser más importante la anticipación. Por lo tanto, la preparación anticipada para este caso en particular y para atender correctamente las amenazas centradas y dirigidas contra el sistema de gestión logística deberá estructurarse como parte inicial de la estrategia un apresto adelantado: por cuenta de este precepto, se adhiere al mismo lo que afirma Esbry (2021), dando cuenta de la importancia de la estrategia y aplicable a destacar una estrategia para dar protección a la información logística

> […] considerar que las características de los conflictos de nuestra era confirman la vigencia del arte de la guerra como principios filosóficos, que van desde lo estratégico a lo táctico, abarcando también áreas de la conducción integral de la guerra como lo económico, la educación, lo político, lo diplomático, la industria, etc. (p. 42)

Lo anterior invocando lo considerado por la obra de Sun Tzu, que apreciaba la importancia de vivir capacitados, dentro de su corriente filosófica centrada en "ganar la guerra antes". De esta manera, es básico que en el EJC se estudie y fructifique convenientemente esta correlación para perfeccionar sus estructuras y operaciones logísticas de sostenimiento para conservar su capacidad operativa ante cualquier amenaza y escenario posible, especialmente las relacionadas con ciberataques, fundamentalmente, los que afectan y puedan estar orientados al debilitamiento del aparato logístico de soporte operacional.

Dicho lo anterior, existen varias teorías, hipótesis o prácticas de manejo, que logran crear un marco de análisis entre la logística militar, hoy FCG sostenimiento, y la relación con la ciberseguridad, que podrían ser base de la formación de literatura y doctrina en logística militar.

Teoría de bienes y tecnología de doble uso[4]

Sostiene que la tecnología y los sistemas desarrollados en terminaciones civiles logran ser manejados para propósitos militares. En este contexto, los métodos de gestión de la cadena de suministro empleados en el ámbito comercial, junto con la tecnología asociada, pueden aplicarse igualmente para alcanzar objetivos y logros militares. Esta realidad subraya la creciente urgencia de salvaguardar estos sistemas contra posibles amenazas cibernéticas.

Sobre este hilo, los métodos empleados en gestión de la cadena de suministro utilizados comercialmente y la tecnología dispuesta en estos también pueden ser manejados para objetivos y logros militares, lo que acrecienta la necesidad de proteger estos sistemas de posibles amenazas cibernéticas. Esta relación se afina bajo la concepción de Buzan (1998):

> los aspectos sobre los que va a incidir esa revolución tecnológica están íntimamente relacionados con el desarrollo de la tecnología del sector civil. El empleo de técnicas de doble uso en el campo de las comunicaciones, los móviles, o la inteligencia, resaltan el carácter unitario de la Revolución Industrial. Se puede así indicar, que toda sociedad industrializada mantiene también un potencial militar, gracias a los conocimientos, recursos materiales, humanos, y financieros, desarrollados. De ahí también, la dificultad de separar las aplicaciones civiles de la tecnología de su empleo para uso militar. (p. 156)

El riesgo compartido en ciberseguridad[5]

Esta práctica señala que las entidades o estructuras empresariales y militares, junto con sus proveedores intervienen en el riesgo de un posible ataque cibernético. En este contexto, se espera que las empresas que proveen servicios de logística militares o generan el canal para su desarrollo tomen medidas para responder por

[4] Producto o un servicio 'que puede destinarse tanto a usos civiles como militares', es decir que generalmente se destina a un uso civil, por ejemplo, en la industria, pero que también puede servir para desarrollar armas o material militar, o viceversa, uso civil en empleo militar (Francia diplomacia, 2014).

[5] Lo que las empresas necesitan es una nueva manera de ver el riesgo y una forma más colaborativa de identificar y abordar los riesgos a los que se enfrentan (PWC, 2024).

la seguridad cibernética de sus técnicas y procedimientos internos, a fin de impedir posibles impactos nocivos en la capacidad de la Fuerza afectando su enfoque de diseño para empleo en provisión de defensa.

Este aspecto se ejemplifica en dos vías. Una vía es la orientación del empleo de los ejércitos y de cómo aportan a su ciberdefensa asumiendo posturas de apoyo tecnológico y su importancia con las cadenas de suministro y su respetivo valor dentro de la estrategia militar. La otra vía es la postura de las empresas proveedoras de tecnología no solo informática, sino la industria proveedora de sistema de armas y equipos de uso crítico. Entonces, se tiene la postura de Fernández (2016), quien relata cómo cada día la tecnología transforma la guerra y la accion de los ejércitos y su logística:

> La guerra es una lógica de transformación que, en ocasiones revierte la situación y lo que era una fortaleza se transforma en una debilidad. Lo que se acrecienta ante fallos, averías y la existencia de vulnerabilidades, que además requieren de una cadena logística compleja. (p. 8)

La segunda vía o postura se identifica con Seguridad en America (2021) que propone no solo comentar sobre la importancia de la ciberseguridad, sino que aduce la importancia de pasar de la teoría a la acción:

> En este dinamismo que vivimos y digitalización, no podemos ignorar hacia donde nos están llevando las tendencias, dentro del marco de seguridad debemos siempre cuidar el balance entre: personas, procesos/procedimientos (bajo marco legal) y la tecnología que cada vez cumple roles más trascendentales en el día a día, apoyándonos a incrementar nuestra eficiencia operacional. (párr. 7)

Lo anterior debe involucrar desde las acciones políticas y posturas de los Estados hasta la menor intervención de actores, pasando por la responsabilidad de interviniente de quienes administran la seguridad de la información militar y la seguridad que debe impartirse en las cadenas de suministro del ejército.

Teoría del control[6]

Sostiene que, en un entorno militar, es forzoso poseer un control amplio sobre toda la cadena de suministro y sus sistemas relacionados. Esto circunscribe la

[6] La teoría de control se ocupa del "sistema de control" de los "sistemas dinámicos" en los procesos y máquinas de ingeniería. El objetivo es desarrollar un modelo o algoritmo que gobierne la aplicación de las entradas del sistema para conducirlo a un estado deseado, minimizando cualquier retardo, sobreimpulso o error de estado estacionario (William, 1996).

proporción de medidas en seguridad cibernética en indivisos semblantes de esa misma cadena de suministro, a partir de la adquisición de materias primas, servicios, bienes destinados a producción y posteriormente llevados al almacenamiento hasta que se involucren en procesos u operaciones de sostenimiento de entrega en áreas de requerimiento o de combate.

> Deben gestionarse las actividades misionales y operativas propias de la entidad y definirse, de manera paralela, controles que ayuden a proteger el activo más valioso: la información. Una organización que desee ser cada día más competitiva debe tener como pilar la protección de la información, evitando su exposición ante personas malintencionadas o posibles ciberataques. (ManageEngine blog, 2022, párr. 1)

Teoría de la resiliencia o ciberresiliencia[7]

Se centra en la capacidad de una organización para recuperarse rápidamente de un ataque cibernético. En este contexto, las empresas de logística militares deben implementar medidas de seguridad cibernética para minimizar los riesgos de un posible ataque y para garantizar una rápida recuperación en caso de que ocurra un incidente.

> A nivel mundial, nos hemos visto afectados por un hecho sin precedentes, que no anticipamos y que tuvimos muy poco tiempo de maniobra para mantenernos a salvo, readaptar formas de trabajo y reajustar nuestros hábitos de consumo [...] Ante este panorama, muchas empresas deben preguntarse ¿cuál es mi capacidad y tiempo de recuperación para que mi operación logística se restablezca ante una eventualidad? La respuesta es: resiliencia. Se trata de un concepto que nuestra cadena de suministro debe tener en su ADN para salir avante de la contingencia. (SAP, 2020, párr. 1-2)

En resumen, estas teorías, hipótesis o prácticas de manejo destacan la importancia de la seguridad cibernética, de la ciberseguridad en la cadena logística militar del EJC, su cadena de suministro y su sistema integrado de gestión de logística, así como de la necesidad de implementar medidas para protegerlos ante posibles vulnerabilidades, que tendrían consecuencias considerables en redundante

[7] La ciberresiliencia o resiliencia cibernética describe la capacidad de un sistema u organización para resistir o recuperarse ante ataques o incidentes cibernéticos. De este modo, una organización ciberresiliente trabaja en pos de proteger sus activos digitales y la continuidad de sus sistemas frente a ciberataques o desastres tecnológicos (S2 Grupo, 2023).

deterioro de las operaciones militares. Por lo tanto, a partir de este anterior cúmulo de conceptos, se edifica la gestión documental de formación de doctrina que involucre el diseño de mayor cantidad de manuales de referencia, de campaña y de técnicas y procedimientos que involucren el desempeño de la táctica que proponga la protección de las cadenas de suministro en el EJC.

Matriz FODA. Ciberdefensa de la cadena de suministro del EJC

La Tabla 3 presenta la matriz FODA que analiza la importancia de aumentar el estudio de la ciberseguridad en la logística militar.

Tabla 4. *Matriz FODA*

	FORTALEZAS	**DEBILIDADES**
ANALISIS FODA	• Mayor seguridad en la gestión de información y datos militares. • Disminución del riesgo de ciberataques y vulnerabilidades en la cadena de suministro. • Compromiso con la modernización y la mejora continua de las capacidades militares.	o Limitaciones presupuestarias para la implementación de medidas de ciberseguridad a gran escala. • Falta de personal capacitado y recursos tecnológicos para implementar medidas de ciberseguridad. • Resistencia al cambio por parte de algunos miembros del personal o proveedores que no estén familiarizados con medidas de ciberseguridad en la logística militar.
OPORTUNIDADES	**ESTRATEGIAS FO**	**ESTRATEGIAS DO**
o Mejorar la eficiencia de la cadena de suministro mediante la implementación de medidas de ciberseguridad. • Aumentar la capacidad de respuesta ante posibles ciberataques, con lo que se mejora la resiliencia. • Reducir, potencialmente, los costos relacionados con la recuperación ante ciberataques gracias a la prevención.	1. Aprovechamiento de recursos: utilizar las plataformas de manejo de información y de recursos y bienes del sistema integrado de gestión logística, pero generar directrices de innovación y ajuste de procesos. 2. Alianzas estratégicas: establecer alianzas con otras organizaciones de la academia y de la empresa dando lugar al aumento de medidas que apoyen la ciberseguridad en la cadena de suministro. 3. Diversificación: usar las fortalezas internas para diversificar las medidas involucrando la mayor cantidad de intervinientes en la cadena de suministro, desde proveedores hasta quienes responden por el manejo de recursos de todo tipo. 4. Expansión geográfica: utilizar las fortalezas internas para ampliar la experiencia de manejo de ciberataques, ubicar personal experto y difundir criterios, procedimientos y estrategias. Propender por generación de equipos interdisciplinares para dar apertura a la investigación y doctrina, a partir de la recolección de información.	1. Desarrollar alianzas estratégicas: utilizar las oportunidades externas para desarrollar alianzas con otras empresas o sectores que puedan ayudar a superar las debilidades internas. 2. Mejorar la capacitación y formación del talento humano que administra la cadena de suministro, mediante directrices de mejoramiento en la capacitación y formación del personal, superando la deficiencia y carencia de habilidades técnicas específicas. Todo orientado desde la academia y la actualización doctrinal. 3. Innovación y desarrollo de nuevos productos o servicios: usar las oportunidades externas para impulsar la innovación y el desarrollo de nuevos programas y estudios que permitan actualizar la doctrina y aumentar el desarrollo académico orientado a evitar los ciberataques a la cadena de suministro de la logística del EJC. 4. Mejorar los procesos internos: aprovechar las oportunidades externas para mejorar los procesos internos de la logística del EJC, a fin de superar las debilidades y mejorar la eficiencia del manejo de la información de la cadena de suministro del sistema integrado de gestión logística.

AMENAZAS	ESTRATEGIA FA	ESTRATEGIA DA
• Falta de apoyo político o recursos disponibles para la implementación de medidas de ciberseguridad. • Incremento en ciberataques y amenazas cibernéticas. • Requerimientos gubernamentales o de la industria que no se ajusten a las capacidades técnicas actuales.	1. Mejorar la calidad y eficiencia: utilizar las fortalezas internas para mejorar la calidad y eficiencia de los procesos de producción y operaciones logísticas que presenten vulnerabilidades en el manejo de la información de la cadena de suministro. 2. Desarrollar nuevas habilidades y competencias: utilizar las fortalezas internas para desarrollar nuevas habilidades y competencias que permitan hacer frente a las amenazas. 3. Buscar nuevos espacios académicos en los centros y estructuras de formación y capacitación. 4. Establecer alianzas estratégicas: utilizar las fortalezas internas para establecer alianzas con otras Fuerzas compartiendo experiencias con las cadenas de suministro que integran la cadena de abastecimiento de las FF. MM.	1. Aumentar la competitividad de la Fuerza y su sistema integrado de gestión logística y de su cadena de suministro mediante la generación de propuestas estratégicas llevada a los actores políticos en busca de apoyo de fortalecimiento ante ciberataques sobre la logística militar. 2. Aumentar la capacidad de adaptación desarrollando nuevas habilidades digitales a partir del desarrollo de la investigación para enfrentar la creciente proliferación de amenazas. 3. Utilizar la academia, la investigación e innovación desde la generación de grupos interdisciplinares que aporten y promuevan los recursos destinados para aumentar las propuestas doctrinales en manejo de ciberataques a la cadena de suministro del EJC.

Fuente: elaboración propia.

De manera general, el resultado de la matriz FODA sugiere que hay beneficios importantes en aumentar el estudio de la ciberseguridad en la logística militar, como aumentar la eficiencia de la cadena de suministro y mejorar la capacidad de respuesta ante posibles ciberataques. Sin embargo, puede que surjan obstáculos como limitaciones financieras y falta de personal capacitado y recursos tecnológicos. Al abordar estos desafíos, el EJC puede avanzar en la mejora de las capacidades operativas y la preparación para enfrentar amenazas, tanto tradicionales como emergentes, sobrevinientes sobre la cadena de logística de la Fuerza, su cadena de suministro y su sistema integrado de gestión logística en la FCG sostenimiento.

Conclusiones

La ciberseguridad y la ciberdefensa son componentes fundamentales para garantizar la integridad y confidencialidad de la información estratégica de la cadena logística del EJC y, en consecuencia, de su sistema integrado de gestión logística. El desarrollo de estudios que relacionen la ciberseguridad, la ciberdefensa y la logística militar permitirá fortalecer las capacidades de la institución para proteger y asegurar los sistemas y redes de información que involucran sistema de adquisición, manejo administrativo, *stocks,* mantenimiento de equipos, capacidades del sistema y la FCG sostenimiento materializada en sus unidades y formas de hacer las cosas.

La ciberseguridad y la ciberdefensa son cruciales para evitar ataques cibernéticos que podrían causar daños significativos en términos de infraestructura, operaciones militares y las que involucren a la seguridad nacional, en general, desde la obtención de información que permita establecer capacidades de funcionamiento del EJC.

Es importante que la academia estructurada desde las organizaciones encargadas de la doctrina y el sistema educativo de la fuerza encargada del entrenamiento y la administración de recursos de logística y sostenimiento, generen el panorama de las necesidades de impacto sobre las cuales se edifiquen los constructos para aumentar un conocimiento especializado y avanzado en el campo de la ciberseguridad, la ciberdefensa y orientado al fortalecimiento de la logística militar aplicada en el EJC, con el fin de formar profesionales altamente capacitados e integrales en estas áreas.

La integración de la ciberseguridad y la ciberdefensa en la logística militar y en la doctrina contribuirá a mejorar la gestión de los recursos y la toma de decisiones, permitiendo una mayor eficiencia operativa y logística.

La falta de estudios relacionados con la ciberseguridad, la ciberdefensa y la logística militar y el sistema integrado de gestión logística del EJC limita el desarrollo de estrategias y tácticas adecuadas para enfrentar los desafíos y amenazas cibernéticas en el ámbito de la cadena de suministro de la Fuerza.

La formación en ciberseguridad y ciberdefensa dentro de la academia militar proporciona habilidades y conocimientos necesarios para prevenir y mitigar los riesgos cibernéticos en el entorno de su cadena de suministro, de ahí la importancia destacada en la intervención de la academia ante este reto.

Un rumbo compuesto de la ciberseguridad, la ciberdefensa y la logística militar con su respectiva cadena de suministro accederá a una alta relación y asistencia entre los semejantes figurantes implicados en el amparo de los sistemas militares.

El adelanto de estos saberes proporcionará la adaptación y modernidad de las tácticas y metodologías manejadas en la ciberseguridad y la ciberdefensa, para hacer frente a hechos, amenazas y vulnerabilidades que nacen asiduamente.

La importancia de que la academia desarrolle estos estudios reside en la necesidad de formar líderes militares competentes para tomar decisiones instruidas y valiosas en el ámbito de la ciberseguridad y la ciberdefensa, en aras de proteger los intereses nacionales y garantizar la seguridad de la cadena de suministro del sistema integrado de gestión logística del Ejercito Nacional de Colombia.

Referencias

Buzan, B. (1998). Introducción a los estudios estratégicos: Tecnología militar y relaciones internacionales. *Cuadernos de Estrategia,* (99), 155-1166. https://dialnet.unirioja.es/servlet/articulo?codigo=4553585

Centro de Doctrina Conjunta [CEDOC] (Ed). (2018). *Manual Fundamental Conjunto MFC 1.0 Doctrina Conjunta.* Sello Editorial ESDEG. https://doi.org/10.25062/MFC10

Corera, G. (2020, 20 de diciembre). SolarWinds: 5 ataques informáticos de Rusia que transformaron la ciberseguridad en Estados Unidos. https://www.bbc.com/mundo/noticias-internacional-55381892

Correa Espinal, A., & Gómez Montoya, R. A. (2008). *Tecnologías de la información en la cadena de suministro. Dyna, 76*(157), 37-48. http://www.scielo.org.co/pdf/dyna/v76n157/a04v76n157.pdf

Council of Supply Chain Management Professionals [CSCMP]. (2023, 20 de octubre). Council of Supply Chain Management Professionals. https://cscmp.org/

Díaz del Río Durán, J. (2011). La ciberseguridad en el ámbito militar. *Cuadernos de Estrategia,* (149), 215-256. https://dialnet.unirioja.es/servlet/articulo?codigo=3837348

Ejército Nacional de Colombia. (2016). *MFRE 4-0 Sostenimiento.* Imprenta Ejército. https://www.cedoe.mil.co/enio/recurso_user/doc_contenido_pagina_web/800130633_4/458784/mfre_4_0_sostenimiento.pdf

Ejército Nacional de Colombia. (2018). *Manual de campaña.* Imprenta Ejército.

Ejército Nacional de Colombia. (2023, 3 de enero). Sistema Integrado de Gestión Logística. https://www.ejercito.mil.co/sistema-integrado-de-gestion-logistica/

Esbry, G. (2021). Pensamiento estratégico de Sun Tzu: Su legado a través de la historia. *Revista Visión Conjunta,* (25), 39-42. http://www.cefadigital.edu.ar/bitstream/1847939/2013/1/ESGCFFAA-revista%20Visi%C3%B3n%20Conjunta-25.pdf

Fernández-Montesinos, F. (2016, 30 de noviembre). Los militares y la tecnología [Documento de análisis, n.º, 72]. https://www.ieee.es/Galerias/fichero/docs_analisis/2016/DIEEEA72-2016_Militares_Tecnologia_FAFM.pdf

Frąckiewicz, M. (2023). El impacto de los satélites militares en la logística militar y las cadenas de suministro. https://ts2.space/es/el-impacto-de-los-satelites-militares-en-la-logistica-militar-y-las-cadenas-de-suministro/

Fuerza Aérea Colombiana [FAC]. (2016). *Manual de doctrina logística -MALOG-.* Imprenta y Publicaciones Fuerzas Militares República de Colombia. https://www.fac.mil.co/sites/default/files/linktransparencia/Planeacion/Manuales/manuales2022/malog_2016.pdf

Fundación Universitaria Internacional de la Rioja [UNIR]. (2022). ¿Qué es la ciberseguridad? Objetivos e importancia en la actualidad. https://colombia.unir.net/actualidad-unir/que-es-ciberseguridad/#:~:text=La%20ciberseguridad%20o%20seguridad%20inform%C3%A1tica,programas%2C%20de%20posibles%20ataques%20digitales.

Ganuza , N. (2020). *Guía de ciberdefensa: Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar.* Junta Interamericana de Defensa. https://www.iadfoundation.org/wp-content/uploads/2020/08/Ciberdefensa10.pdf

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la investigación* (6.a ed.). Mc Graw-Hill. https://academia.utp.edu.co/grupobasico-clinicayaplicadas/files/2013/06/Metodolog%C3%ADa-de-la-Investigaci%C3%B3n.pdf

Hitzler, R., & Honer, A. (2016). Los métodos cualitativos. En H. Sánchez (ed.), *Análisis para el estudio y la enseñanza de la ciência política: La metodologia de la ciencia política* (pp. 59-68). Universidad Nacional Autónoma de México. https://archivos.juridicas.unam.mx/www/bjv/libros/13/6180/6.pdf

IBM. (s. f.). ¿Qué es un ciberataque? https://www.ibm.com/es-es/topics/cyber-attack

ISIL. (2023). Diferencias entre la cadena de suministro y la de abastecimiento. https://isil.pe/blog/logistica/diferencias-suministro-abastecimiento/#:~:text=Actividades%3A%20la%20cadena%20de%20suministro,y%20la%20gesti%C3%B3n%20de%20pedidos.

Jiménez Jiménez, I. (2021). Elementos que identifican los métodos comparados. *Collectivus, Revista de Ciencias Sociales, 8*(2), 167-192. https://doi.org/10.15648/Collectivus.vol8num2.2021.3134

Joyanes Aguilar, L. (2010). Introducción: Estado del arte de la ciberseguridad. En Ministerio de Defensa (Ed.), C*iberseguridad: Retos y amenazas a la seguridad nacional en el ciberespacio* (págs. 13-46). Imprenta del Ministerio de Defensa de España. https://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

Lifeder. (2020). Investigación bibliográfica: Definición, tipos, técnicas. https://www.lifeder.com/investigacion-bibliografica/#:~:text=La%20investigaci%C3%B3n%20bibliogr%C3%A1fica%20o%20documental,selecci%C3%B3n%20de%20fuentes%20de%20informaci%C3%B3n

MangeEngine. (2022, 21 de julio). ¿En qué consiste un control en ciberseguridad? https://blogs.manageengine.com/espanol/2022/07/21/que-es-control-en-ciberseguridad.html

Martínez Corona, J. I., Palacios Almón, G. E., & Oliva Garza, D. B. (2023). *Guía para la revisión y el análisis documental: propuesta desde el enfoque investigativo.* Ra Ximhai: Revista Científica de Sociedad, Cultura y Desarrollo Sostenible, 19(1), 67-83. https://dialnet.unirioja.es/servlet/articulo?codigo=8851658

Ministerio de Defensa Nacional [Mindefensa]. (2018). *Guía metodológica de planeamiento por capacidades*. Ministerio de Defensa Nacional. http://capacitas.mindefensa.gov.co/storage/biblioteca/Guia_Metodologica_de_Planeacion_por_Capacidades.pdf

Ministerio de Defensa Nacional [Mindefensa]. (2023). *Sistema de Información Logística SILOG*. Ministerio de Defensa Nacional. https://www.mindefensa.gov.co/irj/portal/Mindefensa/contenido?NavigationTarget=navurl://9f049c2f279e9248da04add30057f515

Montanyá, O. (2021, 4 de enero). La logística: de la guerra al arte. https://micromegas.bsm.upf.edu/2021/01/04/la-logistica-de-la-guerra-al-arte/

NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE]. (2023, 19 de octubre). *NATO recognises cyberspace as a 'Domain of Operations' at warsaw summit.* https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/

Organización del Tratado del Atlántico Norte [OTAN]. (2020). *Allied Joint doctrine for cyberspace operations.* NATO Standardization Office. https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

Parlamento Europeo, & Consejo de la Unión Europea. (2019). *Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo* de 17 de abril de 2019. relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad»). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0881&from=FR

Ponce Talacon, H. (2007). La matriz FODA: Alternativa de diagnóstico y determinación de estrategias de intervención en diversas organizaciones. *Enseñanza e Investigación en Psicología, 12*(1), 113-130. https://www.redalyc.org/pdf/292/29212108.pdf

Proofpoint. (2023). Ataque a la cadena de suministro (Supply Chain Attack). https://www.proofpoint.com/es/threat-reference/supply-chain-attack

Rodríguez Gómez , D. (s. f.). Elección de la metodología de investigación. En *El proyecto de investigación* (pp. 33-35). Universitat Oberta de Catalunya. https://openaccess.uoc.edu/bitstream/10609/147625/3/ElProyectoDeInvestigacion.pdf

Rodríguez Jiménez, A., & Pérez Jacinto, A. O. (2017) *Métodos científicos de indagación y de construcción del conocimiento. Revista Escuela de Administración de Negocios,* (82), 175-195. https://journal.universidadean.edu.co/index.php/Revista/article/view/1647

Sánchez Acevedo, M. E. (2020). La ciberseguridad y la ciberdefensa, la necesidad de generar estrategias de investigación sobre las temáticas que afectan la seguridad y defensa del Estado. En E. S. Guerra & G. E. Medina-Ochoa (Eds.), *La seguridad en el ciberespacio: Un desafío para Colombia* (pp. 34-38). Editorial ESDEG. https://doi.org/10.25062/9789584288929.01

SAP. (2020, 6 de abril). Construyendo la cadena de suministro resiliente en tiempos de contingencia. https://news.sap.com/latinamerica/2020/04/construyendo-la-cadena-de-suministro-resiliente-en-tiempos-de-contingencia/

Seguridad en América. (2021, 13 de junio). Ciberseguridad, menos teoría y más acción. https://www.seguridadenamerica.com.mx/noticias/articulos/27840/ciberseguridad-menos-teorIa-y-mAs-acciOn

Unión Internacional de Comunicaciones (UTI). (2018). *Guía para la elaboración de una estrategia nacional de ciberseguridad:* Participación estratéginca en la ciberseguridad. Unión Internacional de Telecomunicaciones. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf

Capítulo 4

Ciencias de punta y tecnologías disruptivas en el ciberespacio y como marco y condición para la ciberdefensa de Colombia*

DOI: https://doi.org/10.25062/9786287602700.04

Carlos Eduardo Maldonado
Universidad el Bosque

Resumen: Este capítulo problematiza la importancia de las ciencias de la complejidad, sus ejes, temas y problemas en el marco de la digitalización del mundo y de la sociedad y, en consecuencia, respecto de la seguridad y defensa nacional; sostiene que las ciencias de la complejidad son ciencias de la vida que se ocupan exactamente de todo aquello de lo cual la ciencia normal se desentiende; señala que existe, asimismo, una tensión esencial entre ciencia y tecnologías, a saber, la ciencia tradicionalmente comporta un principio de democracia, mientras que, por su parte, la historia de la tecnología fue siempre la de tecnologías *prima facie* militar, y concluye que las ciencias de la complejidad permiten superar o resolver esta tensión.

Palabras clave: ciencias de la complejidad; computación; digitalización; vida.

* Capítulo de libro resultado del proyecto de investigación *"Tecnologías disruptivas, logística, seguridad y defensa nacional en el ciberespacio"*, del grupo de investigación *"Ciberespacio Tecnología e Innovación"*, de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado C por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) y registrado con el código COL0181179. Los puntos de vista y los resultados de este capítulo pertenecen a los autores y no necesariamente reflejan los de las instituciones participantes.

Carlos Eduardo Maldonado
Posdoctorado Visiting Scholar, Universidad de Pittsburgh, Estados Unidos. Posdoctorado Visiting Research Professor, Catholic University of America, Estados Unidos. Academic Visitor, Facultad de Filosofía, Universidad de Cambridge, Inglaterra. Doctor en Filosofía, K. U. Leuven, Bélgica. Profesor titular, Universidad El Bosque, Colombia. Profesor titular, Universidad del Rosario.
https://orcid.org/0000-0002-9262-8879 - Contacto: **maldonadocarlos@unbosque.edu.co**

Citación APA: Maldonado, C. E. (2024). Ciencias de punta y tecnologías disruptivas en el ciberespacio como marco y condición para la ciberdefensa de Colombia. En M. E. Realpe Díaz, & A. M. González González (Eds.), *Tecnologías disruptivas, logística y seguridad y defensa nacional en el ciberespacio* (pp. 111-142). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602700.04

TECNOLOGÍAS DISRUPTIVAS, LOGÍSTICA Y SEGURIDAD Y DEFENSA NACIONAL EN EL CIBERESPACIO
ISBN impreso: 978-628-7602-69-4
ISBN digital: 978-628-7602-70-0
DOI: https://doi.org/10.25062/9786287602700

Colección Ciberseguridad y Ciberdefensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2024

Introducción

Toda la historia de la tecnología es la historia de tecnología *prima facie* militar, esto es, para efectos de defensa, protección, control, ataque, seguridad. La historia de la tecnología es la historia de tecnología militar, belicista o guerrerista; para el caso, da igual. Desde la invención del fuego, pasando por la rueda, la aguja de tejer o hilar, el hacha, hasta hace poco. Con una notable excepción: el nacimiento de internet. Si bien diversos intentos de orígenes de internet tenían una intención militar —es toda la historia de Arpa, primero, en 1958; luego la historia en torno a Arpanet, en 1969—, internet nace como un asunto eminentemente civil y para beneficio de la humanidad, gracias al CERN —el Centro Europeo de Investigación Nuclear—, en 1989. Este hecho marca una inflexión singular en toda la historia de la tecnología.

Diversos Estados, fuerzas y corporaciones han intentado controlar internet, con distintas motivaciones y justificaciones. Es sencillamente imposible. Si bien, la inmensa mayoría de la sociedad permanece aún ignorante acerca de estos procesos, intentos y políticas, así como de un uso inteligente de internet. Quizás la mejor expresión de intento de control sobre internet sea la red Eschelon (Maldonado, 2019a). El control o la imposibilidad de control sobre internet forma parte, sin la menor duda, de una de las más álgidas aristas de la complejidad, del mundo y del conocimiento. ¿Complejidad del mundo y del conocimiento? La pregunta remite inmediatamente a las ciencias de la complejidad.

Este capítulo presenta y discute las articulaciones más importantes de las ciencias de la complejidad; genéricamente llamadas también *ciencias de punta;* en marcado contraste con la ciencia normal, hegemónica o clásica; tres maneras diferentes de apuntar en una sola y misma dirección. El "paradigma dominante", diría Thomas Kuhn, en una expresión —paradigma— con la que él mismo,

posteriormente no estuvo de acuerdo; frente al cual Kuhn habría destacado o bien la idea de "nuevo(s) paradigma(s)", o bien, mucho mejor, la revolución científica.

Por su parte, desde su nacimiento en la Grecia antigua —específicamente, en el tránsito de la Grecia arcaica a la Grecia clásica—, la ciencia siempre ha implicado democracia; una implicación que, sin embargo, no es fácil ni directa. Como habremos de ver posteriormente. En efecto, la ciencia nace en la Grecia clásica después de la Tiranía de los Treinta, y gracias al gobierno de Solón y Pericles. Nacen, primero los humanistas —que eran exactamente los sofistas; con los cuales Platón y Aristóteles se disputaban—, y luego también nace lo mejor de la filosofía, la astronomía, la geometría, la lógica, la aritmética y la medicina; y con ellas, claro, lo mejor de las artes. Esta historia de las relaciones entre ciencia y democracia ha sido suficientemente escrita a lo largo de la historia tanto como de la geografía.

Así las cosas, asistimos a una tensión esencial. Se trata de la tensión entre la ciencia y tecnología. Aquella, de corte marcadamente democrático en el sentido filosófico de la palabra. Este sentido se condensa en la expresión: *logos didomai* que en griego significa tanto pedir o demandar razones como dar, suministrar o aportar razones. Que era lo que se hacía, originariamente, en la plaza pública; en el ágora. Y luego se tecnifica en el Liceo y en la Academia. La tecnología, en general, por el contrario, con un espíritu distintivamente beligerante, defensivo y guerrero en la acepción sociológica de la palabra.

Toda la historia ha sido la tensión y la complementariedad, según el caso y el momento entre ciencia y tecnología. Significativamente, cuando T. Kuhn escribe su famoso libro sobre las revoluciones científicas, en 1962, las relaciones entre revoluciones científicas y revoluciones técnicas o tecnológicas eran de uno a cuatro. Es decir, por cada revolución teórica o conceptual había cuatro revoluciones técnicas o tecnológicas. Basta con recordar, digámoslo de pasada, que la revolución de Watson y de Crick y el descubrimiento de la estructura del ADN, importante como es o como fue, no fue una revolución teórica; sino técnica o tecnológica. Pues bien, para 2012, la relación entre revolución científica y revolución tecnológica había aumentado en una proporción de uno a diecisiete.

Asistimos a un enorme avance del conocimiento. Pero la gran mayoría de estos avances son técnicos, por minimalistas. Necesitamos una magnífica revolución teórica o conceptual. No es este el lugar para ahondar en ello.

Simple y llanamente, estamos haciendo muchas cosas, sin que necesariamente entendamos lo que estamos haciendo o cuáles son las consecuencias de lo que hacemos, o cuáles los marcos y contextos de lo que hacemos (*big picture*). O lo que es equivalente, todo parece indicar que la gestión del conocimiento en general —*knowledge management*— pareciera estar poco preocupada por la dimensión teórica del conocimiento —esto es, la investigación básica— y favoreciera mucho mejor la investigación experimental y aplicada.

Como quiera que sea, hoy no existen ya dos cosas: la ciencia, de un lado, y las tecnologías, de otra parte. No en vano, fue G. Hottois quien acuñó consiguientemente el concepto de *tecnociencia*. Las tecnologías adquieren el manto, mucho más adecuado, de ingenierías. Y la ingeniería es ciencia aplicada.

Este trabajo pivota en torno de las ciencias de la complejidad, su importancia y su sentido, en este caso, los estudios sobre seguridad y defensa. A partir de la emergencia del liberalismo, de un lado; asimismo, de otra parte, subsiguientemente, con la constitución del Estado-nación, los temas de seguridad y defensa se abrogaron, en general al Estado; y los organismos y fuerzas pertinentes.

Pues bien, ya desde sus orígenes en Locke, Hobbes y Rousseau, notablemente, los temas de seguridad y defensa hacen referencia a la protección y el cuidado de la vida. No del Estado o de un tipo de gobierno. (Habría que volver a leer a los clásicos del pensamiento liberal). Así las cosas, la tesis de este capítulo es que existen y se vienen desarrollando ciencias y tecnologías de punta que resultan altamente necesarias y pertinentes para el cuidado y la afirmación de la vida. Debemos poder conocerlas y apropiárnoslas, todos. En Colombia, a la fecha, estas ciencias y tecnologías son ampliamente desconocidos por todos los sectores gubernamentales y estatales. Bastaría una mirada cuidadosa, desde los documentos Conpes hasta los programas de desarrollo (PND); desde las distintas jurisprudencias de las altas Cortes, hasta los documentos más sensibles de las Fuerzas Militares y de Policía; o bien, desde las declaraciones y documentos del episcopado, hasta los más importantes centros del sector privado, como la Andi, y muchos más; en fin, desde las leyes aprobadas en el Congreso de la República hasta los documentos de las distintas misiones de ciencia y tecnología habidas; por ejemplo. Las ciencias de la complejidad permanecen, a la fecha, como un plato propio de las comunidades académica y científica. Los más cercano que han llegado algunos es al pensamiento sistémico. Y eso es aún muy lejano de la complejidad. Esta es la novedad de este texto.

Revoluciones científicas y tecnológicas (o industriales)

La expresión *ciencias de punta* es una manera genérica de señalar un abanico, un mosaico de ciencias y disciplinas, de técnicas y tecnologías, cada vez más entrelazadas, que han venido emergiendo con fuerza. Existe, hoy por hoy, un muy evidente avance en el conocimiento. Crecientemente emergen nuevas ciencias y disciplinas, nuevas tecnologías y comprensiones. La razón no es difícil: nunca había habido en la historia de la humanidad el número de matemáticos, biólogos, ingenieros y demás que hay hoy. Y jamás había habido tanta gente con maestrías y doctorados. En numerosas áreas podría decirse algo semejante. Vivimos, literalmente, una edad de luz.

Comprender la ciencia y la tecnología comporta poner, abiertamente, sobre la mesa, las tres revoluciones científicas habidas hasta la fecha (Maldonado, 2020a). La primera, la revolución de la ciencia clásica o moderna, cuyos dos ápices son la revolución copernicana y el desarrollo de la mecánica clásica, un trabajo que va desde Galileo hasta Newton; y con Newton, más recientemente, el desarrollo de la mecánica estadística en el siglo XIX con los trabajos de Maxwell y Gibbs. La Primera Revolución Científica tardó cuatro siglos en llevarse a cabo y produjo, como grandes construcciones, la mecánica clásica, la termodinámica, la microbiología, todas las ciencias sociales y humanas a partir del programa formulado por A. Comte, el padre del positivismo, y con muchas dificultades, la biología. *Grosso modo,* abarca desde los trabajos de Bacon, Descartes y Galileo, hasta 1905, exactamente. En las postrimerías de la ciencia clásica, comienza a nacer la ecología.

En el plano de la tecnología, se trató de la máquina de vapor, inventada por Watt en 1769 y la consiguiente maquinización del trabajo y de la sociedad. Esta circunstancia da lugar a la Primera Revolución Industrial. La maquinización de la sociedad se extiende, crecientemente, a prácticamente todos los planos de la sociedad.

La Segunda Revolución Científica va desde 1900 hasta la fecha. Consiste en la teoría cuántica. Esta comprende, cronológicamente, a la física cuántica, la química cuántica, todas las tecnologías basadas en principios o en comportamiento a cuánticos, la biología cuántica y, más recientemente, las ciencias sociales cuánticas (Maldonado, 2019b). A su vez, la teoría cuántica conoce dos momentos. El primero, que cabe denominar *clásico,* que va desde 1900 hasta 1934, con el famoso *paper* EPR, en referencia a sus autores, Einstein, Podolsky y Rosen. El segundo abarca desde los trabajos de Bohm y Feynman hasta la fecha. Y que da lugar a la

computación cuántica, el procesamiento cuántico de la información, la teleportación, el estudio de los fenómenos de tunelamiento y la criptografía. El factor que traza la división entre los periodos de la cuántica es el nacimiento de la física nuclear, a raíz de la Segunda Guerra Mundial, el Proyecto Manhattan y el subsiguiente desarrollo de la Guerra Fría, que tiene como punto de inflexión la invención de la bomba de hidrógeno por parte de la entonces URSS, en 1952.

La Segunda Revolución Científica tarda décadas en llevarse a cabo. En la escala tecnológica, el fenómeno más importante fue el nacimiento del computador y de la computación, no sin antecedentes, gracias a A. Turing. Sin la menor duda, el computador y la computación es la más importante de todas las herramientas y tecnologías jamás desarrolladas por los seres humanos, incluso por encima del dominio del fuego, la invención de la escritura, la rueda o la aguja de tejer o de hilar.

Finalmente, la Tercera Revolución Científica comienza en 1948 con el famoso artículo de Shannon y Weaver. Se trata de la revolución de la información y que se extiende hasta la fecha dando lugar a las redes sociales, nacidas todas hacia 2012. Esta revolución tarda años en efectuarse.

Tecnológicamente, entre aproximadamente los mismos tiempos, tienen lugar la Segunda, la Tercera y la Cuarta Revoluciones Industriales.

La Segunda consiste en la producción en serie y sucede a partir de los años 1910, en el marco de la Primera Guerra Mundial. La Segunda Revolución Industrial es formulada en 2011 y consiste en la importancia de internet. Con la red, se trata del nacimiento de la inteligencia artificial. La Tercera Revolución Industrial es identificada en 2016 y consiste en la síntesis de las dimensiones física, biológica y digital del mundo y de la sociedad.

Existe un alejamiento entre la Primera y la Segunda Revoluciones Industriales con respecto de la Tercera y la Cuarta y, al mismo tiempo, existe una tendencia de aproximación entre la Tercera y la Cuarta Revoluciones Industriales.

Pues bien, hay, al mismo tiempo, un distanciamiento cada vez mayor entre la Segunda y la Tercera Revoluciones Científicas, y un acercamiento entre la Tercera y la Segunda Revoluciones Científicas.

Este es el panorama grueso de la ciencia y la tecnología. Sin embargo, algunas particularidades significativas tienen lugar también. Quizá la más importante es la siguiente.

Hacia los años 1960 nacen nuevas ciencias —atención al plural—, fundadas en problemas de frontera. Cronológicamente, estas ciencias como síntesis son la siguientes:

Ciencias cognitivas

Nacen originalmente en el MediaLab del MIT hacia los años 1960. Se definen por un problema, a saber: qué es el conocimiento, para lo cual introducen un neologismo: *cognition* (cognición), para diferenciarlo del conocimiento (*knowledge*). Mientras que este es claramente antropológico, la cognición sirve para designar un problema consistente en el hecho de que las bacterias conocen, las plantas y los animales, al igual que los seres humanos, pero, además, los computadores son también susceptibles de conocimiento.

Ciencias de la Tierra

En los años 1970 se confirma una idea formulada en los años 1930 por Wegener: la tectónica de placas y la deriva continental. La Tierra es un sistema dinámico. Al mismo tiempo, la exploración del espacio exterior, un programa de investigación inaugurado por la antigua Unión Soviética pone de manifiesto que puede haber otros planetas como la Tierra. Nacen la exobiología, la astroquímica y la astrofísica. Ya en 1964 había nacido la cosmología como ciencia, conocida como la teoría inflacionaria del *big-bang*.

Ciencias del espacio

Estrechamente relacionadas con las anteriores, las ciencias del espacio consisten en la dúplice investigación sobre el espacio exterior en la búsqueda de exoplanetas, tanto como en la exploración del ecosistema en el que se encuentra el sistema solar y, a su vez, la Vía Láctea. Desde una perspectiva terrestre, se busca si eventualmente existen ciclos biogeoquímicos. Los agujeros negros y la búsqueda de comprensión del origen del universo constituyen algunas de las aristas más importantes.

Ciencias de la salud

Después del nacimiento de la medicina científica en el siglo XIX como fisiología, se produce una magnífica eclosión de ciencias y disciplinas vinculadas a la medicina y al estudio de la enfermedad. De un lado, todas las especializaciones médico-clínicas y médico-quirúrgicas y, de otro lado, el nacimiento de campos anexos y el fortalecimiento de la industria farmacéutica constituye una dimensión fantástica con enormes logros en numerosos campos, hasta la fecha.

Ciencias de materiales

A partir de los años 1980 hasta la fecha, el avance en la física e ingeniería de materiales no conoce descanso, con impactos en todas las áreas de la vida de la sociedad. Actualmente, el grafeno cobra una importancia singular, permeando lo mejor de la tecnociencia. La nanotecnología adquiere un papel singular en este espectro.

Ciencias de la vida

Estrechamente vinculadas con las ciencias de la salud, las ciencias de la vida consisten en la hibridación entre geología y microbiología, paleontología, botánica y geografía física. Es prácticamente imposible girar la cabeza y no encontrar vida; desde los extremófilos, pasando por los virus y bacterias hasta la escala humana. Significativamente, más allá de la escala humana, se trata, recientemente, también de la inteligencia y la vida artificiales.

Ciencias de la complejidad

En 1984 nacen las ciencias de la complejidad —sobre las cuales volveremos en la sección inmediatamente siguiente— dedicadas al estudio de dinámicas no-lineales, radicalmente distintas de toda la ciencia clásica o moderna. Luego de su nacimiento, en los más importantes centros e institutos de investigación, universidades, estamentos de los Gobiernos nacionales y ocasionalmente también en el sector privado, se crean espacios dedicados expresamente al estudio de sistemas de complejidad creciente.

Es importante resaltar que existen numerosos vínculos entre las ciencias como síntesis señaladas, posibles a partir de problemas de frontera.

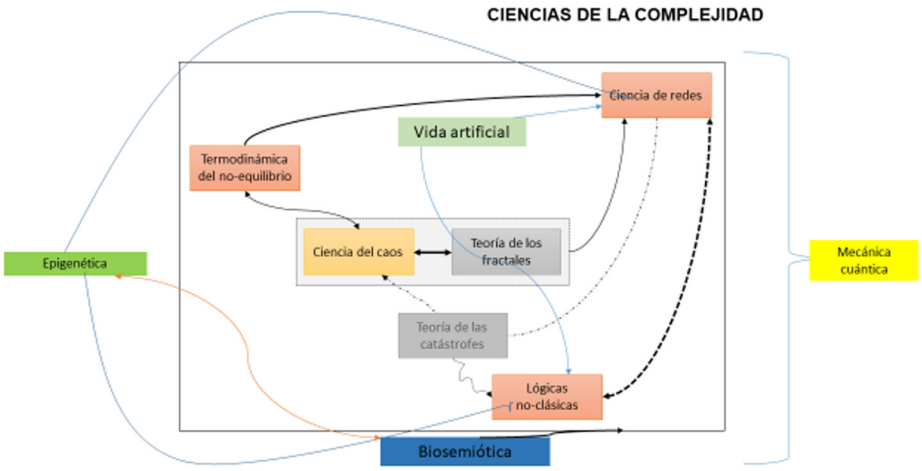
Por lo demás, en otro plano, entre finales del siglo XX y comienzos del siglo XXI aparecen las tecnologías convergentes. Estas son conocidas con el acrónimo NBIC+S. Se trata, respectivamente, de la nanotecnología, la biotecnología, las tecnologías de la información, las tecnologías del conocimiento y la dimensión social de la tecnología. (Hablar hoy por hoy de las TIC es un arcaísmo, por decir lo menos).

Sintetizando, una revolución científica es una revolución en la cosmovisión, en la forma de comprensión del mundo, la naturaleza y el universo, y del propio ser humano, dicho en general. Por su parte, una revolución industrial es una revolución en la forma como se organiza el trabajo y, con él, la sociedad.

Ciencias de la complejidad. Caracterización

Las ciencias de la complejidad nacen, conceptual, semánticamente, en 1984. Sin embargo, sus orígenes se remontan —*avant la lettre*—, al descubrimiento del cálculo por parte de Leibniz y de Newton, a las contribuciones de Gödel y de Turing, y al siempre infaltable impacto de los trabajos distintos, como son entre sí, de Hilbert y de Poincaré. Este trabajo no quiere elaborar una historia de los antecedentes, directos e indirectos de las ciencias de la complejidad. Antes bien, se trata de su caracterización, de su especificidad. Dicho esto, debe quedar claro que toda la investigación de punta en el mundo (*spearhead science*) pasa, medularmente, por las ciencias de la complejidad. Entenderlas es *conditio sine qua non* para su estudio e implementación en cualquier plano o contexto. La Figura 1 presenta el panorama general de las ciencias de la complejidad.

Figura 1. *Panorama general de las ciencias de la complejidad*



Fuente: elaboración propia.

La primera de las ciencias de la complejidad, la teoría del caos, se caracteriza porque pone en evidencia que la complejidad de un fenómeno, sistema o comportamiento consiste en su impredecibilidad. Nacida en el contexto de la meteorología, el caos no solamente hace evidente que las cosas en general son, más pronto que tarde, impredecibles, que la impredecibilidad no puede en manera alguna ser descartada, sino, por consiguiente, hace de este un tema explícito de estudio e investigación.

Un sistema caótico es un sistema altamente ordenado, pero que es impredecible. ¿Existen fenómenos y comportamientos que son predecibles? Esto es, ¿mediana o aproximadamente predecibles? Desde luego. Allí no trabaja la complejidad. Para esa clase de fenómenos predecibles existen otras herramientas, que no tienen absolutamente nada de complejidad, tales como la planeación, la prospectiva, los estudios y la teoría de probabilidad. La impredecibilidad hace referencia al hecho de que las cosas pueden ser predecibles tan solo a corto plazo; y cuanto más corto plazo, mejor. Pero que a mediano y a largo plazo, los fenómenos son crecientemente impredecibles. Desde la meteorología, el estudio del caos se extiende de fenómenos y comportamientos naturales y sociales o humanos.

Dicho lo anterior, no todas las cosas son complejas. Es más, la inmensa mayoría de cosas no lo son. Las ciencias de la complejidad trabajan únicamente en esos fenómenos que pueden ser identificados como complejos; esto es, de complejidad creciente. De suerte que a la pregunta: ¿Qué es o por qué surge la complejidad? Aparece inmediatamente una (primera) respuesta: debido a la naturaleza impredecible de las cosas. Gracias a la ciencia del caos, estamos haciendo ciencia de la impredecibilidad, por primera vez en la historia de la humanidad.

Contemporánea con la ciencia del caos, en los años 1970, surge la geometría de fractales. Se trata del reconocimiento explícito de que la naturaleza posee una dimensión fractal, en contraste con la forma clásica de entender los fenómenos naturales, basada en la geometría euclidiana. Más exactamente, la geometría de fractales consiste, dicho de manera sucinta, en una doble característica. De un lado, en la dimensión fractal que quiere significar que la estructura de una parte se corresponde con la estructura del todo; técnicamente, ello se denomina *autosimilitud;* y es objeto de mediciones matemáticas, esencialmente, basadas en iteraciones.

De otra parte, al mismo tiempo, la geometría de fractales comporta la idea de que la naturaleza es irregular. Son las irregularidades las que dan qué pensar en el marco de esta geometría, y demanda, al mismo tiempo, la capacidad de ver irregularidades; patrones y rupturas de patrones. La geometría de fractales ha sido conformada en el estudio de fenómenos humanos, naturales y también de sistemas artificiales, notablemente tecnológicos.

Dicho lo anterior, es preciso advertir que existen innumerables geometrías y que cada geometría describe un mundo propio, aparte. En una circunstancia afortunada, pero fortuita, digamos que en 1977 nace otra de las ciencias de la complejidad: la teoría de *catástrofe.* Catástrofe es el término que se usa en una teoría de origen matemático para designar cambios súbitos, imprevistos, irreversibles.

Como se aprecia inmediatamente, no es del interés de las ciencias de la complejidad estudiar tendencias, vectores, matrices. Muy por el contrario, se trata de estudiar dinámicas, cambios, espacios, procesos que tienen lugar súbitamente y que son o pueden ser irreversibles y que son, por lo tanto, imprevistos. No es difícil ver las conexiones entre varias de las ciencias de la complejidad.

Aunque no es el objeto directo de este trabajo, hay que decir inmediatamente que las matemáticas de la complejidad no son matemáticas de sistemas continuos. Muy por el contrario, sin las matemáticas de sistemas discretos. Esto quiere decir que, de una parte, la estadística normal —distribuciones normales, de Gauss, de Poisson, de Bernouilli, gama y otras, no son del interés, en modo alguno, en complejidad—. Asimismo, de otro lado, campos como el cálculo, las ecuaciones diferencias, la noción de límite, el estudio de funciones y otros más no entran en consideración en complejidad. Debe ser posible una profundización y apropiación de las matemáticas de sistemas discretos.

En 1977, I. Prigogine recibió el Premio Nobel de química por sus contribuciones a la termodinámica del no-equilibrio y por haber introducido en la ciencia lo que la ciencia no tenía: el tiempo (Prigogine, 2003). Los sistemas complejos, es lo que pone de manifiesto la termodinámica del no-equilibrio, son sistemas abiertos —no existen ni son posibles sistemas cerrados o aislados—, y lo más importante que les sucede es la flecha del tiempo, a saber: la flecha de un tiempo creciente, generador de vida, finalmente.

El equilibrio, en cualquier sentido y contexto, es siempre provisional. Más idóneamente cabe hablar de ausencia de equilibrios o, lo que es equivalente, de equilibrios dinámicos. El término técnico con el que se designan esta clase de fenómenos y sistemas es como estructuras disipativas.

Mientras que el tiempo fue un factor que siempre se descartó en el estudio de los asuntos del mundo, los estudios de Prigogine dejan ver que la complejidad existe debido justamente al tiempo. Y este no puede ser considerado como un marco de probabilidades o como un tema que va de suyo (*taken for granted*). Antes bien, el tiempo es el generador de dinámicas de no-equilibrio; en una palabra, no-lineales.

De otra parte, es la termodinámica de los fenómenos alejaos del equilibrio la que pone en evidencia que las estructuras disipativas son autoorganizativas. Esto es, las cosas verdaderamente importantes en el mundo y en la naturaleza no son el objeto de sistema de control, en ningún sentido de la palabra, sino espontáneos y por ellos mismos, robustos. La autoorganización es un enfoque o aproximación altamente importante que forma parte de las ciencias de la complejidad (Camazine et al., 2003).

Otra de las ciencias de la complejidad es la vida artificial. Nacida en 1989 por iniciativa de C. Langton, se trata de un programa estrictamente filosófico con la ayuda de la computación. La vida artificial tiene como finalidad entender qué es la vida y cómo surge, cuáles son sus dinámicas y su lógica, análogamente a cómo, en sus orígenes, la inteligencia artificial hacía lo mismo respecto de la mente o la inteligencia, con el desarrollo de la máquina de Turing. Así, sin la menor duda, la inteligencia artificial y la vida artificial constituyen, por así decirlo, dos caras de una sola y misma moneda.

Esta observación permite resaltar que las ciencias de la complejidad son el resultado de la computación, tanto como que, a su vez, constituyen activamente al desarrollo de la computación (Pagels, 1991).

En este sentido, el trabajo con complejidad es, distintivamente, el trabajo con computación, simple y llanamente como una herramienta, a saber: como la mejor herramienta desarrollada para trabajar con posibilidades.

En efecto, la complejidad no se ocupa de lo real, lo que está a la mano, lo existente, en cualquier acepción de la palabra. Para eso no hace falta complejidad. Basta la ciencia normal. Muy por el contrario, el más importante de todos los rasgos metodológicos y heurísticos de las ciencias de la complejidad es que estudian espacios de fase de fenómenos reales. Esto quiere decir, que se trata de estudiar los espacios de posibilidades de evolución de un fenómeno cualquiera. Nunca comprenderemos nada si no atendemos a los espacios de fase. Técnicamente dicho, estos espacios de fase se conocen como el *espacio de Hilbert,* en referencia a D. Hilbert. Otra manera como se ha interpretado a los espacios de fase, que permiten entonces trabajar con transiciones de fase de primero y de segundo orden, es como adyacentes posibles.

Lo real, en cualquier sentido del término, aparece por consiguiente tan solo un subconjunto de un conjunto mayor que lo comprende y lo hace posible, a saber, el mundo de las posibilidades. De las posibilidades y no de las probabilidades. Al cabo, pensar lo posible mismo comporta incluso pensar en imposibilidades. Las ciencias de la complejidad son ciencia incluso de lo imposible. Estamos haciendo ciencia de lo imposible, hoy en día (Maldonado, 2021).

En los años 2001 a 2003 nace otra de las ciencias de la complejidad: la ciencia de redes complejas. De esta suerte, la complejidad de un fenómeno se encuentra en función de las redes en las que se inscribe o a las que da lugar. Básicamente, las redes complejas son de tres tipos: redes de mundo pequeño, redes aleatorias y redes libres de escala. Vivimos un mundo alta y crecientemente conectado en

muchos sentidos, y son estas redes las que permiten entender por qué la complejidad. Esto es, por ejemplo, por qué la impredecibilidad o los cambios súbitos e imprevistos o la ausencia de equilibrios.

Quizás el mayor o mejor descubrimiento de la ciencia de redes sean los fenómenos de sincronía o sincronización, que suceden en todas las escalas de la naturaleza; incluso ya desde los sistemas físicos inanimados. Esta sincronización es conocida técnicamente como el *efecto Kuramoto*. La sincronía es un fenómeno espontáneo, que no necesita de centralidad ni de jerarquías para ser entendido.

A fortiori, existen fenómenos de sincronicidad en los sistemas naturales tanto como en los sistemas humanos. La complejidad permea a la naturaleza y, por lo tanto, la no-linealidad.

Esta es la mayor dificultad que plantean las ciencias de la complejidad y sus tecnologías y herramientas para una estructura mental formada clásicamente. Existen dinámicas espontáneas (*order-for-free,* se dice en el lenguaje técnico). Existen fenómenos de autoorganización, de abajo hacia arriba (*bottom-up*), que no requieren, en absoluto, procesos verticales, de arriba abajo (*top-down*). Este es un tema que tiene que ver directa y necesariamente con la topología que es, si cabe la expresión, el basamento matemático de la complejidad.

Como se aprecia sin dificultad, se trata de una serie de estructuras, dinámicas, procesos que nada tienen que ver con la cultura clásica: emergencias, no-linealidad, autoorganización, sincronización, orden espontáneo, ausencia de jerarquía y centralidad. Son estos rasgos y estructuras mentales las que permiten entender por qué la mayoría de las empresas, los Estados y las instancias de gobierno alrededor del mundo saben de complejidad, se han enterado de alguna manera, pero tienen serias dificultades para asumirla, implementarla, desplegarla enteramente. Manifiestamente, se trata de una revolución científica.

Un rasgo común a todas las ciencias de la complejidad aparece inmediatamente, después del panorama anteriormente presentado, ante una mirada sensible. La complejidad consiste en ver los fenómenos, dinámicas, procesos o estructuras o bien como sistemas vivos, o bien como sistemas que exhiben vida. En manifiesto contraste con toda la ciencia clásica, determinantemente mecanicista y determinista. Una radical transformación de cualquier mirada en cualquier plano o contexto que se quiera.

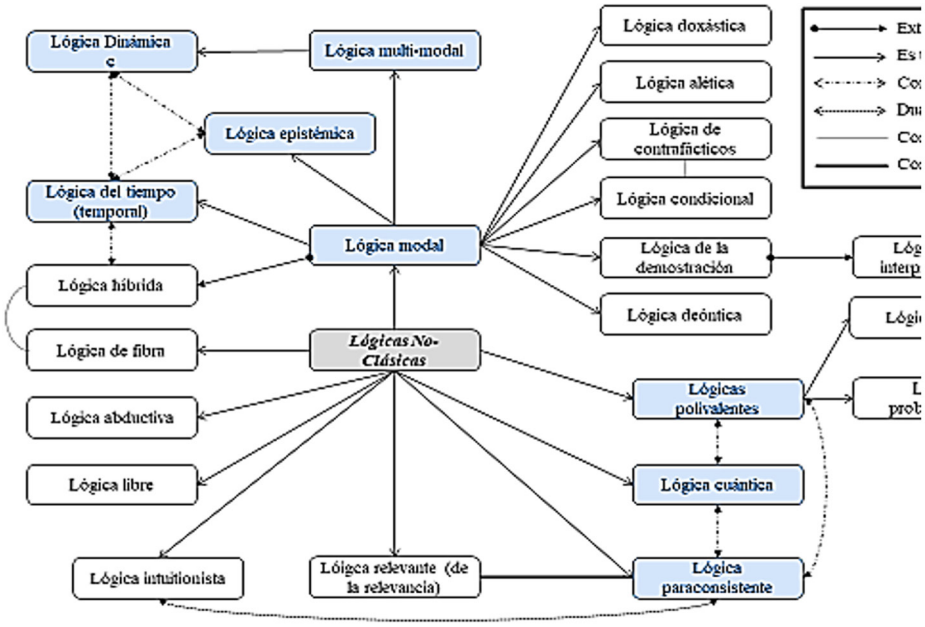
Adicionalmente, siguiendo siempre la Figura 2, otra de las ciencias de la complejidad son las lógicas no-clásicas (LNC). Hay que decir que esta idea es específicamente latinoamericana, en general, y constituye una de las contribuciones de

América Latina a la historia de la ciencia, por ejemplo, análoga al concepto de autopoiesis de Maturana y de Varela, o a las lógicas paraconsistentes de N. da Costa, o igualmente a las economías de escala, introducidas originariamente por M. Max Neef —*economías de pies descalzos,* las denominaba Max Neef—, por ejemplo. Nunca, nadie más, ni del lado de los lógicos, ni tampoco del lado de los complejólogos vio y estableció esta relación.

Las LNC constituyen un continente amplio de lógicas alterativas, la mayoría, y unas cuantas, complementarias a la lógica formal clásica también llamada *lógica estándar.* Se trata de la lógica que puede ser designada de cuatro maneras, así: como lógica matemática, lógica proposicional, lógica simbólica o lógica de predicados. Es, en cualquier caso, lógica de primer orden.

Las LNC ponen inmediatamente sobre la mesa el reconocimiento de que existe un pluralismo lógico; por lo tanto, un pluralismo de sistemas de verdad. En otras palabras, no existe una verdad única. Ciertamente un motivo de escándalo para la visión clásica. La Figura 2 ilustra el panorama de las LNC.

Figura 2. *Panorama de las lógicas no-clásicas (LNC)*



Nota: La Figura 2, sin embargo, no pretende ser completa.
Fuente: elaboración propia con base en Maldonado (2020b).

La idea fundamental es que existe un pluralismo lógico. Por consiguiente, varios mundos son posibles, lógicamente hablando. Es importante atender al hecho de que la semántica de las LNC es la semántica de mundos posibles. Se entiende así, y se refuerza, la idea de que pensar y trabajar con complejidad consiste en trabajar con posibilidades e incluso con imposibilidades.

Tal es, podemos decir, sucintamente el panorama clásico de las ciencias de la complejidad. Hay una manera apropiada de comprenderlas, dicho de forma negativa. Las ciencias de la complejidad pueden ser idóneamente comprendidas como el rechazo a cualquier forma de dualismo, determinismo, mecanicismo y reduccionismo.

Pues bien, exactamente en esta misma atmósfera y espíritu, hay dos ciencias que pueden idóneamente ser incluidas entre las ciencias de la complejidad. Se trata de la epigenética y a biosemiótica.

La epigenética, no sin antecedentes, nace en 2005 y tiene el mérito de superar la dualidad cultura-naturaleza. No solamente heredamos y trasmitimos genes; además heredamos y transmitimos experiencias. Para 2005 estaba establecido que sucede hasta tres generaciones. Para 2021, queda establecido que es un proceso que abarca hasta ocho generaciones. La epigenética ha sido confirmada en plantas, animales y seres humanos.

Como se entiende sin ninguna dificultad, la escisión entre ciencias naturales y ciencias humanas, o entre ciencias exactas y artes, o igualmente entre naturaleza y cultura es hoy por hoy perfectamente insostenible. Cualquier acción o decisión sobre un plano afecta inmediatamente al otro plano.

Por su parte, la biosemiótica se articula en tres dominios principales: la antroposemiótica, la zoosemiótica y la fitosemiótica. En todos los casos, el tema es el de la producción de signos, señales, códigos, patrones y mensajes en las escalas de los sistemas vivos. Los sistemas vivos leen signos y señales, los interpretan y correspondientemente crean nuevas señales y mensajes, constituyendo así un fantástico campo informacional que atraviesa, constituye y comprende la dinámica de los sistemas vivos en general: plantas, animales y seres humanos, dicho en general.

Como quiera que sea, es fundamental observar a la izquierda de la Figura 1. Se trata de la mecánica cuántica. La mecánica cuántica es, sin la menor duda, el punto de apoyo arquimédico de todo el edificio científico y tecnológico del mundo, hoy. Se trata de la más robusta, la más conformada, la más verificada, la más falseada de todas las teorías científicas. Ha sido confirmada y falseada hasta el onceavo

decimal: 0.00000000001. No hay absolutamente ninguna teoría que tenga semejante solidez.

La mecánica cuántica es (sencillamente) un muy técnico y difícil aparato matemático dedicado a estudiar fenómenos y comportamientos cuánticos. Se trata de fenómenos caracterizados, entre otros rasgos, por no-localidad, superposición, indeterminación, complementariedad, entrelazamiento, teleportación, superposición, tunelamiento, exclusión de Pauli y otros más. Manifiestamente, se trata de una teoría altamente contraintuitiva que, literalmente, no se funda para nada en el peso de la percepción natural o de los sentidos.

La mecánica cuántica es la mejor teoría jamás desarrollada para explicar fenómenos como: el universo, el mundo, la naturaleza, los seres humanos, la vida, en cualquier acepción o sentido de la palabra. Simple y llanamente, es imposible hoy llevar a cabo una explicación, una comprensión, y mucho menos una decisión, al margen de un conocimiento, por lo menos básico, pero sólido de la mecánica cuántica.

Digámoslo sin ambages: las ciencias de punta, dicho en general, y las ciencias de la complejidad, dicho en particular, son imposibles al margen de la mecánica cuántica. Pues bien, es justamente esta la que se articula en cinco dominios: la física, la química, las tecnologías, la biología y las ciencias sociales cuánticas.

Sería deseable presentar las disciplinas y aproximaciones de las ciencias de la complejidad. Por ejemplo, la inteligencia de enjambre, que hace referencia a que, en la naturaleza, tanto como en sistemas naturales, hay momentos en que hay colectivos que deciden actuar como un individuo, ya que así obtienen mejores resultados que si actuaran colectivamente. Los cardúmenes, los pájaros, los insectos sociales, las partículas subatómicas o las gacelas, por ejemplo, han sido ejemplos bien estudiados. Los seres humanos no han terminado de aprender estos comportamientos; ciertamente no aquellos que se rigen por los modos occidentales de pensar y de vivir.

Asimismo, habría que hacer referencia al concepto y los procesos de emergencia. Pensar en complejidad es todo lo contrario a pensar en términos de causalidad e incluso de multicausalidad; sus variantes, tales como "análisis multivariado o multidimensional" y otros. Propiedades o comportamientos emergentes quiere significar que no hay ninguna proporcionalidad entre el *input* y el *output.* El *output* es mucho más y muy diferente al *input.*

Una observación final se impone. Es perfectamente distinto *sistémico* de *complejo,* una confusión muy extendida que impera, allá afuera, incluso en el mundo

científico y académico. No es este el lugar para subrayar criterios de demarcación (Maldonado, 2023a).

Como quiera que sea, un muy claro rasgo de familia permea y define a las ciencias de la complejidad. Se trata de pensar los fenómenos como sistemas vivos o bien, lo que es equivalente, como sistemas que exhiben vida. Esta idea tiene muy serias consecuencias de orden al mismo tiempo epistémico y moral.

Herramientas matemáticas de la complejidad

Las ciencias de la complejidad son esencialmente dos cosas. De un lado, un muy robusto aparato epistemológico compuesto por diferentes ciencias, disciplinas, aproximaciones y comprensiones. Un somero panorama acaba de ser esbozado. Asimismo, son un conjunto de técnicas y herramientas muy sofisticadas. Me ocupo a continuación de estas últimas.

A título introductorio para esta sección hay que decir que existen tres clases de ciencia hoy en día que se corresponden con tres métodos o metodologías, perfectamente distintos. Se trata de la ciencia por inducción, la ciencia por deducción —las cuales corresponden a los modelos de ciencia de la Primera Revolución Científica— y la ciencia por modelamiento y simulación. Correspondientemente, cabe hablar genéricamente de tres formas principales de métodos científicos, así: métodos cualitativos, métodos cuantitativos —ocasionalmente, métodos mixtos o híbridos, que son la combinación de los anteriores— y el modelamiento y simulación como método científico.

De manera significativa, el trabajo en ciencia, mucho más que en campos, áreas, comportamientos o dinámicas, consiste en el trabajo, discusión y desarrollo de modelos. Son tres los ejes de trabajo al respecto: 1) cómo surge o se formula un modelo; 2) cómo se sostiene o se mantiene un modelo, y 3) cómo se tumba o se echa abajo un modelo. Naturalmente, puede tratarse de un modelo económico, político, educativo, financiero u otros. Pues bien, una taxonomía de modelos comprende las siguientes configuraciones:

Un modelo conceptual

Por defecto, este queda ya, en principio, siempre incluido. Se trata de la elaboración que resulta de la puesta en claro de un estado-del-arte. El modelo puede ser, genéricamente, dicho, un modelo teórico o conceptual. En los proyectos de investigaciones justamente lo que se designa como el marco teórico o como el marco conceptual. Es lo mínimo que una buena investigación puede o debe tener. Es lo normal, en todo caso.

Un modelo matemático

Existen, *grosso modo*, dos tipos de matemáticas. Las matemáticas de sistemas continuos y las matemáticas de sistemas discretos. Así las cosas, el modelo matemático comprende dos opciones. Como queda dicho, las matemáticas de la complejidad son matemáticas de sistemas discretos. Volveré sobre esta idea a continuación.

Un modelo lógico

Existen dos grandes dimensiones de la lógica. La lógica formal y las lógicas no-clásicas (LNC). Por consiguiente, un modelo lógico admite dos posibilidades. Todo depende de la fuerza de innovación o de la apuesta de riesgo del investigador. Como queda dicho, las LNC admiten una diversidad de opciones. Al respecto, todo depende de las capacidades propias de cada investigador.

Un modelo informacional

Hace referencia al uso de lenguajes de programación ya existentes. Hay numerosos lenguajes de programación para distinto uso.

Un modelo computacional

Hace referencia no ya al uso de un lenguaje de programación, sino, adicionalmente, al desarrollo de código. Esto es, debe ser posible que una buena investigación escriba código, en el estudio y explicación de un fenómeno, problema o sistema.

Quisiera decirlo de manera expresa. Una investigación debe, por lo menos, tener dos de los modelos anteriores. Por defecto, ya tiene uno: el modelo conceptual o teórico. Adicionalmente debería tener otro más. Todo depende de las fortalezas y capacidades de aprendizaje de un investigador o grupo de investigación.

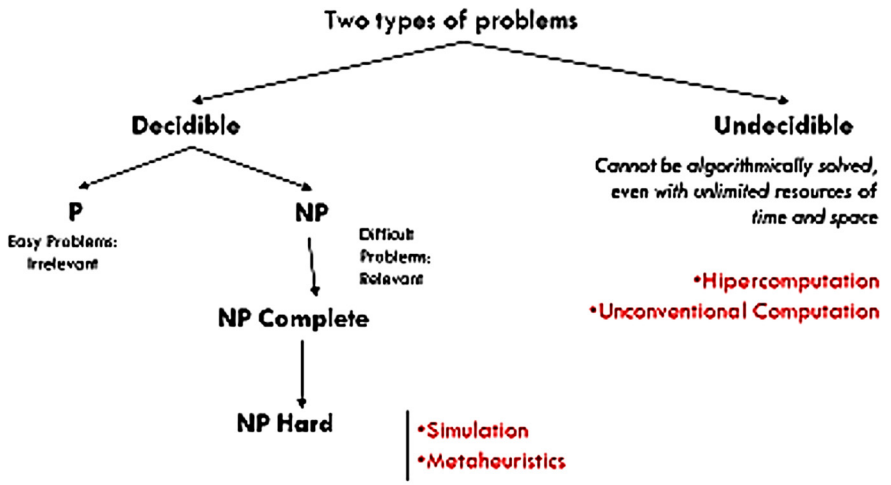
Dicho lo anterior, es importante atender a una distinción fina, pero no difícil, para nada. Una cosa es el modelamiento y otra, muy distinta, es la simulación. Los sistemas lineales pueden modelarse. Solo los sistemas no-lineales pueden simularse. Dicho esto, no es, para nada imposible, que existan vínculos entre el modelamiento y la simulación. En otras palabras, la finalidad del modelamiento es la aplicación o puesta en marcha de un modelo. Por su parte, la finalidad de una simulación es comprender o explicar muy bien un sistema determinado.

Sin ser exhaustivo, presento a continuación, de manera sumaria, las principales herramientas de la complejidad. Vale señalar que estas son herramientas exclusivas o distintivas de las ciencias de la complejidad. De esta suerte, es absolutamente indispensable al mismo tiempo desarrollar una estructura mental con

base en el corpus teórico (= las ciencias de la complejidad) y las herramientas. No una cosa más que la otra.

Una primera herramienta fundamental es la teoría de la complejidad computacional. La Figura 3 ilustra en qué consiste:

Figura 3. *Teoría de la complejidad computacional*



Fuente: elaboración propia con base en Maldonado y Gómez (2011).

La idea de base no es difícil. Todos los problemas se resuelven en un tiempo dado. Pues bien, la forma más básica de designar los tiempos de resolución de un problema hace referencia a la (capacidad de) computación (respecto de un problema). Así, todos los problemas, en ciencia o en la vida, pueden dividirse, desde este punto de vista en dos grupos: los problemas indecidibles y los decidibles. La indecibilidad —o decibilidad— de un problema no quiere significar para nada que no se puedan decidir o que no se puedan decir. Antes bien, en el caso de los problemas indecidibles se trata de la dificultad —mucho mejor, la imposibilidad— de resolverlos en un tiempo, un espacio, con insumos cualesquiera, dado un algoritmo real o posible. En otras palabras, es imposible saber si un problema puede resolverse o no y cuándo, puesto que no existe ni es posible un algoritmo para ello.

La distinción entre problemas decidibles e indecidibles se deriva del décimo problema formulado por D. Hilbert, conocido como el problema de la detención (*das Haltungsproblem*) (Gray, 2003).

Los problemas indecidibles convocan, consiguientemente, para su comprensión y resolución computación no-convencional. Quizás el caso más conspicuo al respecto sea la hipercomputación, cuya expresión más acabada es la hipercomputación biológica. Algunos ejemplos de problemas indecidibles son: la inequidad, la pobreza, el conocimiento, la salud, la vida.

Por su parte, los problemas decidibles son aquellos que, o bien disponen de un algoritmo, o bien es posible desarrollar algún algoritmo para su resolución; así no exista aún. P hace referencia a un tiempo polinomial; NP, a un tiempo no-polinomial. Técnicamente, se los conoce como los problemas P versus NP. Estos forman parte, a su vez, de los problemas del Premio Milenio, que son los últimos problemas en matemáticas por resolver, de acuerdo con el Instituto Clay. La expresión más elemental de los tiempos polinomiales son los tiempos físicos o cronológicos, susceptibles de ser manejados en términos de agendas, cronogramas, organigramas y otras distribuciones semejantes. Sería largo y prolijo explicar las derivaciones de los problemas NP en términos de los problemas duros y los completos. Sin embargo, la bibliografía al respecto es prolija y, en muchos aspectos, no muy técnica.

Ahora bien, es importante señalar que la teoría de la complejidad computacional formal parte de una teoría de mucho mayor calado, a saber: la teoría de los problemas complejos (Maldonado, 2022), supuesto que emerge el problema, altamente sensible, de distinguir cuáles y por qué razón unos problemas pueden propiamente ser designados como problemas complejos. Digámoslo de manera explícita: no todos los problemas son complejos, en el sentido preciso de la palabra. Es más, la mayoría de los problemas, en ciencia como en la vida, no son rigurosamente complejos.

En general y de manera clásica, cada ciencia o disciplina posee una heurística. Esta consiste básicamente en la capacidad de resolución de un problema. Con frecuencia, se la asimila, asimismo, a la capacidad de innovación de una ciencia o disciplina. Pues bien, hacia los años 1980-1990 emergen, exactamente en el estudio de sistemas y comportamientos caracterizados por complejidad, las metaheurísticas. Estas son un de las herramientas distintivas de la complejidad.

Su rasgo más sobresaliente consiste en la identificación —con diferentes criterios, algunos de los cuales son técnicos, como homeomorfismos— de grupos de problemas en búsqueda de espacios de solución. El énfasis se sitúa en el plural.

Digámoslo de manera directa y precisa. Cuando en investigación en general se formula la delimitación de un problema —por ejemplo, en términos de delimitación metodológica y demás—, se hace ciencia normal. La ciencia normal existe

para no resolver —verdaderamente— los problemas. Tan solo para desplazarlos o posponerlos. La idea de *revoluciones científicas* se entiende muy bien. Ya sea en la perspectiva de T. Kuhn o bien en la propia de la tradición francesa, con los trabajos de Koyré, Bachelard y Canguilhem.

Las metaheurísticas, si se quiere, son mucho más eficaces, ya que reúnen grupos de problemas, sin limitarse a un problema cada vez, y se buscan espacios de soluciones apara problemas que comparten criterios semejantes (Maldonado, 2013).

Las metaheurísticas, a su vez, se articulan en una variedad de aproximaciones y estrategias tales como las metaheurísticas multinivel, híbridas, P, y NP —en conexión directa con los problemas P versus NP antes mencionados—, evolutivas, inspiradas en la naturaleza, de búsqueda local o global, de búsqueda estocástica o dispersa y varias más. Se trata, manifiestamente, de un terreno amplio, sugestivo y distintivamente complejo.

Por lo demás, queda dicho, las matemáticas de la complejidad son matemáticas de sistemas discretos. Sus principales articulaciones incluyen los conjuntos parcialmente ordenados (*posets,* en inglés). Las cosas, en el mundo, en ocasiones, no pueden resolverse u ordenarse sino de manera provisional y parcial. Pues bien, en esto consiste este capítulo. Adicionalmente, las matemáticas de la complejidad abarcan los conjuntos extremos, la geometría discreta y combinatoria, la teoría de probabilidades discretas, todos los problemas combinatorios igualmente conocidos como complejidad combinatoria, la teoría de juegos —incluyendo los juegos evolutivos— y a teoría de la decisión racional, la topología (ya mencionada), algunas de las LNC y todas las matemáticas de los sistemas computacionales, que incluyen a los grafos y los hipergrafos.

Como se aprecia sin dificultad, se trata de una arena amplia y sugestiva. Es evidente, así, que se trata de tecnologías disruptivas en toda la línea de la palabra. El carácter disruptivo hace referencia al distanciamiento respecto de las técnicas y herramientas tradicionales y en boga.

Una observación se impone aquí. Es siempre importante distinguir en ciencia en general lo trivial y lo no-trivial. Es trivial hacer uso de herramientas existentes. Es no-trivial darse a la tarea de desarrollar nuevas herramientas e instrumentos. Es trivial hacer generalizaciones, con las justificaciones que se quiera. Es no-trivial hacer uso de cuantificadores particulares e incluso singulares. Esta idea de lo trivial y lo no-trivial merece un espacio propio en ámbitos como la metodología de la investigación científica, la lógica y la epistemología de la ciencia; claro, con sus derivaciones aplicadas y experimentales.

Tres herramientas fundamentales deben ser mencionadas en este mismo contexto. Las tres tienen con ver con mediciones.

De un lado, se trata de un asunto importante, aunque difícil que es la medición de la entropía. Como es sabido, la entropía de un sistema define —cuantitativamente— el desorden del sistema considerado. Pues bien, genéricamente dicho, existen tres aproximaciones, cronológicamente consideradas: la medición de Boltzmann, la de Shannon y la de Zurek. Las dos primeras hacen referencia la termodinámica clásica o de sistemas aislados o cerrados. La de Zurek, por el contrario, se ocupa de la termodinámica de sistemas complejos. Es fundamental al respecto tener en cuenta que la termodinámica es una sola ciencia; que o bien considera sistemas aislados, en cuyo caso la entropía es inevitable o más bien segura; y en otro caso, en la termodinámica de los sistemas complejos, o incluso de los sistemas cuánticos, los procesos de información admiten graduaciones dinámicas (Zurek, 1990).

De otra parte, al mismo tiempo, existe el problema de la medición de la incertidumbre de un sistema. Más propiamente, se trata —en realidad— de la medición de la indeterminación, para lo cual el referente necesario es W. Heisenberg. Y con él, una vez más, el entronque entre complejidad y cuántica. Es sencillamente imposible medir al mismo tiempo el ligar y la dirección de un fenómeno cualquiera, incluso en el mundo clásico. En el mundo clásico, todo parece indicar que los seres humanos necesitan seguridades y certezas de toda índole. La indeterminación es un rasgo ontológico del mundo mismo o del universo. Todo apunta, dicho sin más ni más, al papel del azar en la economía del universo y de la vida.

Pues bien, estrechamente relacionado con la medición anterior, la tercera medición importante en los marcos del estudio de los sistemas dinámicos no-lineales es la medición de la aleatoriedad. Pues bien, existe un camino tripartito al respecto gracias a los trabajos de Kolmogorov, Gödel y Chaitin; el primero, en el marco de las matemáticas; el segundo, en el de la lógica, y el tercero, en el de los sistemas computacionales. No escapa a una mirada sensible la estrecha conexión entre estas tres áreas.

Finalmente, una herramienta conspicua y perfectamente distintiva de las ciencias de la complejidad es una distribución estadística absolutamente singular de la complejidad: las leyes de potencia (*power law*). Originalmente llamada también como la ley de Zipf, por su descubridor, las leyes de potencia aparecen a plena luz del día gracias a la geometría de fractales, en especial, debido a las contribuciones de Mandelbrot.

Las leyes de potencia son distribuciones estadísticas que trabajan en términos perfectamente distintos, a medias, medianas, promedios, tendencias, vectores o

matrices. Concentrada específicamente en escalas log/log, las leyes de potencia permiten identificar no solamente diversas escalas e impactos, sino lo que en la estadística normal se denominan *excepciones;* esto es, todo aquello que queda por fuera de las parametrizaciones.

Las leyes de potencia tienen el mérito de identificar, sin la menor duda, cuándo hay una dinámica compleja. En otras palabras, siempre que se identifica la presencia o dinámica de una ley de potencia, sin duda alguna, estamos ante la presencia de un fenómeno complejo. Esto es, un fenómeno con cualquiera de las características o atributos ya mencionado en este trabajo.

Las leyes de potencia permiten identificar no solamente la estructura de un sistema, sino, además, su dinámica en relación con otras semejantes o próximas, algo que las demás distribuciones estadísticas no hacen. La escala log/log hace referencia a la capacidad de concreción o condensación de mucha información (se trata de escalas logarítmicas).

Muy importante, adicionalmente: el estudio de fenómenos, sistemas o comportamientos que exhiben o se fundan en leyes de potencia pone de manifiesto que, en la naturaleza, tanto como en la sociedad, existen fenómenos de criticalidad autorganizada (Bak, 1996).

La criticalidad autoorganizada empata perfectamente con varias aristas de las ciencias de la complejidad; notablemente, con el estudio de fenómenos alejados del equilibrio, técnicamente llamados *equilibrios puntuados,* con la vida artificial y con fenómenos y propiedades emergentes. Esta idea es fundamental desde el punto de vista epistemológico, y todo lo que ello comporta. La complejidad se sitúa en la antípoda de la causalidad, en cualquier acepción de la palabra. En verdad, la causalidad solo existe, tan solo, a escala local y bajo condiciones controladas. Pero a niveles meso y macro y en condiciones que no se controlan, la causalidad deja de existir por completo. Es entonces cuando emergen otras semánticas, otras herramientas, otras ciencias y disciplinas que son justamente las de las ciencias de la complejidad.

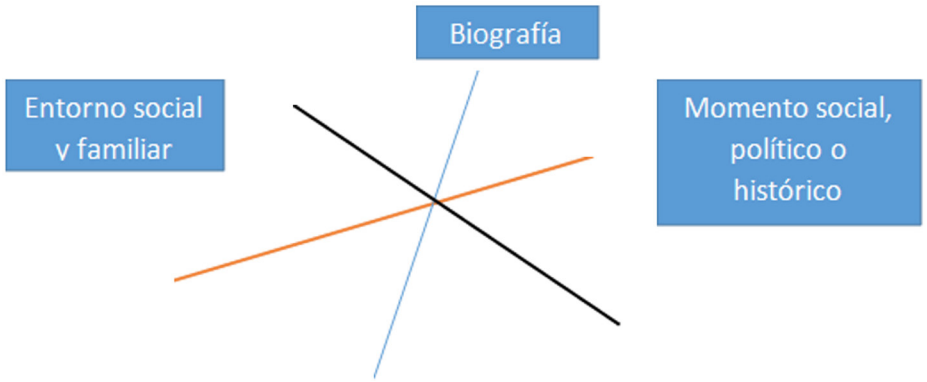
El debate internalismo vs. externalismo en ciencia

Hay un aspecto altamente sensible en la forma de entender la ciencia en general —la ciencia y la tecnología— y de gestionarlas. Se trata de lo que en el marco de la

historia y la filosofía de la ciencia es conocido como el *debate entre internalismo y externalismo*. Esto es, la discusión sobre si los avances en ciencia y tecnología son el resultado de discusiones sobre conceptos, herramientas, experimentos y demás, o bien, si, adicional y en ocasiones principalmente, los avances o retrocesos se explican también por factores externos al pensamiento y a la investigación, y que tienen que ver con circunstancias sociales, económicas, culturales, militares o políticas, principalmente. La historia de la ciencia es prolífica al respecto.

La buena comprensión de lo que sea la ciencia en general y cómo sea posible consiste en la articulación de estos dos aspectos; algo que se dice fácilmente, pero que es sumamente difícil de llevar a cabo. La Figura 4 ilustra en qué consiste la buena explicación y gatillamiento de la ciencia:

Figura 4. *Ejes definitorios de la ciencia y su gestión*



Fuente: elaboración propia.

La Figura 4 permite entender qué es en general la investigación, en cualquier campo o área del conocimiento, cómo emerge y cómo se hace posible. El triunfo o el fracaso de una idea, de un personaje, de una teoría es el resultado del cruce entre tres factores: la biografía, el entorno social o familiar y el momento social o político o histórico.

Manifiestamente, las experiencias personales de cada quien, en toda la extensión de la palabra: afectos, sexualidad, aprendizajes, dificultades y azares marcan el primer eje de la investigación. Asimismo, el entorno familiar y social, la educación recibida, por lo tanto, el aprendizaje de idiomas extranjeros, la formación en música o las destrezas físicas, por ejemplo, constituyen referentes sutiles pero inescapables de la inteligencia de cada quien. Y, finalmente, las eventualidades sociales o

económicas, golpes de Estado o guerras, paz o concordia y armonía sociales son determinantes para el estudio y la formación de ideas e intuiciones. El estudio de las biografías de artistas, filósofos o científicos, el estudio de épocas, sociedades y momentos históricos, en fin, estudio de las teorías y modelos mismos están permeados, explícita o implícitamente, por estos tres ejes articuladores.

Pues bien, a los planes de educación, de investigación y las políticas públicas más les valdría ampliar sus ventanas de observación, por así decirlo, y admitir un esquema como el que sugiere la Figura 4. El éxito o el fracaso personal o colectivo, en cualquier escala y contexto, está definido por estos tres ejes. He aquí la complejidad de la articulación entre teoría, biografía y entorno social de la investigación, la ciencia y la tecnología.

Sin ambages, es imposible entender la ciencia de punta y las tecnologías emergentes únicamente desde una perspectiva internalista. Un delicado, sensible y dinámico balance con el externalismo es siempre recurrente; aunque nunca evidente.

Se entienden así, mucho mejor, dos ideas, dos ideas directrices de este trabajo: la ciencia en general siempre comporta democracia, mientras que la tecnología ha sido, hasta el nacimiento de internet, un asunto distintivamente militar. El balance entre la dimensión militar y la civil de la vida marca tensiones esenciales (Kuhn, 1996) en la complejidad de la vida y del conocimiento.

Dicho en otras palabras, una buena comprensión de la ciencia y la tecnología no es diferente a la comprensión, la vivencia y la gestión, en sentido amplio, de dimensiones como la psicología, la antropología, la salud y la estética. Sin estas nada bien se entiende de la ciencia y a la tecnología. En otras palabras, como se aprecia sin dificultad, se trata de una sensible y fina articulación entre las humanidades, las ciencias sociales y humanas, y las ciencias e ingenierías.

Aproximación al ciberespacio y la ciberdefensa

Los temas de seguridad y defensa hacen referencia, en el primero y más importante de los sentidos, a temas, dinámicas, problemas y actuaciones en medio de incertidumbre, con fenómenos esencialmente imprevisibles, con una inmensa capacidad de improvisación, mucho aprendizaje y rápido, en fin, de dinámicas no-lineales en toda la línea de la palabra.

Los temas de seguridad y defensa, quiero sostenerlo, hacen referencia mucho más que a la defensa de la institucionalidad, a la defensa del territorio y de la vida, de la naturaleza misma. Pues bien, es absolutamente indispensable que un Estado

cualquiera conozca a profundidad lo mejor de la investigación de punta, trabaje con ella y contribuya a divulgarla.

Dicho política y jurídicamente, las instituciones no se deben al Estado o la república, sino a la nación. Es decir, se deben a la gente, al territorio, a la protección y defensa de la naturaleza. Las instituciones son simple y llanamente medios, herramientas o instrumentos de cara al fin: la finalidad es la defensa, el cuidado, la exaltación, el posibilitamiento y la gratificación de la vida. De la vida humana, tanto como de la vida en general; por decir lo menos, en el marco de la geografía nacional. Y muchas veces, también más allá de la geografía.

Manifiestamente, es claro que las indicaciones anteriores están lejos de ser un lugar común en medio de una atmósfera institucionalizada en el mundo. Me refiero explícitamente al institucionalismo y el neonstitucionalismo.

Nos encontramos, en el país y en el mundo, en el marco de las guerras de quinta generación. Todo es debido a un fenómeno social y cultural sin parangones en la historia de la familia humana. Se trata del tránsito de la analogización del mundo y de la sociedad a su digitalización.

Vivimos un mundo, hoy por hoy, inmensamente rico. Rico en datos. Hoy ya no existen, ni es posible hablar, de variables, en cualquier sentido de la palabra. Una cifra, un gesto, una letra, un movimiento, una relación, un nombre, por ejemplo, son datos. Y los datos se comprenden en el trasfondo de los sistemas informacionales y computacionales. La vida en general es imposible de espaldas a la computación, en general.

Como es suficientemente sabido, internet se articula en la información superficial —en la famosa analogía con un iceberg— y la información existente en la web profunda, que es, de lejos, la mayoría.

La inteligencia, *lato sensu,* pasa hoy por hoy por el conocimiento de los sistemas informacionales y computacionales y la navegación y conocimiento de internet, en toda la extensión de la palabra. Digámoslo de manera puntual: la inteligencia humana pasa hoy por hoy, medularmente, por desarrollar o adquirir una mentalidad de *hacker.* Hoy, las mejores empresas, universidades y corporaciones admiten en sus cuerpos directivos, por ejemplo, no solamente al vicepresidente de mercadeo, digamos, al responsable de logística, a la persona a cargo del personal en general y todos lo demás; además, se incluye la presencia de un *hacker,* que tiene dos funciones principalmente: una, impedir el *hackeo* de la propia empresa, organización o institución, cualquier que sea, o bien, igualmente, la de *hackear* a la competencia.

La ciberdefensa, dicho de manera genérica, no solamente atañe dimensiones estatales o gubernamentales; además, industriales, empresariales y de conocimiento. El conocimiento es el verdadero *asset* de cualquier organización. Es el *know-how* y vale, literalmente, un potosí.

Ayer, la principal forma de espionaje era exclusivamente militar. Hoy, además, es civil, industrial y demás. Esta idea implica un reconocimiento elemental.

La información no pesa nada; se la puede guardar el tiempo que sea necesario, acumular de muchas maneras y compartimentar según sea necesario; asimismo, la información puede ser compartida, sin perderla. Y siempre se puede hacer uso de ella con cualquier finalidad, en el momento en que se quiera. Todo ello apunta a la importancia de la huella digital. (Digamos, entre paréntesis, que la huella digital es imborrable; pero que sí se la puede ocultar; lo cual requiere conocimientos técnicos de computación e información).

Contra todas las apariencias, las cosas más importantes en el mundo suceden, ampliamente, en el ciberespacio, que es, exactamente el espacio de la digitalización del mundo y de la realidad. Con el reconocimiento expreso ya mencionado: la inmensa mayoría de la información se encuentra en la web profunda (*Deep web*). Si la Unesco ha señalado, con razón, que actualmente la principal forma de analfabetismo es el analfabetismo tecnológico, la inmensa mayoría de ciudadanos y sus organizaciones —de toda índole—permanecen como analfabetas funcionales debido, entre otras razones, a su ignorancia para navegar por la web profunda. Las políticas de datos abiertos (*open data*), tanto como de ciencia abierta (*open science*) pasan, medularmente por este ámbito.

Las ciencias de la complejidad así lo saben, lo trabajan y despliegan capacidades de investigación al respecto.

Existen relativamente numerosos trabajos sobre complejidad y temas militares; son sólidos los centros de investigación alrededor del mundo sobre estos dos ejes. Existe, asimismo, alguna revista especializada en el tema. Tirios y Troyanos saben de la importancia de las ciencias de la complejidad. *Lato sensu*, de cara a temas álgidos como democracia, libertad, interés nacional, posicionamiento geoestratégico, control, seguridad, defensa y ataque; y todas sus derivaciones e intertextos. No es este el centro del presente capítulo, sencillamente por razones de espacio. Un sólido estado-del-arte, que, si cabe la expresión, el A, B, C de una buena investigación, así lo pone/pondría en evidencia.

En cualquier caso, es evidente que en la medida en que la información va siendo depositada en forma digital, queda tanto asegurada como expuesta, por

paradójico que parezca. Los temas que aparecen entonces son los de encriptación, criptografía, decodificación y codificación, todo lo cual remite a la interfaz entre cuántica y complejidad (Maldonado, 2010).

El ciberespacio es el mundo de la criptografía, hoy por hoy. Actualmente, la batalla, por así decirlo, la van ganando los *encriptores* —un tema puntual apasionante es la criptografía cuántica—. Sin embargo, con el desarrollo de la computación cuántica la relación se reversará en favor de los *desencriptores*; sin importar los tecnicismos usados por los primeros, siendo uno de los más confiables el trabajo con la función Z de Riemann.

La ciberdefensa, el ciberespacio y los temas relativos a ciberseguridad atraviesan transversalmente por la Figura 1, ya presentada.

Conclusiones

Asistimos actualmente a un magnífico desarrollo de las ciencias e ingenierías como jamás había sucedido en la historia de la humanidad. La más importante tarea de todos aquellos que, de alguna manera, pivotan en torno al conocimiento —esto es, el conocimiento, la información, la educación, la cultura en sentido amplio, la investigación— consiste en mantenerse al día, tanto como sea posible, en el estado-del-arte. La dificultad estriba en los ritmos y los entrelazamientos de dichos desarrollos. Afortunadamente, existen numerosos canales para poder hacerlo. Un solo ejemplo: los *briefings* de la revista *Nature* —una de las más importantes en el mundo— que podemos recibir cada día.

Quisiera subrayarlo: lo mejor de la investigación de punta en el mundo pasa por las ciencias de la complejidad. Basta con echar una mirada a los más importantes centros de pensamiento, en sentido amplio, alrededor del mundo.

Dicho negativamente, las ciencias de la complejidad se ocupan de todo aquello de lo cual la ciencia normal se desentiende. Por ejemplo, movimientos irregulares; o la incertidumbre y la indeterminación; o la impredicibilidad; o los cambios súbitos, imprevistos e irreversibles; o la ruptura de los equilibrios y de control; o bien, las posibilidades e incluso las imposibilidades de lo real; o bien, igualmente lo que queda por fuera de las parametrizaciones. La lista podría ampliarse, sin dificultad alguna.

Para ello, las ciencias han desplegado un dúplice aparato: uno, conceptual; y el otro, instrumental. Sin embargo, ambos son una sola y misma cosa. La distinción es puramente analítica.

Desde cualquier punto de vista, hoy por hoy, la buena inteligencia consiste en la articulación de dos planos, paralelos y complementarios: la inteligencia humana y la inteligencia técnica. La mejor expresión de esta última es la inteligencia artificial. La mejor expresión de la primera… aún no es enteramente claro en qué consista.

La inteligencia artificial configura una de las mejores sedimentaciones de las ciencias de la complejidad (Maldonado, 2023b). La Tabla 1 precisa esta idea:

Tabla1. Relaciones *entre inteligencia artificial y vida artificial*

INTELIGENCIA ARTIFICIAL	VIDA ARTIFICIAL
Turing Test: Distinguir la mente humana de la máquina	Entender la vida por medio de la computación
Turing Test: Distinguir la mente humana de la máquina	Entender la vida por medio de la computación
Asociativismo vs. Conexionismo	Algoritmos genéticos
Redes neuronales	*Bottom-up*
Top-Down	

Fuente: elaboración propia.

La idea que se sigue de la Tabla 1 no es difícil. La inteligencia artificial (IA) y la vida artificial (VA) son, al cabo, una sola y misma cosa; a pesar de sus orígenes en marcos y momentos diferentes.

Así las cosas, bien entendidos, los temas y problemas de ciberespacio y ciber-defensa se fundan en la IA/VA. Todo lo demás es sencillamente operacional.

Son tiempos turbulentos y fluctuantes; son dinámicas inciertas e inestables; en fin, son circunstancias y relaciones caóticas las que demandan nuevas y mejores herramientas de todo orden. Teóricas o conceptuales, tanto como de la mejor tecnología posible o imaginable. Son los retos y problemas los que nos quieren inteligentes; no los propósitos voluntaristas ni las ideas, por bien intencionadas que sean. Pues bien, la inteligencia no es otra cosa que el nombre que le damos a la clave para acceder, si cabe la metáfora, al aprendizaje y la adaptación.

Terminemos con una analogía sutil. Manifiestamente que las ciencias de la complejidad constituyen una revolución científica. Son, dicho sin más ni más, aún, actualmente, ciencia alternativa. La razón no es difícil y la explica mucho mejor la medicina o a biología: ante un cuerpo nuevo, extraño, todo organismo se cierra

inmediatamente al mismo y lo rechaza. El organismo quiere preservarse a sí mismo, y en principio cualquier cuerpo nuevo constituye una amenaza. Pues bien, en verdad, la amenaza no es el cuerpo nuevo: sino el propio organismo, que no pudo desplegar la inteligencia suficiente para conservarse a sí mismo: homeostasis. Lo que ignora el organismo es que no logra sanar y recuperarse, en absoluto, si no modifica sustancialmente su propio metabolismo. De eso va la vida: de procesos y redes metabólicos. Y sí, es posible transformar, modificar el propio metabolismo. Lo que está en juego es la salud y la vida.

Referencias

Bak, P. (1996). How nature works: *The science of self-organized criticality.* Springer Verlag.

Camazine, S., Deneubourg, J.-L., Franks, N. R., Sneyd, J., Theraulaz, G., & Bonabeau, E., (2003). *Self-organization in biological systems.* Princeton University Press.

Gray, J. J. (2003). *El reto de Hilbert: Los 23 problemas que desafiaron a la matemática.* Crítica.

Kuhn, T. (1996). *La tensión esencial: Estudios selectos sobre la tradición y el cambio en el ámbito de la ciencia*. Fondo de Cultura Económica.

Maldonado, C. E. (2010). Una nota sobre criptología y complejidad: Un caso de complejidad y administración. *Innovar, 20*(38), 5-12. https://revistas.unal.edu.co/index.php/innovar/article/view/22280/23192

Maldonado, C. E. (2013). Un problema fundamental en la investigación: Los problemas P vs. NP. *Revista Logos Ciencia & Tecnología, 4*(2), 10-20. https://doi.org/10.22335/rlct.v4i2.186

Maldonado, C. E. (2019a). Sociedad de la información, políticas de información y resistencias: Complejidad, internet, la red Echelon, la ciencia de la información. Desde Abajo.

Maldonado, C. E. (2019b). Quantum Theory and the social sciences. *Momento,* (59E), 34-47; https://revistas.unal.edu.co/index.php/momento/article/view/81645/0

Maldonado, C. E. (2020a). *Camino a la complejidad: Revoluciones científicas e industriales: Investigación en complejidad.* Asociación Rujotay Na'oj.

Maldonado, C. E. (2020b). *Pensar: Lógicas no-clásicas* (2.ª ed.). Universidad El Bosque.

Maldonado, C. E. (2021). Epistemología de la imposibilidad o ciencia de la indeterminación. *Cinta de Moebio,* (70), 44-54. https://cintademoebio.uchile.cl/index.php/CDM/article/view/61586

Maldonado, C. E. (2022). Teoría de los problemas complejos. *Cinta de Moebio,* (74), 109-120. https://doi.org/10.4067/S0717-554X2022000200109

Maldonado, C. E. (2023a). A systemic problem cannot be solved systemically. *Cinta de Moebio*, (77), 79-88. https://doi.org/10.4067/S0717-554X2023000200079

Maldonado, C. E. (2023b). *Inteligencia artificial y ética.* Desde Abajo.

Maldonado, C. E., & Gómez-Cruz, N. (2011). *El mundo de las ciencias de la complejidad.* Universidad del Rosario.

Pagels, H. (1991). *Los sueños de la razón: El ordenador y los nuevos horizontes de las ciencias de la complejidad.* Gedisa.

Prigogine, I. (2003). *Is future given?*. World Scientific.

Zurek, W. H. (Ed.). (1990). Complexity, entropy, and the physics of information: CRC Press.

Capítulo 5

El poder en la era digital: perspectivas sobre el ciberpoder*

DOI: https://doi.org/10.25062/9786287602700.05

Milena Elizabeth Realpe Díaz
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este capítulo analiza las dinámicas que tienen lugar en el ciberespacio; expone cómo empieza a hablarse de ciberpoder en el ámbito general del poder; examina las acepciones del término de acuerdo con diferentes perspectivas regionales y en el entendido de que se define según como se comprenda y dónde se localice; describe el poder desde la perspectiva militar de EE. UU. y desde la óptica de la Unión Europea, y amplía la comprensión del ciberpoder, a partir de su localización, todo lo cual apunta a establecer estimaciones adecuadas de este objeto de estudio.

Palabras clave: ciberconflicto; ciberespacio; ciberpoder; ciberseguridad; poder.

* Capítulo de libro resultado del proyecto de investigación "*Tecnologías disruptivas, logística, seguridad y defensa nacional en el ciberespacio*", del grupo de investigación *"Ciberespacio Tecnología e Innovación"*, de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado C por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) y registrado con el código COL0181179. Los puntos de vista y los resultados de este capítulo pertenecen a los autores y no necesariamente reflejan los de las instituciones participantes.

Milena Elizabeth Realpe Díaz
Teniente Coronel del Ejército Nacional de Colombia. Doctoranda en Estudios Estratégicos, Seguridad y Defensa, y magíster en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Magíster en Seguridad de la Información, Universidad de los Andes, Colombia. Especialista en Seguridad de Redes de Computadores, Universidad Católica de Colombia. Especialista en Seguridad Física y de la Informática, Escuela de Comunicaciones del Ejército, Colombia. Especialista en Seguridad de la Información, Universidad de los Andes. Ingeniera de sistemas, Universidad Cooperativa de Colombia. Jefe de la Maestría en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia.
https://orcid.org/0000-0003-4345-6182 - Contacto: **milena.realpe@esdeg.edu.co**

Citación APA: Realpe Díaz, M. E. (2024).El poder en la era digital: perspectivas sobre el ciberpoder. En M. E. Realpe Díaz, & A. M. González González (Eds.), *Tecnologías disruptivas, logística y seguridad y defensa nacional en el ciberespacio* (pp. 143-166). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602700.05

TECNOLOGÍAS DISRUPTIVAS, LOGÍSTICA Y SEGURIDAD Y DEFENSA NACIONAL EN EL CIBERESPACIO
ISBN impreso: 978-628-7602-69-4
ISBN digital: 978-628-7602-70-0
DOI: https://doi.org/10.25062/9786287602700

Colección Ciberseguridad y Ciberdefensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2024

Introducción

La revolución tecnológica de los últimos años del siglo XX tuvo un impacto profundo en la forma en que las personas se relacionan entre sí y perciben el mundo que les rodea. La llegada de la internet y la digitalización de la información revolucionaron la forma en que la información se transmitía y se procesaba. Por su parte, la revolución de las tecnologías de la información actuó remodelando las bases materiales de una nueva sociedad. Las tecnologías de la información se tornaron en herramientas indispensables para la generación de riqueza, el ejercicio del poder y la creación de códigos culturales (López, 2002). De acuerdo con Castells, este tiempo donde ocurrió la revolución tecnológica correspondió a un intervalo histórico, durante el cual el desarrollo alcanzado por las tecnologías de la información ocasionó un cambio en la cultura material de la sociedad, pues influyó de manera considerable en las distintas actividades realizadas por el hombre, no como una fuente exógena de afectación sino directa (Castells, 2001, p. 112).

Adicionalmente, el desarrollo e implementación de las tecnologías provocó una transformación acelerada de la base material de la sociedad, que afectó profundamente la forma en que las personas se relacionan entre sí y perciben el mundo que les rodea, dando lugar a la *sociedad de la información,* lo que significa que estas tecnologías están presentes en la vida diaria de las personas y son utilizadas en una variedad de actividades, desde el trabajo y la educación hasta el entretenimiento y la comunicación interpersonal. Como lo afirma Estudillo, se trata de una sociedad en la que las nuevas tecnologías y la información afectan la estructura social en diferentes ámbitos de la vida de los seres humanos como la economía y el bienestar social (2002, pp. 83-84). Asimismo, Castells (1996) sostiene que las tecnologías de la información y la comunicación (TIC) son la fuerza impulsora

detrás de la transformación de la sociedad, y que han permitido la creación de una economía global y la conexión en tiempo real de personas de todo el mundo.

Como lo establece Perlroth (2022), la internet como muchas otras cosas que ahora nos damos cuenta, nos ha dejado conectados de forma inextricable. Las vulnerabilidades digitales que afectan a uno afectan a todos. La barrera entre lo físico y lo digital es cada vez más insignificante. Es verdad que todo "se puede interceptar", y la mayoría de lo que nos importa ya se ha interceptado: nuestros datos personales, propiedad intelectual, empresas químicas, centrales nucleares e incluso las propias ciberarmas del país (p. 475). Con esta percepción, el progreso tecnológico y la internet son considerados factores del cambio social y, en este contexto, como lo afirman De Vergara y Trama, (2017), la internet y los desarrollos tecnológicos también han tenido un impacto significativo en el carácter de las guerras y los conflictos, así coinciden varios autores del siglo XXI, lo que reitera los postulados de Clausewitz en cuanto a que "estos son como un camaleón que cambian de carácter según sea su naturaleza, propósito, la manera en que se los conduce, la tecnología y el ambiente operacional donde tienen lugar" (p. 58).

Surge así, el ciberespacio que es el escenario común donde tienen lugar todas aquellas interacciones de orden social, comercial, industrial, tecnológico y militar entre personas, organizaciones, instituciones, bancos y ejércitos; allí, actúan también las amenazas, tanto criminales como aquellas que orientan sus esfuerzos contra la estabilidad de los Estados, vinculadas por lo general a otro país rival o enemigo. Estas acciones materializan los ciberconflictos, "un tipo de conflicto que se lleva a cabo en el ciberespacio y que puede involucrar operaciones militares, de inteligencia, de propaganda y de sabotaje, en el que los actores utilizan herramientas y técnicas cibernéticas para alcanzar sus objetivos" (Singer & Friedman, 2021, p. 2), una escalada mayor de tales hostilidades en el ciberespacio deriva en una ciberguerra, "…una forma grave de ciberataque disruptivo por parte de una nación al ciberespacio de otra nación, cruzando la línea para ser considerado un uso de la fuerza, en ese momento entran en juego cuestiones del derecho de la guerra" (Hunker, 2010, p.4). De esta manera, surge un nuevo concepto: *ciberpoder,* definido como "la capacidad de utilizar el ciberespacio para crear ventajas e influenciar eventos en todos los entornos operativos y en todos los instrumentos del poder" (Kuehl, 2009, p. 25).

Como lo define Mitchell (1995), el ciberespacio es una nueva dimensión, digital, sin fronteras, un espacio de comunicación e intercambio de información que se ha convertido en una parte integral de la vida cotidiana de muchas personas. Es una realidad en que

> las nuevas tecnologías traen oportunidades y vulnerabilidades para los países más desarrollados y al mismo tiempo contribuyen a aumentar la brecha tecnológica hacia los países en vías de desarrollo, especialmente en lo que se refiere a los campos de la seguridad y la defensa nacional. (Ferreira, 2018, p. 36)

Si bien la tecnología trajo consigo muchos beneficios, también planteó nuevos desafíos éticos, políticos y legales que aún se están tratando de abordar. Si se analizan las múltiples fuentes de información, la tecnología es cada día más accesible y permite que surjan nuevas amenazas procedentes de regímenes ilegítimos, grupos terroristas, grupos al margen de la ley y delincuencia organizada, quienes pueden tener acceso al ciberterrorismo, ciberdelincuencia, armas de destrucción masiva, mercado negro armamentístico, etc. Esto implica un cambio en la idea de la amenaza tradicional procedente de enemigos identificados (CESEDEN, 2012, p. 126).

Lo anterior divisa una gran preocupación no solo nacional sino internacional, pues si bien la relación entre la sociedad de la información y el ciberespacio ha traído grandes beneficios en términos de comunicación y globalización, también ha creado una serie de riesgos y desafíos para la sociedad y es importante que se tomen medidas para abordar estos problemas y garantizar que los beneficios de la tecnología se utilicen de manera responsable y equitativa.

Del poder al ciberpoder

Históricamente, se solía creer que la potencia de un país dependía de aspectos como su ubicación geográfica, sus recursos nacionales, el número de habitantes y su riqueza, ya que se consideraban elementos esenciales para el desarrollo del poderío militar (Tellis et al., 2009). Tradicionalmente, la capacidad de un país para salvaguardar sus fronteras de posibles ataques, a la par que exhibía la capacidad de amenazar a naciones vecinas, se percibía como el símbolo máximo de su fuerza nacional. No obstante, con la transición a la Cuarta Revolución Industrial, las concepciones sobre el poder nacional han evolucionado, incorporando el concepto de una revolución del conocimiento. Esta transformación anticipa un cambio significativo en la importancia, otorgada a la tecnología de la información y la innovación en la estructura y dinámica de la sociedad.

La evolución en la concepción del poder, desde las nociones tradicionales basadas en factores geográficos y económicos hacia un nuevo paradigma de

ciberpoder, refleja la adaptación necesaria a la Cuarta Revolución Industrial. En esta transición, la relevancia de la tecnología de la información y de la interconexión digital se convierte en un elemento crucial. La capacidad de aprovechar el ciberespacio para alcanzar objetivos estratégicos y tácticos redefine el panorama de la influencia y la seguridad en un contexto tanto nacional como internacional. A medida que las tecnologías digitales siguen evolucionando, se hace imperativo abordar esta emergente dimensión del poder en la era contemporánea, donde la tecnología y la información desempeñan un papel central en la configuración de las dinámicas de poder y las relaciones globales.

Migrar del poder al ciberpoder implica adoptar una serie de medidas y estrategias que permitan aprovechar las capacidades y recursos del ciberespacio para lograr objetivos estratégicos y tácticos. Adicionalmente, requiere una transformación significativa en la manera en que las naciones, organizaciones y actores individuales influyen en el escenario global. Esto debido a la creciente importancia de las tecnologías de información, comunicaciones y de operación, así como a la interconexión mediante internet (Kuelh, 2009). La transición de una estructura de poder convencional hacia un paradigma de ciberpoder implica la creciente preeminencia de las tecnologías digitales y el ciberespacio en la configuración de la influencia y la seguridad en un contexto tanto nacional como internacional. A medida que estas tecnologías continúan su evolución, se vuelve imperativo el análisis y la adaptación a esta emergente dimensión del poder en la era contemporánea.

En síntesis, el poder tradicional y el ciberpoder son dos conceptos que se entrelazan en la actualidad. Por una parte, todo poder puede caracterizarse como "la producción, en y por las relaciones sociales, de efectos sobre los actores que moldean su capacidad para controlar su destino" y solo se hace evidente por los efectos que tiene sobre los demás (Barnett & Duvall, 2005). Y por otra, el ciberpoder puede entenderse como la variedad de poderes que circulan en el ciberespacio y que dan forma a las experiencias de quienes actúan en el ciberespacio y por medio de él (Jordan, 1999, p. 3). El ciberpoder "no se crea simplemente para existir, sino más bien para apoyar el logro de objetivos más amplios... mediante los elementos del poder nacional: político, diplomático, informativo, militar y económico". (Kuehl, 2009, pp. 41-42). El ciberpoder es una de las últimas incorporaciones al árbol genealógico del poder, dado lo reciente que aún es la digitalización de nuestras sociedades y el surgimiento del ciberespacio.

Del ciberespacio al ciberpoder

Para trazar una evolución del ciberespacio, desde sus orígenes hasta la sociedad contemporánea es menester mencionar que este escenario es considerado un dominio estratégico debido a su capacidad para transformar la sociedad, influir en la economía y la política y afectar la seguridad y la defensa de los países. Sobre esta premisa, es preciso reconocer que *ciberespacio* es un término que viene siendo usado desde hace aproximadamente medio siglo y que, por lo tanto, es natural exponer su evolución; es así como fue presentado por primera vez en el libro *El shock del futuro,* de Alvin Toffler (1970); posteriormente, fue utilizado y recreado por William Gibson en sus obras *Burning Chrome* (1982) y *Neuromancer* (1984) y, en consecuencia, cuenta con múltiples definiciones como la establecida por Bauman: "el ciberespacio es un espacio de incertidumbre y ambigüedad, donde las identidades y las relaciones sociales pueden ser construidas y deconstruidas con facilidad" (Bauman, 2000). Para Castells,

> el ciberespacio es un espacio virtual que se extiende más allá del mundo físico, en el que los usuarios pueden interactuar, colaborar, crear y compartir información y conocimiento, y en el que la tecnología de la información y las comunicaciones juegan un papel central. (Castells, 2010, p. 69)

La historia de la humanidad es también la bitácora de las constantes confrontaciones entre civilizaciones y pueblos. La Modernidad, por su parte, trajo consigo dos guerras mundiales, posiblemente las más sangrientas hasta ahora conocidas; sin embargo, cabe conceder que estas dieron origen a diversas iniciativas formales institucionalizadas, como la ONU, y a un número importante de planteamientos teóricos que, por ejemplo, revitalizaron la romántica idea kantiana de la paz perpetua (Kant, 1795), o definieron o reforzaron las nociones y la necesidad de acatar los derechos humanos (DD. HH.), el Derecho Internacional Humanitario (DIH), las leyes de la guerra (LOW) en su expresión tradicional que divide el *Jus ad Bellum* (la decisión y causas de dar inicio a la guerra), del *Jus in Bello* (que regula la conducción durante la guerra).

La idea kantiana era romántica e incluso anacrónica; no obstante, materialmente acertada, pues la creación de una liga de naciones era una apuesta plausible, así se hubiera visto después su ineficacia operativa o el surgimiento de nuevas formas de conflicto y opresión a sus expensas, bajo la bandera de la intervención humanitaria o las operaciones de paz. Al respecto, Fisher (2011) señala: "Las

intervenciones humanitarias pueden adoptar una gran variedad de formas, desde la aportación de ayuda hasta el uso de la fuerza militar" (p. 221). Es inevitable citar a Kant, para poner en contraste las buenas ideas e intenciones con las realizaciones políticas pragmáticas y sus resultados e impactos.

> Artículos preliminares de una paz perpetua entre los Estados. 1) Ningún Estado independiente (pequeño o grande, lo mismo da) podrá ser adquirido por otro Estado mediante herencia, cambio, compra o donación. 2) Los ejércitos permanentes (*miles perpetuus*) deben desaparecer por completo con el tiempo. 3) Ningún Estado debe inmiscuirse por la fuerza en la constitución y el Gobierno de otro Estado. (Kant, 1795, pp. 247-249)

Hasta aquí dejaremos esta reflexión solo para hacer notar que las regulaciones de la guerra y los conflictos humanos evidentemente se quedan cortas y resultan inapropiadas para atender las exigencias de los ciberconflictos, tanto más complejos, difusos y condicionados.

El *orden global postmoderno,* como es adecuado llamarlo, habitualmente se estudia desde las relaciones internacionales, la ciencia y la filosofía política. Según Gómez (2017):

> es decir, en cuanto a la estructura, los actores, los procesos y sus relaciones, el poder y fenómenos como la violencia. La estructura está determinada por la inclinación hacia el modelo ordenado o anárquico del sistema internacional, la posición de los actores por el rol que desempeñan, y los procesos operan en función de las interacciones de conflicto o cooperación. (p. 59)

Según Hardt y Negri (2004):

> en el orden global contemporáneo se libra una guerra global permanente donde los actores, aun sin perseguir objetivos comunes y a pesar de sus desigualdades se ven forzados a cooperar […] El imperio gobierna un orden global fracturado por divisiones y jerarquías internas, y abatido por la guerra perpetua. El estado de guerra es inevitable en el imperio […] la guerra se está convirtiendo en un fenómeno general, global e interminable que erosiona la distinción entre la guerra y la paz, de manera que no podemos imaginar una paz verdadera, ni albergar una esperanza de paz, entre otras cosas porque también la distinción tradicional entre la guerra y la política se desvanece, hasta tal punto de que la guerra se está convirtiendo en el principio organizador básico de la sociedad, no la política. (p.8)

Lo que destaca del planteamiento de Hardt y Negri acerca del orden global contemporáneo es que la noción misma de *potencia mundial* se ha erosionado; si bien es cierto, existen actores clave que luchan incansablemente por la hegemonía económica, como China, o geoestratégica, como Rusia, las interdependencias complejas, esa suerte de necesidad de recursos vitales e intereses dispersos, hacen que la cooperación, la disuasión o incluso el engaño sean lógicas válidas para prosperar y obtener ventaja, máxime que muchos de esos activos son intangibles, productos del conocimiento, *software,* ciberarmas disponibles al mejor postor, libres del control de los Estados; así lo refleja la investigación de Nicole Perlroth registrada en su libro, *Así es como me dicen que acabará el mundo:*

> Durante décadas, bajo la protección de niveles clasificatorios y acuerdos de confidencialidad, el gobierno de EE. UU. se convirtió en el principal acaparador de días cero del mundo. Los agentes del gobierno de EE. UU. pagaron un alto precio (primero, miles; después, millones de dólares) a los *hackers* dispuestos a vender sus códigos para forzar cerraduras y su silencio. Pero luego, EE. UU. perdió el control de su provisión y del mercado. Ahora esos días cero están en manos de naciones hostiles y mercenarios a los que no les importa si tu voto se pierde, se contamina tu agua o si nuestras centrales nucleares colapsan. (Pelroth, 2022, p.1)

Estudiar el poder ciberespacial permite comprender las amenazas actuales. En un mundo cada vez más digitalizado, las operaciones militares y la seguridad nacional dependen en gran medida de los sistemas ciberespaciales. Comprenderlos permitirá tener claro el camino para proteger los intereses nacionales, mantener la estabilidad internacional y fomentar el avance científico y tecnológico en el campo de la seguridad cibernética.

Foucault (1966) afirma que el conocimiento científico está ligado a relaciones de poder y cómo el discurso científico puede ser utilizado para justificar formas de dominación social. Estudiar el poder ciberespacial constituye un factor esencial, porque el ciberespacio se ha convertido en un componente fundamental de las actividades militares modernas. En este contexto, los conflictos militares actuales a menudo implican operaciones cibernéticas, que pueden tener un impacto significativo en la capacidad de un país para protegerse o llevar a cabo operaciones militares.

En los contextos de guerra, pero también en escenarios donde esta no ha sido declarada —como afirmarían Hardt y Negri, en el contexto de guerra global

permanente—, han venido suscitándose diferentes tipos de incidentes en el ciberespacio, ataques o conflictos que reflejan la competencia por el poder entre los diferentes Estados, empresas u organismos nacionales e internacionales. Valeriano y Maness sostienen que, en el ciberespacio, la competencia por el poder y la influencia son elementos centrales en la ciberseguridad y el ciberconflicto. Este enfoque tiene importantes implicaciones para la política y la seguridad internacional, ya que el ciberespacio se convierte en un nuevo ámbito de competencia estratégica en el sistema internacional (Valeriano & Maness, 2015).

Es momento de decir que, sobre la premisa de guerra global permanente, han surgido formas de librarla que han dado origen a definiciones, tales como guerras de quinta generación, guerras híbridas, ciberguerras o ciberconflictos, incluso la guerra especial —desarrollada doctrinariamente por el US Army— en el Manual de operaciones especiales del Ejército de los EE. UU., ADP 3-05 (2012, p. 9) y, por supuesto, las MDO (operaciones multidominio). Todas ellas tienen en común que son libradas, se sirven o involucran en mayor o menor medida acciones en el ciberespacio; en consecuencia, su comprensión es necesaria al momento de valorar el poder ciberespacial en cada una de ellas.

Un alto número de acciones tiene lugar en el ciberespacio; además, se puede afirmar sin prevenciones que estas son ejecutadas por actores estatales, por fuerzas de inteligencia y agencias; se conducen operaciones mediáticas y en el ciberespacio, no declaradas generalmente, de las que solo alcanzamos a ver sus efectos. Para nuestro objeto de estudio, esto resulta *a priori* inabordable o incluso inútil, pero en verdad se trata justamente de la fuente de nuestra indagación. ¿Qué tipo de ciberarmas se emplean? ¿Cómo operan? ¿Qué tanto tiene que ver la inteligencia artificial en todo esto? Y lo que resulta de mayor interés: ¿Cómo, siendo clandestinas estas capacidades, pueden valorarse como parte del arsenal o ciberpoder de un Estado?

Las guerras híbridas, según el Instituto LISA "son aquellas que combinan el uso de la fuerza militar con otros elementos como pueden ser los ciberataques, la manipulación de la información mediante internet y redes sociales, o vectores de presión económica" (Instituto LISA). En ellas, el ciberespacio tiene dos funciones: como herramienta para realizar operaciones de información y acciones afines, o como campo de batalla, donde se persiguen objetivos específicos del adversario. En este escenario, el uso de armas cibernéticas es masivo y suele ser más evidente y regulado incluso doctrinariamente su uso, concebidas como operaciones en el ciberespacio; los estudios de caso serán sumamente útiles para determinar en qué medida.

Antes de abordar los ciberconflictos, se introduce la denominada *guerra especial,* diseñada por la RAND corporation (2016) y definida como:

> una forma peculiar de guerra y como una estrategia para proteger y alcanzar los intereses nacionales de EE. UU. , desde una perspectiva realista que presta poca atención a las implicaciones éticas de los procedimientos. Se considera justificado y permisible intervenir en otros países de forma indirecta o subrepticia, y sacar provecho en beneficio de intereses unilaterales, evitando comprometer tropas y recursos en confrontaciones decisivas. (p. III)

En muchos casos, la guerra especial puede concebirse como una guerra no evidente, en la cual, según Libicki (2012) "Las innovaciones, tanto tecnológicas como organizativas, en las últimas décadas han creado un potencial de una guerra no evidente, en la que la identidad del lado combatiente e incluso el mero hecho de la guerra resultan completamente ambiguos" (p. 19). Libicki (2012) señala:

> […] además que el ataque tecnológico —ciberguerra, guerra espacial, guerra electrónica, guerra de drones— y otras estrategias de largos antecedentes históricos como el sabotaje, el asesinato y el uso de minas forman parte del espectro de acciones que se pueden llevar a cabo de forma no evidente; en todas ellas, la ambigüedad es la base de la falta de evidencia: se desconoce el actor mas no el acto. Algunos incidentes bélicos no evidentes serían claramente actos de guerra si fueran evidentes. (p. 19)

Resulta indiscutible, pero lo afirmamos una vez más. Para el estudio del ciberpoder, este tipo de guerra suma complejidades al momento de ponderar y estimar los activos y recursos que en verdad un Estado dispone o por aquellos que paga por poner al servicio de estos fines cuestionables.

En este tipo de conflictos bélicos, las diferencias políticas y las marcas de poder global, se manifiestan en acciones económicas, militares, de información y afectaciones de la población civil, y establecen un caldo de cultivo que es aprovechado por los diferentes actores globales para potenciar el poder del ciberespacio como un campo de operaciones, no solamente con objetivos estratégicos en las infraestructuras críticas cibernéticas y de información, sino como un lago de información donde las operaciones cibernéticas y cognitivas se consolidan como la fuente fundamental de un conflicto híbrido (Cano, 2021). Lo anteriormente expuesto permite concebir la importancia que tiene el ciberespacio en la actualidad y cómo su evolución puede afectar la seguridad, la estabilidad y el desarrollo de las naciones.

El presidente y fundador del Foro Económico Mundial Klaus Schwab y autor del libro *La Cuarta Revolución Industrial* (Schwab, 2017) afirma:

> La Cuarta Revolución Industrial promete grandes cambios sociales, esta revolución tecnológica alterará por completo los productos que elaboramos, cómo los elaboramos, cómo interactuamos y, sobre todo, quiénes somos. Como era de esperarse, aquel potencial caracterizado por la promesa de la automatización y la interconexión de los ecosistemas físicos con los digitales (Internet de las cosas, implantes neurales, prótesis inteligentes, etc.) no solo ofrecerían beneficios, sino que, consecuentemente, también supondrían peligros. La guerra también experimentará cambios. (p. 2)

Las citadas palabras de Schwab nos presentan una forma de conflictos tanto más complejos, donde las amenazas pueden no provenir ni estar vinculadas con actores de otro país y sin embargo ser capaces de poner en riesgo activos estratégicos de los Estados; se trata de una situación de amenazas desbordadas ante las cuales, sin duda, las respuestas tradicionales resultarán inoperantes y, virtualmente, se requerirá de un poder militar ciberespacial redefinido y posiblemente hoy inexistente en la mayoría de fuerzas de defensa del globo.

Desde el componente estratégico, el ciberespacio ha sido reconocido como un ámbito de importancia estratégica para el poder militar por muchos autores y organizaciones. En este contexto, Castells señala que el ciberespacio es un espacio de poder global que tiene el potencial de transformar el funcionamiento de la sociedad y el Estado. Según el autor, las redes digitales permiten la creación de nuevas formas de organización política, económica y social que pueden desafiar el poder de las instituciones tradicionales (Castells, 2001). Aunado a esto, Kramer (2009) argumenta que el ciberespacio es una dimensión fundamental del ciberpoder y la seguridad nacional, porque los conflictos en el ciberespacio pueden tener consecuencias devastadoras para la infraestructura crítica de los países y para la seguridad de los ciudadanos. En la sociedad moderna, el ciberespacio se ha convertido en un espacio fundamental para la actividad política, económica y militar y el papel que juega la inteligencia artificial y la ciberdefensa en la gestión de los conflictos cibernéticos (Arellano, 2019). En este sentido, Psychogiou (2022) establece que el ciberespacio se ha convertido en el quinto espacio de batalla en un panorama de seguridad cada vez más complejo, y las amenazas cibernéticas han sido parte del ámbito de la seguridad internacional (p. 1).

Lo anteriormente expuesto da cuenta de que el ciberespacio se ha convertido en una herramienta fundamental para el funcionamiento de las sociedades modernas, y los países que tienen la capacidad de controlar y dominar el ciberespacio tienen una ventaja significativa en el ámbito militar, económico y político. El ciberespacio se ha convertido en un campo de batalla en el que los países pueden llevar a cabo operaciones encubiertas sin necesidad de una intervención militar directa, lo que les permite alcanzar objetivos estratégicos sin sufrir las consecuencias de un conflicto armado. Nace entonces una forma relativamente nueva de conflicto: el *ciberconflicto,* que toma más relevancia a medida que se incrementan la dependencia de la tecnología y la interconexión global de los sistemas de información.

Los ciberconflictos deberían considerarse como una amenaza a la seguridad y defensa nacional, porque el ciberespacio se ha convertido en una dimensión crucial para la vida económica, política y social de las naciones; un entorno virtual donde las actividades de comunicación y el intercambio de información tienen lugar mediante redes interconectadas, tecnologías y humanos. A propósito, Thomas Rid ha definido los ciberconflictos como el uso de medios cibernéticos para desencadenar, intensificar o prolongar un conflicto armado en el mundo real (Rid, 2012). Carr y Tikk argumentan que "El ciberconflicto es un conflicto que involucra la utilización de herramientas y técnicas cibernéticas para causar daño o perturbar los sistemas informáticos de los adversarios, y que puede tener consecuencias significativas en términos de seguridad, política y economía" (Carr & Tikk, 2021, p. 6). En complemento, Singer y Friedman afirman que el ciberconflicto es "un conflicto que se lleva a cabo a través del ciberespacio y que puede involucrar operaciones militares, de inteligencia, de propaganda y de sabotaje, en el que los actores utilizan herramientas y técnicas cibernéticas para alcanzar sus objetivos" (Singer & Friedman, 2021, p. 2). Aunque las definiciones estudiadas muestran un amplio espectro de perspectivas sobre el tema, todas coinciden en que el ciberconflicto implica el uso de tecnologías de información y operación, para llevar a cabo acciones hostiles en el ciberespacio, ya sea para dañar o perturbar los sistemas tecnológicos de los adversarios, o para lograr objetivos políticos, militares, económicos o de otro tipo.

Entre tanto, Alberts y Hayes sostienen que los ciberconflictos se han convertido en una amenaza real para la seguridad nacional, ya que los sistemas informáticos y de comunicaciones son esenciales para el funcionamiento de la economía, el gobierno y la defensa. Los autores advierten que los ciberataques pueden tener consecuencias graves para la infraestructura crítica y la sociedad en general (Alberts & Hayes, 2003). En la actualidad, la naturaleza de la guerra y la seguridad

han cambiado con la evolución de la tecnología y la aparición del ciberespacio como nuevo campo de batalla, lo que presenta desafíos únicos y requiere un enfoque multidisciplinario. Diversos autores han abordado la importancia del estudio de los ciberconflictos. Por ejemplo, Kramer argumenta que la ciberseguridad es fundamental para la seguridad nacional y que los Estados deben tener en cuenta los aspectos tecnológicos, políticos y sociales de los ciberconflictos. Por su parte, Libicki, aborda el concepto de *ciberdisuasión* y la amenaza como parte de las represalias que pueden ayudar a disuadir a los agresores cibernéticos. Los ciberconflictos son una expresión del poder en la sociedad de la información, donde el control de la información y la tecnología es fundamental (Libicki, 2018).

Como se señaló, uno de los retos para estudiar el ciberpoder, que exhibe a la par una notable ventaja estratégica de los ciberconflictos, es que estos pueden ser llevados a cabo de manera encubierta, sin necesidad de una gran inversión de recursos materiales y financieros, y con la posibilidad de causar un gran impacto en la infraestructura crítica de un país o de una organización. Además, los ciberataques pueden ser lanzados desde cualquier parte del mundo, lo que hace que sea difícil atribuir la responsabilidad a un actor específico. Clarke argumenta que el ciberespacio ofrece una ventaja estratégica a los adversarios, porque les permite operar sin ser detectados y afectar sistemas críticos como infraestructuras, redes de comunicaciones y sistemas militares (Clarke, 2010). Esta nueva forma de conflicto permite a los actores estatales y no estatales nivelar el campo de juego contra adversarios más fuertes, considerando que el ciberespacio es un dominio en el que el tamaño y la capacidad económica no son necesariamente determinantes para el éxito de un ataque. Kramer sostiene que los ciberconflictos pueden proporcionar a los actores una ventaja táctica, ya que les permiten penetrar en sistemas de información y comunicación de los adversarios para obtener información clasificada o alterar los sistemas de comando y control (Kramer, 2009).

Otra de las ventajas estratégicas de los ciberconflictos es su capacidad para producir daños y afectar objetivos clave sin necesidad de una fuerza militar convencional. Mediante ciberataques, pueden causar daños significativos a los sistemas de infraestructura crítica, como los de energía, transporte, salud y finanzas, lo que puede tener consecuencias graves para la economía y la sociedad en su conjunto. Según Rid (2013), los ciberconflictos permiten a los actores poderosos "proyectar su poder en el ciberespacio sin el costo de las operaciones militares convencionales" (p. 4). Esto les permite infligir daños significativos a los sistemas de infraestructura crítica, sistemas financieros y de comunicaciones, entre otros,

sin necesidad de poner en riesgo a su propia fuerza militar. Los ciberataques pueden ser utilizados como una forma de coerción y disuasión en las relaciones internacionales; para enviar mensajes a otros actores internacionales y amenazar con mayores consecuencias si se cumplen ciertas condiciones (Libicki, 2009, pp. 11-12). Fernández (2022) afirma que:

> […] de 2021 a la actualidad los ciberataques están siendo usados como arma no convencional entre Estados, los principales implicados siguieron siendo los países que anteriormente tenían gran actividad en el ciberespacio, es decir, EE. UU. , China, Rusia y la Unión Europea, a los que se van sumando otras naciones hasta ahora poco beligerantes en la lucha cibernética, como India, así como otros actores que siempre estuvieron activos, casos Corea del Norte, Israel o Irán. (Fernández, 2022, pp. 313-314)

De estas afirmaciones, se puede inferir que la ventaja estratégica de los ciberconflictos radica en su capacidad para infligir daños significativos sin necesidad de poner en riesgo la propia fuerza militar y en su capacidad para ser utilizados como una forma de coerción y disuasión en las relaciones internacionales, por lo que el poder militar ciberespacial representa una necesidad latente en la agenda de los países; sin embargo, no se puede perder de vista que esta realidad complejiza la forma en que los Estados-nación definen, valoran y adquieren su poder militar ciberespacial.

El ciberpoder es una forma de proyección de poder en la era digital y su desarrollo es esencial para la seguridad y defensa de las naciones. Así lo argumenta Sánchez (2019), al señalar que el poder ciberespacial es una herramienta crítica para la seguridad y defensa nacional, ya que permite a los Estados proteger sus sistemas informáticos críticos y asegurar su soberanía en el ciberespacio. Los autores sostienen que el ciberpoder es un componente integral de la seguridad nacional y que su desarrollo debe ser una prioridad para los Gobiernos. Según Segal (2017), el poder ciberespacial se refiere a la capacidad de controlar y explotar el ciberespacio para lograr objetivos políticos, económicos o militares, ya sea mediante la protección de la propia infraestructura crítica o la interrupción de la de los adversarios.

El ciberpoder permite obtener la superioridad o supremacía en el ciberespacio. Su disputa puede proporcionar a un país una ventaja estratégica en términos de seguridad nacional, política, económica y militar. Al tener un dominio fuerte en el ciberespacio, un país puede proteger sus propios sistemas de información y

comunicación y, al mismo tiempo, espiar, sabotear o interrumpir los sistemas de otros países. Además, el ciberespacio es una plataforma vital para la economía digital y la innovación tecnológica, lo que significa que un país con una ventaja en el ciberespacio puede ganar una posición de liderazgo en el comercio mundial y la tecnología. Por lo tanto, la disputa por la superioridad o la supremacía en el ciberespacio se ha convertido en una parte importante de la competencia geopolítica actual. Los países compiten por la superioridad y supremacía en el ciberespacio porque consideran que el control de la información y las comunicaciones en este ámbito es fundamental para su seguridad, economía e influencia en el mundo. Los países están compitiendo por la superioridad en el ciberespacio y esto está afectando la seguridad nacional y las relaciones internacionales (Sanger, 2018).

Los países compiten por la superioridad en el ciberespacio para mantener la seguridad nacional, proteger los intereses económicos y garantizar la estabilidad política y social (Tikk & Kerttunen, 2020) Los países compiten por la superioridad en el ciberespacio porque la información y el conocimiento son los recursos más valiosos del mundo actual y porque el control de estos recursos es clave para el poder y la influencia (Stavridis & Farkas, 2012), lo que da cuenta de la importancia que representa para una nación u organización desarrollar el ciberpoder y disputar su superioridad o supremacía.

El poder cibernético se ha convertido en un elemento fundamental para la seguridad nacional y la defensa de los Estados, debido a que los ciberataques pueden causar graves daños a la infraestructura crítica y a la economía de los países (Cujabante et al., 2020; Libicki, 2018; Valeriano & Maness, 2020).

Perspectivas sobre el ciberpoder

De acuerdo con Nye (2011), no solo los tipos y las fuentes de poder de los países han cambiado; los cambios se presentan también en el contexto internacional, es decir, el escenario donde conviven los Estados; a propósito, destaca que los países tienen que convivir con otros actores no gubernamentales (s. p.). Las perspectivas del ciberpoder son amplias y variadas. En primer lugar, el ciberpoder se considera una herramienta esencial para la proyección de poder en el mundo moderno. A diferencia del poder tradicional, que se basa en la fuerza física y la coerción, el ciberpoder se basa en la capacidad de influir y controlar el comportamiento de los individuos por medio del ciberespacio. Aunque el ciberespacio aún no se ha utilizado como medio para demostrar el poder duro convencional de la coerción y las

amenazas respaldadas por la fuerza física, sí presenta un medio adecuado para la proyección del poder blando de atracción e imitación. A continuación, se presentan las perspectivas del ciberpoder analizadas desde las voces militares o estratégicas estadounidenses (Kuehl, 2009; Nye, 2010) en contraposición con las acepciones de Dunn respecto del ciberpoder en la Unión Europea (Dunn, 2018).

Para continuar este análisis se hace necesario comprender lo que he denominado *localización del ciberpoder*, que sigue dos tendencias: la primera puede vincularse con las definiciones de ciberpoder militar y corresponde a una perspectiva reduccionista que concibe el ciberespacio como medio de gestión que debe ser preservado para retener la iniciativa; de allí que los esfuerzos operacionales se orienten a generar protocolos para la defensa de activos estratégicos, en ocasiones no de la nación sino de las fuerzas, lo cual es aún más limitante. La otra perspectiva, que puede denominarse *comprehensiva*, se profiere con la definición de ciberestrategia o de ciberpoder integrado a otros dominios o al poder nacional; incorpora y expande el núcleo y capacidades asociadas al ciberpoder en función exclusiva del dominio ciberespacial y suma o se integra a otros componentes.

Ciberpoder en EE. UU.

Para comprender el ciberpoder desde la teoría del ciberpoder militar propuesta por el Gaines (2015), se hace necesario entender los términos y principios que forman la base de esta teoría y ayudan a comprender y aplicar las operaciones en el ciberespacio en el contexto de las operaciones conjuntas y la expansión del poder de combate:

- Ciberespacio: dominio global que abarca elementos físicos, lógicos y personales en el ámbito cibernético.
- Ciberpoder: aplicación de conceptos operativos, estrategias y funciones que emplean operaciones en el ciberespacio para expandir el poder de combate y lograr objetivos militares.
- Estrategia militar cibernética: desarrollo y empleo de capacidades operativas en el ciberespacio integradas con otras capacidades en diferentes dominios para expandir el poder de combate y lograr los objetivos militares.
- Terreno clave en el ciberespacio: cualquier elemento físico, lógico o personal del ciberespacio que, si es interrumpido, degradado o destruido, limita el poder de combate y otorga una ventaja marcada a uno de los combatientes.

- Espacios cibernéticos militares: diferentes ciberespacios que existen, teniendo en cuenta su diversidad y heterogeneidad.

Sobre estos preceptos, la teoría propuesta por Gaines plantea que la integración de las operaciones del ciberespacio con las operaciones conjuntas puede ampliar el poder de combate conjunto de varias maneras (Kern, 2015).

Las operaciones en el ciberespacio presentan una serie de ventajas estratégicas. En primer lugar, ofrecen una mayor capacidad de ataque, lo que permite a las fuerzas conjuntas perturbar la infraestructura de comunicación y comando del enemigo, debilitando significativamente su capacidad de respuesta. Además, estas operaciones brindan una mejor defensa al permitir a las fuerzas conjuntas proteger sus propias redes y sistemas contra ataques cibernéticos, asegurando la integridad de su poder de combate. Asimismo, las operaciones cibernéticas proporcionan una mayor conciencia situacional al recopilar información en tiempo real sobre las actividades y capacidades del enemigo, lo que facilita la toma de decisiones fundamentadas y la adaptación ágil a situaciones cambiantes (DoD, 2011).

Por último, estas operaciones tienen la capacidad de apoyar y potenciar otras capacidades militares, como las operaciones terrestres, marítimas y aéreas, lo que se traduce en un aumento de la eficacia y la coordinación en operaciones conjuntas, ya sea neutralizando defensas enemigas antes de un ataque convencional o proporcionando apoyo en términos de inteligencia y comunicaciones durante operaciones combinadas. En general, la integración de las operaciones del ciberespacio en operaciones conjuntas amplía el poder de combate conjunto al proporcionar nuevas formas de ataque y defensa, mejorar la conciencia situacional y potenciar otras capacidades militares (Gaines, 2015).

Ciberpoder en la Unión Europea

Impulsada por preocupaciones sostenidas sobre las amenazas del ciberespacio, la ciberseguridad se ha convertido en un tema prioritario en las agendas políticas de los Estados y organizaciones internacionales y supranacionales, entre ellas la Unión Europea (UE). El debate político asociado se centra en medidas políticas para dominar el comportamiento en el ciberespacio, a fin de convertirlo de un lugar rebelde e inseguro en uno más estable, confiable y ordenado. En el centro de esta discusión se encuentran cuestiones fundamentales de poder y control (Dunn, 2018).

La dificultad con el concepto de ciberpoder es que aún no existen análisis sistemáticos (empíricos) del tema; de hecho, el cuerpo de literatura sobre el ciberpoder es pequeño y fragmentado. Los textos existentes, incluidos aquellos que abordan específicamente el ciberpoder europeo (Klimburg & Tirmaa-Klaar, 2011; Sliwinski, 2014a, 2014b), son de naturaleza principalmente orientada a políticas que vienen acompañados de una comprensión contextualmente restringida del poder que no necesariamente es fácilmente aplicable a otras políticas y contextos (Dunn, 2018). Por lo general, abordar las cuestiones de poder mediante la investigación empírica, en lugar de hacerlo de manera conceptual, teórica o normativa, conlleva una serie de desafíos. Estos desafíos se evidencian en la extensa literatura escrita sobre diversos aspectos del poder en las relaciones internacionales y los esfuerzos realizados para cuantificarlo.

De acuerdo con Dunn (2018), la UE asume el ciberpoder de diversas maneras. En primer lugar, la UE reconoce la importancia de la ciberseguridad y ha desarrollado políticas y estrategias para abordar las amenazas cibernéticas (Manners, 2002). La UE utiliza diferentes instrumentos, instituciones y agencias para ejercer diferentes formas de ciberpoder, tanto interna como externamente. Internamente, la UE emplea arreglos voluntarios, incentivos, diálogo, cooperación y coordinación para fortalecer su ciberpoder.

Desde una perspectiva externa, la UE aboga por una política de cooperación que se fundamenta en la promoción del ciberespacio como un ámbito de libertades y derechos fundamentales. No obstante, se admite que la UE carece de un enfoque estratégico unificado para ejercer de manera deliberada su ciberpoder. A pesar de que la UE cuenta con la capacidad de utilizar elementos cibernéticos no estatales en apoyo de sus políticas, no existe una estrategia claramente definida para aprovechar plenamente su ciberpoder. A medida que la tecnología de la información se vuelve un componente cada vez más central en la convergencia de problemáticas de seguridad, se reconoce que cualquier actor político con ambiciones regionales o globales debe involucrarse en el ámbito cibernético. Por lo tanto, se sugiere que la UE debe desarrollar un tipo de ciberpoder que se sustente en la resiliencia y los valores fundamentales de la UE, tales como la prevención, la integridad y el multilateralismo (Dunn, 2018). En suma, la UE asume el ciberpoder con políticas y estrategias de ciberseguridad, utilizando diferentes instrumentos y agencias, tanto interna como externamente. Sin embargo, se reconoce la necesidad de desarrollar un enfoque estratégico integrado para ejercer plenamente su ciberpoder.

Conclusiones

La transformación del ciberespacio hacia el ciberpoder representa un cambio fundamental en la concepción del poder en la era contemporánea. Este cambio ha sido impulsado por avances tecnológicos que han convertido el ciberespacio, de simple medio de comunicación, a un campo estratégico donde se libran batallas por la influencia, la seguridad y la supremacía. El ciberpoder no solo implica la capacidad de controlar y manipular el ciberespacio, sino también la habilidad de ejercer influencia y lograr objetivos políticos, económicos y sociales por medios digitales.

Las diversas perspectivas sobre el ciberpoder reflejan la complejidad y las múltiples dimensiones de este fenómeno. Por un lado, algunas visiones resaltan las oportunidades que ofrece el ciberespacio para la innovación, la colaboración y el empoderamiento ciudadano. Desde esta perspectiva, el ciberpoder se considera una fuerza democratizadora que amplía el acceso a la información, facilita la participación ciudadana y estimula el desarrollo económico y social.

Por otro lado, existen enfoques más críticos que alertan sobre los riesgos y desafíos asociados al ciberpoder. Estas visiones advierten sobre la creciente vulnerabilidad de las infraestructuras críticas ante ciberataques, la pérdida de privacidad y seguridad de los datos personales, así como el potencial de manipulación y desinformación en línea para socavar la democracia y los derechos humanos.

En este contexto, comprender y abordar las diversas perspectivas sobre el ciberpoder es crucial para diseñar políticas y estrategias efectivas que fomenten un uso responsable y ético del ciberespacio. Esto implica fortalecer la ciberseguridad, salvaguardar los derechos digitales de los individuos y promover una gobernanza inclusiva y transparente del ciberespacio a nivel nacional e internacional. En última instancia, el desafío radica en aprovechar las oportunidades que brinda el ciberpoder para impulsar el progreso y el bienestar humano, al tiempo que se mitigan los riesgos y se enfrentan los desafíos planteados por esta nueva dimensión del poder en el siglo XXI.

Referencias

Alberts, D. S., & Hayes, R. E. (2003). *Power to the edge: Command... Control... in the information age*. CCRP Publication Series. http://www.dodccrp.org/files/Alberts_Power.pdf

Arellano, A. (2019). *Ciberconflicto: La nueva amenaza global.* Instituto de Ingeniería UNAM.

Barnett, M., & Duvall, R. (2005). Power in international politics. *International Organization, 59*(1), 39-75. https://doi.org/10.1017/S0020818305050010

Bauman, Z. (2000). *Modernidad líquida*. Fondo de Cultura Económica.

Cano, J. J. (2021). Los conflictos híbridos y el poder de los algoritmos. *Revista Sistemas,* (161), 62-72. https://doi.org/10.29236/sistemas.n161a6

Carr, M., & Tikk, E. (2021). *International law and cyber conflict: Responding to new challenges*. Cambridge University Press.

Castells, M. (1996). *La era de la información: Economía, sociedad y cultura* (Vol. 1, La sociedad red). Alianza Editorial.

Castells, M. (2001). *La galaxia internet.* Plaza & Janes.

Castells, M. (2010). *The information age: Economy, society, and culture* (Vol 1., The rise of the network society). John Wiley & Sons.

Centro Superior de Estudios de la Defensa Nacional [CESEDEN]. (2012). *El ciberespacio: Nuevo escenario de confrontación.* Ministerio de Defensa Nacional. https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografia_126.pdf

Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it.* Harper Collins.

Cujabante Villamil, X. A., Bahamón Jara, M. L. ., Prieto Venegas, J. C. ., & Quiroga Aguilar, J. A. (2020). Ciberseguridad y ciberdefensa en Colombia: Un posible modelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova, 18*(30), 357-377. https://doi.org/10.21830/19006586.588

DoD. (2011). *Department of Defense Dictionary of Military and Asociated Terms.* DoD. https://irp.fas.org/doddir/dod/jp1_02.pdf

Dunn, C. M. (2018). Europe's cyber-power. *European Politics and Society, 19*(3), 304-320. https://doi.org/10.1080/23745118.2018.1430718

Estudillo, J. G. (2002). *Visibilidad de la producción académica de feministas mexicanas a través de una base de datos* [Tesis de pregrado, Universidad Nacional Autónoma de México].

Ferreira da Silva, P. (2018). Oportunidades y desafíos de tecnologías emergentes: La importancia de la industria aeroespacial para Brasil. *Revista Fuerza Aérea-EUA,* (2), 36-48.

https://www.airuniversity.af.edu/Portals/10/JOTA/Journals/Volume%201%20Issue%202/Spanish/05-peterson_s.pdf

Foucault, M. (1970). *El orden del discurso.* Fabula Tusquets Editores.

Gibson, W. (1982). *Burning Chrome.* Ace Books.

Gibson, W. (1984). *Neuromante.* Minotauro.

Gómez Rodríguez, G. A. (2017). *Riesgos de transgresión moral del militar en la post-modernidad* [Tesis, Universitat de Barcelona]. Repositorio UB. https://diposit.ub.edu/dspace/bitstream/2445/119533/1/GAGR_TESIS.pdf

Hardt, M., & Negri, A. (2004). *Multitud: guerra y democracia en la era del imperio.* Debate.

Hunker, J. (2010). *Cyber war and cyber power: Issues for NATO doctrine* [Research Paper, N.º 62]. https://ciaotest.cc.columbia.edu/wps/nat/0031912/f_0031912_25908.pdf

Jordan T., (1999). *Cyberpower: The culture and politics of cyberspace and the internet*. Routledge.

Kant, M. (1795/2010). *La paz perpetua*. Porrúa.

Kern, S. (2015). *Expanding combat power through military cyber power theory* [Tesis de maestría, Joint Advanced Warfighting School]. Repositorio institucional. https://apps.dtic.mil/sti/pdfs/ADA621664.pdf

Klimburg, A., & Tirmaa-Klaar, H. (2011). Cybersecurity and cyberpower: Concepts, conditions, and capabilities for cooperation for action within the EU. European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2011/433828/EXPO-SEDE_ET(2011)433828_EN.pdf

Kramer, F. D., Starr, S. H., & Went, L. K. (2009). *Cyberpower and national security.* Potomac Books, Inc.

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. En F. D. Kramer, S. H. Starr & L. K. Wentz, *Cyberpower and National Security* (pp. 1-17). https://ndupress.ndu.edu/Media/News/Article/1216674/cyberpower-and-national-security/

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar.* RAND Corporation. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Libicki, M. C. (2012). Cyberspace is not a warfighting domain. *Isjlp,* (8), 321. https://heinonline.org/HOL/LandingPage?handle=hein.journals/isjlpsoc8&div=17&id=&page=

Libicki, M. C. (2018). Expectations of cyber deterrence. *Journal of Strategic Studies, 41*(1-2), 44-57. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-4/Libicki.pdf

Lisa Institute. (s. f.) ¿Qué es la guerras híbridas y cómo nos afectan las amenazas híbridas. https://www.lisainstitute.com/blogs/blog/guerra-hibrida-amenazas-hibridas#:~:text=En%20los%20%C3%BAltimos%20a%C3%B1os%20cobran,o%20vectores%20de%20presi%C3%B3n%20econ%C3%B3mica

MacDonald, D. B. (2009). *Thinking history, fighting evil: Neoconservatives and the perils of historical analogy in American politics.* Lexington Books.

Madden, D., Hoffmann, D., Johnson, M., Krawchuk, F., Nardulli, B. R., Peters, J. E., Robinson, L., & Doll, A. (2016, 23 de febrero). *Toward operational art in special warfare.* Rand Corporation. https://www.rand.org/pubs/research_reports/RR779.html

Manners, I. (2002). Normative power Europe: A contradiction in terms? *Journal of Common Market Studies, 40*(2), 235-258. https://doi.org/10.1111/1468-5965.003

Mitchell, W. J. (1995). *City of bits: Space, place, and the Infobahn.* MIT Press.

Nye, J. S. (2010). *Cyber power.* Harvard Kennedy School.

Nye, J. S., (2011). *The future of power.* Public Affairs.

Pelroth, N. (2022). *Así es como me dicen que acabará el mundo.* Tendencias.

Psychogiou, V. (2022) Cyberspace: Is NATO doing enough? https://finabel.org/wp-content/uploads/2022/02/cyberspace-is-nato-doing-enough-1.pdf

Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies, 35*(1), 5-32. https://doi.org/10.1080/01402390.2011.608939

Sánchez, M. E. (2019). La ciberseguridad y la ciberdefensa, la necesidad de generar estrategias de investigación sobre las temáticas que afectan la seguridad y defensa del Estado. En G. Medina (Ed.), *La seguridad en el ciberespacio: un desafío para Colombia* (pp. 27-59). Escuela Superior de Guerra "General Rafael Reyes Prieto". https://doi.org/10.25062/9789585216549.01

Sanger, D. E. (2018). *The perfect weapon: War, sabotage, and fear in the cyber age.* Crown.

Schwab, K. (2017). *La cuarta revolución industrial.* Debate.

Segal, H. (2017). *Cyber-security at a frantic time: A rational plan.* Canadian Global Affairs Institute.

Singer, P. W., & Friedman, A. (2021). *Cybersecurity and cyberwar: What everyone needs to know.* Oxford University Press.

Sliwinski, K. F. (2014a). European union – Cyber power in the making. *Asia-Pacific Journal of EU Studies, 12*(1), 1-22. https://www.researchgate.net/publication/317717658_European_Union_-_cyber_power_in_the_making

Sliwinski, K. F. (2014b). Moving beyond the European union's weakness as a cyber-security agent. *Contemporary Security Policy, 35*(3), 468-486. https://10.1080/13523260.2014.959261

Stavridis, J., & Farkas, E. N. (2012). The 21st century force multiplier: Public–private collaboration. *The Washington Quarterly, 35*(2), 7-20. https://doi.org/10.1080/0163660X.2012.665336

Tikk, E., & Kerttunen, M. (Eds.). (2020). *Routledge handbook of international cybersecurity.* London: Routledge.

Toffler, A. (1970). *Future Shock.* Bantam House.

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system.* Oxford University Press.

Valeriano, B., Jensen, B., & Maness, R. C. (2020). *Cyber strategy: The evolving character of power and coercion.* Oxford University Press.

Vergara, E., Trama, G., Uriona, M. N., Ortiz, J. U., & Destro, L. A. (2018). *Operaciones militares cibernéticas: Planeamiento y ejecución.* Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. https://cefadigital.edu.ar/bitstream/1847939/939/1/CAVI-II%20-%20OMC%20DE%20VERGARA.pdf


EDITORIAL ESDEG

Tecnologías disruptivas, logística, seguridad y defensa en el ciberespacio

La presente obra desarrolla un análisis profundo de las tendencias actuales, desentrañando el entramado de amenazas y ataques que se gestan en las redes, invisibles, pero potencialmente devastadoras. Las tecnologías disruptivas, al reemplazar rápidamente las infraestructuras existentes, plantean desafíos cruciales para la ciberseguridad y la ciberdefensa nacional. ¿Cuál es el impacto de las tecnologías disruptivas y la logística global en el mantenimiento de la seguridad y la defensa en el ciberespacio?

EDITORIAL ESDEG

ISBN 978-628-7602-69-4