EDITORIAL ESDEG

Transformación digital y ciberseguridad en Colombia: desafíos estratégicos para sectores de infraestructura crítica

Colección Ciberseguridad y Ciberdefensa

Editores
Milena Elizabeth Realpe Díaz

Angélica María González González

Transformación digital y ciberseguridad en Colombia: desafíos estratégicos para sectores de infraestructura crítica

Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Colombia

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

Transformación digital y ciberseguridad en Colombia: desafíos estratégicos para sectores de infraestructura crítica

MILENA ELIZABETH REALPE DÍAZ
ANGÉLICA MARÍA GONZÁLEZ GONZÁLEZ
(EDITORAS)

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., 2026

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

Transformación digital y ciberseguridad en Colombia: desafíos estratégicos para sectores de infraestructura crítica, Milena Elízabeth Realpe Díaz y Angelica María González González, editoras -- Bogotá D.C. :Sello Editorial ESDEG, 2026.

302 páginas: ilustraciones y tablas; 24 cm.
Incluye referencias bibliográficas al final de cada capítulo

ISBN impreso: 978-628-7818-63-7
E- ISBN: 978-628-7818-64-4

(Colección Ciberseguridad y Ciberdefensa)

1.Ciberseguridad – Colombia 2.Ciberdefensa – Colombia 3.Inteligencia artificial – Colombia 4.Política pública – Colombia i.Caro Cancelado, Fabio Leonardo,Mayor General, (prefacio) ii.Realpe Díaz, Milena Elizabeth (editor - autor) iii.González González, Angélica María, (editor – autor) iv.Cano Londoño, Ana Catalina, (autor) v.Serrano Cuervo, Aldemar, (autor) vi.Toro Mora, Cristian Mauricio,(autor) vii.Melo Mendoza, Jeison Stiven, (autor) viii.Sanchez Gómez, Erika Tatiana, (autor) ix.Amaya Piracoca, Miguel Anderson, (autor) x.Flórez Cáceres, Mónica Lissette, (autor) xi.ColombiaEscuela Superior de Guerra "General Rafael Reyes Prieto"(ESDEG).

SCLC UA929C7 2026
SCDD 363.325

Registro Catalográfico SIBFuP 991410034007231

Archivo descargable en formato MARC en: https://short.do/nuMR2B

Transformación digital y ciberseguridad en Colombia: desafíos estratégicos para sectores de infraestructura crítica
Primera edición, 2026

Editoras:
Milena Elizabeth Realpe Díaz
Angélica María González González

Cubierta:
Lina María Marcela Lozada con base en imágenes de Gemini IA.

Colección Seguridad y Defensa

ISBN impreso: 978-628-7818-63-7
ISBN digital: 978-628-7818-64-4
DOI: https://doi.org/10.25062/9786287818644

2026 Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Vicedirección de Investigación
Sello Editorial ESDEG
Carrera 11 Nº. 102-50 Bogotá D.C., Colombia
www.esdeglibros.edu.co

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".

El contenido de este libro corresponde exclusivamente al pensamiento de los autores y es de su absoluta responsabilidad. Las posturas y aseveraciones aquí presentadas son resultado de un ejercicio académico e investigativo que no representa necesariamente la posición oficial ni institucional de las instituciones participantes, la Escuela Superior de Guerra "General Rafael Reyes Prieto", las Fuerzas Militares de Colombia y el Ministerio de Defensa Nacional.

Los libros publicados por el Sello Editorial ESDEG son de acceso abierto bajo una licencia Creative Commons: Reconocimiento-NoComercial-SinObrasDerivadas.
https://creativecommons.org/licenses/by-nc-nd/4.0/

Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Colombia

Mayor General
Fabio Leonardo Caro Cancelado
DIRECTOR

Brigadier General
Jaime Andrés Valencia Monsegny
SUBDIRECTOR

Coronel
Aldemar Serrano Cuervo
VICEDIRECTOR DE INVESTIGACIÓN

EDITORIAL **ESDEG**

Coronel
Aldemar Serrano Cuervo
JEFE SELLO EDITORIAL ESDEG

Erika Ramírez Benítez
EDITORA LIBROS ESDEG

Felipe Solano Fitzgerald
CORRECTOR DE ESTILO

Lina Marcela Manrique Lozada
DIAGRAMADORA

EDITORIAL ESDEG

Contenido

Prefacio 09-10
MG. Fabio Leonardo Caro Cancelado

Introducción 11-14
CR. Milena Elizabeth Realpe Díaz

Capítulo 1
Fundamentos de la gobernanza digital y la ciberseguridad en Colombia 15-36
Milena Elizabeth Realpe Díaz

Capítulo 2
Gobernanza digital para el sector defensa y seguridad: una necesidad latente 37-68
Ana Catalina Cano Londoño

Capítulo 3
Innovación y adaptación: capacidades militares frente a amenazas emergentes en la Guerra Tecnológica Contemporánea 69-118
Aldemar Serrano Cuervo

Capítulo 4
Ciberseguridad en el Comando Conjunto Cibernético de Colombia: desafíos y oportunidades 119-150
Cristian Mauricio Toro Mora

Capítulo 5
Ciberseguridad en el sector universitario colombiano: diagnóstico, desafíos y recomendaciones para un entorno digital seguro 151-182
Jeison Stiven Melo Mendoza

Capítulo 6
Firewall humano y la protección de infraestructura crítica: modelo marco de formación en ciberseguridad 183-238
Erika Tatiana Sánchez Gómez

Capítulo 7
Madurez de la implementación de la inteligencia artificial en ciberseguridad en el sector salud en Colombia 239-268
Miguel Anderson Amaya Piracoca

Capítulo 8
Cooperación internacional en ciberseguridad y gobernanza digital 269-294
Mónica Lissette Flórez Cáceres

Epílogo
Legado, prospectiva y llamado a la acción 295-302

Prefacio

Mayor General Fabio Leonardo Caro Cancelado
Director de la Escuela Superior de Guerra "General Rafael Reyes Prieto"

En un mundo donde las fronteras físicas han cedido protagonismo a los dominios digitales, la soberanía nacional ya no se defiende únicamente con batallones y armamento, sino también con arquitecturas inteligentes, algoritmos y protocolos de ciberseguridad. En este contexto de transformación acelerada, la colección de escritos que presenta este libro no es simplemente un panorama académico: es una hoja de ruta estratégica para quienes tienen la responsabilidad de proteger la nación en el siglo XXI.

Esta transformación hacia el dominio digital ha permeado, pues, los sectores más importantes de la vida nacional en Colombia (la industria, la salud, la educación, la defensa nacional y el gobierno), lo que no solo genera oportunidades extraordinarias, sino que también expone vulnerabilidades que actores hostiles, tanto estatales como no estatales, están dispuestos a explotar. Cada sistema de información comprometido, cada dato sensible filtrado, cada infraestructura crítica atacada representa una amenaza directa a la estabilidad del Estado, a la confianza de los ciudadanos y a la continuidad de los servicios esenciales. La magnitud del desafío exige respuestas igualmente ambiciosas: políticas públicas robustas, marcos normativos actualizados, talento humano especializado y una cultura organizacional orientada a la seguridad y, en especial, a la defensa.

Este libro nace de la confluencia de distintos campos del conocimiento e investigadores multidisciplinares: oficiales de las Fuerzas Militares, expertos en ciencia y tecnología y académicos sociales comprometidos con el desarrollo nacional. Cada uno de sus capítulos ha sido concebido no como un ejercicio intelectual aislado, sino como una contribución deliberada a la construcción de un ecosistema de ciberseguridad que Colombia necesita con urgencia. Desde los fundamentos de la gobernanza digital hasta la cooperación internacional, y desde el análisis del sector salud hasta la formación del talento humano como primer escudo de defensa, la colección ofrece una mirada panorámica y al mismo tiempo profunda sobre los retos que enfrenta el país.

Resulta entonces relevante que este proyecto emerja en un momento en que el mundo registra niveles sin precedentes de ataques cibernéticos a infraestructuras críticas. Hospitales paralizados por *ransomware,* redes eléctricas comprometidas, sistemas de defensa infiltrados y datos gubernamentales sustraídos son titulares recurrentes en el escenario global. La pregunta pertinente no es si Colombia será objetivo de tales amenazas, sino si estará suficientemente preparada para prevenirlas, detectarlas o neutralizarlas. Esta obra responde, con rigor académico y visión estratégica, a ese imperativo nacional.

Como institución formadora del liderazgo estratégico de las Fuerzas Militares de Colombia, la Escuela Superior de Guerra "General Rafael Reyes Prieto" asume con orgullo el respaldo a investigaciones de esta naturaleza. La seguridad nacional en la era digital no puede construirse sin la participación de pensadores capaces de anticipar amenazas, diseñar respuestas sistémicas y articular esfuerzos entre el Estado, la academia, el sector privado y la comunidad internacional. Esta obra encarna precisamente ese espíritu: el de la inteligencia al servicio de la patria.

A cada lector, ya sea funcionario público, oficial de las Fuerzas Militares, académico social, profesional del sector tecnológico o ciudadano comprometido con el futuro del país, se le extiende una invitación formal y sincera: recorra estas páginas con la misma convicción con que sus autores las escribieron. Aquí encontrará no solo diagnósticos, sino propuestas; no solo problemas, sino soluciones; no solo historia, sino prospectiva. Colombia tiene en este libro una herramienta para anticiparse al futuro. El momento de prepararse es ahora.

Introducción

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

La presente obra colectiva constituye una respuesta académica y estratégica a uno de los desafíos más apremiantes que enfrenta Colombia en la era digital: la protección de sus infraestructuras críticas y la consolidación de una gobernanza digital robusta en todos los sectores de importancia estratégica nacional. Cada capítulo ha sido elaborado por investigadores y especialistas con experiencia directa en sus respectivos campos, lo cual garantiza una combinación inusual de rigor conceptual y pertinencia práctica.

A continuación, se presenta una síntesis orientadora de cada capítulo, diseñada para guiar al lector en la navegación de esta obra y para destacar la contribución específica de cada sección al conjunto del conocimiento producido.

El capítulo 1, "Fundamentos de la gobernanza digital y la ciberseguridad en Colombia", de la Coronel Milena Elizabeth Realpe Díaz, establece los pilares conceptuales y normativos sobre los cuales se edifica la presente obra. La autora introduce al lector en el universo de la gobernanza digital, articulando sus principios fundamentales con el marco regulatorio colombiano e internacional, operativamente establece con precisión la relación indisoluble entre una gobernanza digital efectiva y una ciberseguridad robusta. Con base en el análisis de los hallazgos de Amazon Web Services (AWS) sobre el estado actual de Colombia en materia de ciberseguridad, Realpe traza un diagnóstico honesto y riguroso de las fortalezas y las brechas que presenta el país en sus diferentes sectores estratégicos. Así, su diagnóstico proporciona al lector el contexto indispensable para comprender los análisis desarrollados en los capítulos subsiguientes.

En el capítulo 2, titulado "Gobernanza digital para el sector defensa y seguridad en Colombia", Ana Catalina Cano Londoño propone un modelo de gobernanza digital específicamente diseñado para responder a los requerimientos de ciberseguridad y cumplimiento regulatorio que demanda el entorno operacional de las Fuerzas Militares colombianas. Específicamente, la autora construye un marco

integral que articula principios de gestión de riesgos, políticas de protección de la información clasificada y lineamientos para la toma de decisiones tecnológicas en contextos de alta sensibilidad, con lo cual se ofrece un instru-mento práctico y estratégico para los líderes del sector.

En el capítulo 3, "Innovación y adaptación: Capacidades militares frente a amenazas emergentes en la guerra tecnológica contemporánea", el Coronel Aldemar Serrano Cuervo examina cómo la convergencia tecnológica reconfigura estructuralmente el carácter de la guerra, desplazando su centro de gravedad desde la destrucción física hacia el control de sistemas, datos, procesos decisionales y la dimensión cognitiva. A partir de un marco analítico que articula niveles estructurales, actorales y tecnológicos, el autor identifica una taxonomía de ocho formas contemporáneas de conflicto (guerra algorítmica, de datos, cognitiva, de sistemas, distribuida, persistente, de velocidad y de dependencia tecnológica) y las vincula con las capacidades militares necesarias para enfrentarlas mediante una matriz aplicada al diseño de fuerzas y la doctrina. El capítulo presta especial atención al contexto colombiano, donde actores híbridos integran control territorial, economías ilícitas digitalizadas y tecnologías emergentes accesibles, y propone orientaciones concretas para la adaptación estratégica de las Fuerzas Militares ante escenarios de conflicto tecnológicamente mediado.

El capítulo 4, "Ciberseguridad en el Comando Conjunto Cibernético de Colombia: desafíos y oportunidades", del Sargento Segundo Cristian Mauricio Toro Mora, sumerge al lector en la realidad operacional del Comando Conjunto Cibernético de Colombia y analiza con profundidad los principales desafíos en ciberseguridad que enfrentan las Fuerzas Militares en el ejercicio de su misión constitucional. El autor identifica las amenazas más relevantes del espectro cibernético —desde el espionaje digital hasta los ataques a sistemas de mando y control—, examina las capacidades actuales de respuesta y señala las oportunidades estratégicas que ofrece el fortalecimiento del ciberdominio como pilar fundamental de la defensa nacional contemporánea.

El capítulo 5 se titula "Ciberseguridad en el sector universitario colombiano: diagnóstico, desafíos y recomendaciones para un entorno digital seguro", de Jeison Stiven Melo Mendoza. En un contexto en el que las instituciones de educación superior colombianas custodian uno de los activos más valiosos del país: el conocimiento y los datos de miles de estudiantes, docentes e investigadores, este trabajo aborda con rigor el diagnóstico de la situación actual de la ciberseguridad en el sector universitario, identificando sus principales vulnerabilidades y la creciente

exposición a ataques cibernéticos. A partir de ese análisis, el autor propone lineamientos concretos en materia de políticas institucionales, estrategias de gestión del riesgo y soluciones tecnológicas orientadas a mitigar amenazas y proteger la integridad de los datos sensibles en un ecosistema académico cada vez más digitalizado.

En el capítulo 6, "Firewall humano: lo que realmente protege la infraestructura crítica - Modelo Marco de Formación en Ciberseguridad", Erika Tatiana Sánchez Gómez plantea una tesis central tan provocadora como irrefutable: el ser humano es simultáneamente el eslabón más débil y el escudo más poderoso de cualquier sistema de ciberseguridad. Desde esta perspectiva, la autora desarrolla un Modelo Marco de Formación en Ciberseguridad basado en tecnologías emergentes y referentes internacionales de vanguardia. Dirigido especialmente a las empresas con infraestructura crítica en Colombia, el modelo propor-ciona una arquitectura pedagógica y metodológica que permite diseñar programas de formación efectivos, capaces de transformar la cultura organizacional y garantizar la continuidad del negocio frente a amenazas cibernéticas en constante evolución.

El capítulo 7, "Madurez en la implementación de inteligencia artificial en ciberseguridad en el sector salud en Colombia", de Miguel Anderson Amaya Piracoca, evalúa con criterio técnico y estratégico el nivel de madurez en la implementación de la inteligencia artificial como herramienta de ciberseguridad en los sistemas e infraestructuras del sector salud del país, que es el repositorio de los datos más íntimos y sensibles de los ciudadanos colombianos. El autor examina tanto los avances logrados como las brechas existentes frente a un panorama de amenazas que incluye el *ransomware,* la exfiltración de historias clínicas y los ataques a dispositivos médicos conectados, lo cual le permite proponer una hoja de ruta para elevar la resiliencia digital del sistema de salud colombiano.

El capítulo 8, "Cooperación internacional en ciberseguridad y gobernanza digital", de Mónica Lissette Flórez Cáceres, amplía el horizonte de análisis hacia el sistema internacional, argumentando que ningún Estado puede enfrentar en solitario los desafíos de la ciberseguridad global. La autora examina la importancia de la cooperación regional y multilateral, las alianzas estratégicas que Colombia ha construido con socios nacionales e internacionales, así como los tratados y marcos normativos internacionales que regulan el ciberespacio. Además, analiza el papel activo que Colombia desempeña y debe fortalecer en la agenda global de ciberseguridad y gobernanza digital, lo cual proyecta al país como un actor regional propositivo y confiable.

Finalmente, el epílogo, de Angélica María González González, presenta las conclusiones de la obra en una reflexión final cohesionada, en la cual se subraya la necesidad de articular la ciberseguridad y la gobernanza digital como ejes transversales de la política pública colombiana. La autora sintetiza las principales lecciones aprendidas de los distintos sectores estudiados, formula recomendaciones concretas orientadas al fortalecimiento de las capacidades nacionales y convoca a los tomadores de decisiones, académicos y profesionales a asumir con renovado compromiso el desafío de construir una Colombia digitalmente segura, soberana y resiliente.

Capítulo 1

Fundamentos de la gobernanza digital y la ciberseguridad en Colombia*

DOI: https://doi.org/10.25062/9786287818644.01

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

Resumen: Este capítulo analiza de manera integral los principales vectores que configuran la ciberseguridad en Colombia: la gobernanza digital, la transformación tecnológica, la resiliencia en infraestructuras críticas, el fortalecimiento del capital humano y el papel de la inteligencia artificial en la ciberdefensa. La reflexión se fundamenta en la *Guía estratégica para mejorar la postura de ciberseguridad de Colombia,* elaborada por Amazon Web Services (AWS, 2024), que emplea el Cybersecurity Capacity Maturity Model for Nations (CMM) de la Universidad de Oxford como marco de referencia. Asimismo, se incorporan lineamientos internacionales de la OEA, la ONU, la OTAN y el Foro Económico Mundial, que permiten contrastar avances, identificar brechas y proyectar escenarios de mejora. Se concluye que Colombia, a través de la inversión sostenida en talento especializado, la cooperación internacional y la consolidación de instituciones resilientes, tiene la oportunidad de convertirse en referente regional en ciberseguridad, lo cual garantizará la confianza digital, el desarrollo económico y la soberanía tecnológica.

Palabras clave: ciberamenazas; ciberseguridad; infraestructuras críticas; gobernanza digital; madurez; resiliencia.

* Capítulo de libro resultado del proyecto de investigación "La gobernanza del ciberespacio a nivel global, regional y nacional: desafíos, oportunidades y estrategias para la soberanía digital", del grupo de investigación "Ciberespacio, Tecnología e Innovación", de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado en 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 la autora y no reflejan necesariamente los de las instituciones participantes.

Milena Elizabeth Realpe Díaz

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. (2026). Fundamentos de la gobernanza digital y la ciberseguridad en Colombia. En M. E. Realpe-Díaz & A. M. González-González (Eds.), *Transformación digital y ciberseguridad en Colombia: Desafíos estratégicos para sectores de infraestructura crítica* (pp. 15-36). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818644.01

TRANSFORMACIÓN DIGITAL Y CIBERSEGURIDAD EN COLOMBIA: DESAFÍOS ESTRATÉGICOS PARA SECTORES DE INFRAESTRUCTURA CRÍTICA
ISBN impreso: 978-628-7818-63-7
ISBN digital: 978-628-7818-64-4
DOI: https://doi.org/10.25062/9786287818644

Colección Ciberseguridad y Ciberdefensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2026

CC BY NC ND

Introducción: gobernanza digital y ciberseguridad en Colombia

La gobernanza digital constituye el conjunto de principios, políticas, normas y capacidades que permiten a los Estados gestionar de manera eficiente, segura y transparente sus procesos de transformación digital. En Colombia, este concepto se ha materializado a través de la Política de Gobierno Digital, que se estableció mediante el Decreto 1008 de 2018, se compiló en el Decreto Único Reglamentario del sector TIC (Decreto 1078 de 2015) y forma parte del Modelo Integrado de Planeación y Gestión (MIPG). Esta política busca garantizar la articulación de los servicios digitales del Estado, la interoperabilidad entre entidades y la protección de los datos ciudadanos. La gobernanza digital, sin embargo, no puede desligarse de la ciberseguridad, ya que esta última constituye el mecanismo habilitante para preservar la integridad, disponibilidad y confidencialidad de los sistemas digitales que sustentan la operación del Estado y de los sectores estratégicos. En este sentido, la Estrategia Nacional de Seguridad Digital posiciona a Colombia como una potencia regional en ciberseguridad, lo cual promueve un sistema resiliente que impulse la confianza digital, el crecimiento económico y el bienestar social. La relación entre gobernanza digital y ciberseguridad adquiere especial relevancia en sectores como la defensa, la salud, la educación y las infraestructuras críticas, donde la protección de activos digitales es fundamental para la seguridad nacional. Según el estudio realizado por Amazon Web Services (AWS) en 2024, Colombia ha logrado avances importantes en la formulación de políticas y en la identificación de capacidades, pero aún enfrenta desafíos en la implementación técnica, la coordinación interinstitucional y la gestión del riesgo en entornos complejos (AWS, 2024).

Este libro se fundamenta en el análisis crítico de la *Guía estratégica para mejorar la postura de ciberseguridad de Colombia*, documento que fue elaborado en 2024 por AWS para la Presidencia de la República de Colombia. Dicha guía tiene como propósito identificar las fortalezas y oportunidades del país en materia de ciberseguridad, así como proponer una hoja de ruta orientada al fortalecimiento de su madurez y gobernanza en este ámbito (AWS, 2024).

Para estructurar su hoja de ruta, AWS emplea el Cybersecurity Capacity Maturity Model for Nations (CMM), desarrollado por el Global Cyber Security Capacity Centre (GCSCC) de la Universidad de Oxford. Específicamente, el CMM proporciona un marco metodológico integral para evaluar las capacidades nacionales en ciberseguridad, el cual abarca dimensiones clave como la formulación de políticas, la cultura de seguridad, la educación, la colaboración interinstitucional y la gestión de riesgos (GCSCC, 2021).

La articulación entre la guía estratégica de AWS y el CMM permite establecer un diagnóstico técnico y político sobre el estado actual de la ciberseguridad en Colombia, así como delinear acciones concretas para avanzar hacia una gobernanza más robusta, resiliente y alineada con estándares internacionales. Según el análisis, Colombia se encuentra en una transición del nivel formativo 2 al nivel establecido 3 de madurez en ciberseguridad, lo cual la posiciona como uno de los países más avanzados en la región, según estudios previos basados en CMM. Sin embargo, la frecuencia y complejidad de los ciberataques están en aumento, lo que subraya la urgencia de fortalecer las capacidades nacionales. En este sentido, la guía propone una meta ambiciosa de alcanzar niveles relativamente altos (4+) —siendo 5 la calificación más alta— en todas las dimensiones a más tardar el año 2028.

Ahora bien, la comprensión de la gobernanza digital en Colombia exige situarla en un marco teórico más amplio que el puramente normativo. Al respecto, Castells (2009) advierte que el poder en la sociedad contemporánea se ejerce y se contesta fundamentalmente a través de redes de comunicación: quien controla los flujos de información define los términos de la organización social y política. Desde esta perspectiva, la gobernanza digital colombiana, materializada en el Decreto 1008 de 2018 y el Modelo Integrado de Planeación y Gestión(MIPG), no puede entenderse únicamente como un conjunto de disposiciones administrativas, sino como un intento del Estado por afirmar su capacidad de ordenar, proteger y legitimar los flujos digitales que sostienen la vida institucional y social del país. La ciberseguridad, en este sentido, no es un componente accesorio de la gobernanza digital: es su condición de posibilidad.

Sin embargo, la mera existencia de marcos normativos no garantiza gobernanza efectiva. DeNardis (2014) demuestra que la gobernanza de internet es, en esencia, una disputa entre actores con intereses divergentes, entre los cuales se cuentan Estados, corporaciones tecnológicas, organismos multilaterales y sociedad civil, por definir quién controla la infraestructura, los estándares y los protocolos sobre los que opera el mundo digital. Colombia, al diseñar su arquitectura de gobernanza digital, enfrenta precisamente esta tensión: debe articular actores públicos fragmentados, regular a actores privados con capacidades técnicas superiores a las del Estado y alinearse simultáneamente con marcos internacionales (OEA, ONU, OTAN) sin perder autonomía soberana. El diagnóstico del CMM, que ubica al país en una transición del nivel formativo al establecido, refleja justamente esta distancia entre la capacidad normativa (relativamente desarrollada) y la capacidad operativa e interinstitucional, aún deficitaria.

Esta brecha entre norma y capacidad tiene raíces estructurales que Kettl (2015) analiza con precisión: la transformación del Estado en la era digital no es un proceso técnico, sino político y organizacional. Las instituciones públicas enfrentan el desafío de gestionar interdependencias complejas, coordinar redes de actores heterogéneos y rendir cuentas en entornos de alta incertidumbre tecnológica, todo ello con estructuras burocráticas diseñadas para contextos analógicos. En el caso colombiano, esto se traduce en dificultades concretas: la coordinación entre ColCERT, el MinTIC, el Ministerio de Defensa y las entidades sectoriales no responde aún a una lógica sistémica de gestión del riesgo, sino a competencias dispersas que generan duplicidades y vacíos de respuesta ante incidentes.

Desde el contexto colombiano específico, Cano (2022) aporta una perspectiva complementaria e indispensable: la ciberseguridad efectiva requiere no solo políticas públicas robustas, sino también una cultura organizacional que integre la seguridad como valor transversal en todos los niveles institucionales. La implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), alineado con la ISO/IEC 27001:2022, es un avance técnico significativo, pero su impacto real depende de que las entidades públicas y privadas lo interioricen como práctica cotidiana y no como cumplimiento formal. La brecha entre el diseño normativo y la ejecución operativa, señalada por el estudio de AWS (2024), es, en buena medida, una brecha cultural y de capacidades humanas, no solo técnica.

La articulación de estos cuatro argumentos permite formular una tesis de mayor alcance: Colombia ha construido una arquitectura normativa de gobernanza digital coherente con estándares internacionales, pero el tránsito hacia niveles

superiores de madurez en ciberseguridad exige una segunda transformación, esta vez de naturaleza institucional, cultural y operativa. Esta transformación implica, en términos de Castells (2009), fortalecer la capacidad del Estado para ejercer poder en las redes y no solo sobre ellas. Asimismo, en términos de DeNardis (2014), requiere desarrollar la agencia política para participar efectivamente en los debates globales de gobernanza. Adicionalmente, de acuerdo con Kettl (2015), demanda rediseñar los mecanismos de coordinación interinstitucional y, finalmente, desde la perspectiva de Cano (2022), anclar la ciberseguridad en una cultura organizacional que la asuma como responsabilidad compartida.

Metodología

Este libro adopta un diseño cualitativo-analítico con estrategia de estudio de caso sobre Colombia, que prioriza el análisis de documentos de política pública y marcos de capacidad en ciberseguridad. El eje metodológico se centra en el análisis de los resultados de la *Guía estratégica para mejorar la postura de ciberseguridad de Colombia* (AWS, 2024), los cuales se interpretan y mapean contra el CMM en su edición 2021, desarrollado por el Global Cyber Security Capacity Centre (2021). La lógica del caso se sustenta en la pertinencia de Colombia como sistema sociotécnico en transformación, en el marco de la Política Nacional de Seguridad Digital y la Estrategia Nacional de Seguridad Digital 2025–2027, que articulan una visión estratégica para fortalecer la resiliencia digital del país (MinTIC, s. f.; MinTIC, 2025). Asimismo, se reconoce la robustez del CMM como marco comparado de referencia para evaluar capacidades nacionales en cinco dimensiones clave: política y estrategia, cultura y sociedad, educación, marcos legales y técnicos, y estándares de respuesta. Asimismo, el enfoque metodológico se fundamenta en los principios del estudio de caso propuestos por Yin (2018), quien destaca su utilidad para comprender fenómenos complejos en contextos reales, especialmente cuando se requiere una aproximación profunda y contextualizada a sistemas en transformación.

Hacia un enfoque de ciberseguridad y transformación digital

La creciente digitalización de los sectores estratégicos en Colombia ha transformado la concepción de la seguridad nacional: la ciberseguridad y la gobernanza

digital son hoy pilares para la resiliencia institucional, la protección de infraestructuras críticas y la continuidad de servicios esenciales. En este marco, el país ha definido la seguridad como habilitador transversal de la Política de Gobierno Digital, materializada en el MSPI, actualizado y alineado con el ISO/IEC 27001:2022, con el fin de resguardar la confidencialidad, la integridad, la disponibilidad y la privacidad de los datos a lo largo de los procesos y activos del Estado. Ello exige controles "por diseño y por defecto", una arquitectura de defensa en profundidad, gestión de riesgos basada en evidencia y mecanismos de continuidad del negocio que integren TI, TO y servicios al ciudadano. Esta visión se articula con la Estrategia Nacional de Seguridad Digital 2025-2027, construida sobre los CONPES 3701, 3854 y 3995, que adopta un enfoque de múltiples partes interesadas centrado en las personas, promueve la innovación responsable e incorpora métricas para seguimiento y rendición de cuentas. En el plano internacional, Colombia reafirma la aplicabilidad del derecho internacional (incluida la Carta de la ONU) al ciberespacio y se alinea con estándares y normas de comportamiento responsable, con lo cual fortalece la cooperación, la protección de derechos y la confianza digital.

Sobre esta base, en los últimos años se registran avances significativos en marcos y estrategias que han robustecido capacidades institucionales, la coordinación intersectorial y una cultura de seguridad alineada con estándares internacionales. Políticas como la Seguridad Digital y el fortalecimiento del Grupo de Respuesta a Emergencias Cibernéticas (ColCERT) han sido críticas para la gestión de riesgos y la respuesta coordinada ante incidentes. No obstante, persiste un incremento sostenido en la frecuencia y sofisticación de los ciberataques. Estos incluyen, por ejemplo, *ransomware* con doble y triple extorsión, campañas de *phishing* altamente dirigidas, compromiso de la cadena de suministro y explotación de vulnerabilidades en ambientes convergentes OT/IT/IoT. Estos vectores impactan sectores estratégicos —financiero, salud, energía, defensa, transporte— y evidencian brechas en ciberhigiene, segmentación de redes y gestión de identidades. Apoyada en técnicas avanzadas como inteligencia artificial generativa, automatización de ataques y uso de *deepfakes*, la evolución del cibercrimen organizado eleva el desafío para la seguridad nacional y demanda cooperación regional y protocolos de intercambio de inteligencia de amenazas.

Por todo lo anterior, Colombia debe reforzar sus capacidades de prevención, detección, respuesta y recuperación para promover una colaboración efectiva entre el sector público, el privado y la academia. En este sentido, la estrategia prioriza la construcción de un ecosistema resiliente que impulse la confianza digital, el

crecimiento económico y el bienestar social. Con este propósito, propone la creación de centros de operaciones de seguridad (SOC) sectoriales, el fortalecimiento de CSIRT/CERT, la realización de ejercicios nacionales de cibercrisis y el desarrollo de marcos de compartición de información (por ejemplo, ISAC).

En el ámbito de defensa, aunque la incorporación de inteligencia artificial, analítica avanzada y computación en la nube optimiza la conciencia situacional y el mando y control, esta también amplía la superficie de ataque y obliga a adoptar principios Zero Trust, la segregación de entornos TO, el *hardening* de plataformas, la seguridad de la cadena de suministro (incluido SBOM) y prácticas DevSecOps. En este contexto, iniciativas como Fuerza Innovación favorecen la co-creación entre el Estado, la empresa, la academia y los centros de I+D para acelerar pilotos de alto impacto, el escalamiento seguro y la transferencia tecnológica hacia capacidades sostenibles.

Con base en el análisis de la *Guía estratégica para mejorar la postura de ciberseguridad de Colombia* (AWS, 2024) y en el CMM del GCSCC, este capítulo presenta una visión integral de avances, brechas y oportunidades a lo largo de diez secciones: 1) fundamentos normativos y estratégicos de la gobernanza digital; 2) gobernanza en defensa y seguridad; 3) desafíos específicos de las Fuerzas Militares; 4) gobernanza digital en educación; 5) formación y capacidades en empresas de infraestructura crítica; 6) innovación y adopción ética de tecnologías emergentes; 7) prioridades para el Ejército Nacional de Colombia; 8) ciberseguridad marítima y poder naval; 9) madurez de inteligencia artificial en salud y protección de datos clínicos, y 10) cooperación internacional. Cada apartado integra métodos de evaluación (por ejemplo, CMM, NIST CSF), indicadores de desempeño, estudios de caso nacionales y regionales, y recomendaciones accionables a 3-5 años con responsables, hitos y métricas de seguimiento. El propósito es traducir marcos internacionales en rutas operativas, adaptadas al contexto colombiano y a la realidad de sus instituciones.

En suma, se propone una hoja de ruta basada en evidencia para consolidar políticas públicas sólidas, desarrollar talento especializado y afianzar una cultura de seguridad digital acorde con las exigencias del entorno global. El enfoque combina cinco vectores: gobernanza y regulación inteligente; capacidades técnicas y operativas; capital humano y cierre de brechas; cooperación internacional y alianzas, y cultura ciudadana y confianza digital. Se sugieren metas medibles, la reducción del Tiempo Medio de Detección (MTTD) y del Tiempo Medio de Respuesta (MTTR), la cobertura de controles y la madurez por dominio CMM. Adicionalmente, se plantean esquemas de financiamiento y mecanismos de auditoría y mejora continua.

La articulación entre conocimiento académico, experiencia operativa y estándares internacionales permite diagnosticar el estado actual, priorizar inversiones y proyectar escenarios de mejora sostenibles, colaborativos y alineados con los intereses estratégicos de la Nación.

Resiliencia cibernética en infraestructuras críticas

La resiliencia cibernética en infraestructuras críticas ha sido objeto de creciente atención en los marcos estratégicos internacionales y nacionales. En Colombia, la Estrategia Nacional de Seguridad Digital 2025-2027 plantea como objetivo específico mejorar la ciberresiliencia nacional mediante el fortalecimiento de la gestión de riesgos, la protección de infraestructuras críticas y el impulso de capacidades de ciberdefensa (Presidencia de la República, 2025). Este enfoque se alinea con la perspectiva del World Economic Forum (WEF), cuyo *Cyber Resilience Compass* (2025) resalta que ninguna organización puede aspirar a una seguridad del 100 %; por ello, la clave reside en la preparación para incidentes, la continuidad de servicios esenciales y la colaboración en ecosistemas interdependientes (WEF, 2025).

En el ámbito académico, la tesis de Sarmiento (2023) sobre ciberataques a infraestructuras críticas subraya la vulnerabilidad de sectores como energía, transporte y salud frente a *ransomware*, ciberespionaje y ataques a sistemas SCADA, y propone planes de recuperación y cooperación público-privada como elementos esenciales para la resiliencia. Por su parte, informes como el *Wavestone Cyber Benchmark 2025* confirman que, aunque la madurez de las organizaciones frente al *ransomware* ha mejorado, aún el 36 % de las medianas y pequeñas empresas se encuentran en situación crítica, circunstancia que acentúa la necesidad de fortalecer la resiliencia más allá de los grandes conglomerados (Wavestone, 2025).

La resiliencia cibernética en infraestructuras críticas exige superar la lógica reactiva de la seguridad perimetral para adoptar un enfoque multidimensional que integre anticipación, adaptación, resistencia y recuperación como funciones interdependientes. En este contexto, Linkov y Palma-Oliveira (2017) proponen un marco multidimensional que distingue cuatro funciones esenciales de la resiliencia: 1) absorber el impacto de un evento adverso, 2) adaptarse a las nuevas condiciones generadas por ese evento, 3) recuperar la funcionalidad del sistema afectado y, finalmente, 4) anticipar escenarios futuros de riesgo mediante el aprendizaje institucional. Esta distinción es crucial para el caso colombiano porque el diagnóstico del CMM y de la Estrategia Nacional de Seguridad Digital 2025-2027 revela una

asimetría preocupante: el país ha avanzado más en las funciones reactivas —recuperación y respuesta a incidentes— que en las funciones proactivas —anticipación y adaptación sistémica—. Al respecto, es importante enfatizar que la resiliencia, entendida en su dimensión plena, no es un estado que se alcanza, sino una capacidad dinámica que se construye y renueva continuamente frente a un entorno de amenazas en permanente evolución.

En entornos donde los sectores estratégicos operan en redes de dependencia mutua, el fallo de un componente puede desencadenar disrupciones sistémicas de alcance imprevisible. En Colombia, donde sectores como la salud, la defensa, el transporte y el sistema financiero comparten infraestructuras digitales y dependen de proveedores tecnológicos comunes, esta interdependencia representa uno de los vectores de riesgo más subestimados. La ausencia de mapas de dependencias actualizados y de protocolos de coordinación entre sectores ante incidentes simultáneos constituye, por tanto, una brecha estructural que ninguna política sectorial puede subsanar por sí sola (Luiijf et al., 2013), especialmente frente a amenazas persistentes avanzadas capaces de operar de forma encubierta durante períodos prolongados en entornos convergentes OT/IT/IoT (Stojanović et al., 2020). La respuesta técnica a este desafío requiere reorientar la arquitectura de los sistemas críticos hacia principios de continuidad operacional bajo condiciones de compromiso, incorporando redundancia, segmentación y diversidad como elementos de diseño estructural (Bodeau & Graubart, 2017). Para Colombia, avanzar en esta dirección implica no solo fortalecer capacidades institucionales de respuesta, sino también rediseñar la lógica con que el Estado concibe, despliega y audita sus infraestructuras digitales esenciales. Por lo tanto, la adopción de este enfoque en los sectores de energía, salud y defensa colombianos implicaría un cambio de paradigma: pasar de arquitecturas diseñadas para la eficiencia operativa a arquitecturas diseñadas para la operación degradada con continuidad de servicios esenciales.

En suma, la resiliencia cibernética en infraestructuras críticas exige un enfoque integral que comprende: defensa en profundidad, los planes de recuperación probados, la cooperación internacional (ONU y OEA) y el desarrollo de capacidades adaptativas frente a un entorno de amenazas en rápida evolución.

Capital humano y brecha de talento en ciberseguridad

El capital humano se ha convertido en un factor crítico para la sostenibilidad de la ciberseguridad en Colombia y América Latina. La demanda de profesionales

especializados crece exponencialmente en sectores estratégicos como finanzas, energía, salud y defensa, mientras que la oferta de talento se mantiene limitada, lo cual crea genera una brecha que impacta directamente en la capacidad de los Estados y de las empresas para responder eficazmente a incidentes cibernéticos. Según el *Estado de la ciberseguridad y la inteligencia artificial en Colombia* (2025), la escasez de capital humano calificado constituye uno de los principales retos para consolidar un ecosistema digital seguro, pues retrasa la implementación de políticas públicas y afecta la resiliencia de las infraestructuras críticas (Cámara Colombiana de Informática y Telecomunicaciones [CCIT], 2025).

El diagnóstico habitual sobre la escasez de profesionales en ciberseguridad tiende a formularse en términos cuantitativos: faltan especialistas, faltan programas, faltan certificaciones. Sin embargo, esta lectura superficial oculta una problemática de mayor profundidad. El *Cybersecurity Workforce Study* de ISC (2024) estima que la brecha global de talento en ciberseguridad supera los cuatro millones de profesionales. No obstante, su hallazgo más significativo no es numérico, sino cualitativo, al revelar que una proporción creciente de las organizaciones no carece de personal en términos absolutos, sino de personal con las competencias adecuadas para enfrentar amenazas específicas en contextos operativos concretos. Esta distinción es fundamental para Colombia, porque sugiere que la respuesta política no puede limitarse a aumentar la matrícula en programas existentes, sino que exige repensar qué tipo de profesionales se forma, con qué metodologías y para qué demandas reales del ecosistema digital nacional.

No obstante, este problema no es exclusivo de Colombia. Informes de la OEA y el Banco Interamericano de Desarrollo (BID, 2019) ya advertían que la región presenta una marcada escasez de profesionales certificados en ciberseguridad. Esta situación limita su capacidad de prevención, detección y respuesta a amenazas complejas. Aunque desde entonces se han fortalecido iniciativas de capacitación, la brecha persiste y se amplía en áreas emergentes como la inteligencia artificial aplicada a la seguridad, la ciberinteligencia y la protección de infraestructuras críticas.

La Estrategia Nacional de Seguridad Digital de Colombia 2025-2027 reconoce esta debilidad estructural y establece como línea de acción prioritaria el desarrollo del talento en seguridad digital, incentivando la creación de programas de formación y fomentando la cultura de seguridad desde etapas tempranas del sistema educativo (Presidencia de la República, 2025). En el ámbito internacional, la OTAN ha promovido el Cyber Defence Pledge (2021), instando a los Estados miembros a invertir en el entrenamiento continuo, la cooperación académica y la creación

de centros de excelencia en ciberseguridad, como el Cooperative Cyber Defence Centre of Excellence (CCDCOE) en Estonia.

La dimensión institucional de este problema encuentra en el marco de competencias de ENISA (2023) una referencia comparada de alta relevancia. El ENISA Cybersecurity Skills Framework establece una taxonomía estructurada de roles, competencias y niveles de dominio que permite a los Estados, las organizaciones y los sistemas educativos hablar un lenguaje común sobre qué significa ser un profesional de ciberseguridad competente. Sin embargo, Colombia carece actualmente de un equivalente nacional institucionalizado, de manera que la multiplicidad de certificaciones internacionales (CISSP, CEH, CompTIA Security+, entre otras) coexiste sin un marco de reconocimiento que las articule con las necesidades específicas del ecosistema digital colombiano, con la estructura de cargos del sector público o con los requerimientos de las infraestructuras críticas nacionales. Esta ausencia genera una paradoja operativa: un profesional con certificaciones internacionales puede no tener las competencias relevantes para el contexto colombiano, mientras que un especialista con experiencia operativa valiosa en entornos nacionales puede carecer del reconocimiento formal que le permita acceder a posiciones estratégicas.

La investigación académica respalda estas prioridades. Wu et al. (2023) subrayan que los programas de formación de talentos en ciberseguridad deben integrar competencias técnicas, estratégicas y éticas, para formar profesionales capaces de enfrentar amenazas híbridas en un entorno global. Asimismo, Ramírez (2024), en su tesis doctoral sobre divulgación de ciberseguridad en empresas latinoamericanas, advierte que la falta de especialistas impacta la gobernanza corporativa, lo cual limita la capacidad de los directorios para supervisar adecuadamente los riesgos digitales.

Finalmente, Schoenfield (2021) aporta una perspectiva que suele estar ausente en los debates sobre formación en ciberseguridad: el perfil del arquitecto de ciberseguridad como figura estratégica que integra conocimiento técnico profundo con capacidad de comunicación ejecutiva, pensamiento sistémico y comprensión del negocio o de la misión institucional. La escasez de perfiles con esta combinación de competencias es especialmente crítica en Colombia, donde las decisiones sobre inversión en ciberseguridad frecuentemente se toman sin la participación de profesionales capaces de traducir el riesgo técnico en lenguaje estratégico comprensible para los tomadores de decisión. La brecha de talento, en este nivel, no es solo operativa sino directiva, lo cual afecta la calidad de la gobernanza de la ciberseguridad en las organizaciones públicas y privadas del país.

Frente a este panorama es importante tener en cuenta que cerrar la brecha de talento en ciberseguridad exige un enfoque integral, el cual implica: invertir en formación universitaria y técnica especializada, fortalecer las certificaciones profesionales, fomentar la participación de mujeres y jóvenes, y articular alianzas entre el Estado, la academia y el sector privado. Solo así se garantizará que la digitalización de la región no se vea comprometida por la falta de capital humano capacitado.

Inteligencia artificial y ciberseguridad: capacidad de respuesta

La inteligencia artificial (IA) se ha consolidado como una de las tecnologías disruptivas con mayor impacto en la configuración de la ciberseguridad contemporánea. Su capacidad para analizar grandes volúmenes de datos, identificar patrones anómalos y automatizar procesos de detección y respuesta convierte a la IA en un habilitador estratégico para fortalecer la seguridad digital. Sin embargo, su integración en los ecosistemas de defensa digital también introduce nuevos vectores de riesgo, tales como ataques adversariales, la manipulación de datos de entrenamiento (*data poisoning*) y las técnicas de *prompt injection* dirigidas a grandes modelos de lenguaje (Cisco, 2025).

En el caso colombiano, la Estrategia Nacional de Seguridad Digital 2025-2027 reconoce explícitamente la necesidad de gestionar los riesgos derivados de la adopción de tecnologías emergentes, incluida la IA, como parte de un esfuerzo más amplio por robustecer la ciberresiliencia nacional (Presidencia de la República, 2025). De forma complementaria, el CONPES 4144 de 2025 plantea la urgencia de superar las bajas capacidades de investigación y desarrollo en IA reforzando la infraestructura de datos, la formación de talento y la cooperación internacional, con el fin de evitar que la dependencia tecnológica incremente la vulnerabilidad del país frente a actores hostiles.

Desde la perspectiva internacional, organismos como la OTAN han definido la IA como una tecnología estratégica para las operaciones de ciberdefensa, lo cual los ha llevado a adoptar principios de uso responsable centrados en la legalidad, la trazabilidad y la rendición de cuentas (NATO, 2021). Por su parte, la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO, 2021) estableció lineamientos éticos que llaman a garantizar la transparencia, el respeto de los Derechos Humanos y la supervisión humana en aplicaciones críticas de IA,

principios que resultan especialmente relevantes cuando se aplican en contextos de seguridad nacional.

La literatura académica refuerza estos planteamientos. Estudios recientes resaltan que la IA no solo incrementa la eficiencia de los centros de operaciones de seguridad (SOC), sino que también permite anticipar ataques mediante sistemas de aprendizaje automático capaces de correlacionar miles de eventos en tiempo real (Xi et al., 2020). No obstante, la investigación también advierte que los modelos de IA son vulnerables a técnicas sofisticadas de manipulación, razón por la cual se exige incorporar mecanismos de validación continua, *red teaming* algorítmico y marcos de gobernanza que garanticen la confiabilidad de sus resultados (Biggio & Roli, 2018).

Específicamente en Colombia, la incorporación de IA en la ciberseguridad abre un escenario dual. Por un lado, constituye una oportunidad para optimizar la capacidad de respuesta ante incidentes, lo cual permite reducir los tiempos medios de detección (MTTD) y de respuesta (MTTR). Por otro, introduce riesgos que pueden comprometer la confianza digital si no se gestionan adecuadamente. En consecuencia, el país requiere avanzar en tres líneas estratégicas: 1) consolidar un marco regulatorio y ético alineado con estándares internacionales; 2) fortalecer la investigación aplicada y la cooperación entre Estado, academia y sector privado, y 3) desarrollar talento humano capaz de diseñar, operar y auditar sistemas de IA en ciberseguridad.

La capacidad de respuesta de Colombia en este ámbito dependerá de la integración efectiva de estos elementos en una estrategia nacional coherente, que aproveche el potencial de la IA como motor de resiliencia sin ignorar los riesgos asociados a su implementación. De este modo, el país no solo podrá enfrentar con mayor eficacia los desafíos del ciberespacio, sino también posicionarse como un actor regional que lidera la transición hacia un ecosistema digital seguro, confiable y soberano.

En Colombia, la Estrategia Nacional Digital 2023-2026 establece la IA como motor de la transformación económica y social, pero reconoce la necesidad de integrar marcos éticos y de seguridad para evitar usos indebidos y garantizar la protección de derechos (Departamento Nacional de Planeación [DNP], 2023). Complementariamente, el reciente CONPES 4144 de 2025 señala que el país presenta bajas capacidades en investigación, desarrollo y adopción de IA, lo cual refuerza la urgencia de invertir en infraestructura, datos y talento digital (CCIT, 2025).

En el ámbito global, la OTAN (2021) lanzó su Artificial Intelligence Strategy, donde plantea la IA como una capacidad esencial para las operaciones de defensa y ciberseguridad, al tiempo que insta a desarrollar principios de uso responsable

basados en legalidad, trazabilidad y responsabilidad. Por su parte, mediante la *Recomendación sobre la ética de la IA,* la UNESCO (2021) establece lineamientos que promueven transparencia, responsabilidad y respeto de los Derechos Humanos en la aplicación de esta tecnología, los cuales resultan fundamentales cuando la IA se emplea en ciberdefensa y seguridad nacional.

En el plano académico, Akdağ (2025) resalta que la convergencia entre IA y ciberpoder redefine la geopolítica digital, lo cual permite a los Estados que dominen esta tecnología proyectar mayor influencia en el ciberespacio. A su vez, investigaciones recientes (Biggio & Roli, 2018; Xi et al., 2020) advierten sobre la necesidad de robustecer los sistemas de aprendizaje automático frente a ataques adversariales y proponen tanto marcos de evaluación estandarizados como pruebas de robustez certificables.

Coordinación interinstitucional: Agencia Nacional de Ciberseguridad

La creciente sofisticación de los ciberataques y la convergencia de amenazas, que afectan tanto al sector público como al privado, han puesto en evidencia la necesidad de contar con una institucionalidad robusta que garantice la coordinación interinstitucional en materia de ciberseguridad. En el caso colombiano, la ausencia de una entidad centralizada con competencias normativas, operativas y presupuestales específicas genera fragmentación en la respuesta frente a incidentes y limita la capacidad de anticipación y resiliencia del ecosistema digital. En este sentido, la *Guía estratégica para mejorar la postura de ciberseguridad de Colombia* (AWS, 2024) advierte que el país requiere la creación de una Agencia Nacional de Ciberseguridad que unifique esfuerzos y actúe como ente rector para alinear las políticas, coordinar los equipos de respuesta a incidentes (CERT/CSIRT) y liderar la protección de infraestructuras críticas.

La creación de una Agencia Nacional de Ciberseguridad en Colombia no es una decisión administrativa de reorganización institucional, sino una elección estratégica sobre el modelo de poder con que el Estado colombiano decide ejercer soberanía en el ciberespacio. En este contexto, su diseño, competencias y autonomía determinarán si el país puede pasar de una gobernanza digital fragmentada a una arquitectura institucional capaz de anticipar, coordinar y responder de forma coherente ante amenazas que no reconocen fronteras sectoriales ni jurisdiccionales.

Este planteamiento se articula con la Estrategia Nacional de Seguridad Digital 2025-2027, la cual establece como objetivo prioritario consolidar la gobernanza de la seguridad digital mediante la cooperación internacional, las alianzas público-privadas y la institucionalización de capacidades permanentes de coordinación (Presidencia de la República, 2025). En la práctica comparada, varios países han creado agencias nacionales como ejes centrales de su política digital. Estados Unidos, por ejemplo, cuenta con la Cybersecurity and Infrastructure Security Agency (CISA), creada en 2018 para liderar la protección de infraestructuras críticas (CISA, 2023). La Unión Europea, por su parte, ha fortalecido su institucionalidad a través de la European Union Agency for Cybersecurity (ENISA), que coordina estándares y cooperación entre Estados miembros (ENISA, 2023). Francia consolidó la Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), mientras que España cuenta con el Instituto Nacional de Ciberseguridad (INCIBE), ambos referentes en el ámbito europeo. Finalmente, en América Latina destaca Chile, que promulgó en 2022 la Ley N.º 21663 y estableció la Agencia Nacional de Ciberseguridad (ANCI), una entidad encargada de coordinar incidentes, emitir directrices y supervisar infraestructuras críticas (Gobierno de Chile, 2022).

Específicamente en Colombia, la creación de una agencia de esta naturaleza permitiría superar vacíos de coordinación, centralizar la gestión de riesgos, fortalecer la cooperación internacional y promover una cultura de ciberseguridad transversal, lo cual posicionaría al país como líder regional en gobernanza digital.

No obstante, la discusión sobre la conveniencia de crear una Agencia Nacional de Ciberseguridad en Colombia suele plantearse en términos organizacionales —qué entidades fusionar, qué competencias trasladar, qué presupuesto asignar—, cuando en realidad su dimensión más profunda es política y teórica. Al respecto, Cavelty y Wenger (2020) demuestran que la institucionalización de la ciberseguridad como política de Estado no es un proceso técnico neutro, sino una expresión de cómo cada sociedad define la relación entre seguridad, soberanía y libertad digital. En este sentido, los Estados que han logrado construir agencias nacionales efectivas no lo han hecho simplemente por decisión ejecutiva, sino porque previamente resolvieron un debate político fundamental: qué actores tienen legitimidad para definir qué constituye una amenaza digital, con qué instrumentos puede el Estado responder a ella y con qué mecanismos de rendición de cuentas opera esa respuesta. Colombia está en el umbral de ese debate, y el diseño institucional que elija condicionará su postura de ciberseguridad por una generación.

Precisamente, la experiencia comparada ofrece lecciones indispensables para este diseño. Al analizar la evolución de ENISA y la arquitectura de ciberseguridad

de la Unión Europea, Christou (2016) identifica una tensión estructural que resulta directamente pertinente para el caso colombiano: la tensión entre centralización y subsidiariedad. Una agencia demasiado centralizada puede generar cuellos de botella operativos, acumular poder sin capacidad real de ejecución sectorial y producir resistencias institucionales que sabotean su efectividad desde adentro. Una agencia demasiado descentralizada, por su parte, reproduce la fragmentación que pretende resolver. El modelo europeo resolvió esta tensión al asignar a ENISA un rol de coordinación normativa, producción de estándares y gestión del conocimiento, mientras que la respuesta operativa ante incidentes permaneció en los equipos nacionales CSIRT. Para Colombia, donde ColCERT opera con recursos limitados y sin autoridad normativa vinculante sobre los sectores, este modelo ofrece una hoja de ruta: una agencia nacional que ejerza rectoría estratégica sin absorber capacidades operativas que deben mantenerse descentralizadas y próximas a los sectores.

La legitimidad histórica e institucional de este tipo de arquitecturas encuentra en Healey (2013) una perspectiva que enriquece el debate colombiano. Su análisis sobre la evolución de la ciberseguridad como política pública en Estados Unidos documenta que las agencias más efectivas no emergieron de decretos aislados, sino de procesos sostenidos de construcción de confianza. Estos procesos involucraron a actores gubernamentales, militares, privados y académicos, quienes reconocieron que su propia seguridad dependía de la seguridad colectiva del ecosistema. Este hallazgo tiene una implicación directa para Colombia: la Agencia Nacional de Ciberseguridad no puede diseñarse como una entidad que impone desde arriba una arquitectura de gobernanza, sino como una plataforma que articula desde adentro los intereses, las capacidades y los incentivos de actores heterogéneos. Su credibilidad ante el sector privado —que gestiona gran parte de las infraestructuras críticas del país— dependerá no de su autoridad legal, sino de su capacidad para generar valor compartido. Este valor incluye inteligencia de amenazas accionable, estándares operativos pertinentes y mecanismos de respuesta coordinada que beneficien a todos los participantes del ecosistema.

Por otra parte, no se puede soslayar la dimensión internacional de este diseño institucional. Al respecto, Nye (2014), al analizar los regímenes internacionales de gobernanza cibernética, advierte que los Estados que carecen de una institución nacional con mandato claro y reconocimiento internacional quedan marginados de los espacios donde se definen las normas, los estándares y los protocolos que ordenan el ciberespacio global. Aunque Colombia participa actualmente en organismos como la OEA, la ONU y el Foro de Gobernanza de Internet, en este

momento carece de una contraparte institucional equivalente a CISA, ENISA o ANSSI que pueda negociar acuerdos de cooperación operativa, firmar memorandos de intercambio de inteligencia de amenazas o representar al país en ejercicios multinacionales de cibercrisis con autoridad y continuidad institucional. La ausencia de esta entidad no es solo un vacío doméstico: es una limitación de la proyección internacional de Colombia como actor relevante en la gobernanza digital, precisamente en el momento en que esa gobernanza se está definiendo con consecuencias de largo plazo.

Finalmente, Dunn Cavelty (2008) aporta una advertencia que debe incorporarse al debate colombiano con seriedad crítica: el proceso de securitización del ciberespacio. Es decir, la construcción discursiva de los riesgos digitales como amenazas existenciales que justifican medidas extraordinarias puede derivar en arquitecturas institucionales que concentran poder de vigilancia y control sin los contrapesos democráticos necesarios. Una Agencia Nacional de Ciberseguridad mal diseñada puede convertirse en un instrumento de vigilancia masiva, de restricción de libertades digitales o de captura por intereses sectoriales específicos. Para Colombia, cuya historia institucional está marcada por tensiones entre seguridad y derechos civiles, este riesgo no es teórico, sino históricamente fundado. Por ello, el diseño de la agencia debe incorporar desde su origen mecanismos robustos de supervisión parlamentaria, auditoría independiente, transparencia en el uso de sus facultades y participación de la sociedad civil, no como concesión retórica, sino como condición estructural de su legitimidad democrática.

La construcción de un futuro digital seguro

En suma, la convergencia entre gobernanza digital, transformación tecnológica, resiliencia de infraestructuras críticas, desarrollo de talento, coordinación interinstitucional mediante una Agencia Nacional de Ciberseguridad y uso estratégico de la inteligencia artificial para la respuesta a incidentes constituye la base de un ecosistema seguro, confiable y sostenible para Colombia. Los avances normativos y estratégicos alcanzados en los últimos años, sumados a la creciente articulación con organismos internacionales como la OEA, la ONU y la OTAN, demuestran que el país no parte de cero. Por el contrario, cuenta con cimientos sólidos para proyectarse como referente regional en ciberseguridad y ciberdefensa. El reto, sin embargo, no es menor: implica cerrar brechas, fortalecer capacidades y anticipar amenazas en un entorno en el que la innovación tecnológica avanza a gran

velocidad. Con visión estratégica, inversión en talento humano y una gobernanza digital colaborativa, Colombia puede no solo enfrentar los riesgos emergentes, sino transformarlos en oportunidades para consolidar su soberanía digital, potenciar su desarrollo económico y garantizar la seguridad nacional en la era digital.

Conclusiones

En conclusión, los diversos ejes abordados —gobernanza digital y ciberseguridad, transformación digital, resiliencia en infraestructuras críticas, capital humano y talento especializado, inteligencia artificial aplicada a la ciberdefensa y la coordinación interinstitucional— configuran un marco integral que responde a los desafíos y las oportunidades del ecosistema digital colombiano. La evidencia demuestra que el país ha avanzado en el diseño de políticas, estrategias y capacidades, aunque persisten brechas significativas que deben atenderse con decisión y visión de largo plazo. El fortalecimiento de la cooperación internacional, la adopción de estándares globales y la consolidación de una cultura de seguridad digital constituyen pilares esenciales para alcanzar una postura robusta frente a las amenazas emergentes. Con una inversión sostenida en innovación, la creación de una Agencia Nacional de Ciberseguridad y el despliegue de inteligencia artificial en la gestión de incidentes, Colombia puede proyectarse no solo como un referente regional en ciberseguridad y ciberdefensa, sino también como un actor capaz de convertir los riesgos del entorno digital en oportunidades estratégicas para su desarrollo y su seguridad nacional.

Referencias

Akdağ, Y. (2025). *Great power cyberpolitics and global cyberhegemony.* Cambridge University Press. https://doi.org/10.1017/S1537592725000040

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Raymond Choo, K. K. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *116*, 102662. https://tinyurl.com/bddv8xtz

Amazon Web Services [AWS]. (2024). *Guía estratégica para mejorar la postura de ciberseguridad: Colombia.* Presidencia de la República de Colombia.

Banco de la República. (2025, 27 de agosto). Sombreado 1: Riesgo cibernético en las infraestructuras financieras: entorno actual, riesgos y avances recientes - Reporte de la Infraestructura Financiera e Instrumentos de Pago 2025. En *Reporte de la infraestructura financiera e instrumentos de pago 2025* [Reporte]. https://tinyurl.com/ms6rahep

Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition, 84,* 317–331. https://doi.org/10.1016/j.patcog.2018.07.023

Bloom, B. S. (1956). *Taxonomy of educational objectives.* Longmans Green.

Bodeau, D., & Graubart, R. (2017). *Cyber resiliency engineering aid: The updated cyber resiliency engineering framework.* MITRE Corporation. https://tinyurl.com/59kath83

Cámara Colombiana de Informática y Telecomunicaciones [CCIT]. (2025). *Estado de la ciberseguridad y la inteligencia artificial en Colombia.* Tanque de Análisis y Creatividad de las TIC (TicTac). https://tinyurl.com/bdfjf58v

Cano, J. J. (2022). *Ciberseguridad empresarial: Reflexiones y retos para los ejecutivos del siglo XXI.* Ediciones de la U.

Castells, M. (2009). *Communication power.* Oxford University Press.

Cavelty, M. D., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy, 41*(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

Christou, G. (2016). *Cybersecurity in the European Union.* Palgrave Macmillan.

Cisco. (2025). *State of AI security report.* Cisco Systems.

DeNardis, L. (2014). *The global war for internet governance.* Yale University Press.

Departamento Nacional de Planeación [DNP]. (2023). *Estrategia nacional digital de Colombia 2023–2026.* Presidencia de la República. https://tinyurl.com/ysauteth

Dunn Cavelty, M. (2008). *Cyber-security and threat politics.* Routledge.

Estay Sepúlveda, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. *Computers & Security, 97,* 101996. https://doi.org/10.1016/j.cose.2020.101996

European Union Agency for Cybersecurity [ENISA]. (2023). *European cybersecurity skills framework.* European Union Agency for Cybersecurity. https://tinyurl.com/fh649cjv

Financial Sector LATAM Report. (2025). *Panorama de amenazas para el sector financiero de LATAM en 2025*. Digi Americas Alliance & Duke University. https://tinyurl.com/yjpeu3hc

Foro Económico Mundial. (2025). *The cyber resilience compass: Journeys towards resilience.* World Economic Forum. https://tinyurl.com/3p6s6rkb

Global Cyber Security Capacity Centre. (2021). *Cybersecurity capacity maturity model for nations (CMM): 2021 edition.* University of Oxford. https://tinyurl.com/2fu4bze7

Healey, J. (Ed.). (2013). *A fierce domain: Conflict in cyberspace, 1986–2012.* Cyber Conflict Studies Association.

IDB/OEA. (2020). *Cybersecurity: Risks, progress and the way forward in LAC.*

Interpol. (2024a). *Informe de evaluación de las ciberamenazas en África.* Interpol. https://tinyurl.com/bdf4u6p7

Interpol. (2024b, 26 de noviembre). *Una operación importante contra la ciberdelincuencia permite detener a 1.006 sospechosos*. https://tinyurl.com/32y9jmnu

ISC². (2024). *Cybersecurity workforce study.* ISC² Inc. https://tinyurl.com/yytyepab

Kettl, D. F. (2015). *The transformation of governance.* Johns Hopkins University Press.

Knowles, M. S., Holton, E. F., & Swanson, R. A. (2015). *The adult learner* (8th ed.). Routledge.

Linkov, I., & Palma-Oliveira, J. M. (2017). *Resilience and risk: Methods and application in environment, cyber and social domains.* Springer. https://tinyurl.com/34u7z2eu

Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M., Allen, J. H., Flynn, S. E., & Seager, T. P. (2013). Measurable resilience for actionable policy. *Environmental Science & Technology, 47*(18), 10108–10110. https://pubs.acs.org/doi/10.1021/es403443n

Luiijf, H. A. M., Nieuwenhuijs, A., Klaver, M. H. A., van Eeten, M., & Cruz, E. (2013). *Empirical findings on critical infrastructure dependencies in Europe and the United States*. Springer.

Ministerio de Defensa Nacional. (2025). *Fuerza innovación.* https://www.mindefensa.gov.co/gsed/fuerza-innovaci%C3%B3n

Ministerio de Relaciones Exteriores. (2025). Posición nacional de Colombia sobre la aplicación del derecho internacional al ciberespacio. https://tinyurl.com/bdz7vu2e

Ministerio de Tecnologías de la Información y las Comunicaciones [MinTic]. (2025). E*strategia nacional de seguridad digital 2025–2027.* MinTic. https://tinyurl.com/mr22bduk

Ministerio de Tecnologías de la Información y las Comunicaciones [MinTic]. (s. f.). Ciberseguridad. https://tinyurl.com/24zdhvxt

Ministerio de Tecnologías de la Información y las Comunicaciones. (2025). Resolución 02277 de 2025. Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia. *D.O.* 3155, 20 de junio de 2025. https://tinyurl.com/ynxbzdxz

Ministerio de Tecnologías de la Información y las Comunicaciones. (s. f.). Política de Seguridad Digital. https://tinyurl.com/yfd4spp9

Naserinia, V., et al. (2021). Cyber resilience for critical infrastructure: A systematic review (Working paper).

North Atlantic Treaty Organization [NATO]. (2021). *NATO's artificial intelligence strategy.* NATO.

North Atlantic Treaty Organization [NATO]. (2024). *Summary of NATO's revised AI strategy.* https://tinyurl.com/2yajus3z

Nye, J. S. (2014). *The regime complex for managing global cyber activities.* Global Commission on Internet Governance. https://tinyurl.com/2tuhyr4b

OAS/CICTE. (2021). *National cybersecurity strategies: Lessons learned and reflections.* OAS. https://tinyurl.com/ypaz2mxr

Organisation for Economic Co-operation and Development [OECD] (2021). *Guide to developing a national cybersecurity strategy.* https://tinyurl.com/wxsca738

Organización de los Estados Americanos [OEA]. (s. f.). Secretaría ejecutiva de CICTE. https://tinyurl.com/3a6jzs64

Ramírez, M. (2024). *La divulgación de información sobre ciberseguridad en empresas cotizadas de América Latina* [Tesis doctoral, Universidad de Granada]. Repositorio Institucional. https://hdl.handle.net/10481/102484

Sarmiento, D. A. (2023). *Ciberataques contra infraestructuras críticas: Desafíos, amenazas y estrategias de protección en la era digital* [Tesis de grado, Universidad Siglo 21]. Repositorio Institucional. https://tinyurl.com/yzeufx6y

Schoenfield, B. (2021). *Secrets of a cyber security architect.* CRC Press.

Stojanović, B., Hofer-Schmitz, K., & Kleb, U. (2020). APT datasets and attack modeling for automated detection methods. *Computers & Security, 92,* 101734. https://doi.org/10.1016/j.cose.2020.101734

United Nations Educational, Scientific and Cultural Organization [UNESCO]. (2021). *Recommendation on the ethics of artificial intelligence.* https://tinyurl.com/4ujdxmvv

Wavestone. (2025). Cyber benchmark 2025 edition. https://tinyurl.com/3ars9zk4

World Economic Forum. (2025). *The cyber resilience compass: Journeys towards resilience.* WFM. https://tinyurl.com/uw8j6ch8

Wu, J., Li, X., & Zhang, Y. (2023). *Training of outstanding talents in cyberspace security.* Springer. https://tinyurl.com/2s49s76v

Xi, B., et al. (2020). Adversarial machine learning for cybersecurity and computer vision. *WIREs Computational Statistics, 12*(5), e1511. https://doi.org/10.48550/arXiv.2107.02894

Yin, R. K. (2018). *Case study research and Applications: Design and methods* (6th ed.). Sage Publishing.

Capítulo 2

Gobernanza digital para el sector defensa y seguridad: una necesidad latente*

DOI: https://doi.org/10.25062/9786287818644.02

Ana Catalina Cano Londoño
Ministerio de Defensa Nacional

Resumen: El artículo propone un modelo de gobernanza digital para el sector defensa y seguridad, cuyo objetivo es fortalecer el cumplimiento normativo, la seguridad digital y la cooperación internacional. La acelerada digitalización, impulsada por la cuarta revolución industrial, ha transformado las relaciones humanas con la tecnología. Esta convergencia ha mejorado procesos, pero también ha generado riesgos, amenazas e incidentes digitales. El artículo analiza los elementos necesarios para una gobernanza en seguridad digital y examina es-tándares internacionales, marcos regulatorios y experiencias comparadas, con el fin de proponer un modelo adaptable al sector. Desde una perspectiva sistémica, se requiere un modelo de gobernanza digital que se alinee con la Política de Ciberdefensa Nacional y la Estrategia Nacional en Seguridad Digital en Colombia 2025-2027. Este modelo debe articular los esfuerzos institucionales, gestionar riesgos, asegurar el cumplimiento regulatorio, fomentar capacidades tecnológicas en defensa y fortalecer el talento humano en esta área. Finalmente, el artículo integra elementos de política pública, estándares técnicos y cooperación internacional en un enfoque estratégico específico para el sector defensa y seguridad.

Palabras clave: amenazas; ciberseguridad; gobernanza digital; información; legislación; tecnología.

* Capítulo de libro resultado del proyecto de investigación "La gobernanza del ciberespacio a nivel global, regional y nacional: desafíos, oportunidades y estrategias para la soberanía digital", del grupo de investigación "Ciberespacio, Tecnología e Innovación", de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado en C por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) y regis-trado con el código COL0181179. Los puntos de vista y los resultados de este capítulo pertenecen a la autora y no reflejan necesariamente los de las instituciones participantes.

Ana Catalina Cano Londoño
Magíster en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Magíster en Derecho Internacional de la Empresa, Universitat de Barcelona, España. Especialista en Derecho Comercial, Universidad del Rosario, Colombia. Abogada. Exviceministra del Grupo Social y Empresarial de la Defensa (periodo 2023-2026), Ministerio de Defensa Nacional de Colombia. **https://orcid.org/0000-0003-2004-7466**
Contacto: **ana.cano@esdeg.edu.co**

Citación APA: Cano-Londoño, A. C. (2026). Gobernanza digital para el sector defensa y seguridad: Una necesidad latente. En M. E. Realpe-Díaz & A. M. González-González (Eds.), *Transformación digital y ciberseguridad en Colombia: Desafíos estratégicos para sectores de infraestructura crítica* (pp. 37-68). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818644.02

TRANSFORMACIÓN DIGITAL Y CIBERSEGURIDAD EN COLOMBIA: DESAFÍOS ESTRATÉGICOS PARA SECTORES DE INFRAESTRUCTURA CRÍTICA
ISBN impreso: 978-628-7818-63-7
ISBN digital: 978-628-7818-64-4
DOI: https://doi.org/10.25062/9786287818644

Colección Ciberseguridad y Ciberdefensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2026

CC BY NC ND

Introducción

La creciente y acelerada adopción de la tecnología en las actividades tanto públicas como privadas, personales como colectivas, ha cambiado no solo la forma en que se relacionan los humanos entre sí, sino también cómo se relacionan con las cosas. El fenómeno de la convergencia, asociada a la Cuarta Revolución —definida como la digitalización de la industria y de los servicios—, se traslada a todos los ámbitos, lo cual no solo mejora algunos aspectos en la vida de las personas, la productividad de las empresas y la gestión de las entidades públicas, sino que también trae consigo un conjunto de incertidumbres, riesgos, amenazas, vulnerabilidades e incidentes de diversos tipos.

En Colombia, la respuesta frente a esta convergencia ha sido progresiva y "por capas": desde el marco de política de las tecnologías de la información y las comunicaciones (TIC) que orientó la masificación del gobierno en línea y el aprovechamiento de las TIC en la gestión pública (Ley 1341 de 2009) hasta la consolidación de garantías asociadas al tratamiento de datos personales (Ley 1581 de 2012).

En 2011, el CONPES 3701 inauguró la arquitectura institucional en ciberseguridad y ciberdefensa, al tiempo que promovió capacidades especializadas para prevenir, coordinar y atender incidentes. Posteriormente, el CONPES 3854 (2016) estableció una política de seguridad digital basada en gestión de riesgos y en un marco institucional de coordinación, cuya conducción al más alto nivel se reforzó con la adenda de 2017. En 2020, el CONPES 3995 actualizó la agenda hacia confianza y seguridad digital, con un énfasis particular en capacidades, articulación y gobernanza. Este enfoque se complementó con los servicios ciudadanos digitales (Decreto 620 de 2020) y, finalmente, con el Decreto 338 de 2022, el cual formaliza lineamientos, modelo e instancias para fortalecer la gobernanza, la gestión del riesgo y la respuesta a incidentes, incluyendo infraestructuras críticas cibernéticas y servicios esenciales.

No obstante, catorce años después del punto de partida, persiste una brecha entre el marco normativo y la resiliencia efectiva, tal como lo evidencia la Estrategia Nacional de Seguridad Digital 2025-2027 (Gobierno de Colombia, 2025) al señalar: "Estos incidentes evidencian la brecha entre la formulación de políticas y su ejecución práctica" (p. 8). En este contexto, resulta necesario formular un modelo de gobernanza digital específico para el sector defensa y seguridad que integre a las Fuerzas Militares, la Policía Nacional y las entidades del Grupo Social y Empresarial de la Defensa (GSED), cierre la distancia entre política y operación, y asegure la coordinación, el cumplimiento y las capacidades sostenibles.

Marcos legales y normativos vigentes en Colombia

Legislación colombiana en gobernanza digital y ciberseguridad

La gobernanza digital en Colombia ha evolucionado como parte de un esfuerzo por modernizar el Estado y garantizar la seguridad en el entorno digital. Antes de abordar cómo ha sido el desarrollo normativo en materia de seguridad digital en Colombia, es fundamental recordar que el país, en su condición de Estado Social y Democrático de Derecho, ha establecido el derecho al *hábeas data* en el artículo 15 de su Constitución Política. Este derecho fundamental garantiza a las personas el acceso a la información que se guarda sobre ellas en bancos de datos y archivos, así como la posibilidad de conocer, actualizar y rectificar dicha información (Consejo de Estado, 2020). En este orden de ideas, se podría decir que este derecho constitucional fundamenta el andamiaje jurídico que regula la protección de datos y el acceso y el uso de las tecnologías de la información en Colombia.

La Ley 1581 de 2012, conocida como Ley de Protección de Datos, tiene por objeto desarrollar el derecho constitucional del referido artículo 15 de la Constitución Política y el derecho a la información consagrado en su artículo 20. Si bien esta ley no regula de manera directa aspectos en ciberseguridad, sí fija los principios y las obligaciones que tienen incidencia en la ciberseguridad, tales como el principio de seguridad de la información y la responsabilidad de las organizaciones en el desarrollo de políticas de seguridad digital.

Por su parte, la Ley 1341 de 2009 define el uso y aprovechamiento de las TIC en Colombia. Específicamente, esta normativa establece los principios orientadores, el papel del Estado, la organización institucional del sector y los derechos y

deberes de los usuarios y proveedores de servicios, al tiempo que crea la Agencia Nacional del Espectro.

Asimismo, dentro del marco jurídico colombiano, se encuentran algunos decretos con fuerza de ley que lo configuran: el Decreto 338 de 2022 es relevante para este artículo, puesto que establece un modelo de gobernanza de seguridad digital en Colombia y crea instancias para su gestión, con el objetivo de fortalecer la confianza en el uso de las Tecnologías de la Información, las Comunicaciones y la Digitalización (TICD). Asimismo, este marco normativo regula la identificación y protección de infraestructuras críticas cibernéticas, junto con la respuesta a incidentes de seguridad digital, aspectos fundamentales para la protección en materia de ciberseguridad.

En la misma perspectiva, el Decreto 767 de 2022 constituye un paso importante en la consolidación del gobierno digital en Colombia porque da un enfoque integral de transformación digital del Estado. Este instrumento establece los lineamientos generales de la política pública en la materia, los cuales orientan a las entidades de la administración pública hacia la creación de valor público mediante servicios digitales confiables, interoperables y centrados en el ciudadano. Asimismo, el Decreto 620 de 2020 regula los servicios ciudadanos digitales, lo cual promueve la interoperabilidad y la digitalización de trámites, una medida que se ha complementado con el CONPES 3995 de 2020. A su vez, el Decreto 1874 de 2021 define una nueva estructura organizacional del Ministerio de Defensa, que incorpora una nueva dependencia estratégica: el CISIRT Defensa, un componente esencial para robustecer la postura de ciberseguridad y ciberdefensa de las unidades cibernéticas de la Fuerza Pública.

Ahora bien, los siguientes documentos del Consejo Nacional de Política Económica y Social (CONPES) se enmarcan en la política pública, donde cumplen una función orientadora y de guía para la acción y la planeación estratégica del Estado: el CONPES 3701 de 2011 establece los lineamientos de política para la ciberseguridad y la ciberdefensa, los cuales buscan desarrollar estrategias nacionales para enfrentar amenazas informáticas y proteger infraestructuras críticas. Además, el CONPES 3854 de 2016 establece la Política Nacional de Seguridad Digital, con un enfoque fundamentado en la gestión del riesgo y la promoción de la cooperación nacional e internacional. Finalmente, el CONPES 3995 de 2020 establece la Política Nacional de Confianza y Seguridad Digital, la cual tiene como objetivo actualizar el marco de gobernanza y fortalecer las capacidades en ciberseguridad.

En este escenario, es relevante señalar que el sector defensa en Colombia ha incorporado estrategias para la digitalización y la ciberseguridad con el propósito de proteger infraestructura crítica y fortalecer la ciberdefensa. En particular, la

Resolución 0463 de 2022 fija requisitos obligatorios de seguridad para soluciones en la nube, incluyendo confidencialidad, integridad y disponibilidad; clasificación de la información conforme a la Ley 1712 de 2014 y la exclusión de datos sensibles y operacionales de las Fuerzas Militares en nubes públicas, salvo excepciones altamente controladas.

Asimismo, esta resolución adopta un enfoque de gestión del riesgo que exige la evaluación de riesgos, las pruebas de penetración, el *ethical hacking,* la correlación de eventos y el control de accesos. Además, incorpora criterios de gobernanza y auditoría, para lo cual requiere la auditoría, la trazabilidad, la entrega de *logs,* el monitoreo y el reporte de incidentes por parte de los proveedores. En conjunto, este marco funciona como un instrumento clave de seguridad digital destinado a proteger la soberanía de los datos, prevenir ciberamenazas y asegurar la continuidad operativa de las misiones institucionales.

Como documentos orientadores en materia de política pública, se destacan la Estrategia Nacional Digital 2023-2026 y la Estrategia Nacional en Seguridad Digital de Colombia 2025-2027. Ambas buscan superar los desafíos digitales en Colombia, preparar un país más resiliente y mejorar la gestión de los riesgos cibernéticos. Específicamente, el objetivo de la Estrategia Nacional Digital 2023-2026 es potenciar la transformación digital para enfrentar desafíos económicos, sociales y ambientales, a la vez que fortalece sus habilitadores, promueve el uso y la apropiación de datos y tecnologías por personas, hogares, entidades públicas y sector productivo, y atiende los riesgos y daños potenciales de la aceleración digital (END 2023-2026). En ese marco, para este artículo se destaca el Eje 3 —orientado a la seguridad y confianza digital—, que plantea lineamientos de regulación y gobernanza para fortalecer la planificación y la coordinación nacional, aumentar la preparación y resiliencia, proteger a las personas, infraestructuras y entidades del Estado para asegurar la prestación de servicios, y desarrollar legislación que propicie un ecosistema digital seguro y confiable (CCIT, 2025).

Por su parte, la Estrategia Nacional de Seguridad Digital 2025-2027 se organiza en cuatro enfoques rectores —toda la sociedad, centrado en el ser humano, gestión de riesgos cibernéticos e innovación y desarrollo de capacidades— y define cuatro objetivos específicos: 1) consolidar la gobernanza, 2) mejorar la ciberresiliencia nacional, 3) desarrollar la fuerza laboral en seguridad digital y 4) actualizar el marco normativo cibernético. Cada uno de estos objetivos cuenta con líneas de acción concretas. A continuación, la tabla 1 resumen los marcos normativos en gobernanza digital y ciberseguridad vigentes en Colombia.

Tabla 1. *Resumen de los marcos normativos en gobernanza digital y ciberseguridad vigentes en Colombia*

Norma	Fecha de expedición	Principales disposiciones	Relación con la gobernanza y la seguridad digital
Ley 1581 de 2012	17-10-2012	Regula la protección de datos en Colombia.	Garantiza la privacidad y seguridad de los datos personales, esenciales para la seguridad digital.
Ley 1341 de 2009	30-06-2009	Define principios y conceptos sobre la sociedad de la información y la organización de las TIC en el país.	Promueve la manifestación del gobierno digital y establece principios para la protección de datos y seguridad en TIC.
Decreto 767 de 2022	16-05-2022	Define el gobierno digital en Colombia con un enfoque integral de transformación digital del Estado.	Mantiene una relación directa y complementaria con la seguridad y la gobernanza digital en Colombia.
Decreto 338 de 2022	08-03-2022	Crea el modelo de gobernanza en seguridad digital y establece lineamientos generales para su fortalecimiento.	Definió roles y responsabilidades entre las entidades del Estado. Establece principios y lineamientos aplicables a todas las autoridades y privadas con funciones administrativas, crea el CSIRT Gobierno, y fomenta la coordinación nacional e internacional en materia de ciberseguridad.
Decreto 620 de 2020	02-05-2020	Reglamenta la operación de los servicios ciudadanos digitales y la interoperabilidad de datos.	Mejora la seguridad digital mediante la regulación del acceso a servicios digitales y la interoperabilidad de datos.
Decreto 1874 de 2021	30-12-2021	Se modifica la estructura del Ministerio de Defensa Nacional.	Se crea el CSIRT Defensa.
CONPES 3701 de 2011	14-06-2011	Establece lineamientos de política para la ciberseguridad y la ciberdefensa en Colombia.	Fortalece la capacidad del Estado para enfrentar amenazas cibernéticas y proteger infraestructuras críticas.
CONPES 3854 de 2016	11-04- 2016	Establece la Política Nacional de Seguridad Digital en Colombia, promoviendo la gestión de riesgos y la confianza en el entorno digital.	Promueve un marco institucional para la seguridad digital, basado en la gestión de riesgos.
CONPES 3995 de 2020	01-07- 2020	Define la Política Nacional de Confianza y Seguridad Digital, enfocándose en la actualización del marco de gobernanza y la adopción de nuevos modelos.	Refuerza la confianza y la seguridad digitales mediante la actualización del marco regulatorio.

Fuente: Elaboración propia.

Regulación sobre tecnologías emergentes: uso de inteligencia artificial, *big data, blockchain* y computación cuántica en seguridad y defensa

El rápido avance y la adopción de las tecnologías digitales ha traído grandes beneficios para la sociedad, razón por la cual estas se han convertido en una parte esencial de las dinámicas y el quehacer de personas, empresas y gobiernos.

En este contexto, tecnologías emergentes como el *blockchain* y la inteligencia artificial (IA) se convierten en herramientas clave para reforzar la defensa contra ciberataques y garantizar la integridad de los datos en el país. No obstante, estas mismas tecnologías, paradójicamente, también representan vulnerabilidades para la defensa cibernética. Por esta razón, es necesario conocer de manera básica cómo está Colombia en la regulación de tecnologías emergentes, lo cual se aborda a continuación.

Política Nacional para la Transformación Digital e Inteligencia Artificial (CONPES 3975 de 2019): este documento establece las bases para la transformación digital del país y promueve el uso estratégico de tecnologías digitales en el sector público y privado. Aunque no se centra exclusivamente en seguridad y defensa, sienta las bases para la adopción de tecnologías como IA y *blockchain* en diversos sectores. También se debe señalar que el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) ha emitido la *Guía de referencia* de *blockchain del MinTIC*, la cual detalla el procedimiento para implementar esta tecnología en el ámbito estatal.

Por su parte, el CONPES 4144 de 2025, que establece la Nueva Política Pública en IA, adopta la Política Nacional de Inteligencia Artificial. Específicamente, este documento impulsa el desarrollo de capacidades en investigación, innovación y uso responsable de la IA, para lo cual incorpora principios éticos, de transparencia y seguridad. En el ámbito de la defensa y la seguridad, la política concibe la IA como un habilitador estratégico para mejorar la ciberdefensa, la gestión de inteligencia táctica, la protección de infraestructuras críticas y la toma de decisiones operacionales basadas en datos.

Es así como la IA y la blockchain en ciberseguridad son estratégicamente cruciales para el sector defensa, dado que permiten fortalecer la protección de infraestructuras críticas, redes militares y sistemas de información sensibles, elementos esenciales para la soberanía, la defensa nacional y la seguridad del Estado. En este contexto, Colombia debe avanzar de manera más acelerada en la actualización e introducción de elementos normativos que permitan hacer frente a las tecnologías disruptivas. Por ello, una de las acciones de la Estrategia Nacional de Seguridad Digital 2025-2027 consiste en crear una hoja de ruta interinstitucional para integrar esfuerzos normativos en seguridad digital.

Análisis del marco referencial internacional

En este apartado se sintetizan los marcos de referencia internacional que proporcionan las pautas para gestionar la seguridad de la información y la ciberseguridad de manera integral con el fin de garantizar la confidencialidad, la integridad y la disponibilidad de los activos críticos.

La norma RFC 2350, Expectativas para Equipos de Respuesta a Incidentes (CSIRTs), define el perfil de un CSIRT, sus responsabilidades y servicios mínimos, tales como el manejo de incidentes, la coordinación y la diseminación de alertas. Con base en lo expuesto previamente, es fundamental para la gobernanza de la seguridad digital disponer de estructuras organizativas y de coordinación interinstitucional, entre las cuales destaca el CSIRT. Por consiguiente, su utilidad para la gobernanza radica en que se constituye como la estructura funcional esperada de un equipo nacional o sectorial de respuesta, lo cual facilita la interoperabilidad y la cooperación internacional.

La norma ISO/IEC 27001 – Gestión de Seguridad de la Información se centra en la administración integral de la información en las organizaciones y, con este fin, proporciona un marco estructurado para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), lo cual garantiza la confidencialidad, la integridad y la disponibilidad de los activos informáticos.

La ISO 31050 – Gestión del Riesgo y Resiliencia Futura es una norma enfocada en la resiliencia organizacional y la gestión de riesgos emergentes, que amplía la visión de gestión de riesgo anticipatoria frente a escenarios complejos como los de ciberdefensa, IA y amenazas híbridas. Como señala el profesor Jeimy Cano (2008) en su interesante artículo "Repensando los fundamentos de la gestión de riesgos: una propuesta conceptual desde la incertidumbre y la complejidad", los modelos tradicionales basados en probabilidad-impacto o frecuencia-severidad resultan insuficientes para abordar riesgos en contextos volátiles, inciertos, complejos y ambiguos (VICA). Por esta razón, esta norma se plantea frente a modelos basados en incertidumbre y complejidad que promuevan el aprendizaje continuo y la simulación de escenarios.

La guía ISO/IEC 27032 – Ciberseguridad establece directrices para mejorar el estado de la ciberseguridad, enfocándose particularmente en la protección de usuarios en el ciberespacio. Asimismo, suministra herramientas para la gestión de amenazas como *phishing, malware* y *hacktivismo,* y para la protección de infraestructuras críticas y la seguridad de la información. Adicionalmente, esta norma contribuye significativamente al reforzar la gobernanza desde una perspectiva

colaborativa e intersectorial, lo cual se logra mediante la integración de roles del Estado, el sector privado y la sociedad civil.

La Directiva NIS2 de la Unión Europea (UE) establece un marco jurídico unificado para garantizar la ciberseguridad en 18 sectores críticos, al tiempo que insta a los Estados miembros a definir estrategias nacionales de ciberseguridad y a colaborar con la UE para la respuesta y la aplicación transfronterizas. En particular, esta directiva también exige a los Estados miembros que mejoren sus capacidades de ciberseguridad y que introduzcan medidas de gestión de riesgos y requisitos de información para entidades de más sectores, así como establecer normas para la cooperación, el intercambio de información, la supervisión y la aplicación de las medidas de ciberseguridad.

El objetivo de esta norma es entonces mejorar la resiliencia y la respuesta ante incidentes en sectores críticos en toda la UE. Como aspectos clave, amplía su alcance a más sectores —energía, salud, transporte, digital y administración pública—, y establece obligaciones más estrictas en gestión de riesgos, respuesta a incidentes, continuidad del negocio y reporte. Adicionalmente, refuerza la cooperación entre los Estados miembros a través del EU-CyCLONe y la CSIRTs Network (Directive (EU) 2022/2555). Específicamente, la Directiva NIS2 de la UE es importante para los objetivos de este artículo por cuanto establece modelos de responsabilidad compartida, supervisión regulatoria y enfoque basado en riesgos, lo cual la convierte en un referente valioso.

A continuación, la tabla 2 sintetiza los aportes de los referentes normativos internacionales en materia de gobernanza digital y ciberseguridad.

Tabla 2. *Marco normativo internacional sobre gobernanza digital y ciberseguridad*

Norma/ directiva	Tipo	Alcance/aplicabilidad	Utilidad para el modelo de gobernanza en seguridad digital
RFC 2350	Estándar técnico (Request for Comments – IETF)	Define los requisitos operativos y servicios mínimos de un CSIRT.	Establece la estructura organizativa y funcional esperada para los CSIRT, elemento esencial en la gobernanza interinstitucional y la cooperación internacional en ciberseguridad.
ISO/IEC 27001	Norma internacional (ISO / IEC)	Proporciona un marco certificable y estructurado para establecer, implementar, mantener y mejorar un SGSI.	Es la base normativa de la gobernanza digital, garantiza la confidencialidad, la integridad y la disponibilidad de la información y define los controles, roles y responsabilidades en la gestión de seguridad.

Norma/ directiva	Tipo	Alcance/aplicabilidad	Utilidad para el modelo de gobernanza en seguridad digital
ISO 31050	Norma internacional (ISO)	Amplía los principios de la ISO 31000 hacia la gestión de riesgos emergentes y resiliencia organizacional, con enfoque anticipatorio ante escenarios complejos y disruptivos (IA, ciberdefensa, amenazas híbridas).	Introduce una visión adaptativa y prospectiva del riesgo.
ISO/IEC 27032	Norma internacional (ISO / IEC, guía complementaria)	Ofrece directrices para mejorar la ciberseguridad y proteger a usuarios, infraestructuras críticas y ecosistemas digitales frente a amenazas como *phishing, malware* y *hacktivismo.*	Fortalece la gobernanza colaborativa al integrar Estado, sector privado y sociedad civil en la protección del ciberespacio. Complementa la 27001 en el ámbito operativo y de gestión de amenazas.
Directiva NIS2 (UE)	Directiva supranacional (Unión Europea)	Aplica a 18 sectores críticos (energía, transporte, salud, digital, administración pública, etc.) e impone obligaciones de gestión.	Es un marco jurídico de referencia global para fortalecer la resiliencia cibernética.

Fuente: Elaboración propia.

Para finalizar, cabe señalar que si bien Colombia ha consolidado un andamiaje jurídico-estratégico para la gobernanza digital y la ciberseguridad, el reto inmediato es pasar del cumplimiento a la capacidad organizacional.

Gobernanza digital en perspectiva internacional: estudio comparado con otros países de Latinoamérica

Con el propósito de desarrollar un análisis comparativo en materia de gobernanza digital aplicada al sector de seguridad y defensa, se seleccionaron cuatro países latinoamericanos: México, Brasil, Chile y República Dominicana. Esta selección responde a la necesidad de contrastar a Colombia con naciones que presentan condiciones estructurales y de política pública comparables, lo cual permite establecer patrones y aprendizajes relevantes. A continuación, se presentan los criterios para la selección de estos países.

- *Desarrollo humano como fundamento de las políticas públicas.* Estos países, al igual que Colombia, cuentan con indicadores de desarrollo humano que reflejan retos y oportunidades similares en términos de equidad

social, acceso a la educación y fortalecimiento institucional. Este factor es crucial, dado que el desarrollo humano constituye la base para la formulación e implementación de políticas digitales inclusivas.

- *Evolución de políticas públicas con estándares de gobernanza.* México, Brasil, Chile y República Dominicana han transitado procesos de modernización institucional que incorporan estándares internacionales de gobernanza digital, orientados hacia la transparencia, la interoperabilidad de sistemas, la gestión de riesgos y la rendición de cuentas.
- *Transformación digital e inclusión tecnológica.* La agenda digital de estos países ha sido objeto de evaluación por organismos multilaterales como la Organización de las Naciones Unidas (ONU), la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y la Unión Internacional de Telecomunicaciones (UIT), a través de indicadores como el ICT Development Index, lo cual garantiza un marco objetivo de medición de avances en conectividad, acceso a internet, infraestructura digital y políticas de inclusión.
- Como criterio adicional, se consideraron países de América Latina con un producto interno bruto (PIB) per cápita igual o superior al de Colombia, una condición que garantiza un análisis en un rango económico semejante. En consecuencia, el estudio de estos cuatro países en contraste con Colombia facilita la identificación de buenas prácticas y desafíos comunes en la gobernanza digital (tabla 3).

Tabla 3. *Análisis comparativo entre países latinoamericanos*

País	Desarrollo humano (2023)	PIB per cápita (USD, 2023 aprox.)	*Rankin* global Firepower (2026)	Índice de innovación Global (2025)	Penetración de internet (%)
Colombia	0.788	6823	43	71	69.1
México	0.789	10 706	36	58	75.6
Brasil	0.786	9951	11	52	81.3
Chile	0.878	16 786	49	51	87.0
República Dominicana	0.776	10 400	115	97	81.2

Fuente: Elaboración propia con base en los datos recolectados de IDH (2023), Global Firepower (2026) Military Strength Ranking yWIPO — Global Innovation Index 2025 (GII Results).

De esta manera, el análisis comparativo se realizará considerando los siguientes criterios: 1) marco normativo y regulador; 2) interacción, articulación y cooperación; 3) tecnología y 4) talento humano.

Es necesario precisar que, al momento de culminarse la redacción del presente capítulo, aún no se había publicado el *Cybersecurity Report 2025*, elaborado en el marco de la colaboración entre la Organización de Estados Americanos (OEA), el Banco Interamericano de Desarrollo (BID) y el Global Cyber Security Capacity Centre de la Universidad de Oxford. No obstante, sus resultados refuerzan tendencias relevantes para el análisis aquí propuesto, pues, según el informe, desde la última evaluación de 2020, la región de América Latina y el Caribe evidencia avances sostenidos y una reducción progresiva de brechas, lo que se refleja en un aumento general de la madurez en las cinco dimensiones del Cybersecurity Capacity Maturity Model (CMM): 1) política y estrategia; 2) cultura y sociedad; 3) conocimiento y capacidades; 4) marcos legales y regulatorios, y 5) estándares y tecnologías. A pesar de dicha trayectoria positiva, el propio reporte advierte que persisten desafíos estructurales, en particular en la calidad del software, la protección de infraestructuras críticas, la limitada inversión en investigación e innovación en ciberseguridad y la baja adopción de seguros cibernéticos, aspectos que continúan condicionando la resiliencia efectiva de los Estados y de los ecosistemas digitales en la región.

Marco normativo y regulador

De acuerdo con el Índice Global de Ciberseguridad 2024 (GCI, 2024), el pilar legal evalúa la solidez del marco jurídico de los países en materia de ciberseguridad. Este criterio incluye la existencia de leyes sustantivas y procesales específicas, la adopción de estándares y tratados internacionales, las disposiciones sobre protección de datos y privacidad, así como los mecanismos de cumplimiento y aplicación judicial. Por lo tanto, a continuación se revisa este aspecto respecto a Colombia, México, Brasil, Chile y República Dominicana.

Colombia

Como se indicó anteriormente, Colombia ha consolidado un marco jurídico en seguridad digital que combina leyes sustantivas, procesales y de protección de datos. En el apartado de legislación nacional en gobernanza digital y ciberseguridad, se hizo referencia a diversas normas, como la Ley 1581 de 2012, que regula la protección de datos personales, y el Decreto 338 de 2022, el cual crea el Modelo de Gobernanza de Seguridad Digital y establece lineamientos para identificar las infraestructuras críticas, la gestión de riesgos y la respuesta a incidentes. Estas disposiciones se complementan con el CONPES 3854 de 2016 y el CONPES 3995 de 2020, documentos que sentaron las bases de la política nacional en esta materia.

A estas se suma la Ley 1273 de 2009, que tipifica los delitos informáticos, cuyo propósito es proteger la confidencialidad, la integridad y la disponibilidad de la información y de los sistemas tecnológicos.

De acuerdo con el Índice Global de Ciberseguridad 2024, Colombia obtuvo 13.37/20 en el pilar de medidas legales, una calificación que la sitúa en el Tier 3 (*Establishing*). Este puntaje refleja un marco jurídico avanzado, aunque todavía en proceso de consolidación frente a los países líderes de la región. En términos generales, Colombia ha avanzado en el fortalecimiento normativo para la ciberseguridad, lo cual ha generado confianza en el entorno digital y ha sentado las bases para una mayor resiliencia en materia de seguridad y defensa. Sin embargo, persiste el desafío de mejorar los mecanismos de aplicación judicial y fortalecer la cooperación interinstitucional a fin de garantizar la efectividad de las normas. Por ello, la adaptación y la adecuación del marco normativo cibernético se establece como una línea de acción dentro de la ENSD 2025-2027.

Mexico

México cuenta con un marco jurídico que incorpora la tipificación de delitos informáticos en el artículo 211 del Código Penal y con dos leyes diferenciadas para la protección de datos: una dirigida a bases de datos públicos y otra a bases de datos privadas (BID & OEA, 2020, p. 125).

De acuerdo con el Índice Global de Ciberseguridad 2024, México obtuvo 18.39/20 en el pilar de medidas legales, lo cual lo sitúa en el Tier 2 (*Advancing*) y, por lo tanto, refleja un alto nivel de madurez normativa en la región. Entre sus fortalezas se encuentran la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que regula el tratamiento de información privada, las reglas de notificación de brechas de seguridad y procedimientos judiciales aplicables, así como su alineación con tratados internacionales. En este sentido, se puede afirmar que México ha consolidado un marco legal integral en ciberseguridad, que sustenta la confianza digital y fortalece la gobernanza de las TIC. No obstante, puede potenciar su impacto reforzando la cooperación interinstitucional e internacional, un aspecto clave para la defensa en entornos digitales.

Brasil

Brasil cuenta con el Decreto Federal N.º 10222, que aprueba la Estrategia Nacional de Ciberseguridad, la cual orienta la coordinación entre actores y establece un consejo nacional en la materia (BID & OEA, 2020). Asimismo, la Ley N.º 12965 – Marco Civil de Internet regula el uso de internet y consagra principios de privacidad,

derechos de los usuarios y obligaciones de los proveedores. Estos instrumentos se complementan con la Ley General de Protección de Datos (LGPD, 2018).

Con base en el Índice Global de Ciberseguridad 2024, Brasil alcanzó la puntuación máxima de 20/20 en el pilar legal, una posición que lo ubica en el Tier 1 (*Role-modelling*), lo cual lo consolida como referente regional y global. Sus fortalezas radican en un marco normativo actualizado que tipifica delitos informáticos, protege datos personales y establece mecanismos de cooperación judicial y acuerdos internacionales. Además, este ecosistema se complementa con instituciones como el CERT.br y el marco de divulgación de vulnerabilidades.

En síntesis, Brasil evidencia cómo un marco normativo robusto y articulado con estructuras operativas especializadas no solo potencia la gobernanza digital, sino que también refuerza las capacidades de seguridad y defensa.

Chile

En Chile, la Ley N.° 19223 de 1993 sanciona los delitos informáticos, mientras que la Ley N.° 19628 regula la protección de datos personales. A estas normativas se suma la reforma constitucional de 2018, que reconoció la protección de datos como un derecho fundamental (BID & OEA, 2020).

Según el Índice Global de Ciberseguridad 2024, Chile obtuvo 14.69/20 en medidas legales y se ubica en el Tier 3 (*Establishing*), lo cual evidencia avances relevantes, aunque todavía por debajo de los líderes regionales. En este sentido, Chile constituye un ejemplo de transición hacia un marco regulatorio más integral, pues si bien ha avanzado en gobernanza digital, todavía debe consolidar mecanismos de evaluación, coordinación interinstitucional y aplicación judicial para lograr mayor resiliencia en materia de seguridad y defensa digital.

República Dominicana

República Dominicana cuenta con la Ley N.º 53-07 sobre Crímenes y Delitos de Alta Tecnología, la cual regula los delitos cibernéticos, y la Ley N.º 172-13, sobre Protección de Datos Personales. Además, la Constitución de 2010 reconoce el derecho de acceso, actualización y rectificación de los datos personales (BID & OEA, 2020).

De acuerdo con el Índice Global de Ciberseguridad 2024, este país alcanza 18.48/20 en el pilar legal y se ubica en el Tier 3 (*Establishing*), un nivel que, a pesar de su alto puntaje, refleja que aún se encuentra en proceso de consolidación y aplicación efectiva de sus normas. Específicamente, sus fortalezas incluyen un marco pionero en la región para regular delitos tecnológicos y datos personales, el cual se complementa con la Estrategia Nacional de Ciberseguridad 2018-2021, que fortaleció la cooperación nacional e internacional.

La República Dominicana constituye un ejemplo de cómo la voluntad política y la cooperación internacional son factores aceleradores en la maduración normativa de la ciberseguridad. A continuación, la tabla 4 sintetiza los principales aspectos normativos y reguladores de los países estudiados.

Tabla 4. *Cuadro comparativo del marco legal según el Índice Global de Ciberseguridad 2024*

País	Puntaje GCI (pilar legal)	TIER	Principales leyes y normas	Fortalezas y observaciones
Colombia	13.37 / 20	Tier 3 – *Establishing*	- Ley 1273 de 2009. - Ley 1581 de 2012. - Decreto 338 de 2022. - CONPES 3854 (2016). - CONPES 3995 (2020).	- Marco jurídico integral con enfoque en delitos informáticos, protección de datos y gobernanza digital. - Alineación con estándares internacionales (CMM, UIT). - Reto: fortalecer la aplicación judicial y la coordinación interinstitucional.
México	18.39 / 20	Tier 2 – *Advancing*	- Código Penal Federal, art. 211: Delitos informáticos. - Ley Federal de Protección de Datos Personales en Posesión de los Particulares. - Ley de Protección de Datos Personales en Posesión de Sujetos Obligados.	- Alto nivel de madurez normativa y técnica. - Reglas claras sobre brechas de seguridad y responsabilidad de proveedores. - Reto: reforzar la cooperación interinstitucional e internacional.
Brasil	20 / 20	Tier 1 – *Role-modelling*	- Ley 12965 (Marco Civil de Internet): Principios y derechos digitales. - Ley General de Protección de Datos (LGPD, 2018). - Decreto 10222 (2020): Estrategia Nacional de Ciberseguridad (E-Ciber).	- Referente regional y global. - Normas robustas e instituciones consolidadas (CERT.br, CGD Ciber). - Cooperación internacional y mecanismos de divulgación de vulnerabilidades. - Gobernanza multisectorial fuerte.

País	Puntaje GCI (pilar legal)	TIER	Principales leyes y normas	Fortalezas y observaciones
Chile	14.69 / 20	Tier 3 – *Establishing*	- Ley 19223 (1993): Delitos informáticos. - Ley 19628: Protección de datos personales. - Reforma constitucional (2018): protección de datos como derecho fundamental. - Ley Marco de Ciberseguridad e Infraestructuras Críticas (2023).	- Avanza hacia un marco moderno e integral. - Fortalece servicios esenciales y resiliencia digital. - Reto: consolidar mecanismos de coordinación y aplicación judicial efectiva.
República Dominicana	18.48 / 20	Tier 3 – *Establishing*	- Ley 53-07: Crímenes y Delitos de Alta Tecnología. - Ley 172-13: Protección de Datos Personales. - Constitución de 2010: Reconoce el derecho de acceso y rectificación de datos. - Estrategia Nacional de Ciberseguridad 2018-2021.	- Marco pionero en la región en delitos tecnológicos y datos personales. - Fuerte cooperación internacional y voluntad política. - Reto: consolidar capacidades operativas y sostenibilidad institucional.

Fuente: elaboración propia con base en los datos recolectados en el Índice Global de Ciber-seguridad 2024 y otras fuentes relacionadas en las referencias.

Interacción, articulación y cooperación

De acuerdo con el Índice Global de Ciberseguridad (GCI, 2024), este pilar evalúa la capacidad de los países para consolidar un sistema de gobernanza digital mediante criterios tanto organizacionales como de cooperación. En este sentido, se consideran factores como la existencia y actualización de una estrategia nacional de ciberseguridad, la presencia de una entidad nacional responsable de su implementación, la conformación de estructuras de coordinación interinstitucional y los mecanismos de evaluación y actualización de la política.

Asimismo, este pilar incluye la protección de infraestructuras críticas, la participación en esquemas de cooperación internacional y regional, la colaboración público-privada y la interacción entre equipos nacionales de respuesta a incidentes (CSIRTs), todo lo cual, en conjunto, refleja el grado de madurez y articulación de un país en materia de seguridad digital. Así, en este pilar los países seleccionados muestran avances diferenciales en la consolidación de sus marcos de gobernanza digital.

Colombia

Colombia ha consolidado un marco estratégico y normativo, el cual se expresa en la Estrategia Nacional de Seguridad Digital 2025-2027 y en el Decreto 338 de 2022, que formaliza el modelo de gobernanza en tres niveles: estratégico, táctico y operativo. Sin embargo, con una puntuación de 10.91/20 del Índice Global de Ciberseguridad 2024, el país aún se encuentra en fase de consolidación institucional.

Es por esto que la Estrategia Nacional de Seguridad Digital 2025-2027 ha establecido que la ausencia de una institución nacional especializada y robusta para coordinar los esfuerzos de seguridad digital en Colombia ha resultado en una fragmentación de las iniciativas y una dispersión de los recursos. Asimismo, evidencia que la limitada cooperación internacional en materia de seguridad digital, especialmente frente a amenazas transfronterizas y el cibercrimen, presenta desafíos para Colombia en el escenario global (ENSD 2025-2027).

México

México cuenta con una estrategia nacional desde 2017 y con mecanismos como el CERT-MX y la Guardia Nacional, que aseguran la coordinación y la colaboración público-privada. No obstante, aunque no cuenta con una ley federal de ciberseguridad, alcanza un puntaje de 17.34/20, lo que refleja un desempeño alto.

Brasil

Brasil presenta el mayor nivel de madurez regional. Gracias a su Política Nacional de Ciberseguridad (PNCiber, 2023) y a la existencia de instancias como el Comité Nacional de Ciberseguridad y el CERT.br, este país alcanza un puntaje de 20/20.

Chile

Con una estrategia implementada desde 2017 y un CSIRT gubernamental dependiente del Ministerio del Interior, Chile ha fortalecido sus estructuras. Su puntaje de 13.41/20 lo sitúa en un nivel intermedio, el cual se encuentra en proceso de consolidación para superar las limitaciones en coordinación y evaluación.

República Dominicana

República Dominicana cuenta con una Estrategia Nacional de Ciberseguridad (Decreto 230-18) y la creación del CSIRT-RD, lo cual le ha permitido construir estructuras de coordinación. Además, con un puntaje de 18.37/20, se posiciona como uno de los países con mejor desempeño organizacional en la región, pese a sus limitaciones de recursos.

En síntesis, el análisis muestra que Brasil y México lideran en articulación interinstitucional y cooperación multiactor, mientras que Colombia avanza en la consolidación de su modelo de gobernanza. Por su parte, Chile y República Dominicana se encuentran en fases de fortalecimiento y, si bien han logrado avances significativos, aún necesitan mejorar los mecanismos de evaluación y articulación con el sector privado. A continuación, la tabla 5 sintetiza los principales avances y retos en materia de interacción, articulación y cooperación en los países estudiados.

Tabla 5. *Cuadro comparativo de la medición de estrategias nacionales y organizaciones de acuerdo con el Índice Global de Ciberseguridad 2024.*

País	Puntaje GCI (*Organizacional measures*)	Estrategia nacional de ciberseguridad	Entidad responsable	Coordinación interinstitucional
Colombia	10.91 / 20	Sí, actualizada (2025-2027)	Presidencia (Dirección de Seguridad Digital).	Sí, a través del Comité Nacional de Seguridad Digital.
México	17.34 / 20	Sí, publicada en 2017.	CERT-MX y Guardia Nacional.	Limitada pero existente.
Brasil	20 / 20	Sí, con PN-Ciber y Plan Nacional (2024).	Comité Nacional de Ciberseguridad.	Sí, a través del Comité Nacional.
Chile	13.41 / 20	Sí, lanzada en 2017.	Subsecretaría del Interior.	Sí, con estructura funcional.
República Dominicana	18.37 / 20	Sí, Decreto 230-18 (2018).	CSIRT-RD y Ministerio de la Presidencia.	Sí, con articulación público-privada.

CGI: Índice Global de Ciberseguridad.

Fuente: Elaboración propia con base en los datos recolectados del Índice Global de Ciberseguridad 2024 y otras fuentes relacionadas en las referencias.

Infraestructura tecnológica segura

Este pilar evalúa la capacidad técnica de los países para garantizar una infraestructura digital segura. Para ello, el GCI 2024 considera, entre otros aspectos, la existencia de un equipo nacional de respuesta a incidentes (CSIRT o CERT) y la supervisión técnica de las infraestructuras críticas. Asimismo, valora la definición de estrategias de respuesta y recuperación ante incidentes, la implementación de procedimientos de contención, mitigación y análisis forense, y la participación en redes técnicas internacionales.

En este último aspecto se destacan elementos como el intercambio de indicadores de compromiso (IOC), la realización de ejercicios conjuntos de ciberseguridad y la membresía en organizaciones globales como FIRST, que fortalecen la cooperación técnica y la capacidad de resiliencia frente a amenazas cibernéticas.

Colombia

Colombia presenta una calificación de 16.22/20 en el Índice Global de Ciberseguridad 2024, apoyada en el ColCERT y en el CSIRT nacional dependiente del Ministerio de Defensa. Su arquitectura, que abarca guías de identificación de infraestructuras críticas y programas de protección sectorial, demuestra una capacidad técnica en detección y respuesta a incidentes. Sin embargo, aún requiere ampliar la madurez de la coordinación intersectorial.

México

México alcanzó un puntaje de 19.6/20 y se destacó por el CERT-MX, operado por la Guardia Nacional y reconocido internacionalmente. Sus protocolos incluyen autenticación segura, cifrado y DNSSEC, además de la supervisión de infraestructuras críticas. La articulación con CSIRT Américas y la OEA-BID fortalece sus capacidades. En particular, el informe del Índice Global de Ciberseguridad 2024 evidencia esta fortaleza al señalar que es necesario seguir fortaleciendo la integración técnica con el sector privado y la actualización continua de procedimientos.

Brasil

Como se ha indicado, Brasil lidera en la región con un puntaje de 20/20, lo cual demuestra capacidades técnicas de referencia. Su CERT.br constituye uno de los equipos más robustos de América Latina, el cual está respaldado por protocolos de respuesta y recuperación, herramientas de conciencia situacional y un marco de divulgación de vulnerabilidades. Además, su activa participación en redes como FIRST lo posiciona como referente global en cooperación técnica.

Chile

Chile se ubica en un nivel intermedio, con un puntaje de 13.81/20. Así, aunque el CSIRT de Gobierno, miembro de CSIRT Américas, asegura un marco operativo básico de respuesta a incidentes, aún persisten desafíos en automatización, monitoreo avanzado y cobertura integral de infraestructuras críticas. Además, la falta de adopción extendida de estándares técnicos limita su avance hacia un nivel de madurez comparable con los países líderes.

República Dominicana

República Dominicana ha mostrado progresos significativos con la creación del CSIRT-RD en 2020, que coordina la protección de infraestructuras críticas y de TI estatales en cooperación con entidades privadas. Su puntuación de 15.74/20

refleja un nivel intermedio-alto, el cual se respalda en su participación en CSIRT Américas y en la cooperación técnica internacional. No obstante, aún es necesario consolidar aspectos como la automatización de respuestas y la implementación de tecnologías avanzadas de protección.

En síntesis, el análisis revela una clara diferenciación regional: Brasil y México destacan como líderes en capacidades técnicas, mientras que Colombia y República Dominicana muestran un nivel intermedio-alto con estructuras en consolidación. Por su parte, Chile avanza de manera gradual, pero aún enfrenta rezagos en robustez técnica y protección de infraestructuras críticas. A continuación, la tabla 6 presenta los principales contrastes en materia de infraestructura tecnológica segura en los países analizados.

Tabla 6. *Cuadro comparativo de la medición sobre infraestructura tecnológica segura según el Índice Global de Ciberseguridad 2024*

País	Puntaje GCI (***Organizacional measures***)	CSIRT/CERT nacional	Fortalezas técnicas	Principales desafíos
Colombia	16.22 / 20	ColCert y CSIRT Nacional (MDN)	Protección de ICCN, programas sectoriales, sistemas de detección y respuesta.	Consolidar la coordinación intersectorial y robustecer la automatización.
México	19.6 / 20	CERT.Mx (Guardia Nacional)	Protocolos de autenticación, cifrado DNSSEC y cooperación internacional.	Mejorar la integración técnica con el sector privado.
Brasil	20 / 20	CERT.br (robusto, referente regional)	Protocolos avanzados, divulgación de vulnerabilidades y participación en FISRT.	Mantener el liderazgo y hacer actualizaciones continuas.
Chile	13.81 / 20	CISIRT de Gobierno (Ministerio del Interior)	Membresía en CSIRT Américas y capacidad operativa básica.	Ampliar cobertura, automatización, monitoreo avanzado y adopción de estándares.
República Dominicana	15.74 / 20	CSIRT RD- (establecido en 2020)	Protección de infraestructuras críticas, cooperación con OEA y BID.	Avanzar en automatización de respuestas y uso de tecnologías avanzadas de protección.

CERT: Equipo de Respuesta ante Emergencias Informáticas.

CSIRT: Equipo de Respuesta a Incidentes de Seguridad Informática.

GCI: Índice Global de Ciberseguridad.

Fuente: Elaboración propia con base en los datos recolectados por el Índice Global de Ciberseguridad 2024 y otras fuentes relacionadas en las referencias.

Talento humano

El talento humano constituye un pilar esencial para la consolidación de la gobernanza digital y la seguridad en el ciberespacio. El Índice Global de Ciberseguridad (GCI, 2024) lo mide en función de la existencia de programas de formación, certificación de competencias, iniciativas de investigación y desarrollo (I+D), así como de mecanismos de retención y actualización de capacidades (ITU, 2024). A continuación, se presenta la situación de los países estudiados en relación con este pilar.

Colombia

Colombia ha avanzado en la formación de talento mediante programas del Servicio Nacional de Aprendizaje (SENA), iniciativas de posgrado en universidades públicas y privadas y la inclusión de la ciberseguridad en políticas nacionales, como el CONPES 3995 de 2020. Por su parte, la Estrategia Nacional de Seguridad Digital 2025-2027 plantea la territorialización de la formación en competencias digitales y técnicas de seguridad, a la vez que busca la articulación con estándares internacionales de medición, tales como el Cybersecurity Capacity Maturity Model (CMM).

Brasil

Brasil cuenta con la Iniciativa Nacional de Educación en Seguridad Cibernética (NICE-BR) y ha impulsado la Política Nacional de Ciberseguridad (PNCiber, 2023), que incluye un eje específico para la formación de capital humano (Gobierno Federal de Brasil, 2023). Su colaboración con universidades e institutos tecnológicos y el fortalecimiento de programas de certificación lo ubican en el nivel más alto del Índice Global de Ciberseguridad 2024 en este pilar.

México

México cuenta con la estrategia nacional de 2017, la cual promovió el desarrollo de currículos en ciberseguridad y alianzas con el sector privado (BID et al., 2020). Sin embargo, no cuenta con una ley federal de ciberseguridad, lo cual limita la creación de un sistema nacional de certificaciones y estándares. Según el Índice Global de Ciberseguridad 2024, México presenta un desempeño alto, sustentado en la operación de su CERT-MX y en la colaboración público-privada en programas de formación (ITU, 2024).

Chile

Chile muestra un nivel intermedio. Su estrategia nacional (2017) incorporó la necesidad de formación en ciberseguridad, pero los programas se concentran en

iniciativas gubernamentales aisladas y en la cooperación con universidades (BID et al., 2020). El Índice Global de Ciberseguridad 2024 le otorga una puntuación moderada, lo que refleja avances en educación formal, aunque aún no consolida un ecosistema nacional articulado de formación y certificación (ITU, 2024).

República Dominicana

República Dominicana ha logrado avances desde la adopción de la Estrategia Nacional de Ciberseguridad (Decreto 230-18), la cual abarca programas de sensibilización y capacitación para funcionarios públicos y operadores de infraestructuras críticas (BID et al., 2020). La creación del CSIRT-RD ha potenciado la transferencia de conocimientos y la cooperación internacional, especialmente con la OEA y el BID. No obstante, el país enfrenta desafíos en la masificación de programas de educación avanzada y en la retención del talento formado.

En conclusión, mientras Brasil y México lideran la región en la consolidación de talento humano en ciberseguridad, Colombia y República Dominicana, a pesar de mostrar avances importantes, aún requieren ampliar la cobertura y la certificación de especialistas. Por su parte, Chile se encuentra en un nivel intermedio. Para Colombia, la experiencia comparada resalta la importancia de institucionalizar un sistema nacional de formación y certificación que esté alineado con marcos internacionales y que cuente con una fuerte participación de la academia y el sector privado. A continuación, la tabla 7 sintetiza los principales elementos en materia de talento humano de los países estudiados.

Tabla 7. *Cuadro comparativo de la medición del talento humano de acuerdo con el Índice Global de Ciberseguridad 2024*

País	Puntaje relativo	Programa de formación	Fortalezas	Principales desafíos
Colombia	Medio (brechas en especialistas certificados).	SENA. Posgrados en universidades. Prioridad dentro de la Estrategia Nacional de Seguridad Digital de Colombia 2025-2027.	Articulación con CMM estándares internacionales.	Ampliar cobertura, descentralizar formación y aumentar certificaciones.
México	Alto (colaboración público-privada).	Currículos en ciberseguridad desde 2017, CERT-MX y alianzas privadas.	Alianza público-privada. CERT MX reconocido.	Aprobar ley federal de ciberseguridad y sistema nacional de certificación.

País	Puntaje relativo	Programa de formación	Fortalezas	Principales desafíos
Brasil	Alto.	NICE-BR universidades, PNCiber 2023 con eje en capital humano.	Sistema nacional robusto de certificación y educación.	Mantener liderazgo global y actualización continua.
Chile	Medio (programas fragmentados, falta de articulación).	Iniciativas en universidades y gobiernos. Estrategia 2017.	Inclusión en la estrategia nacional y cooperación académica.	Consolidar ecosistema nacional de formación y certificaciones.
República Dominicana	Medio-alto (avances en capacitación pública, retos en retención).	Capacitación con OEA y BID - CSIRT-RD desde el 2018.	CSIRT-RD como plataforma de formación y transferencia de conocimiento.	Ampliar educación avanzada y retener talento especializado.

Fuente: Elaboración propia con base en los datos recolectados del Índice Global de Ciberseguridad 2024 y otras fuentes relacionadas en las referencias.

De este modo, el análisis comparativo permite identificar patrones de gobernanza digital en América Latina que aportan lecciones valiosas para el fortalecimiento de la ciberseguridad en el sector de seguridad y defensa en Colombia. Este análisis revela que los países con mejores desempeños no solo han desarrollado marcos legales y técnicos sólidos, sino que también han logrado articular de manera coherente la cooperación internacional y la formación de capacidades humanas (ITU, 2024). De manera general, los resultados evidencian que el liderazgo en ciberseguridad no depende exclusivamente del tamaño económico, sino de la capacidad de los Estados para diseñar políticas estratégicas coherentes, consolidar infraestructuras técnicas, promover la formación de talento humano especializado y fomentar esquemas de cooperación regional y global. Este liderazgo depende, asimismo, de una voluntad política promovida por una política pública que guíe y oriente los resultados hacia el cumplimiento de los principios y valores de un Estado. En el caso de Colombia, un claro ejemplo de esto es la protección del *hábeas data* a través del uso de las tecnologías.

Propuesta de modelo de gobernanza digital para el sector seguridad y defensa

Como se planteó en la introducción, el propósito de este artículo es proponer un modelo de gobernanza en seguridad digital para el sector de seguridad y defensa, que no se limite a la parte normativa y referencial expuesta, sino que incorpore

los hallazgos de un ejercicio de simulación estratégica en el que las entidades del Grupo Social y Empresarial del sector Defensa (GSED) pusieron a prueba sus capacidades de respuesta, coordinación y gobernanza frente a incidentes cibernéticos de alto impacto. El ejercicio, que contó con la participación de las Fuerzas Militares, la Policía Nacional y entidades clave del ecosistema digital en Colombia (como COLCERT, CCOCI y el CISIRT Defensa), evaluó la capacidad de articulación institucional, identificó vacíos y, con base en ello, permitió medir la madurez del modelo de gobernanza y sugerir un modelo aplicable al sector.

Para el ejercicio se utilizó el Modelo de Madurez de la Ciberseguridad en las Naciones (CMM), diseñado para evaluar la capacidad de ciberseguridad a escala nacional y desarrollado por el Global Cyber Security Capacity Centre (GCSCC) de la Universidad de Oxford. Este modelo se compone de cinco dimensiones (o ejes) que representan el espectro de la capacidad en ciberseguridad de un Estado: política y estrategia de ciberseguridad; cultura y sociedad relacionada con seguridad digital; desarrollo de conocimientos y capacidades; marcos jurídicos y regulatorios; y estándares y tecnología. A su vez, mediante tres ejercicios de simulación se evaluaron seis aspectos: cooperación y coordinación institucional; procedimientos; medios técnicos; comunicación estratégica; continuidad del negocio y protección de activos críticos, y nivel de conocimiento del talento humano. El ejercicio se desarrolló con los equipos de cada entidad del GSED, quienes respondían una serie de preguntas después de cada simulación, y fueron evaluados por los equipos del COLCERT, CCOCI, CISIRT Defensa, así como por las Fuerzas Militares y la Policía, con una calificación de 1 a 5 (1 la más baja y 5 la más alta). Con base en la matriz de evaluación, el resultado general fue 3,09 (Nivel 3: Definido). Por lo tanto, con el CMMI Cybermaturity Platform (CMMI Institute, Carnegie Mellon) como marco, una meta a mediano plazo sería escalar al Nivel 4 (Cuantitativamente Gestionado), en el que los procesos no solo estén definidos, sino que se midan, monitoreen y mejoren con base en datos y métricas. El resultado esperado es un ecosistema de defensa más resiliente, capaz de anticiparse, responder y recuperarse de incidentes cibernéticos, lo cual garantiza continuidad operacional y protección de derechos.

Modelo de Gobernanza para el Sector de Seguridad y Defensa

Propósito y alcance

- Propósito: consolidar la gobernanza de la ciberseguridad en el ecosistema defensa-seguridad, con metas de madurez CMMI nivel 4.

- Alcance institucional: Fuerzas Militares, Policía Nacional, entidades del GSED y dependencias del Ministerio de Defensa.
- Principios rectores: legalidad, rendición de cuentas, visión estratégica, enfoque en derechos, inclusividad multiactor, multidimensionalidad, consenso y sostenibilidad (figura 1 y tabla 8).

Figura 1. *Estructura institucional del modelo de gobernanza sugerido para el sector de seguridad y defensa en Colombia*

Fuente: Elaboración propia.

Tabla 8. *Resumen de los niveles, instancias, roles y sustento normativo/estándar*

Nivel	Instancia / actor	Rol / responsabilidad	Norma / estándar
Estratégico	Consejo Nacional de Seguridad Digital de Defensa (CNSDD).	Define política, prioriza capacidades y presupuesto; supervisa métricas de madurez sectorial.	Decreto 338/2022; CONPES 3701/2011; CONPES 3995/2020.
Coordinación	Comité Sectorial de Seguridad Digital y Ciberdefensa.	Implementa lineamientos, consolida riesgos sectoriales y coordina ejercicios TTX y auditorías.	Decreto 1078/2015; Ley 1341/2009 (Gobierno Digital TIC).
Operativo	CISIRT Defensa / CCOCI / COLCERT/ Centro cibernético policial.	Monitoreo, detección, análisis, respuesta e intercambio de información sobre incidentes.	CONPES 3854/2016; RFC 2350; ISO/IEC 27035, NIST SP 800-61 R3 (Computer Security Incident Handling Guide).
Técnico	CSIRT de Fuerzas, y entidades GSED.	Aplicación de controles ISO 27001; forense, vulnerabilidades, cumplimiento y reporte de KPI.	ISO/IEC 27001; Resolución MSPI 500/2021.

Nivel	Instancia / actor	Rol / responsabilidad	Norma / estándar
Innovación	Centro de Excelencia en Ciberseguridad y Ciberdefensa (ESDEG).	Formación, investigación aplicada, simulaciones, doctrina y lecciones aprendidas.	Política CTI sector defensa; NIST NICE / ENISA Skills Framework.
Supervisión	Oficina de Gobernanza, Riesgo y Cumplimiento Cibernético (OGRC).	Auditoría, evaluación de madurez, certificaciones y transparencia ante el CNSDD.	COBIT 2019; ISO/IEC 27004, NIST Cybersecurity Framework (CSF) 2.0; La función de gobernar del NIST.

Fuente: elaboración propia, con base en las fuentes relacionadas en las referencias.

Principios rectores (ENISA adaptados al sector defensa)

Con base en los principios propuestos por la Agencia de la Unión Europea para la Ciberseguridad ENISA (European Union Agency for Cybersecurity):

- Mandato legal y rendición de cuentas: roles y responsabilidades formalizados; reportes periódicos; trazabilidad de decisiones.
- Visión estratégica: alineación entre Estrategia Nacional de Seguridad Digital 2025-2027 y Política de Ciberdefensa.
- Enfoque en derechos y ciudadanía: respeto al *hábeas data* y privacidad; seguridad como medio para bienestar y legitimidad.
- Inclusividad y participación múltiple: gobernanza multiactor: Estado, industria, academia, sociedad civil y aliados internacionales.
- Multidimensionalidad: cultura, talento, tecnología, procesos, jurídico y cooperación internacional integrados.
- Orientación al consenso: decisión colegiada y confianza entre actores; protocolos de coordinación y escalamiento.
- Sostenibilidad y recursos: fondo sectorial y APP para capacidades, I+D y talento; eficiencia y priorización basada en riesgo.

Procesos de madurez (Nivel 4 – CMMI) [T3]

A continuación, la tabla 9 presenta los principales procesos, indicadores y estándares del modelo de gobernanza.

Tabla 9. *Procesos clave, indicadores y estándares vinculados a la operación cuantitativa de la ciberseguridad sectorial*

Dimensión	Acción clave	Indicadores (KPI)	Estándares / herramientas
Gestión cuantitativa del riesgo	FAIR + ISO 31000/31050; valoración ALE y escenarios críticos.	Porcentaje de activos críticos evaluados; ALE; porcentaje de riesgos mitigados según umbral.	ISO 31000/31050; COBIT 2019.

Dimensión	Acción clave	Indicadores (KPI)	Estándares / herramientas
Medición y control	Cuadro de mando sectorial y *dashboards* en tiempo real.	MTTD, MTTC, MTTR; porcentaje de vulnerabilidades corregidas; cobertura de parches.	NIST CSF 2.0; ISO/IEC 27004
Automatización y predictividad	SOC Sector Defensa con IA, TIP e integración ATT&CK.	Porcentaje de correlación automatizada; TPR; tiempo de anticipación de amenazas.	MITRE ATT&CK; NIST SP 800-61 r2.
Gestión del conocimiento	Integrar los informes de lecciones aprendidas (post-incidente) como entrada directa para la revisión y mejora continua de los Planes de Continuidad de Negocio (BCP) y de Recuperación ante Desastres (DRP).	Número de informes consolidados; porcentaje de recomendaciones implementadas.	ISO/IEC 27035; ISO 22301.
Cultura y talento	Plan anual de formación y certificación; simulaciones periódicas (red/blue/purple).	Porcentaje de personal certificado (CISM/CISSP/CEH); tasa de *click* en *phishing;* tiempo de respuesta.	ENISA Skills; NIST NICE.

Fuente: Elaboración propia con base en los datos recolectados del Índice Global de Ciberseguridad 2024 y otras fuentes relacionadas en las referencias.

Resultados esperados y métricas de madurez

- Nivel CMMI 4 alcanzado: procesos medidos y controlados cuantitativamente.
- Reducción del MTTD/MTTR y aumento del TPR en incidentes relevantes. Cobertura de parches y remediación sobre activos críticos > 95 %.
- Convergencia de doctrina, capacitación y práctica operativa (ESDEG).
- Transparencia y rendición de cuentas: auditorías cruzadas y reporte al CNSDD.
- Cooperación internacional efectiva (OEA / CSIRT Americas, OTAN, socios regionales).

Conclusiones

Tanto la normativa como los documentos de estrategia evidencian un marco de gobernanza digital en evolución, con énfasis en la seguridad digital, la ciberresiliencia, la innovación y la colaboración interinstitucional, así como en la protección de infraestructuras críticas y el desarrollo del talento humano. Sin embargo, cabe destacar que en el contexto actual, plasmado en la Estrategia Nacional de Seguridad Digital de Colombia 2025-2027, se hace patente que los recientes

incidentes cibernéticos, tanto en organizaciones públicas como privadas, evidencian la persistente vulnerabilidad de las infraestructuras críticas cibernéticas y los servicios esenciales, así como la brecha existente entre el andamiaje normativo y su implementación real. Por ello, resulta imperativo cerrar esta brecha entre la norma y la acción.

Sin embargo, el esfuerzo no solo radica en fortalecer el marco normativo, sino que también exige la consolidación de infraestructuras técnicas, la articulación de la cooperación interinstitucional y la potenciación de la formación de talento humano, dado que estos constituyen factores estratégicos que permitirán avanzar hacia una gobernanza digital más resiliente y efectiva en Colombia, especialmente en el ámbito de la seguridad y defensa.

El desafío radica, pues, en lograr una implementación articulada que contemple métricas claras, capacidades sostenibles y un enfoque estratégico en infraestructuras críticas y gestión de incidentes. Este logro se materializa a través de un liderazgo en ciberseguridad, cuya valía no se mide por el tamaño económico, sino por la coherencia entre la política pública, la capacidad técnica, la cooperación interinstitucional y el talento humano, así como por la visión y el apoyo de la alta dirección y las instancias de decisión.

Referencias

Amazon Web Services [AWS]. (2024). Guía estratégica para mejorar la postura de ciber-seguridad: Colombia. Presidencia de la República de Colombia.

Banco Interamericano de Desarrollo [BID] & Organización de los Estados Americanos [OEA]. (2020). *Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe.* https://tinyurl.com/2tw6a8at

Brownlee, N., & Guttman, E. (1998). *RFC 2350: Expectations for computer security incident response.* The Internet Society. https://www.ietf.org/rfc/rfc2350.txt

Cámara Colombiana de Informática y Telecomunicaciones [CCIT], & Tanque de Análisis y Creatividad de las TIC [TicTAc]. (2023). *Estado de la ciberseguridad y la inteligencia artificial en Colombia.* CCIT. TIC; TicTac. https://tinyurl.com/5c7usteu

Cano, J. J. (2018). Repensando los fundamentos de la gestión de riesgos: Una propuesta conceptual desde la incertidumbre y la complejidad. *Revista Ibérica de Sistemas e Tecnologias de Informação (RISTI), (E15),* 76–87. https://tinyurl.com/2fe43rx4

CMMI Institute. (2016). CMMI Cybermaturity Platform Model Development. https://cmmiinstitute.com/getattachment/439bd454-ccfe-4285-9407-e7f7a48d810d/CMMI-CP-Model-Development-Approach.pdf

Congreso de Colombia. (2022). *Proyecto de ley presentado por el senador David Luna.* Senado de la República de Colombia. https://www.senado.gov.co

Congreso de Colombia. (2023). *Proyecto de ley por la cual se crea la Agencia Nacional de Seguridad Digital y Asuntos Espaciales.* https://tinyurl.com/37hvbyv7

Decreto 338 de 2022: Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones. Presidencia de la República. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866

Decreto 620 de 2020: Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011. los literales e. j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales. Presidencia de la República de Colombia. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=118337

Delgado-Paz, R. M., Guerrero Acaro, M. E., & Rentería-Pierola, J. L. (2022). *Buenas prácticas para la adopción del marco de seguridad digital para sistemas de control industrial en activos críticos nacionales* [Tesis de maestría, Universidad Peruana de Ciencias Aplicadas]. Repositorio Institucional. https://repositorioacademico.upc.edu.pe/handle/10757/666990

Del-Real, C. (2022). Panorama institucional de la gobernanza de la ciberseguridad en España. *Revista de Estudios Jurídicos y Criminológicos, 6,* 15–51. https://doi.org/10.25267/REJUCRIM.2022.i6.03

Departamento Nacional de Planeación [DNP]. (2011). *CONPES 3701: Lineamientos de política para ciberseguridad y ciberdefensa.* https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Departamento Nacional de Planeación [DNP]. (2016). *CONPES 3854: Política nacional de seguridad digital.* https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Departamento Nacional de Planeación [DNP]. (2020). *CONPES 3995: Política nacional de confianza y seguridad digital.* https://colaboracion.dnp.gov.co/cdt/Conpes/Econ%C3%B3micos/3995.pdf

European Union Agency for Cybersecurity [ENISA]. (2021). *National cybersecurity strategies: Practical guide on development and execution (updated).* ENISA.

Foro Económico Mundial. (2024). 4 leyes sobre ciberseguridad que han cambiado el panorama. https://es.weforum.org/stories/2024/10/la-normativa-de-ciberseguridad-sufrio-grandes-cambios-en-2024-esto-es-lo-que-hay-que-saber

International Organization for Standardization [ISO], & International Electrotechnical Commission [IEC]. (2012). *27032:2012 — Guidelines for cybersecurity.* International Organization for Standardization. https://www.iso.org/standard/44375.html

International Organization for Standardization [ISO], & International Electrotechnical Commission [IEC]. (2022). *27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* International Organization for Standardization. https://www.iso.org/standard/27001

International Organization for Standardization [ISO]. (2019). ISO *22301:2019 security and resilience — Business continuity management systems.* ISO. https://www.iso.org/obp/ui/en/#!iso:std:75106:en

International Telecommunication Union [ITU]. (2024). Índice global de ciberseguridad (GCI) 2024. https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

Ley 1341 de 2009: Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las TIC. Congreso de Colombia. *D.O.* 47426 de julio 30 de 2009. https://tinyurl.com/3k2c429b

Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de Colombia. *D.O.* 48587 de octubre 18 de 2012. https://tinyurl.com/yc2x23w7

Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]. (2023). *Estrategia nacional digital 2023–2026.* Gobierno de Colombia. https://www.dnp.gov.co/LaEntidad_/subdireccion-general-prospectiva-desarrollo-nacional/direccion-desarrollo-digital/Paginas/estrategia-nacional-digital-de-colombia.aspx

Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]. (2025). *Estrategia nacional de seguridad digital de Colombia 2025–2027.* Gobierno de Colombia. https://www.mintic.gov.co/portal/715/articles-403023_recurso_2.pdf

Ministerio TIC. (s. f.). Buenas prácticas. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Iniciativas/Buenas-practicas/

MITRE Corporation. (2024). *ATT&CK® framework*. https://attack.mitre.org

Naser, A. (Coord.). (2021). *Gobernanza digital e interoperabilidad gubernamental: Una guía para su implementación* [Documentos de Proyectos, LC/TS.2021/80]. CEPAL. https://www.cepal.org/es/publicaciones/47018-gobernanza-digital-interoperabilidad-gubernamental-guia-su-implementacion

National Institute of Standards and Technology [NIST]. (2012). *SP 800-61 Rev. 2: Computer security incident handling guide.* https://csrc.nist.gov/pubs/sp/800/61/r2/final

National Institute of Standards and Technology [NIST]. (2024). *Framework for improving critical infrastructure cybersecurity (Version 2.0).* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Organización de las Naciones Unidas [ONU]. (2020). *Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional.* https://docs.un.org/es/A/76/187

Organización de las Naciones Unidas [ONU]. (2021). La ciberseguridad en las organizaciones del sistema de las Naciones Unidas. https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_spanish.pdf

Organización de los Estados Americanos [OEA]. (s. f.). Ciberseguridad. https://www.oas.org/ext/es/seguridad/prog-ciber

Organización para la Cooperación y el Desarrollo Económicos [OCDE]. (2014). *Recommendation of the Council on digital government strategies.* OECD Publishing. https://legalinstruments.oecd.org/api/print?ids=306&lang=en&utm_source=chatgpt.com

Organización para la Cooperación y el Desarrollo Económicos [OCDE]. (2020). *The OECD digital government policy framework: Six dimensions of a digital government (OECD Public Governance Policy Papers, No. 2).* OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/10/the-oecd-digital-government-policy-framework_11dd6aa8/f64fed2a-en.pdf

Organización para la Cooperación y el Desarrollo Económicos [OCDE]. (2021). *The e-leaders handbook on the governance of digital government*. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/12/the-e-leaders-handbook-on-the-governance-of-digital-government_2523ea2c/ac7f2531-en.pdf

Organización para la Cooperación y el Desarrollo Económicos [OCDE]. (2002). Directrices de la OCDE para la seguridad de sistemas y redes de información: Hacia una cultura de seguridad. https://www.oecd.org/es/publications/directrices-de-la-ocde-para-la-seguridad-de-sistemas-y-redes-de-informacion_9789264065819-es.html

S2 Grupo. (2024). Normativas de ciberseguridad: Cuáles debe cumplir tu empresa. https://s2grupo.es/normativas-de-ciberseguridad-cuales-debe-cumplir-tu-empresa/

Savaş, S., & Karata, S. (2022). *Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. Int Cybersecur Law Rev, 3*(1), 7–34. https://doi.org/10.1365/s43439-021-00045-4

Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. *International Cybersecurity Law Review, 3,* 7–34. https://doi.org/10.1365/s43439-021-00045-4

Systems Audit and Control Association [ISACA]. (2019). *COBIT 2019 framework: Governance and management objectives.* ISACA. https://netmarket.oss.aliyuncs.com/df5c71cb-f91a-4bf8-85a6-991e1c2c0a3e.pdf

UNAD Noticias. (2025, 5 de marzo). Ciberseguridad en Colombia: Integrando Blockchain e inteligencia artificial para fortalecer la protección digital. https://noticias.unad.edu.co/index.php/2025/7325-ciberseguridad-en-colombia-integrando-blockchain-e-inteligencia-artificial-para-fortalecer-la-proteccion-digital

Unión Europea. (s. f.). NIS2 Directive: securing network and information systems. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Capítulo 3

Innovación y adaptación: capacidades militares frente a amenazas emergentes en la Guerra Tecnológica Contemporánea*

DOI: https://doi.org/10.25062/9786287818644.03

Aldemar Serrano Cuervo

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El capítulo analiza la transformación del carácter de la guerra en el contexto de la convergencia tecnológica, la cual ha generado amenazas emergentes que desbordan los enfoques tradicionales de la estrategia. En este marco, se plantea como hipótesis que dicha convergencia reconfigura estructuralmente la forma de hacer la guerra y desplaza su centro de gravedad hacia sistemas, datos, procesos decisionales y la dimensión cognitiva. A partir de un marco analítico integrado que articula niveles estructurales, actorales y tecnológicos, se identifican y explican estas amenazas y su interacción sistémica. El hallazgo central demuestra que esta convergencia produce una taxonomía de nuevas formas de guerra-algorítmica, de datos, cognitiva, de sistemas, distribuida, persistente, de velocidad y de dependencia tecnológica que redefinen la competencia estratégica contemporánea. Como aporte, el capítulo propone una matriz que vincula amenazas, formas de guerra y capacidades militares, orientada a fortalecer la adaptación estratégica de las Fuerzas Militares frente a escenarios híbridos tecnológicamente habilitados en el contexto colombiano.

Palabras clave: amenazas emergentes; capacidades militares; convergencia tecnológica; defensa nacional; guerra algorítmica; guerra multidominio.

* En el desarrollo de este capítulo se emplearon herramientas de inteligencia artificial generativa como apoyo en tareas de revisión lingüística, organización estructural y mejora de la claridad expositiva, sin embargo, estas herramientas no fueron utilizadas para la generación autónoma de contenido conceptual, formulación de argumentos ni desarrollo de aportes teóricos. El diseño analítico, la interpretación estratégica y las conclusiones corresponden íntegramente a la autoría del investigador, de manera que la verificación de la información, la coherencia académica y la responsabilidad intelectual del contenido final son asumidas exclusivamente por el autor.

Aldemar Serrano Cuervo

Coronel del Ejército Nacional de Colombia, docente e investigador en Estudios Estratégicos de Seguridad y Defensa. Estancia postdoctoral en Pensamiento Complejo, Multiversidad Mundo Real Edgar Morin, México. Doctor en Logística y Gestión de Cadenas de Suministros, Universidad de La Sabana, Colombia. Magíster en Seguridad y Defensa Nacionales, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Administrador de Empresas, Universidad Militar Nueva Granada, Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. Vicedirector de Investigación, Jefe del Doctorado en Estudios Estratégicos, Seguridad y Defensa y Jefe del Sello Editorial ESDEG. **https://orcid.org/0000-0003-3344-3177**
Contacto: **aldemar.serrano@esdeg.edu.co**

Citación APA: Serrano-Cuervo, A. (2026). Innovación y adaptación: Capacidades militares frente a amenazas emergentes en la Guerra Tecnológica Contemporánea. En M. E. Realpe-Díaz & A. M. González-González (Eds.), *Transformación digital y ciberseguridad en Colombia: Desafíos estratégicos para sectores de infraestructura crítica* (pp. 69-118). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818644.03

TRANSFORMACIÓN DIGITAL Y CIBERSEGURIDAD EN COLOMBIA: DESAFÍOS ESTRATÉGICOS PARA SECTORES DE INFRAESTRUCTURA CRÍTICA
ISBN impreso: 978-628-7818-63-7
ISBN digital: 978-628-7818-64-4
DOI: https://doi.org/10.25062/9786287818644

Colección Ciberseguridad y Ciberdefensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2026

CC BY NC ND

Introducción

El entorno estratégico contemporáneo se encuentra inmerso en una transformación acelerada derivada de la convergencia entre tecnologías digitales, sistemas de información y capacidades militares avanzadas, lo cual reconfigura las condiciones bajo las cuales se desarrolla la guerra (Freedman, 2013). Esta transformación, a su vez, altera la arquitectura misma del conflicto al modificar los mecanismos mediante los cuales los actores perciben el entorno, estructuran sus capacidades y ejecutan la confrontación estratégica. Como resultado, la guerra se desenvuelve en un entorno caracterizado por alta complejidad, incertidumbre estructural e interdependencia sistémica, donde los efectos se producen a través de la interacción entre múltiples dominios y no únicamente mediante la confrontación directa de fuerzas (Gray, 2015).

Las Fuerzas Militares enfrentan una brecha estructural entre la velocidad de la innovación tecnológica y su capacidad institucional de adaptación, lo cual limita su habilidad para anticipar, comprender y responder de manera efectiva a las amenazas emergentes (Baylis et al., 2019). Esta brecha trasciende el plano técnico y adquiere una dimensión estratégica, en la medida en que dificulta la traducción de avances tecnológicos en capacidades militares operacionales coherentes. En consecuencia, las fuerzas deben operar en entornos multidominio donde interactúan dimensiones físicas, digitales y cognitivas, bajo condiciones de presión temporal y degradación informacional, lo que exige nuevas formas de integración entre tecnología, doctrina y toma de decisiones (Luttwak, 2001).

La persistencia de enfoques centrados en la lógica de destrucción física y superioridad convencional limita la comprensión del conflicto contemporáneo, dado que las amenazas actuales se materializan en sistemas de información, redes digitales y procesos decisionales que condicionan la acción militar antes de que esta se exprese en el terreno físico (Rid, 2020). El problema estratégico central no

radica únicamente en enfrentar nuevas amenazas, sino en comprender la transformación del carácter de la guerra y redefinir las capacidades militares a partir de una lógica sistémica. Precisamente, este desafío adquiere particular relevancia en contextos como el colombiano, donde la convergencia entre actores no estatales, economías ilícitas y tecnologías accesibles configura entornos de guerra híbrida tecnológicamente habilitada.

La digitalización progresiva de las sociedades y de las estructuras militares ha incrementado la dependencia de infraestructuras tecnológicas interconectadas, lo cual ha generado nuevas superficies de vulnerabilidad explotables por actores estatales y no estatales (Singer & Friedman, 2014). En consecuencia, esta dependencia transforma a los sistemas de información, las redes de comunicación y los datos en objetivos estratégicos, lo que amplía el campo de batalla hacia dominios donde la confrontación se desarrolla mediante la manipulación, la degradación o la interrupción de sistemas críticos.

De manera simultánea, la disponibilidad de tecnologías de doble uso ha permitido que actores no estatales accedan a capacidades previamente reservadas a los Estados, lo que ha reducido las asimetrías tradicionales y ha facilitado la adopción de modelos operativos más complejos (Kaldor, 2012). Esta democratización tecnológica no solo amplía el acceso a medios, sino que también permite su integración en configuraciones híbridas donde se combinan instrumentos militares, informacionales, económicos y tecnológicos, lo cual dificulta la atribución y complica la respuesta estatal (Liang & Xiangsui, 1999).

La interacción de estos factores configura un entorno de conflicto persistente en el cual la distinción entre guerra y paz se difumina, lo cual genera dinámicas de competencia estratégica continua donde la coerción se ejerce de manera indirecta, distribuida y multidimensional (Hoffman, 2007). En este escenario, la superioridad estratégica depende cada vez más de la capacidad para recolectar, procesar y explotar información, influir en la percepción de actores clave y afectar los procesos de toma de decisiones del adversario.

La presente investigación sostiene que la guerra contemporánea experimenta un desplazamiento progresivo de su centro de gravedad desde la destrucción física de las fuerzas adversarias hacia el control de sistemas, datos, procesos decisionales y dimensiones cognitivas (Clausewitz, 2007). Sin embargo, este desplazamiento no altera la naturaleza política de la guerra, sino que transforma profundamente su carácter al redefinir los mecanismos mediante los cuales se genera ventaja estratégica en el entorno actual (Gray, 2015).

A partir de esta premisa, se plantea que las amenazas emergentes no constituyen fenómenos aislados, sino manifestaciones de un sistema de conflicto integrado que da lugar a nuevas formas de hacer la guerra. Estas incluyen dinámicas como la guerra algorítmica, la guerra de datos, la guerra cognitiva, la guerra de sistemas y la guerra de dependencia tecnológica, en las cuales la ventaja estratégica se define por la capacidad de integración, adaptación y control de arquitecturas complejas.

El aporte central de este estudio consiste en desarrollar una arquitectura analítica que articula tres niveles: amenazas emergentes, formas contemporáneas de guerra y capacidades militares necesarias para enfrentarlas. Esta propuesta se materializa en una matriz que permite vincular cada tipo de amenaza con implicaciones doctrinales y cognitivas, de manera que constituye un modelo aplicable al análisis estratégico y al diseño de políticas de defensa en entornos caracterizados por alta complejidad e incertidumbre.

El capítulo articula los desarrollos conceptuales de la gobernanza digital y la ciberseguridad con la teoría de la guerra y los estudios estratégicos, con el propósito de explicar cómo las amenaza emergentes derivadas de la convergencia tecnológica transforman el carácter del conflicto contemporáneo. Su aporte radica en la identificación sistemática de nuevas formas de hacer la guerra y en la traducción de estas en implicaciones concretas para el desarrollo de capacidades militares. De este modo, el análisis propone un marco analítico que permite comprender su funcionamiento, anticipar su evolución y, finalmente, orientar la adaptación institucional en entornos caracterizados por alta complejidad, incertidumbre y competencia multidominio.

Una de las manifestaciones más críticas de esta transformación se observa en el desarrollo de tecnologías cuánticas en el ámbito de la criptografía, que sustenta la seguridad de las comunicaciones militares, los sistemas de mando y control y las operaciones de inteligencia (Nielsen & Chuang, 2010). En este contexto, la capacidad potencial de los computadores cuánticos para comprometer los esquemas de cifrado actuales introduce un riesgo estructural para la integridad y confidencialidad de la información estratégica, lo cual afecta directamente la coherencia de los sistemas de defensa (ETSI, 2015).

En el ámbito operacional, la degradación de los sistemas criptográficos impacta la funcionalidad del mando y control, la transmisión segura de órdenes y la protección de datos críticos, lo que puede comprometer la conducción de operaciones en tiempo real (Singer & Friedman, 2014). Asimismo, los sistemas de inteligencia, vigilancia y reconocimiento dependen de la integridad de la información para sustentar la toma de decisiones, lo cual amplifica el impacto de una posible ruptura criptográfica en toda la arquitectura militar.

La criptografía postcuántica se configura como una capacidad estratégica esencial para preservar la resiliencia de los sistemas militares frente a amenazas emergentes. En este sentido, su desarrollo e implementación constituyen un proceso de adaptación doctrinal, organizacional y estratégica que refleja la necesidad de anticipar transformaciones profundas en el entorno de la guerra contemporánea.

Marco teórico y conceptual: naturaleza, carácter y centro de gravedad en la guerra tecnológica

Naturaleza de la guerra

La guerra constituye un fenómeno político caracterizado por la confrontación organizada entre voluntades que buscan imponer decisiones estratégicas bajo condiciones de fricción, incertidumbre y resistencia recíproca. Precisamente, esta comprensión conserva plena vigencia en el entorno contemporáneo, pues permite distinguir entre la estructura permanente del conflicto y las formas históricas a través de las cuales este se manifiesta. La esencia de la guerra no se encuentra en los medios específicos empleados en cada época, sino en la relación conflictiva entre actores que compiten por imponer su voluntad en escenarios de alta complejidad (Clausewitz, 2007).

Sin embargo, la convergencia tecnológica introduce transformaciones significativas en la forma en que se desarrollan las operaciones, amplía los espacios de confrontación y acelera la producción de efectos, mientras mantiene intacta la lógica política del fenómeno bélico. La inteligencia artificial, la automatización, las capacidades cibernéticas, los sistemas autónomos y las arquitecturas digitales modifican instrumentos, ritmos y vulnerabilidades del conflicto; esta distinción resulta esencial para el análisis estratégico, ya que permite comprender las amenazas emergentes como expresiones de un cambio en el carácter de la guerra y no como una ruptura con su naturaleza.

Carácter de la guerra

El carácter de la guerra expresa la forma concreta en que el conflicto se desarrolla en función de condiciones tecnológicas, organizacionales, doctrinales e históricas específicas, de manera que su transformación responde a cambios en los medios disponibles, en la estructura de los actores y en la configuración del entorno operacional. En el contexto contemporáneo, la convergencia entre inteligencia artificial,

conectividad global, automatización y procesamiento masivo de datos ha alterado de manera profunda la forma en que se construyen las operaciones, se distribuyen los efectos y se genera la ventaja estratégica (Freedman, 2013).

El entorno operacional se proyecta hacia dominios donde la información, los datos, la conectividad y los procesos de decisión adquieren centralidad operacional. En este contexto, la eficacia militar se vincula con la capacidad de integrar sistemas, sostener flujos de información confiables, coordinar funciones interdependientes y operar bajo presión temporal en entornos dinámicos. La lógica de la confrontación se reorganiza alrededor de la adaptación, la integración funcional y la explotación de información en tiempo real, lo que redefine las condiciones de generación del poder militar (Strachan, 2008).

Centro de gravedad en la guerra tecnológica

El concepto de *centro de gravedad* mantiene utilidad analítica cuando se entiende como el elemento que sostiene la capacidad de acción de un actor en conflicto. En la guerra contemporánea, ese elemento se desplaza progresivamente hacia arquitecturas complejas que integran información, conectividad, coordinación y decisión, dado que la cohesión de una fuerza depende de la integridad de sus redes, de la confiabilidad de sus datos y de la estabilidad de sus sistemas de mando y control (Luttwak, 2001).

Este desplazamiento introduce una vulnerabilidad estructural de alto valor estratégico. La manipulación de datos, la degradación de redes, la alteración de señales y la interrupción de procesos de decisión producen efectos operacionales y estratégicos sin requerir confrontación cinética directa. El centro de gravedad adquiere una forma distribuida, interdependiente y técnicamente mediada, lo que explica la creciente orientación de las amenazas emergentes hacia sistemas, redes, plataformas y ciclos decisionales. En consecuencia, la capacidad de preservar la coherencia funcional del sistema propio y afectar la del adversario se configura como un factor determinante de la ventaja estratégica.

Vigencia de Sun Tzu y Clausewitz en la guerra tecnológica contemporánea

La vigencia de Sun Tzu radica en la centralidad que concede al conocimiento del adversario, al manejo de la información, al engaño y a la flexibilidad operativa como bases de la ventaja estratégica. Este enfoque adquiere nueva densidad en un entorno donde las operaciones sobre datos, percepciones, redes y procesos de decisión permiten producir efectos de alto alcance mediante acciones indirectas.

La importancia contemporánea de la desinformación, de la manipulación algorítmica y de las operaciones cognitivas confirma la continuidad de estos principios en el contexto tecnológicamente mediado (Sun Tzu, 2009).

Asimismo, la vigencia de Clausewitz se expresa en la permanencia de la guerra como fenómeno político y en la subordinación de los medios a fines estratégicos definidos por la conducción del poder. En particular, esta perspectiva conserva plena utilidad porque sitúa las tecnologías emergentes dentro de marcos políticos, institucionales y geoestratégicos concretos. Por consiguiente, las capacidades tecnológicas adquieren significado en función de proyectos de poder, intereses nacionales y decisiones estratégicas. Esta lectura impide atribuir autonomía política a la tecnología y mantiene la relación entre medios y fines como eje interpretativo del conflicto (Clausewitz, 2007).

La articulación de ambos enfoques proporciona una base conceptual sólida para interpretar la guerra contemporánea. El control de la información, la flexibilidad, la desarticulación del adversario y la subordinación de la fuerza a fines políticos configuran una clave analítica robusta para comprender la convergencia tecnológica sin perder de vista la estructura fundamental del fenómeno bélico.

La revisión de naturaleza, carácter y centro de gravedad permite establecer que la guerra contemporánea se desarrolla sobre una reconfiguración estructural del entorno estratégico, en la cual la tecnología modifica la integración de medios, la organización de efectos y la producción de ventaja sin alterar la lógica esencial del conflicto. De este modo, esta transformación desplaza el énfasis analítico hacia sistemas, información y procesos de decisión como soportes crecientes de la capacidad estratégica.

Sobre esta base conceptual, las formas contemporáneas de la guerra deben entenderse como manifestaciones operativas de la transformación del carácter del conflicto. Su análisis, a su vez, permite identificar cómo la convergencia tecnológica reorganiza la relación entre capacidades, vulnerabilidades y objetivos estratégicos, lo cual establece nuevas condiciones para la acción militar y para la defensa nacional.

Transformación del carácter de la guerra: marco operacional contemporáneo

Guerra híbrida

Constituye una forma de conflicto en la cual diferentes instrumentos de coerción se integran dentro de una misma lógica estratégica para producir efectos

acumulativos sobre el adversario. Su rasgo central radica en la articulación deliberada de medios convencionales, irregulares, informacionales, económicos y tecnológicos, orientados a explotar vulnerabilidades de manera simultánea en distintos niveles. Esta forma de guerra modifica la percepción del conflicto porque desdibuja las fronteras entre combate, presión política, manipulación del entorno y coerción indirecta, lo cual dificulta la atribución y fragmenta la respuesta estatal (Hoffman, 2007).

La convergencia tecnológica intensifica esta lógica al facilitar la coordinación de acciones distribuidas mediante plataformas digitales, sistemas de comunicación, redes sociales, drones comerciales y mecanismos de financiamiento descentralizado. Como resultado, el conflicto deja de presentarse como una secuencia lineal de choques entre fuerzas y pasa a estructurarse como un sistema de presión continua sobre la capacidad del adversario para interpretar, coordinar y decidir. En este entorno, la eficacia estratégica depende de la integración sostenida de medios heterogéneos dentro de una arquitectura operativa coherente (Freedman, 2013).

Guerra multidominio

La guerra multidominio expresa una transformación estructural en la forma como se genera poder militar, al establecer que los efectos estratégicos resultan de la interacción simultánea entre dominios físicos y no físicos. En este contexto, las operaciones contemporáneas se desarrollan en un entorno donde tierra, aire, mar, ciberespacio, espectro electromagnético, espacio y dimensión cognitiva forman parte de una misma arquitectura de confrontación. De este modo, la acción en un dominio produce consecuencias sobre otros, lo que convierte al conflicto en un sistema de interdependencias operacionales y no en una suma de espacios separados (Gray, 2015).

Esta condición redefine la maniobra y la construcción de capacidades, pues la ventaja se produce a partir de la capacidad de sincronizar efectos, sostener conectividad operativa y preservar coherencia funcional frente a perturbaciones múltiples. La integración multidominio incrementa el potencial de coordinación entre sensores, redes, mando y control, inteligencia y efectores, al tiempo que amplía la exposición a vulnerabilidades en cascada. En consecuencia, una arquitectura más integrada dispone de mayor capacidad operativa, pero también de mayor sensibilidad frente a la degradación de nodos críticos de información, comunicación o decisión (Luttwak, 2001).

Guerra irrestricta

La guerra irrestricta amplía el campo de la confrontación al incorporar cualquier instrumento capaz de afectar al adversario como medio de acción estratégica. Esta aproximación posee una relevancia analítica fundamental, ya que permite comprender la expansión del conflicto hacia ámbitos económicos, tecnológicos, jurídicos, financieros e informacionales, donde la presión se ejerce mediante mecanismos que producen efectos de alto impacto sin que se requiera un combate directo. Esta lógica desplaza la atención desde la fuerza militar entendida en sentido restringido hacia el conjunto de recursos que sostienen la capacidad de acción del Estado (Liang & Xiangsui, 1999).

En el entorno tecnológicamente mediado, esta expansión adquiere profundidad adicional debido a la dependencia de infraestructuras digitales, cadenas de suministro, estándares tecnológicos, plataformas de conectividad, sistemas financieros y ecosistemas de datos. Desde esta perspectiva, la manipulación de información, la explotación de dependencias tecnológicas, la presión sobre redes logísticas y la alteración de flujos financieros producen efectos estratégicos sobre la estabilidad estatal, la gobernabilidad y la continuidad funcional. Por lo tanto, la guerra irrestricta ofrece una clave de lectura esencial para comprender por qué las amenazas emergentes se proyectan más allá del campo militar e inciden directamente en la estructura general de la seguridad nacional (Kaldor, 2012).

Zona gris y conflicto persistente

El concepto de zona gris designa una modalidad de competencia estratégica caracterizada por la ambigüedad, la gradualidad y la persistencia: su lógica consiste en cumplir objetivos políticos mediante acciones que acumulan ventajas reales sin activar una respuesta militar convencional de gran escala. Esta forma de conflicto opera por debajo del umbral de la guerra abierta y se desarrolla a través de presiones continuas que erosionan capacidades, legitimidad y margen de maniobra del adversario (Mazarr, 2015).

La convergencia tecnológica fortalece esta dinámica al facilitar operaciones encubiertas, manipulación informacional, coordinación digital distribuida, presión económica y explotación continua de redes críticas. Estas herramientas permiten sostener un estado de confrontación de baja visibilidad y alta eficacia, lo cual resulta especialmente útil para actores que buscan alterar el equilibrio estratégico sin asumir los costos de una guerra abierta. La zona gris convierte la persistencia en un atributo central del conflicto contemporáneo y exige capacidades orientadas a la gestión de amenazas distribuidas, acumulativas y prolongadas (Strachan, 2008).

Implicaciones operacionales

La primera implicación operacional de esta transformación radica en la necesidad de construir capacidades integradas bajo una lógica sistémica, puesto que la eficacia militar depende de la capacidad de conectar sensores, redes, decisiones y efectos en arquitecturas funcionales capaces de operar bajo condiciones de fricción, ambigüedad y presión temporal. La planeación, el entrenamiento y la doctrina deben responder a esta exigencia mediante estructuras que aseguren continuidad operativa y coordinación entre funciones interdependientes (Luttwak, 2001).

La segunda implicación corresponde a la centralidad del dominio cognitivo y de la guerra informacional, ya que la confrontación contemporánea incluye la disputa por la percepción, por la interpretación del entorno y por la confianza en la validez de la información disponible. En este contexto, la capacidad de influir en la lectura de la situación, proteger la integridad informacional y sostener la cohesión institucional adquiere un valor estratégico equivalente al de las capacidades cinéticas. Además, la defensa requiere proteger la arquitectura de sentido que sostiene la decisión, además de la infraestructura material que sostiene la operación.

La tercera implicación es la adaptación tecnológica permanente como condición de eficacia militar. La incorporación de sistemas avanzados exige integración en arquitecturas resilientes que aseguren protección de datos, redundancia funcional, seguridad de redes y capacidad de recuperación frente a la degradación parcial del sistema. La ventaja estratégica se construye a partir de la capacidad de aprender, adaptarse y sostener funcionalidad bajo presión, característica que transforma la capacidad militar en una propiedad del sistema en su conjunto y no exclusivamente de las plataformas individuales (Hoffman, 2007).

La guerra híbrida, la guerra multidominio, la guerra irrestricta y la zona gris expresan manifestaciones operativas de una misma transformación del carácter de la guerra. Todas ellas revelan, además, un conflicto más integrado, expandido, persistente y dependiente de sistemas interconectados. La tecnología actúa como factor de aceleración y articulación al permitir que medios diversos se combinen en secuencias funcionales orientadas a desgastar, desorganizar y condicionar al adversario.

Esta transformación del carácter de la guerra modifica la arquitectura de la confrontación al reorganizar la relación entre medios, información, decisión y efectos, de modo que la integración de sistemas, la dependencia de redes, la centralidad del dato, la expansión del dominio cognitivo y la aceleración de los ciclos decisionales configuran un entorno donde la vulnerabilidad adquiere un carácter sistémico.

En este marco, las amenazas emergentes constituyen la expresión operativa de esa reconfiguración. Así, la convergencia tecnológica, la digitalización del

conflicto, la interdependencia de infraestructuras y la compresión del tiempo estratégico producen un espacio de confrontación expandido, persistente, multidominio y de difícil atribución, en el cual la coerción se ejerce mediante la degradación de sistemas, la alteración de procesos de decisión y la afectación de la percepción. El análisis de estas dinámicas permite identificar la lógica de producción de las amenazas contemporáneas y comprender por qué representan un desafío estructural para la seguridad y la defensa nacional.

Dinámicas que generan las amenazas emergentes

Convergencia tecnológica

La convergencia tecnológica constituye el punto de partida para comprender la emergencia de nuevas amenazas en la guerra contemporánea, pues no radica en la aparición aislada de tecnologías, sino en su integración funcional dentro de sistemas que combinan inteligencia artificial, sensores distribuidos, automatización, computación en la nube y redes de comunicación. Esta convergencia transforma la manera en que se produce la información, se construye la situación operacional y se ejecuta la decisión militar, lo que da lugar a un entorno en el que la superioridad depende de la capacidad de integrar y explotar estos sistemas de manera coherente (Bousquet, 2009).

Desde una perspectiva operacional, esta integración impacta directamente en funciones críticas como el mando y control, la inteligencia, la vigilancia y el reconocimiento (ISR) y el *targeting*. La capacidad de detectar, identificar, procesar y actuar sobre objetivos se acelera y se vuelve más precisa, pero al mismo tiempo se hace dependiente de la integridad de los sistemas que la soportan. Esto introduce una vulnerabilidad estructural: la disrupción de uno de estos componentes puede degradar el conjunto del sistema. En consecuencia, la convergencia tecnológica no solo amplía las capacidades militares, sino que también genera nuevas superficies de ataque que pueden ser explotadas por adversarios estatales y no estatales.

Digitalización del conflicto

La digitalización del conflicto representa una transformación en la base material sobre la cual se desarrolla la guerra, pues a medida que las funciones militares

dependen de *software,* datos y redes, el combate deja de estar sustentado exclusivamente en medios físicos y pasa a depender de la integridad de sistemas digitales. Esta transición implica que la alteración de datos, la manipulación de software o la interrupción de redes pueden producir efectos estratégicos comparables a los de una acción cinética (Rid, 2020).

En el ámbito militar, esta dependencia se refleja en sistemas de mando y control, plataformas de inteligencia, sistemas de navegación, logística digitalizada y arquitectura de comunicaciones. La degradación de estos sistemas afecta directamente la capacidad de coordinación, la precisión en la ejecución de operaciones y la velocidad de respuesta. Por esta razón, la digitalización no debe entenderse como un fenómeno técnico, sino como una condición estructural del conflicto contemporáneo, en la cual el control del entorno digital se convierte en un factor decisivo de la superioridad estratégica (Singer & Friedman, 2014).

Interdependencia sistémica

La interdependencia sistémica describe la forma en que las capacidades militares se integran en redes más amplias que abarcan infraestructuras críticas, sistemas civiles y plataformas tecnológicas. Esta condición implica que la eficacia operacional depende no solo de los medios militares, sino también de la estabilidad de sistemas externos que sostienen la energía, las comunicaciones, el transporte y el flujo de datos. En este contexto, la guerra se inserta en una arquitectura compleja donde las fronteras entre lo militar y lo civil se vuelven difusas (Perrow, 1999).

Esta interdependencia introduce una lógica de vulnerabilidad en cascada. La afectación de un nodo crítico puede generar efectos que se propagan a través del sistema, lo que degrada funciones clave como la logística, el mando y control o la inteligencia. Desde el punto de vista estratégico, esta situación implica que el adversario puede obtener ventajas significativas sin enfrentar directamente a las fuerzas militares, sino mediante la explotación de dependencias estructurales. Esta condición es particularmente relevante en entornos donde las infraestructuras civiles y militares están profundamente interconectadas, lo cual amplía el espectro de amenazas y complejiza la defensa (Luttwak, 2001).

Compresión del tiempo estratégico

La compresión del tiempo estratégico constituye una de las transformaciones más críticas del conflicto contemporáneo. Específicamente, la velocidad de procesamiento de información, la automatización de sistemas y la conectividad global han reducido drásticamente los tiempos de decisión, lo cual ha generado un

entorno en el que la ventaja depende de la capacidad de actuar más rápido que el adversario, de manera que el ciclo de decisión se convierte en un elemento central del poder militar (Virilio, 2006).

Esta aceleración impacta directamente en la conducción de operaciones, lo que exige a los comandantes tomar decisiones en plazos cada vez más cortos y con información que puede ser incompleta o manipulada. Esta dinámica no solo incrementa el riesgo de error, sino que también crea oportunidades para adversarios que buscan saturar, confundir o interferir en los procesos de decisión. En este sentido, la velocidad deja de ser un factor táctico y se convierte en una variable estratégica, donde la capacidad de mantener coherencia bajo presión temporal define la eficacia del sistema militar (Strachan, 2008).

La interacción de estas dinámicas —convergencia tecnológica, digitalización del conflicto, interdependencia sistémica y compresión del tiempo estratégico— configura el entorno en el cual emergen las amenazas contemporáneas, ya que estas no son el resultado de una sola tecnología o de un único factor, sino de la convergencia de múltiples variables que operan de manera simultánea y se refuerzan entre sí. Por esta razón, no pueden ser analizadas de forma aislada, sino como manifestaciones de una transformación estructural del carácter de la guerra.

En este contexto, la guerra se redefine como un fenómeno sistémico, donde la superioridad depende de la capacidad de integrar información, proteger redes, sostener procesos de decisión y operar en entornos altamente interconectados. Por consiguiente, las amenazas emergentes surgen de las vulnerabilidades generadas por esta configuración, de tal manera que comprender estas dinámicas no es un ejercicio descriptivo, sino una condición necesaria para identificar con precisión los riesgos estratégicos. Además, Es, sobre todo, fundamental para definir las capacidades militares que deben desarrollarse con el objetivo de enfrentarlos en un entorno de conflicto tecnológicamente mediado, persistente y acelerado.

Mapa expandido de amenazas emergentes

Nivel estructural

Las amenazas emergentes no aparecen en el vacío, sino que se incuban en una transformación estructural del conflicto en la cual la guerra híbrida, la guerra multidominio, la guerra irrestricta y la zona gris funcionan como marcos de organización estratégica. En ese plano, la amenaza deja de ser un hecho puntual y se

convierte en una capacidad de presión continua, distribuida y adaptable. Por esta razón, lo decisivo es que estos marcos permiten combinar instrumentos heterogéneos, sincronizar acciones en distintos dominios y producir efectos políticos sin necesidad de una confrontación abierta o formalmente declarada.

La guerra híbrida aporta la lógica de integración de medios convencionales, irregulares, informacionales y tecnológicos, mientras que la guerra multidominio introduce la simultaneidad de efectos entre espacios físicos y no físicos. A su vez, la guerra irrestricta expande la confrontación hacia ámbitos económicos, legales, tecnológicos y comunicacionales, y la zona gris ofrece el ambiente operativo donde la coerción puede mantenerse por debajo del umbral de la guerra convencional. Por eso, este primer nivel no describe amenazas particulares, sino la arquitectura dentro de la cual esas amenazas se vuelven viables, persistentes y estratégicamente útiles (Freedman, 2013).

Nivel actoral

El segundo nivel corresponde a los actores que explotan ese entorno estructural. La transformación del carácter de la guerra ha reducido la distancia funcional entre actores estatales y no estatales, porque tecnologías comerciales, plataformas digitales, servicios en la nube y sistemas no tripulados de bajo costo han democratizado capacidades antes restringidas a grandes potencias. Esto permite que actores no estatales, *proxies,* redes criminales tecnológicas, redes transnacionales y actores híbridos con acceso a tecnologías duales participen en dinámicas de coerción con efectos estratégicos desproporcionados respecto de sus recursos materiales (Kaldor, 2012).

En el escenario actual los *proxies* siguen siendo particularmente relevantes porque permiten a los Estados proyectar poder con ambigüedad y reducir costos políticos, mientras que las redes criminales tecnológicas combinan financiación ilícita, movilidad transnacional y explotación digital. En contextos como el colombiano, esta convergencia es especialmente sensible porque grupos armados, economías ilegales y herramientas tecnológicas accesibles pueden articularse en formas de presión híbrida que afectan la seguridad, la gobernabilidad y la infraestructura crítica. El resultado es un panorama actoral más fragmentado, flexible y difícil de atribuir, donde la innovación tecnológica incrementa la capacidad de aprendizaje y adaptación de los adversarios (Williams, 2001).

Nivel tecnológico

Amenazas cognitivas e informacionales

Las amenazas cognitivas e informacionales operan sobre la percepción, la interpretación y el juicio, su objetivo no es destruir primero la capacidad física del adversario, sino erosionar su confianza, desorganizar su lectura de la situación y alterar la calidad de sus decisiones. En ese ámbito se ubican la desinformación automatizada, las *deepfakes* estratégicas, la manipulación algorítmica, el *microtargeting* psicológico y las operaciones de influencia. Su peligrosidad no radica solo en su capacidad de mentir, sino en su habilidad para modelar entornos de interpretación y segmentar audiencias con una precisión que antes no existía (Rid, 2020).

La desinformación automatizada aprovecha sistemas de recomendación, *bots* y amplificación algorítmica para saturar el espacio informativo y degradar la distinción entre señal y ruido. Las *deepfakes estratégicas,* por su parte, introducen una amenaza cualitativamente distinta, ya que atacan la confianza en la evidencia visual y auditiva, lo cual puede comprometer el liderazgo, la legitimidad y la cohesión institucional. Por su parte, la manipulación algorítmica y el *microtargeting* psicológico permiten que la influencia deje de ser masiva para volverse personalizada, lo cual posibilita el ajuste de mensajes a perfiles cognitivos, vulnerabilidades emocionales y patrones de comportamiento. En el ámbito militar y estratégico, esta personalización puede dirigirse contra decisores, tropas, la opinión pública o comunidades críticas para la defensa, con el propósito de afectar la moral, la disciplina, la legitimidad o la voluntad política (Zuboff, 2019).

Amenazas cibernéticas

Las amenazas cibernéticas deben ser entendidas como campañas de acceso, permanencia, reconocimiento y explotación, no como simples eventos de intrusión. Las Advanced Persistent Threats (APT), el espionaje digital, el sabotaje a sistemas de C2 (Command and Control) y C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance), la intrusión persistente y los ataques a nube y entornos compartidos constituyen la forma más madura de esta lógica, cuya ventaja principal es que permite mapear la arquitectura del adversario, identificar sus dependencias y preparar efectos estratégicos antes de la confrontación abierta o en paralelo a ella (Singer & Friedman, 2014).

El espionaje digital aporta un conocimiento de sistemas, personas, rutinas y flujos de información, mientras que la intrusión persistente garantiza una permanencia silenciosa. Por otra parte, el sabotaje a C2/C4ISR afecta la capacidad de

mando, control, inteligencia, vigilancia, reconocimiento y sincronización operativa, mientras que los ataques a la nube amplían el alcance del daño, puesto que comprometen arquitecturas compartidas en las que una sola brecha puede propagarse a múltiples sistemas. Estas amenazas son especialmente críticas porque no solo afectan la disponibilidad o confidencialidad, sino que pueden degradar la confianza del mando en sus propios sistemas. Cuando una fuerza duda de la integridad de su red, de sus datos o de su cuadro de situación, la ventaja del adversario aumenta incluso sin destrucción física visible (Libicki, 2009).

Inteligencia artificial avanzada

La inteligencia artificial avanzada añade una capa nueva de vulnerabilidad porque introduce automatización en tareas de evaluación, priorización, reconocimiento y apoyo al mando. Esto incluye la automatización decisional, los ataques adversariales, el *data poisoning,* la manipulación de modelos de Intelligence, Surveillance and Reconnaissance (ISR) y el reconocimiento de objetivos, así como la dependencia de sistemas de recomendación. La amenaza central consiste en que el error puede ser inducido dentro del sistema mismo y luego escalar a decisiones operacionales o estratégicas equivocadas (Russell, 2019).

Específicamente, los ataques adversariales alteran las entradas para inducir salidas falsas, mientras que el *data poisoning* contamina el conjunto de entrenamiento y corrompe el comportamiento del modelo desde su origen. Por otra parte, la manipulación de modelos ISR distorsiona la clasificación de objetos, alertas y patrones, en tanto que la dependencia de sistemas de recomendación puede llevar al mando a adoptar decisiones apoyadas en inferencias opacas o defectuosas. En términos estratégicos, esto significa que el adversario ya no necesita solo destruir sensores o bloquear redes: puede atacar la lógica cognitiva automatizada que organiza la percepción del campo de batalla, lo cual constituye sin duda una vulnerabilidad de primer orden en toda guerra algorítmica (Scharre, 2018).

Sistemas autónomos

Los sistemas autónomos transforman el combate al hacer posible la acción distribuida, escalable y persistente mediante, por ejemplo, enjambres, drones, sistemas no tripulados cooperativos y, en general, mecanismos de saturación del campo de batalla. La amenaza no reside exclusivamente en la plataforma individual, sino en la lógica colectiva que estos sistemas introducen: velocidad, redundancia, dispersión y capacidad de sobrecarga sobre defensas pensadas para amenazas secuenciales o unitarias (Scharre, 2018).

La lógica de enjambre es particularmente desafiante porque reduce la eficacia de la defensa tradicional al multiplicar vectores de aproximación y reducir el costo de la pérdida individual. Los drones permiten vigilancia, ataque, corrección de fuego, engaño y reconocimiento a bajo costo. Por su parte, los sistemas cooperativos añaden coordinación y reparto de funciones, y la saturación resultante obliga al adversario a gastar recursos de alto valor para neutralizar medios relativamente baratos. Esta asimetría económica y operacional explica por qué actores estatales y no estatales encuentran en la autonomía un multiplicador de poder especialmente atractivo (Boulanin & Verbruggen, 2017).

Espectro expandido y redes 5G/6G

Las redes 5G y las futuras 6G deben ser comprendidas como infraestructuras estratégicas de conectividad y no solo como avances comerciales en telecomunicaciones. Así, la disputa por la infraestructura de red, el acceso al espectro como activo estratégico, la dependencia de infraestructura digital externa y la geopolítica tecnológica de redes configuran el nuevo campo de competencia. Su importancia militar radica en que soportan transmisión masiva de datos, sensores distribuidos, coordinación de sistemas autónomos, internet industrial y arquitecturas de decisión basadas en baja latencia (Kania, 2020).

El riesgo estratégico aparece cuando la infraestructura sobre la cual descansa una parte del ecosistema digital nacional depende de proveedores externos, estándares contestados o capas de red vulnerables a interrupción, acceso o manipulación. En ese escenario, la red deja de ser un servicio y se convierte en un multiplicador de poder, pues quien controla la infraestructura, los estándares y los puntos críticos de conectividad puede influir sobre la resiliencia operativa del Estado, sobre la circulación de información y sobre la capacidad de sostener operaciones complejas en contextos de crisis.

Amenazas electromagnéticas

Las amenazas electromagnéticas actúan sobre la capa funcional que conecta comunicaciones, navegación, sensores y sincronización. Específicamente, el *jamming,* el *spoofing,* la negación de comunicaciones y la degradación de sensores y navegación son mecanismos de degradación sistémica que permiten afectar la operatividad militar sin necesidad de destrucción visible. En este terreno, el objetivo no es únicamente cegar al adversario, sino romper la coherencia de su sistema, interrumpir su coordinación y sembrar incertidumbre sobre la fiabilidad de sus señales (Luttwak, 2001).

Específicamente, el *jamming* interfiere la transmisión, mientras que el *spoofing* induce señales falsas que desvían plataformas o alteran posiciones. Por su parte, la negación de comunicaciones aísla unidades y retrasa decisiones, y la degradación de sensores o navegación reduce precisión, conciencia situacional y sincronización. En conjunto, estas amenazas revelan que la guerra contemporánea se libra también en la capa invisible de las funciones, donde una fuerza puede conservar sus plataformas y sin embargo perder la capacidad de emplearlas de manera eficaz (Freedman, 2013).

Tecnologías cuánticas

Las tecnologías cuánticas introducen amenazas disruptivas porque afectan la relación entre el secreto, la detección y la precisión. La ruptura criptográfica es la dimensión más visible, puesto que compromete la seguridad en comunicaciones, claves y datos sensibles; los sensores avanzados prometen mejorar detección y seguimiento; la navegación de precisión puede reducir dependencia de señales tradicionales, y todo ello genera un riesgo directo para la soberanía informacional (Nielsen, 2010).

La importancia estratégica de esta categoría radica en que altera la ecuación de confianza sobre la cual descansan sistemas militares y estatales. En consecuencia, si una arquitectura criptográfica deja de ser segura, la integridad de la información, del mando y de la coordinación queda comprometida. Asimismo, si los sensores cuánticos alteran la relación entre ocultamiento y detección, cambian también las condiciones de supervivencia operativa. Por consiguiente, la cuestión cuántica no debe considerarse futurista en un sentido superficial, sino como una advertencia sobre la necesidad de preparación anticipada en criptografía poscuántica, resiliencia de comunicaciones y soberanía tecnológica (Preskill, 2018).

Dominio espacial

El dominio espacial es hoy una infraestructura funcional del poder militar. La negación satelital, la interferencia orbital, la degradación de Positioning, Navigation, Timing (PNT) / Global Positioning System (GPS) y la pérdida de sincronización y conciencia situacional no son amenazas periféricas, sino que representan una amenaza directa al sistema que sostiene navegación, comunicaciones, alerta, inteligencia y temporalidad operativa. Cuando ese sistema falla, la fuerza no solo pierde precisión, sino que también pierde coherencia y ritmo (Bowen, 2020). La relevancia de esta amenaza crece porque buena parte de la acción militar moderna presupone disponibilidad continua de posicionamiento, tiempo, enlace y

observación, lo cual implica que la negación del dominio espacial obliga a operar con menor precisión, menor sincronización y menor capacidad de integrar efectos entre dominios. De ahí que el espacio no pueda seguir siendo tratado como soporte pasivo, sino que debe entenderse como un dominio de confrontación cuya degradación afecta directamente la eficacia militar en tierra, mar, aire y ciberespacio (Moltz, 2019).

Infraestructura financiera como vector de ataque

La infraestructura financiera se ha convertido en un vector de ataque estratégico porque sostiene la circulación de valor, la financiación de operaciones, la evasión de controles y la resistencia económica. En esta categoría se incluyen la Society for Worldwide Interbank Financial Telecommunication (SWIFT), criptomonedas militarizadas, economía digital de guerra y narcofinanciamiento mediante flujos ilícitos digitalizados. Su relevancia para la seguridad y la defensa aumenta cuando actores armados, criminales o estatales hostiles utilizan estas herramientas para financiar coerción, ocultar transacciones o sortear regímenes de vigilancia (Farrell & Newman, 2019; Garzón, 2020).

En contextos como el colombiano, esta amenaza adquiere una dimensión adicional, puesto que las economías ilícitas ya poseen experiencia en adaptación financiera y, además, la digitalización de esos circuitos puede ampliar su resiliencia, su capacidad de anonimato y su inserción transnacional. La amenaza no consiste solo en "financiarse mejor", sino en sostener estructuras armadas, redes logísticas y operaciones de influencia con menor fricción frente al control estatal. Por ello, la infraestructura financiera debe ser leída como parte del ecosistema de conflicto, no como un problema separado de seguridad económica (Garzón, 2020).

Infraestructura crítica

La infraestructura crítica reúne sistemas sin los cuales el Estado pierde continuidad funcional: energía, telecomunicaciones, transporte, nodos logísticos y redes interdependientes entre el ámbito civil y militar. Estas infraestructuras son objetivos estratégicos porque no solo sostienen la vida económica y social, sino también la capacidad de despliegue, abastecimiento, comunicación y coordinación de la defensa (Perrow, 1999).

Es importante enfatizar que la amenaza adquiere profundidad cuando se entiende su carácter sistémico. Un ataque a la energía afecta las telecomunicaciones, mientras que una interrupción logística compromete la movilidad y el abastecimiento, y una degradación del transporte obstaculiza el despliegue y la respuesta,

factores que, al interactuar con la interdependencia civilmilitar, multiplican el impacto. El resultado es una vulnerabilidad en cascada que permite al adversario obtener efectos estratégicos mediante la afectación de nodos bien seleccionados, en lugar de intentar destruir la totalidad del sistema (Luttwak, 2001).

Bioamenazas habilitadas por inteligencia artificial

Las bioamenazas habilitadas por inteligencia artificial (IA) constituyen una categoría particularmente sensible porque combinan el potencial de la biotecnología con la aceleración analítica de sistemas digitales. De este modo, el diseño de agentes, la bioingeniería acelerada, los riesgos *dual-use* y la convergencia biodigital reducen las barreras de entrada en tareas que antes exigían mayor tiempo, experticia e infraestructura. No obstante, la IA no crea por sí sola el peligro biológico, sino que puede acelerar la búsqueda, la optimización y la simulación de procesos con implicaciones de seguridad (National Academies of Sciences, Engineering, and Medicine, 2018).

Su importancia estratégica reside en que desplaza el problema desde la bioseguridad hacia el terreno de la defensa, en tanto que el riesgo *dual-use* implica que herramientas válidas para investigación legítima pueden, a su vez, facilitar usos maliciosos. Esta circunstancia obliga a pensar en vigilancia tecnológica, inteligencia preventiva, gobernanza científica y articulación entre defensa, salud, ciencia y seguridad, pues esta amenaza evidencia que la convergencia tecnológica no solo cambia la guerra en dominios clásicos, sino que expande el repertorio de riesgo hacia escenarios de alto impacto y difícil atribución (Koblentz, 2020).

Cadena de suministro tecnológica

La amenaza a la cadena de suministros tecnológica es estructural porque compromete la confianza en el origen y la integridad de los componentes sobre los cuales descansa la capacidad militar. *Hardware* comprometido, *software* vulnerable, la dependencia de semiconductores y el sabotaje estructural no son incidentes aislados, sino vectores mediante los cuales un adversario puede introducir vulnerabilidades desde etapas previas al despliegue operacional (Lewis, 2021).

Esta amenaza es grave porque opera antes del combate y, en muchos casos, sin ser detectada: un componente alterado, una actualización comprometida o una dependencia excesiva de proveedores críticos pueden introducir fallas sistémicas en comunicaciones, sensores, plataformas o capacidades de procesamiento. Por ello, la cadena de suministro se convierte en un frente de seguridad nacional y de defensa, ya que la autonomía estratégica depende también de saber

de dónde vienen, cómo se verifican y quién controla los insumos críticos del poder militar (Defense Critical Supply Chain Task Force, 2021).

Datos y ecosistema digital

Los datos y el ecosistema digital constituyen un terreno central de poder porque de ellos depende la construcción del conocimiento estratégico. La explotación de *big data,* la manipulación de *datasets,* el robo de datos estratégicos y el control del conocimiento del adversario son, en efecto, las dinámicas que transforman la información en un recurso de combate. La amenaza no reside únicamente en la pérdida de secretos, sino en la posibilidad de que el adversario adquiera una imagen de la realidad más completa, más rápida o más susceptible de manipulación que la que posee la propia organización (Kitchin, 2014).

Por ejemplo, cuando los *datasets* alimentan sistemas de inteligencia artificial, ISR o apoyo al mando, su manipulación puede alterar no solo el conocimiento disponible, sino también la forma en que este se traduce en decisión. En este sentido, el dato deja de ser un mero archivo para convertirse en infraestructura cognitiva del poder. Quien controla, corrompe o captura este flujo de conocimiento adquiere una ventaja que puede ser decisiva, incluso sin necesidad de superioridad cinética inmediata (Mayer-Schönberger, 2013).

Amenaza interna aumentada por inteligencia artificial

La IA amplifica un riesgo clásico de seguridad: el *insider threat*. Concretamente, lo que cambia es la escala, la velocidad y la capacidad de explotación de este riesgo. Un actor interno con acceso legítimo puede utilizar herramientas de IA para identificar vulnerabilidades, clasificar información sensible, automatizar filtraciones o modelar patrones de seguridad de forma mucho más eficiente que en el pasado (Greitzer, 2014).

Esta categoría merece especial atención en organizaciones militares, puesto que el daño potencial no se limita al robo de información, sino que la explotación asistida por IA desde dentro puede facilitar sabotaje, reconocimiento interno, extracción masiva de datos y preparación de accesos persistentes para terceros. En instituciones complejas, donde la confianza organizacional es indispensable, esta amenaza es especialmente delicada porque combina acceso, legitimidad aparente y capacidad de daño multiplicada por herramientas avanzadas (Shaw, 2015).

Características sistémicas de las amenazas

Las amenazas emergentes comparten seis características que explican por qué no pueden abordarse con enfoques fragmentados: simultaneidad, convergencia, ambigüedad, persistencia, baja atribución y alta velocidad. La simultaneidad significa que varias amenazas pueden operar al mismo tiempo sobre distintos subsistemas, y la convergencia indica que suelen combinarse entre sí. Además, la ambigüedad y la baja atribución dificultan la respuesta, mientras que la persistencia impide tratarlas como episodios aislados. Finalmente, la alta velocidad comprime el tiempo de reacción del Estado y de las Fuerzas Militares (Gray, 2015).

Estas características muestran que el mapa de amenazas no debe interpretarse como un inventario, sino como la representación de un entorno estratégico interdependiente. La importancia del análisis reside, precisamente, en identificar cómo estas amenazas funcionan, qué explotan y qué efectos producen sobre el mando y control, la información, la infraestructura, la legitimidad, la soberanía tecnológica y la capacidad de decisión. Solo a partir de esta comprensión integrada es posible avanzar al siguiente nivel del capítulo, el cual consiste en explicar cómo dichas amenazas generan nuevas formas de hacer la guerra y qué capacidades militares deben fortalecerse para enfrentarlas con eficacia estratégica (Freedman, 2013).

Las amenazas emergentes analizadas se configuran como componentes de una arquitectura de coerción sistémica en la cual distintos vectores tecnológicos operan sobre vulnerabilidades estructurales del Estado y de las Fuerzas Militares. En este entorno, la competencia estratégica se organiza en torno al control de funciones críticas del sistema —percepción, información, sincronización, operación y financiamiento—, lo cual configura un espacio de confrontación donde la capacidad de acción depende de la integridad de dichas funciones. La tabla 1 sintetiza esta lógica articulando dominios de competencia, objetos de control y efectos sobre el centro de gravedad.

Tabla 1. *Arquitectura de coerción sistémica en la guerra contemporánea*

Dominio de competencia estratégica	Vector tecnológico	Objeto de control	Mecanismo de coerción	Vulnerabilidad estructural	Impacto sobre el centro de gravedad
Cognitivo	IA, plataformas y algoritmos.	Percepción y voluntad.	Manipulación informacional.	Confianza social.	Desarticulación de la legitimidad.
Informacional	*Big data*, ISR y redes.	Conocimiento del entorno.	Control y distorsión del dato.	Integridad informacional.	Superioridad decisional.

Dominio de competencia estratégica	Vector tecnológico	Objeto de control	Mecanismo de coerción	Vulnerabilidad estructural	Impacto sobre el centro de gravedad
Sistémico-digital	Ciber, *software* y redes.	Funcionamiento del sistema.	Infiltración y degradación.	Interdependencia tecnológica.	Disrupción operativa.
Electromagnético	Espectro y señales.	Sincronización operativa.	Negación y engaño.	Dependencia de señales.	Descoordinación táctica.
Espacial	Satélites y PNT.	Orientación y tiempo.	Interferencia y negación.	Infraestructura orbital.	Pérdida de conciencia situacional.
Autónomo	Drones y enjambres.	Capacidad de respuesta.	Saturación distribuida.	Rigidez defensiva.	Sobrecarga del sistema.
Financiero	SWIFT y cripto.	Flujos económicos.	Exclusión / evasión.	Interdependencia financiera.	Coerción económica estratégica.
Infraestructural	Energía y telecomunicaciones.	Funcionalidad estatal.	Interrupción sistémica.	Interconectividad crítica.	Colapso parcial del Estado.
Biotecnológico	IA +bioingeniería.	Seguridad biológica.	Optimización de agentes.	Regulación limitada.	Riesgo estratégico ampliado.
Interno	IA + insider.	Integridad organizacional.	Explotación interna.	Confianza institucional.	Compromiso estructural.

Fuente: Elaboración propia.

La tabla 1 evidencia que la guerra contemporánea se estructura como una disputa por el control de sistemas interdependientes, en la cual cada dominio representa una capa funcional cuya alteración incide directamente sobre la capacidad de decisión, coordinación y ejecución del adversario. La convergencia de estos dominios habilita mecanismos de coerción acumulativa que operan mediante la degradación progresiva de la coherencia sistémica, lo que desplaza el centro de gravedad hacia la integridad de los procesos que sostienen la acción estratégica. En este sentido, la ventaja no se deriva exclusivamente de la superioridad material, sino del control efectivo sobre dichas funciones críticas, lo cual posiciona la resiliencia, la adaptación y la protección sistémica como condiciones estructurales de la defensa nacional.

De las amenazas a las nuevas formas de guerra

Como se ha señalado a lo largo del capítulo, la mutación decisiva de la guerra contemporánea no proviene de la simple acumulación de amenazas emergentes, sino de la forma en que estas se acoplan dentro de arquitecturas tecnológicas,

organizacionales y cognitivas que alteran la producción del poder militar. Así, cuando datos, sensores, plataformas, redes, algoritmos y sistemas de mando interactúan en tiempo real, el conflicto deja de organizarse alrededor del choque directo entre fuerzas y pasa a estructurarse en torno al control de procesos: percibir antes, interpretar mejor, decidir con mayor coherencia y actuar con menor latencia. En ese punto, la amenaza ya no puede leerse como un incidente autónomo, porque su efecto depende de la posición que ocupa dentro del sistema total de combate. Esa es la razón por la cual el mapa de amenazas solo adquiere pleno sentido cuando se traduce en nuevas formas de guerra. La convergencia tecnológica reordena la gramática del conflicto y desplaza el centro de gravedad hacia la integridad del sistema decisional y la estabilidad funcional de las redes que sostienen la acción militar.

Esta transición obliga a hacer un cambio metodológico en el análisis estratégico: la pregunta central ya no es únicamente qué amenaza existe, sino cómo varias amenazas se integran para producir una forma específica de coerción. Una amenaza cibernética aislada puede comprometer una red; una algorítmica, degradar una clasificación, y una campaña de influencia, afectar percepciones. Sin embargo, cuando estas tres capas convergen sobre el mismo ecosistema militar, el efecto resultante es cualitativamente distinto, pues se degrada la conciencia situacional, se contamina la recomendación operativa, se introduce duda en la decisión y se erosiona la confianza del mando en su propio sistema. En términos estratégicos, la novedad no reside en la herramienta individual, sino en la capacidad de ensamblar amenazas heterogéneas en secuencias funcionales que modifican la lógica del combate y de la conducción operacional (Bousquet, 2009).

Ejemplos de convergencia

La primera convergencia decisiva vincula la inteligencia artificial y los datos, de la cual emerge la guerra algorítmica. Esta forma de guerra se manifiesta cuando los procesos de detección, clasificación, priorización y recomendación pasan a depender de modelos que transforman grandes volúmenes de datos en decisiones operativamente significativas. En el plano militar, esto afecta directamente la arquitectura ISR, la selección de objetivos, la asignación de recursos y la construcción del cuadro de situación, pues el punto crítico radica en que el sistema decisional se vuelve dependiente de la calidad del dato, de la robustez del modelo y de la integridad del proceso de inferencia. Cuando un adversario manipula datos de entrada, contamina conjuntos de entrenamiento o fuerza salidas erróneas mediante perturbaciones adversariales, no está atacando un sensor aislado, sino que está atacando la lógica de producción del conocimiento operacional. La guerra

algorítmica se define, por tanto, por la disputa sobre la cadena completa que transforma información en decisión militar (Russell, 2019).

La segunda convergencia articula las redes digitales, la infraestructura crítica y la dependencia tecnológica, de cuya interacción emerge la guerra de sistemas. Esta forma de guerra se produce cuando la capacidad de combate depende de una arquitectura interconectada donde comunicaciones, logística, datos, navegación, mando y control y soporte energético funcionan como subsistemas acoplados. En ese entorno, la destrucción física de una plataforma puede ser menos decisiva que la degradación de la red que la conecta, del software que la coordina o del nodo logístico que la sostiene. La guerra de sistemas explota precisamente esa condición: identifica dependencias críticas, ataca nodos de alto valor funcional y provoca efectos en cascada que degradan la coherencia del conjunto. Su lógica central consiste en desorganizar la arquitectura operativa del adversario hasta el punto en que este conserve medios materiales, pero pierda la capacidad de emplearlos de forma sincronizada, confiable y eficaz (Luttwak, 2001).

La tercera convergencia reúne desinformación, personalización algorítmica y explotación de datos conductuales, lo cual da origen a una forma más sofisticada de guerra cognitiva. Esta se distingue porque la influencia deja de ser masiva y se vuelve precisa, adaptativa y persistente. El objetivo ya no consiste en difundir mensajes engañosos, sino en intervenir sobre los mecanismos mediante los cuales una audiencia específica interpreta la realidad, jerarquiza riesgos y decide cómo actuar. En el ámbito militar y estratégico, esta intervención puede afectar la moral, la percepción de legitimidad, la confianza en el mando y la disposición a sostener el esfuerzo operacional. De este modo, la guerra cognitiva aumentada adquiere una profundidad inédita, puesto que opera sobre la arquitectura psicológica y social de la decisión, valiéndose de plataformas digitales, analítica de comportamiento y segmentación de alta precisión para modular voluntades en tiempo real (Rid, 2020).

La cuarta convergencia, que amalgama capacidades cuánticas, intrusión cibernética y arquitectura de mando y control, propicia una lucha por la superioridad informacional. Esta forma de guerra emerge cuando la ventaja depende de preservar la confidencialidad, la integridad, la disponibilidad y la autenticidad de los flujos de información que nutren al mando. En este contexto, la dimensión cuántica amenaza la seguridad criptográfica, mientras que la dimensión cibernética amplía la capacidad de acceso, manipulación e interrupción, en tanto que la dimensión C2 convierte cualquier alteración de la información en una perturbación inmediata

del proceso de conducción. El resultado es una competencia por dominar el ciclo informacional completo: quién protege mejor sus redes, quién niega mejor las del adversario y quién conserva la capacidad de decidir en condiciones de incertidumbre inducida. La superioridad informacional no se reduce a poseer más datos, sino que consiste en sostener un ecosistema de decisión confiable mientras se degrada el del contrario (Dowling & Milburn, 2003).

La consecuencia estratégica de estas convergencias es inequívoca: la tecnología reconfigura la forma de hacer la guerra porque reorganiza la relación entre percepción, decisión, coordinación y poder. Por lo tanto, el conflicto ya no puede analizarse como una suma de amenazas técnicas separadas, sino que cada amenaza adquiere densidad estratégica cuando se integra en una secuencia funcional que altera la arquitectura del combate. De ahí que las nuevas formas de guerra no deban ser entendidas como etiquetas conceptuales, sino como manifestaciones operativas de una mutación profunda en el carácter de la guerra. Cuando el dato estructura la decisión, la red sostiene la maniobra, la influencia modela la voluntad y la velocidad comprime el tiempo de respuesta, la guerra cambia de forma objetiva y verificable (Freedman, 2013).

Ese cambio tiene una implicación inmediata para la defensa: las capacidades militares tradicionales resultan insuficientes cuando no incluyen resiliencia sistémica, superioridad informacional, protección cognitiva, gobernanza del dato, robustez algorítmica y seguridad de la arquitectura C2. La transición desde las amenazas hacia las nuevas formas de guerra establece, por tanto, el fundamento lógico de la siguiente sección del capítulo, pues el problema ya no es describir tecnologías emergentes, sino identificar qué tipo de fuerza militar puede sobrevivir, comprender y dominar un conflicto organizado alrededor de sistemas complejos, decisiones aceleradas y vulnerabilidades integradas.

Las convergencias descritas no deben interpretarse como agregaciones tecnológicas, sino como configuraciones funcionales que alteran componentes críticos del poder militar. De este modo, la interacción entre datos, redes, algoritmos y arquitecturas de mando produce efectos diferenciados según la función que se ve comprometida: percepción, conocimiento, decisión, coordinación o control. La tabla 2 sintetiza esta lógica al vincular convergencias tecnológicas con funciones militares específicas, formas de guerra emergentes y resultados estratégicos asociados.

Tabla 2. *Convergencias tecnológicas y mutación funcional del poder militar*

Convergencia tecnológica dominante	Función militar alterada	Forma de guerra emergente	Resultado estratégico
IA + datos + modelos de inferencia.	Producción de conocimiento operacional y decisión.	Guerra algorítmica.	Vulneración del juicio militar y pérdida de confiabilidad decisional.
Redes + infraestructura crítica + dependencia tecnológica.	Coherencia funcional del sistema de combate.	Guerra de sistemas.	Desorganización operativa y pérdida de capacidad de empleo sincronizado.
Desinformación + personalización algorítmica + datos conductuales.	Percepción, legitimidad y voluntad.	Guerra cognitiva aumentada.	Erosión de cohesión, confianza y sostenimiento del esfuerzo estratégico.
Ciber + capacidades cuánticas + arquitectura C2/C4ISR.	Integridad del ciclo informacional y del mando.	Guerra por la superioridad informacional.	Degradación del control, incertidumbre inducida y ruptura del proceso de conducción.

Fuente: Elaboración propia.

La tabla 2 muestra que la transformación del conflicto contemporáneo se produce a través de la alteración selectiva de funciones críticas del sistema militar, más que mediante la destrucción directa de capacidades físicas; de hecho, cada convergencia tecnológica incide sobre una dimensión específica del poder —conocimiento, decisión, cohesión o control— y genera formas de guerra que operan sobre la coherencia del sistema en su conjunto. Esta dinámica permite ejercer coerción mediante la degradación progresiva de la capacidad de comprender, decidir y actuar, lo que desplaza el centro de gravedad hacia la integridad funcional del sistema y establece la resiliencia como condición determinante de la superioridad estratégica.

Nuevas formas de hacer la guerra en el entorno tecnológico

Guerra algorítmica

La guerra algorítmica se configura cuando la arquitectura decisional militar se estructura alrededor de sistemas que transforman datos en inferencias operacionales mediante modelos de IA. En este entorno, los sensores ISR, los sistemas de vigilancia, las plataformas de reconocimiento y las redes de información alimentan modelos que clasifican objetivos, priorizan amenazas y sugieren cursos de acción. La decisión no desaparece del ámbito humano, pero queda mediada por una capa

algorítmica que organiza la percepción del entorno operacional, lo cual condiciona la forma en que el mando interpreta la situación y actúa sobre ella (Russell, 2019).

El mecanismo crítico reside en la integridad de la cadena datomodelo-decisión. Cuando un adversario interviene en esa cadena mediante manipulación de datos, ataques adversariales o contaminación de conjuntos de entrenamiento, introduce errores estructurales en el proceso de inferencia; estos errores no son evidentes, porque se presentan como salidas plausibles dentro del sistema. En términos operacionales, esto puede traducirse en una identificación incorrecta de objetivos, una priorización errónea de amenazas o una asignación ineficiente de recursos. La guerra algorítmica, por tanto, desplaza el combate hacia el control de la lógica que convierte información en decisión, lo cual hace que la confiabilidad del sistema decisional sea un objetivo estratégico central (Scharre, 2018).

Guerra de datos

La guerra de datos emerge cuando el valor estratégico se concentra en la capacidad de capturar, procesar y explotar información para construir superioridad cognitiva sobre el adversario. En las arquitecturas militares contemporáneas, el dato alimenta inteligencia, planificación, *targeting* y evaluación de efectos. Esta acumulación de datos permite modelar patrones de comportamiento, anticipar movimientos y reducir la incertidumbre en la toma de decisiones, con lo cual el dato se erige como un recurso operativo equivalente a la maniobra o al fuego (Kitchin, 2014).

El mecanismo de esta forma de guerra consiste en controlar el ciclo completo del dato: recolección, almacenamiento, procesamiento, análisis y explotación. De este modo, un actor que logra acceder a los datos del adversario puede reconstruir su lógica operativa, mientras que la manipulación de *datasets* puede distorsionar la imagen que el adversario tiene de la realidad. Esta doble capacidad, que implica conocer al otro y hacer que este se equivoque, convierte al dato en un instrumento de poder decisional. Por consiguiente, la guerra de datos no busca únicamente información, sino que aspira a controlar el conocimiento que estructura la acción militar del adversario (Mayer-Schönberger, 2013).

Guerra cognitiva aumentada

Se produce cuando las capacidades tecnológicas permiten intervenir de manera sistemática sobre los procesos mentales que sostienen la decisión individual y colectiva. Mediante plataformas digitales, analítica de comportamiento y segmentación avanzada, es posible diseñar operaciones de influencia dirigidas a públicos específicos, ajustando mensajes a sus patrones cognitivos, emocionales y

sociales. Esta dinámica transforma la información en un instrumento de intervención directa sobre la voluntad (Rid, 2020).

El mecanismo operativo se centra en la construcción y la explotación de vulnerabilidades cognitivas. Mediante el uso de datos conductuales, algoritmos de recomendación y microsegmentación, se pueden introducir narrativas diseñadas para reforzar percepciones erróneas, generar desconfianza o fragmentar la cohesión. En el ámbito militar, esto puede afectar la moral de las tropas, la confianza en el mando o la legitimidad de la operación. La guerra cognitiva aumentada no busca únicamente influir, busca reconfigurar la forma en que el adversario interpreta la realidad, lo que altera la calidad de su decisión estratégica (Zuboff, 2019).

Guerra de sistemas

La guerra de sistemas se caracteriza por dirigir la acción ofensiva contra la arquitectura funcional que sostiene la capacidad militar del adversario, la cual incluye mando y control, sistemas de información, logística, comunicaciones e infraestructura crítica, todos ellos integrados en redes interdependientes. En este contexto, la eficacia militar depende de la coherencia del sistema más que de la potencia individual de sus componentes (Luttwak, 2001).

La operación consiste en identificar y atacar nodos críticos dentro de esa arquitectura para generar efectos en cascada. La degradación de las comunicaciones afecta la coordinación, la alteración de los sistemas de información distorsiona la conciencia situacional y la interrupción logística limita la capacidad de sostenimiento. Estos efectos no se manifiestan como destrucción inmediata, sino como desorganización progresiva del sistema. Este proceso culmina en un colapso funcional en el que la fuerza conserva sus medios, pero pierde la capacidad de emplearlos de manera sincronizada y efectiva, lo cual redefine la noción de derrota en términos de desintegración operativa (Freedman, 2013).

Guerra distribuida

La guerra distribuida surge cuando la capacidad de combate se organiza en una red de nodos autónomos, interconectados y capaces de operar de manera coordinada sin depender de un centro único de control. Esta lógica se apoya en sistemas no tripulados, enjambres, unidades con autonomía táctica y estructuras organizacionales flexibles que permiten actuar simultáneamente en múltiples puntos del espacio operacional (Scharre, 2018).

El mecanismo de operación se basa en la dispersión, la redundancia y la adaptabilidad. La distribución de capacidades reduce la vulnerabilidad frente a ataques

concentrados, puesto que la pérdida de un nodo no compromete el conjunto. Al mismo tiempo, la coordinación entre nodos permite generar efectos acumulativos sin necesidad de concentración física. Sin embargo, el riesgo estratégico radica en la disolución de los centros tradicionales de gravedad, un fenómeno que no solo dificulta la identificación de un punto decisivo, sino que también impone la necesidad de replantear la lógica de la maniobra y la defensa.

Guerra persistente

La guerra persistente se define por la continuidad del conflicto en el tiempo, sin una delimitación clara entre guerra y paz. En este entorno, las acciones se desarrollan de manera constante mediante operaciones cibernéticas, informacionales, económicas y tecnológicas que mantienen presión sobre el adversario sin alcanzar niveles de confrontación abierta.

El mecanismo estratégico consiste en sostener una dinámica de desgaste continuo que afecta recursos, atención y voluntad. La ausencia de un punto de inicio o final claro dificulta la movilización y la respuesta, lo cual obliga al adversario a operar en un estado permanente de alerta. Este tipo de guerra transforma la temporalidad del conflicto, donde la ventaja no depende de una victoria decisiva, sino de la capacidad de resistir, adaptarse y sostener la presión en el largo plazo.

Guerra de velocidad

La guerra de velocidad se configura cuando la ventaja estratégica depende de la capacidad de reducir el tiempo entre la detección, la decisión y la acción, ya que la integración de sensores, el procesamiento de datos y la automatización permiten acortar el ciclo decisional, lo que genera una ventaja crítica en entornos donde la rapidez determina la eficacia (Virilio, 2006).

El mecanismo central es la compresión del tiempo operativo, pues a medida que el ciclo decisional se acelera, el margen para la deliberación se reduce, lo cual incrementa la dependencia de sistemas automatizados y procesos preconfigurados. Esta dinámica, sin embargo, introduce un riesgo estructural inherente: la posibilidad de errores amplificados por la velocidad. Así, un sistema que no logra mantener coherencia bajo presión temporal puede fallar incluso sin intervención directa del adversario. En este contexto, la guerra de velocidad convierte el tiempo en un recurso estratégico, de manera que dominar la latencia del sistema equivale a dominar el ritmo del conflicto (Strachan, 2008).

Guerra de dependencia tecnológica

Surge cuando el control de plataformas, infraestructura digital, semiconductores, *software* y estándares tecnológicos determina la capacidad operativa de un actor, lo cual implica que en este entorno la dependencia de sistemas externos introduce vulnerabilidades que pueden ser explotadas mediante acceso, restricción o manipulación (Segal, 2016).

El mecanismo estratégico consiste en controlar los puntos críticos de la arquitectura tecnológica, lo que incluye el acceso a redes, el suministro de componentes, la gobernanza de estándares y la dependencia de plataformas digitales. Un actor que controla estos elementos puede condicionar la capacidad operativa del adversario sin recurrir a la confrontación directa, lo cual conlleva el riesgo de una dominación sin combate abierto, donde la dependencia tecnológica se convierte en una forma de coerción estructural que limita la autonomía estratégica y redefine las condiciones del poder en la guerra contemporánea (Farrell & Newman, 2019).

Las formas contemporáneas de guerra expresan configuraciones específicas del poder militar, las cuales derivan de la convergencia entre amenazas tecnológicas, estructuras operativas y procesos decisionales. Cada una de estas configuraciones emerge cuando determinados vectores tecnológicos alteran funciones críticas del sistema —como la producción de conocimiento, la conducción, la coordinación o la legitimidad— y obligan a una reconfiguración simultánea de capacidades, doctrina y pensamiento militar. La tabla 3 sintetiza esta relación al articular amenazas habilitantes con las exigencias operativas, doctrinales y cognitivas que definen la adaptación estratégica en entornos de conflicto tecnológicamente mediado.

Tabla 3. *Arquitectura funcional de las formas contemporáneas de guerra y su traducción en capacidades, doctrina y mente militar*

Forma de guerra	Amenazas que la habilitan	Capacidad militar requerida	Implicación doctrinal	Implicación cognitiva
Guerra algorítmica	IA avanzada, *data poisoning,* manipulación de modelos ISR y automatización decisional.	Arquitectura de IA operacional certificada, *pipelines* de datos auditables, validación cruzada humano-máquina en C2, resiliencia algorítmica en ISR y *targeting.*	Doctrina de integración humano-máquina en combate, control humano significativo en sistemas autónomos y gobernanza de IA militar.	Pensamiento probabilístico, interpretación de modelos y juicio crítico frente a inferencias algorítmicas.

Forma de guerra	Amenazas que la habilitan	Capacidad militar requerida	Implicación doctrinal	Implicación cognitiva
Guerra de datos	*Big data* y *datasets* manipulados, robo de datos estratégicos y explotación masiva de información.	Arquitectura de superioridad informacional, gobernanza del ciclo del dato, fusión ISR- datos-decisión, protección de integridad y trazabilidad de datos.	*Data-centric warfare,* integración estructural del dato en C2 y doctrina de dominio informacional.	Pensamiento analítico avanzado, capacidad de inferencia y lectura crítica de datos complejos.
Guerra cognitiva aumentada	Desinformación automatizada, *deepfakes, microtargeting* y manipulación algorítmica.	Arquitectura de defensa cognitiva, capacidades de contrainfluencia e integración de operaciones informacionales en C2.	Doctrina de operaciones en el dominio cognitivo, protección de legitimidad y cohesión institucional.	Pensamiento crítico estructurado, resiliencia cognitiva y capacidad de identificar la manipulación.
Guerra de sistemas	Ciberataques, guerra electromagnética, infraestructura crítica y cadena de suministro comprometida	Arquitectura C2 resiliente, redundancia multidominio, continuidad operativa bajo degradación y protección de infraestructura crítica.	Doctrina de operaciones en sistemas complejos, combate en entornos degradados e integración multidominio real.	Pensamiento sistémico, comprensión de interdependencias, análisis estructural del combate.
Guerra distribuida	Enjambres, drones, sistemas autónomos, nodos descentralizados	Capacidad de mando distribuido, coordinación de nodos autónomos y arquitectura de control descentralizado con coherencia operativa.	Doctrina de *mission command* en entornos tecnológicos, descentralización del mando y operaciones nodales.	Adaptabilidad operativa, iniciativa táctica y toma de decisiones descentralizada.
Guerra persistente	Zona gris, guerra híbrida, *proxies* y presión continua multidominio.	Capacidad de operación permanente, sostenimiento estratégico prolongado y resiliencia institucional y organizacional.	Doctrina de competencia continua, estrategia prolongada y gestión de conflicto persistente.	Resiliencia estratégica, disciplina operativa, y capacidad de actuar en ambigüedad.
Guerra de velocidad	IA, sensores avanzados, automatización y fusión de datos en tiempo real.	Arquitectura de decisión acelerada, integración ISR-C2-efectores y reducción de latencia operativa.	Doctrina de aceleración decisional, ciclos OODA comprimidos y dominio del tiempo operacional.	Intuición estratégica, toma de decisiones bajo presión temporal y pensamiento en entornos dinámicos.
Guerra de dependencia tecnológica	5G/6G, semiconductores, plataformas digitales, estándares tecnológicos y tecnologías cuánticas.	Soberanía tecnológica, control de infraestructura crítica digital y autonomía en componentes estratégicos.	Doctrina de seguridad tecnológica, independencia estratégica y control de ecosistemas tecnológicos.	Pensamiento estratégico-tecnológico y comprensión de dependencias estructurales.

Fuente: Elaboración propia.

La organización del análisis en bloques responde a la necesidad de identificar configuraciones funcionales de convergencia en las que distintas formas de guerra interactúan sobre funciones críticas del sistema militar. Estas configuraciones, lejos de operar de manera aislada, producen efectos estratégicos al alterar simultáneamente conocimiento, percepción, coordinación y decisión, lo cual desplaza el centro de gravedad hacia la integridad del sistema. De esta manera, el análisis por bloques permite capturar cómo se reconfigura el poder en la guerra contemporánea a través del control de dichas funciones.

Bloque 1: guerra algorítmica + guerra de datos

La convergencia entre guerra algorítmica y guerra de datos reconfigura la producción del poder militar porque desplaza la superioridad hacia el control del ciclo que transforma los datos en decisión. En este nuevo escenario, el dato deja de operar como insumo y se convierte en elemento estructurante del conocimiento operacional, integrado en arquitecturas donde la IA organiza la percepción, prioriza la información y orienta la acción. En este contexto, la arquitectura ISR se extiende hacia procesos de inferencia y decisión, lo cual convierte la integridad del dato y la robustez del modelo en condiciones críticas del mando (Russell, 2019).

La disputa estratégica se traslada hacia el control de ese ciclo: quien controla los datos, los modelos y los procesos de inferencia controla la producción del conocimiento y, por extensión, la decisión militar. Específicamente, la manipulación de *datasets* o la degradación de modelos no genera fallas técnicas aisladas, sino que introduce distorsiones sistemáticas en la lectura del entorno que afectan la asignación de recursos, la priorización de objetivos y la conducción operacional. Así, la guerra se estructura como una competencia por dominar la arquitectura que convierte la información en acción, lo cual exige gobernanza del dato, validación algorítmica y resiliencia del sistema decisional (Kitchin, 2014).

Bloque 2: guerra cognitiva aumentada + guerra de sistemas

La interacción entre guerra cognitiva aumentada y guerra de sistemas desplaza el objetivo del conflicto hacia el control simultáneo de la percepción y del funcionamiento del adversario. La dimensión cognitiva interviene la forma como se interpreta la realidad, mientras que la dimensión sistémica afecta la capacidad de actuar sobre ella, lo cual genera un efecto acumulativo que compromete la coherencia del sistema militar (Rid, 2020).

La afectación estratégica no se limita al daño físico, sino que se expresa en la pérdida de confianza en los sistemas que sostienen la acción. Un sistema degradado,

una red comprometida o una infraestructura afectada producen incertidumbre, que se amplifica cuando la información también es manipulada. De este modo, la convergencia de ambas dimensiones permite erosionar simultáneamente la comprensión y la ejecución, lo que altera la capacidad de decisión en su núcleo. En este entorno, la doctrina debe integrar operaciones informacionales, cibernéticas y convencionales, mientras la mente militar debe operar en condiciones de incertidumbre inducida y mantener coherencia en sistemas degradados (Freedman, 2013).

Bloque 3: guerra distribuida + guerra persistente + guerra de velocidad

La convergencia entre guerra distribuida, persistente y de velocidad introduce una presión estructural sobre las formas tradicionales de organización militar. Esta presión surge porque se elimina la centralidad de nodos únicos, se disuelve la secuencialidad del conflicto y se comprime el tiempo decisional. La ventaja estratégica se desplaza hacia organizaciones capaces de coordinar nodos distribuidos, sostener operaciones continuas y decidir en ciclos temporales reducidos (Mazarr, 2015).

Dado que este entorno reconfigura la lógica del mando, la coherencia ya no puede sostenerse mediante un control centralizado, sino que debe construirse a partir de principios compartidos y de una capacidad de adaptación local. La combinación de dispersión, persistencia y velocidad transforma la guerra en una dinámica continua donde la capacidad de adaptación, la sincronización flexible y la resiliencia organizacional determinan la eficacia operativa. Como consecuencia, la superioridad se define por la capacidad de operar con información incompleta y decidir bajo presión temporal (Gray, 2015).

Bloque 4: guerra de dependencia tecnológica

La guerra de dependencia tecnológica introduce una dimensión estructural del conflicto, en la que el control de la infraestructura tecnológica condiciona la capacidad de acción militar. En este marco, elementos cruciales como las redes, los semiconductores, las plataformas y los estándares no solo constituyen la base operativa, sino que su control define los límites reales del poder (Farrell & Newman, 2019).

De esta manera, la disputa estratégica se traslada hacia el control de las condiciones tecnológicas que hacen posible la guerra, dado que la dependencia introduce vulnerabilidades explotables mediante restricción de acceso, manipulación o interrupción de sistemas críticos. En consecuencia, la capacidad de combate ya no depende exclusivamente de los medios disponibles, sino también de la autonomía

para sostenerlos. Bajo este prisma, la seguridad tecnológica se convierte en un componente central de la defensa, por lo que la mente militar debe incorporar una comprensión estratégica de la tecnología como estructura de poder (Segal, 2016).

Escenario prospectivo 2035: configuración de la guerra en entornos de coerción sistémica

El horizonte 2035 opera como una referencia de maduración sistémica que permite proyectar la configuración del conflicto cuando las dinámicas analizadas —convergencia tecnológica, integración multidominio y coerción sobre funciones críticas— alcanzan un nivel de consolidación estructural. Cabe señalar que esta sección no busca anticipar una fecha, sino modelar la lógica de la guerra cuando estas capacidades operan de forma integrada, simultánea y sostenida, lo cual define un entorno en el que el poder se ejerce sobre sistemas, datos, decisión y percepción.

Escenario base de confrontación híbrida sistémica

Hacia 2035, el entorno regional se configura como un sistema de confrontación híbrida persistente en el que múltiples actores compiten simultáneamente sobre la arquitectura funcional del Estado: actores estatales, *proxies* y organizaciones no estatales operan con acceso a tecnologías avanzadas y, en consecuencia, generan un espacio de conflicto distribuido, ambiguo y de intensidad variable. La confrontación se manifiesta como presión continua sobre sistemas de información, procesos decisionales, infraestructuras críticas y percepción social, lo cual desplaza el centro de gravedad hacia la integridad funcional del sistema y su capacidad de sostener coherencia bajo perturbación (Gray, 2015).

La arquitectura operacional militar se define por la interdependencia entre sistemas ISR, redes de mando y control, plataformas digitales y capacidades automatizadas. Dentro de este marco, la IA estructura la producción de conocimiento operacional y condiciona la decisión, mientras que las capacidades cibernéticas habilitan acceso persistente, reconocimiento encubierto y degradación selectiva de sistemas críticos. Asimismo, los drones y sistemas autónomos amplían la vigilancia y la acción distribuida, mientras que las operaciones de desinformación de precisión intervienen sobre la percepción, la legitimidad y la cohesión social. Todos estos elementos, junto con la presión económica —articulada mediante circuitos financieros digitales y disrupciones logísticas—, completan un esquema de coerción multidimensional que actúa de manera simultánea sobre el sistema estatal.

Variables geopolíticas estructurales de la competencia tecnológica

La consolidación de una geopolítica tecnológica basada en el control de estándares, infraestructuras digitales y cadenas de suministro críticas define la estructura de la competencia internacional hacia 2035. La disputa por redes 5G/6G, servicios de nube, semiconductores, IA y capacidades cuánticas configura un entorno donde el acceso y el control de estos sistemas determina la posición relativa de los Estados y condiciona su capacidad de acción estratégica. Los conflictos regionales se insertan en esta arquitectura global, donde la defensa depende del grado de integración o dependencia respecto a ecosistemas tecnológicos dominados por actores externos (Segal, 2016).

La dependencia estructural de infraestructuras digitales introduce vulnerabilidades sistémicas, asociadas al uso de arquitecturas no soberanas en comunicaciones, almacenamiento de datos, plataformas de gestión y redes críticas, las cuales habilitan mecanismos de acceso, restricción y manipulación que afectan la continuidad operativa y la integridad funcional del sistema estatal. La fragmentación regional limita la coordinación estratégica, reduce la capacidad de respuesta conjunta y amplía el margen de acción de actores oportunistas en entornos de competencia distribuida. La democratización tecnológica amplía el acceso a drones, capacidades de intrusión digital, IA comercial y mecanismos de financiación digital, lo cual reduce las barreras de entrada y permite a actores no estatales generar efectos estratégicos en escenarios de conflicto tecnológicamente habilitado (Kaldor, 2012).

Condiciones estructurales de vulnerabilidad y activación del conflicto

El escenario descrito se activa por la convergencia de condiciones estructurales que amplifican vulnerabilidades del sistema estatal y facilitan su explotación en múltiples dominios. La debilidad institucional ocupa un lugar central porque reduce la capacidad de integrar inteligencia, regular entornos digitales, proteger infraestructuras críticas y coordinar respuestas multidominio. En ese contexto, la fragmentación de la respuesta faculta al adversario para operar en las intersecciones entre dominios y, así, transformar vulnerabilidades dispersas en efectos estratégicos acumulativos.

La interdependencia de infraestructuras críticas constituye una condición adicional de alta relevancia, puesto que la conectividad entre sistemas de energía, comunicaciones, datos, transporte y plataformas de gestión incrementa la

exposición a perturbaciones localizadas con capacidad de propagación en cascada sobre múltiples sectores. La vulnerabilidad sistémica se define así por la posibilidad de que la afectación de un nodo crítico degrade la funcionalidad del conjunto y comprometa la continuidad operativa del Estado (Perrow, 1999).

Además, la brecha de talento en IA, ciberseguridad, análisis de datos y arquitectura de sistemas limita la capacidad de comprender, auditar y adaptar entornos tecnológicos complejos, y esta vulnerabilidad se profundiza debido a la baja soberanía tecnológica, que restringe el control sobre componentes críticos, estándares, plataformas e infraestructura digital.

En el caso colombiano, estas condiciones interactúan con la presencia de actores armados no estatales, economías ilícitas y territorios con densidad institucional variable, lo cual configura un entorno donde la tecnología amplifica la capacidad de los actores irregulares para explotar vulnerabilidades estructurales y generar efectos estratégicos desproporcionados (Pécaut, 2017).

Escenario disruptivo de degradación sistémica y pérdida de coherencia funcional

El escenario disruptivo se configura cuando múltiples vectores de ataque convergen de manera sincronizada sobre la arquitectura funcional del Estado. Esta secuencia puede iniciarse con operaciones cibernéticas persistentes que comprometen redes de mando y control, sistemas de información y bases de datos críticas, lo cual introduce incertidumbre sobre la integridad de la información. Simultáneamente, ataques electromagnéticos y degradación de señales afectan comunicaciones, navegación y sincronización, lo cual reduce la capacidad de coordinación operativa. En paralelo, campañas de desinformación de alta precisión amplifican la confusión, erosionan la confianza institucional y generan presión social sobre las decisiones del liderazgo (Rid, 2020).

A medida que la crisis evoluciona, la manipulación de datos y la posible degradación de mecanismos criptográficos introducen dudas sobre la confiabilidad de los sistemas y afectan directamente el proceso decisional. La pérdida de confianza en la información disponible genera retrasos, errores de interpretación y decisiones subóptimas. En este entorno, actores no estatales aprovechan la descoordinación para expandir control territorial, intensificar actividades ilícitas y aumentar su capacidad de influencia. El sistema no colapsa necesariamente por destrucción física, sino por una pérdida de coherencia funcional, la cual se produce cuando los elementos que lo componen dejan de operar de manera integrada (Nielsen, 2010).

Implicaciones estratégicas para la defensa en entornos de coerción sistémica

La implicación estratégica de este escenario es que la victoria ya no puede definirse exclusivamente en términos de superioridad cinética. En su lugar, la capacidad decisiva radica en mantener la integridad del sistema bajo condiciones de presión simultánea, preservar la confiabilidad del ciclo de información y decisión, y sostener la coherencia operativa en entornos degradados. La resiliencia sistémica se convierte en el eje de la defensa, entendida como la capacidad de absorber perturbaciones, mantener funciones críticas y adaptarse rápidamente a condiciones cambiantes (Gray, 2015).

La superioridad informacional se configura como condición necesaria para el ejercicio efectivo del mando, mientras que la capacidad de adaptación determina la continuidad estratégica en escenarios de incertidumbre. Para las Fuerzas Militares, esto implica una transformación en el diseño de capacidades, orientada hacia arquitecturas resilientes de mando y control, protección del ecosistema de datos, defensa cognitiva, seguridad de infraestructuras críticas y desarrollo de soberanía tecnológica. El escenario prospectivo no describe una posibilidad lejana, sino que constituye una tendencia estructural que ya está en desarrollo y que redefine las condiciones bajo las cuales se ejerce el poder en la guerra contemporánea (Freedman, 2013).

Configuración del conflicto en Colombia: expresión operativa de la coerción sistémica

Configuración y adaptación de actores híbridos en el entorno colombiano

El escenario colombiano contemporáneo evidencia una mutación progresiva de los actores armados hacia configuraciones híbridas con capacidad de integración tecnológica: las disidencias de las FARC-EP, el ELN y las estructuras del crimen organizado transnacional han evolucionado desde organizaciones insurgentes o criminales tradicionales hacia sistemas adaptativos que combinan control territorial, economía ilícita, redes digitales y capacidades tecnológicas accesibles. Esta transformación no implica una transición hacia formas convencionales de guerra, sino que incorpora selectivamente tecnologías que potencian su capacidad de

observación, coordinación, financiación y coerción, lo que reduce las asimetrías frente al Estado en dimensiones específicas del conflicto (Pécaut, 2017).

Estos actores operan como sistemas socio-técnicos en los que la violencia armada se articula con flujos financieros digitales, plataformas de comunicación, redes transnacionales y mecanismos de influencia local, y cuya estructura organizacional tiende a la descentralización operativa, lo cual propicia la resiliencia frente a la acción estatal. Esta lógica se aproxima a formas de guerra distribuida y persistente, donde la continuidad de la operación no depende de un centro único de gravedad, sino de la capacidad de mantener múltiples nodos funcionales conectados a través de redes formales e informales (Williams, 2001).

Integración operativa de tecnologías emergentes en el conflicto colombiano

El entorno colombiano presenta manifestaciones concretas de tecnologías que configuran nuevas formas de hacer la guerra. En este contexto, los drones comerciales han dejado de ser únicamente herramientas de observación y se han convertido en plataformas ISR de bajo costo que permiten vigilancia persistente, identificación de objetivos y apoyo a operaciones ilícitas. Su potencial evolutivo incluye funciones de saturación, entrega de cargas y coordinación táctica, lo cual los convierte en multiplicadores de capacidad para actores no estatales (Scharre, 2018).

Específicamente, las plataformas digitales operan como infraestructuras de mando distribuido que facilitan la comunicación segura, la coordinación en tiempo real y el anonimato relativo. Simultáneamente, las criptomonedas y los sistemas financieros digitales han introducido mecanismos de financiamiento resiliente que reducen la dependencia de circuitos tradicionales y dificultan la trazabilidad por parte del Estado. La desinformación, amplificada mediante redes sociales y algoritmos de recomendación, permite intervenir en la percepción de comunidades específicas, lo cual afecta la legitimidad institucional y facilita el control social indirecto. Estas tecnologías no operan de manera aislada, sino que se integran en ecosistemas operativos donde la información, el financiamiento y la acción armada se articulan en tiempo real (Zuboff, 2019).

Configuración de riesgos sistémicos en el entorno colombiano

El riesgo estructural para Colombia radica en su integración dentro de modelos operativos híbridos que combinan dimensiones criminales, militares e informacionales, una convergencia que permite a los actores ilegales ejercer dominio territorial

mediante el control de flujos económicos, la gestión de información y la manipulación de percepciones. El resultado es una forma de gobernanza criminal tecnificada que compite con la presencia estatal en determinadas regiones (Kaldor, 2012).

La guerra de datos se manifiesta en la capacidad de los actores para recolectar información local, identificar patrones de comportamiento y anticipar movimientos de la fuerza pública. La guerra cognitiva se expresa en la construcción de narrativas que legitiman su presencia o deslegitiman la acción estatal. La guerra de sistemas se evidencia en la posibilidad de afectar infraestructura crítica local o de explotar su vulnerabilidad para generar presión sobre comunidades y autoridades. Esta integración convierte el conflicto colombiano en un escenario donde las formas de guerra descritas previamente no son abstractas, sino operativas y observables (Garzón, 2020).

Asimismo, la expansión hacia el ciberespacio y el entorno cognitivo amplía el alcance de estos actores más allá del territorio físico, lo cual les confiere la capacidad de influir en redes sociales, utilizar plataformas digitales y acceder a herramientas tecnológicas para proyectar poder sin necesidad de tener una presencia física constante. Esta realidad, a su vez, introduce una dimensión adicional de riesgo, ya que la confrontación se desplaza hacia espacios menos visibles, pero estratégicamente relevantes, lo cual compromete la capacidad del Estado para mantener el control, la legitimidad y la coherencia operativa.

De manera prospectiva, la evolución de estos actores en Colombia indica una transición hacia configuraciones operativas más integradas, donde el control territorial se articula con capacidades digitales y proyección en el entorno cognitivo. La combinación de vigilancia basada en drones, explotación de datos locales, plataformas digitales y economías ilícitas tecnificadas permite consolidar esquemas de operación más resilientes y adaptativos. En este contexto, la ventaja estratégica no se define únicamente por la capacidad de ejercer coerción física, sino por la capacidad de estructurar información, anticipar dinámicas del entorno y afectar procesos decisionales. Esta convergencia transforma el conflicto en un sistema donde lo físico, lo digital y lo cognitivo operan de manera simultánea, de modo que amplía el alcance de actores no estatales y complejiza la respuesta del Estado.

Implicaciones estratégicas para la defensa y la adaptación institucional

La manifestación de estas dinámicas en Colombia confirma que la transformación del carácter de la guerra constituye una realidad en desarrollo. Las Fuerzas Militares enfrentan un entorno definido por sistemas híbridos que integran

tecnología, economía y control social, donde la amenaza trasciende las estructuras armadas visibles. Por ello, esta condición exige una adaptación orientada a la construcción de capacidades sistémicas que permitan comprender, integrar y responder a configuraciones complejas del conflicto (Gray, 2015).

La relevancia institucional se expresa en la reconfiguración del diseño de capacidades militares para operar en entornos donde la información, la tecnología y la percepción determinan la eficacia estratégica. Esta reconfiguración implica, por tanto, fortalecer arquitecturas de mando y control resilientes, desarrollar superioridad informacional, integrar capacidades de defensa cognitiva y asegurar la protección de infraestructuras críticas. En este sentido, la preparación se debe enfocar en desarrollar la capacidad de operar en condiciones de degradación, incertidumbre y presión simultánea en múltiples dominios (Freedman, 2013).

Colombia constituye un entorno donde convergen dinámicas globales de transformación del conflicto con condiciones locales que amplifican su impacto. Se trata, por lo tanto, de un espacio en el cual diversas formas avanzadas de guerra contemporánea manifiestan sus operaciones. Así, la interacción entre actores híbridos, tecnologías accesibles y vulnerabilidades estructurales organiza la competencia en torno al control de sistemas, procesos decisionales y voluntades, lo cual desplaza el eje de la confrontación hacia la coherencia funcional del sistema. En este escenario, la capacidad de anticipar, comprender y adaptarse determina la eficacia operativa de las Fuerzas Militares y la sostenibilidad del control estratégico del Estado.

Desde esta perspectiva, la ventaja se define por la capacidad de mantener la coherencia sistémica bajo presión constante, por lo cual la ausencia de adaptación acelera la erosión del control estratégico y reduce la capacidad de decisión efectiva. Estas condiciones permiten que actores estructuralmente más débiles exploten con mayor eficacia la lógica del conflicto contemporáneo y condicionen el equilibrio de poder en el entorno nacional.

Transformación del militar y de la educación militar

Combatiente cognitivo-tecnológico

La transformación del carácter de la guerra redefine la naturaleza del combatiente, pues el militar contemporáneo actúa dentro de sistemas complejos donde la percepción, la construcción del conocimiento y la decisión están mediadas por

arquitecturas digitales, flujos de datos y procesos algorítmicos. Debido a estas condiciones, el combatiente cognitivo-tecnológico no opera únicamente tecnología, sino que interactúa con sistemas que estructuran la interpretación del entorno y condicionan la acción, lo cual implica que la competencia estratégica se desplaza hacia la coherencia del sistema decisional, donde la integración entre humano y máquina define la eficacia operacional (Gray, 2015).

Esta condición introduce una tensión estructural entre el juicio profesional y la inferencia algorítmica, puesto que la decisión se construye a partir de modelos que procesan datos a gran escala y generan recomendaciones operativas. En este escenario, el riesgo radica en la opacidad de los sistemas, en la posibilidad de error estructural y en la delegación acrítica de la interpretación del entorno. Por ello, el combatiente debe desarrollar capacidad de validación, cuestionamiento y control sobre los sistemas, para lo cual es clave que fortalezca el pensamiento probabilístico, la comprensión de sesgos algorítmicos y la toma de decisiones en condiciones de incertidumbre inducida (Scharre, 2018).

Además, dado que la acción militar se define por la comprensión multidominio, el combatiente interpreta efectos en los dominios físico, cibernético, electromagnético, espacial y cognitivo como una arquitectura interdependiente. Por esta razón, la interacción humano-máquina constituye el núcleo del proceso decisional, pues la ventaja depende de la capacidad de integrar sistemas con criterio estratégico (Bousquet, 2009).

Transformación cognitiva de la mente militar

La transformación cognitiva es central porque busca que el pensamiento militar evolucione desde modelos lineales hacia esquemas sistémicos orientados a comprender interacciones, vulnerabilidades, resiliencia y propagación de efectos. Desde esta perspectiva, la guerra se interpreta como una arquitectura dinámica donde las acciones generan consecuencias indirectas que afectan múltiples niveles del sistema (Strachan, 2008).

La velocidad, la complejidad y la ambigüedad operan como condiciones estructurales del combate, razón por la cual la mente militar debe actuar con información incompleta, identificar patrones en entornos saturados de datos y sostener coherencia decisional bajo presión constante. En este sentido, la confrontación se desarrolla en sistemas de información, arquitecturas digitales y entornos cognitivos que condicionan la percepción y la acción (Freedman, 2013).

Además, la mente militar debe integrar dimensiones físicas, informacionales y cognitivas en un mismo marco analítico (Gray, 2015), pues la finalidad estratégica

incorpora la degradación del sistema del adversario, la manipulación de la percepción, la dislocación del proceso decisional y la afectación de la coherencia funcional, elementos que producen efectos equivalentes o superiores a la destrucción física.

Implicación educativa y transformación doctrinal

El análisis que se realizó en este capítulo hace evidente que la educación militar es un factor estratégico de primer orden, pero su transformación no consiste en adicionar contenidos tecnológicos, sino que implica rediseñar la formación para desarrollar capacidades cognitivas alineadas con la guerra contemporánea. La alfabetización estratégica en IA, análisis de datos, arquitectura de sistemas, ciberseguridad y dependencia tecnológica permite formar decisores capaces de comprender límites, riesgos y potencialidades de los sistemas empleados.

Esta formación, que incorpora validación de sistemas automatizados, interpretación de inferencias algorítmicas y toma de decisiones en entornos degradados, orienta su entrenamiento a operar bajo latencia reducida y presión multidominio. Además, la educación militar integra teoría de la guerra, estudios estratégicos y comprensión tecnológica en una arquitectura formativa coherente.

En este escenario, la innovación se institucionaliza como capacidad organizacional, de manera que la experimentación, el aprendizaje continuo y la adaptación doctrinal se convierten en funciones permanentes, de tal manera que el juicio profesional se redefine como la capacidad de integrar tecnología y criterio humano en decisiones complejas. En conclusión, la transformación educativa constituye la base para la evolución doctrinal, en la medida en que determina la capacidad de la fuerza para operar en sistemas, sostener coherencia bajo presión y ejercer poder en la guerra contemporánea.

Implicaciones estratégicas para la defensa, la doctrina y el Estado

Defensa nacional: integración de capacidades y coherencia operativa

La defensa nacional se redefine a partir del tránsito desde una lógica centrada en plataformas hacia una lógica centrada en capacidades integradas, de manera que el valor de los medios depende de su inserción en arquitecturas que articulen datos, redes, mando y control, resiliencia sistémica y defensa cognitiva. La eficacia

militar se expresa entonces en la capacidad de sostener la coherencia operativa en condiciones de degradación, incertidumbre y presión multidominio. En este sentido, la prioridad estratégica se orienta a la protección del ciclo de información, la resiliencia del mando y control, la reducción de dependencias críticas y la adaptación continua del sistema, lo cual desplaza la ventaja desde la posesión de medios hacia su integración y empleo coherente (Gray, 2015; Freedman, 2013).

Doctrina: operación multidominio y control del sistema decisional

La doctrina evoluciona hacia un marco que integra operaciones multidominio, guerra cognitiva y resiliencia sistémica como condiciones estructurales del combate. La generación de efectos se basa en la interacción simultánea de dominios en tiempo reducido, lo que incluye la operación en entornos de negación informacional, degradación de sistemas, mando distribuido e integración humano-máquina. En este escenario, la superioridad se define por la capacidad de preservar la coherencia del sistema decisional, influir en la percepción y sostener la capacidad de decidir en condiciones adversas. Así, la doctrina se orienta a representar la guerra en transformación mediante la integración de operaciones informacionales, cibernéticas y convencionales en una lógica unificada de acción (Strachan, 2008; Freedman, 2013).

Estado: soberanía tecnológica y arquitectura de seguridad sistémica

El Estado enfrenta una reconfiguración de la seguridad nacional como función sistémica que integra dimensiones tecnológicas, informacionales y económicas. Específicamente, la soberanía tecnológica condiciona la capacidad de acción estratégica mediante el control de infraestructuras digitales, plataformas, semiconductores y estándares, de manera que la protección de infraestructuras críticas y del ecosistema informacional y financiero garantiza la continuidad funcional del sistema. Por lo tanto, es evidente que no solo se necesita una preparación poscuántica para proteger las comunicaciones y los datos sensibles frente a capacidades emergentes de ruptura criptográfica, sino que además la respuesta estatal requiere una arquitectura integrada que articule defensa, regulación tecnológica, inteligencia, infraestructura y política pública para consolidar la seguridad como función transversal del poder del Estado (Segal, 2016; Gray, 2015).

Conclusiones

El desarrollo del capítulo confirma que la convergencia tecnológica reconfigura el carácter de la guerra mediante la integración de sistemas digitales, IA y arquitecturas de información que transforman los mecanismos de generación de poder. También se argumentó que la guerra conserva su naturaleza política, mientras su carácter evoluciona en función de la interacción entre tecnología, organización y entorno estratégico, lo cual redefine las condiciones en las cuales se produce la ventaja militar.

En particular, las amenazas emergentes que se analizaron responden a dinámicas sistémicas donde la IA, la digitalización, la automatización y la conectividad configuran un espacio de confrontación estructurado sobre la gestión de la información y la articulación de capacidades distribuidas. En este contexto, la confrontación se organiza alrededor del control de sistemas, procesos y flujos de datos, mediante el cual se establecen nuevas formas de coerción basadas en la capacidad de intervenir, degradar o condicionar el funcionamiento del adversario (Gray, 2015).

Como consecuencia de lo anterior, el centro de gravedad experimenta un desplazamiento hacia la coherencia funcional de los sistemas, de modo que la estabilidad del proceso decisional, la integridad del dato, la resiliencia de las redes y la superioridad informacional determinan la capacidad de acción estratégica en entornos caracterizados por alta complejidad y presión temporal. En este sentido, la ventaja se fundamenta en la capacidad de sostener la funcionalidad del sistema propio mientras se afecta la del adversario en niveles operacionales y estratégicos.

Específicamente, el caso colombiano evidencia la materialización de estas dinámicas, pues actores no estatales articulan control territorial con economías ilícitas digitalizadas, explotación de información y proyección sobre la dimensión cognitiva. Esta configuración les permite estructurar modelos de poder que combinan presencia física, control informacional y capacidad de adaptación tecnológica, lo cual amplía el alcance de la acción estratégica en escenarios híbridos (Kaldor, 2012).

Frente a este panorama, la respuesta estratégica se orienta al desarrollo de capacidades militares integradas que aseguren la coherencia sistémica, la protección de la información y la continuidad del proceso decisional, incluso en condiciones de degradación. Por esta razón, resulta claro que la integración multidominio, la resiliencia de infraestructuras críticas, la superioridad informacional y la formación de decisores con pensamiento sistémico constituyen condiciones necesarias para operar en el entorno contemporáneo.

En términos generales, este análisis también muestra claramente que la estructura de la guerra contemporánea se fundamenta en la interacción entre

sistemas, datos, cognición y resiliencia, lo cual redefine el centro de gravedad y establece nuevas condiciones para la competencia estratégica. En el contexto colombiano, esta transformación exige un proceso de adaptación que permita a las instituciones sostener el control estratégico en entornos donde actores híbridos operan con alta flexibilidad, acceden a tecnologías duales y tienen la capacidad de proyectarse más allá del dominio físico. La gravedad de esta problemática hace necesario enfatizar que la defensa nacional debe articular tecnología, doctrina y pensamiento estratégico en una lógica de integración que permita preservar la capacidad de decisión y asegurar la eficacia operativa en escenarios caracterizados por velocidad, ambigüedad y complejidad (Freedman, 2013).

En este marco, para comprender el conflicto contemporáneo se deben tener claro dos elementos clave: por una parte, que la ventaja estratégica se construye a partir de la capacidad de estructurar, proteger y explotar sistemas complejos en entornos de alta incertidumbre, y, por otra, que el control de datos, la coherencia de los procesos decisionales y la resiliencia de las arquitecturas operacionales configuran las nuevas condiciones de eficacia militar. En el caso colombiano, esta realidad implica enfrentar actores que combinan control territorial con capacidades digitales y proyección cognitiva, lo cual demanda una transformación profunda en la concepción, el desarrollo y el empleo del poder militar. En conclusión, la adaptación estratégica debe integrar tecnología, doctrina y formación en una lógica sistémica que permita sostener la capacidad de decisión y preservar el control estratégico en escenarios caracterizados por la velocidad, la ambigüedad y la convergencia tecnológica.

Referencias

Anthropic. (2026). *Claude* [modelo de lenguaje]. https://www.anthropic.com/

Boulanin, V., & Verbruggen, M. (2017). *Mapping the development of autonomy in weapon systems.* Stockholm International Peace Research Institute. https://www.sipri.org/publications/2017/policy-reports/mapping-development-autonomy-weapon-systems

Bousquet, A. (2009). *The scientific way of warfare: Order and chaos on the battlefields of modernity*. Columbia University Press.

Bowen, B. E. (2020). *War in space: Strategy, spacepower, geopolitics.* Edinburgh University Press.

Brown, C. R., Watkins, A., & Greitzer, F.L. (2013). *Predicting insider threat risks through linguistic analysis of electronic communication.* 2013 46th Hawaii International Conference on System Sciences, Wailea, HI, USA, 2013 (pp. 1849–1858), https://doi.org/10.1109/HICSS.2013.453

Clausewitz, C. von. (2007). *De la guerra.* La Esfera de los Libros.

Defense Critical Supply Chain Task Force. (2021). *Report of the Defense Critical Supply Chain Task Force.* U.S. Government Publishing Office.

Dowling, J. P., & Milburn, G. J. (2003). Quantum technology: The second quantum revolution. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 361*(1809), 1655–1674. https://doi.org/10.1098/rsta.2003.1227

ETSI. (2015). *Quantum safe cryptography and security: An introduction, benefits, enablers and challenges* [ETSI White Paper N.° 8]. European Telecommunications Standards Institute. https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security, 44*(1), 42–79. https://doi.org/10.1162/isec_a_00351

Freedman, L. (2013). *Strategy: A history.* Oxford University Press.

Garzón, J. C. (2020). *El crimen organizado en América Latina: Manifestaciones, facilitadores y reacciones.* Fundación Ideas para la Paz.

Gray, C. S. (2015). *The strategy bridge: Theory for practice.* Oxford University Press.

Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars.* Potomac Institute for Policy Studies. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Kaldor, M. (2012). *New and old wars: Organized violence in a global era* (3rd ed.). Stanford University Press.

Kania, E. B. (2020). Securing our 5G future. *Center for a New American Security.* https://www.cnas.org/publications/reports/securing-our-5g-future

Kitchin, R. (2014). *The data revolution: Big data, open data, data infrastructures and their consequences.* Sage.

Koblentz, G. D. (2020). Emerging technologies and the future of CBRN terrorism. *The Washington Quarterly, 43,* 177–196.

Lewis, J. A. (2021). Shaping the ground for bilateral cybersecurity negotiations. *China Int Strategy Rev, 3,* 115–122. https://doi.org/10.1007/s42533-021-00081-z.

Liang, Q., & Xiangsui, W. (1999). *Unrestricted warfare.* PLA Literature and Arts Publishing House. https://www.c4i.org/unrestricted.pdf

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar.* RAND Corporation. https://www.rand.org/pubs/monographs/MG877.html

Luttwak, E. N. (2001). *Strategy: The logic of war and peace* (Rev. ed.). Belknap Press of Harvard University Press.

Mayer-Schönberger, V. (2013). *Big data: A revolution that will transform how we live, work, and think.* Houghton Mifflin Harcourt.

Mazarr, M. J. (2015). *Mastering the gray zone: Understanding a changing era of conflict.* U.S. Army War College Press. https://press.armywarcollege.edu/monographs/428/

Moltz, J. C. (2019). *The politics of space security: Strategic restraint and the pursuit of national interests* (3rd ed.). Stanford University Press.

National Academies of Sciences, Engineering, and Medicine. (2018). *Biodefense in the age of synthetic biology.* National Academies Press.

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information.* Cambridge University Press.

OpenAI. (2026). *ChatGPT (versión basada en GPT-5.3)* [modelo de lenguaje]. https://chat.openai.com/

Pécaut, D. (2017). *La experiencia de la violencia.* La Carreta Editores.

Perplexity AI. (2026). *Perplexity AI* [motor de búsqueda basado en inteligencia artificial]. https://www.perplexity.ai/

Perrow, C. (1999). *Normal accidents: Living with high-risk technologies* (2nd ed.). Princeton University Press.

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare.* Farrar, Straus and Giroux.

Russell, S. (2019). *Human compatible: Artificial intelligence and the problem of control.* Viking.

Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war.* W. W. Norton & Company.

Segal, A. (2016). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age.* PublicAffairs.

Shaw, E. D., & Stock, H. V. (2015). *Behavioral risk indicators of malicious insider theft of intellectual property: Misreading the writing on the wall* [Withe Paper]. Incident Management Group; Symantec. https://static1.squarespace.com/static/596a623ba5790afcec9c024e/t/59c9e063a803bb62117213c0/1506402404657/Symantec+Malicious+Insider+Whitepaper+FINAL2.pdf

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know.* Oxford University Press.

Strachan, H. (2008). *The direction of war: Contemporary strategy in historical perspective.* Cambridge University Press.

Sun Tzu. (2009). *The art of war* (S. B. Griffith, Trans.). Oxford University Press. (Original work published ca. 500 BCE)

Virilio, P. (2006). *Speed and politics.* Semiotext(e).

Williams, P. (2001). *Transnational criminal networks.* RAND Corporation.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* PublicAffairs.

Capítulo 4

Ciberseguridad en el Comando Conjunto Cibernético de Colombia: desafíos y oportunidades*

DOI: https://doi.org/10.25062/9786287818644.04

Cristian Mauricio Toro Mora
Comando Conjunto Cibernético (CCOCI-COGFM)

Resumen: El presente capítulo analiza los desafíos y oportunidades en materia de ciberseguridad que enfrenta el Comando Conjunto Cibernético de Colombia (CCOCI), entidad responsable de liderar la defensa cibernética del país en el ámbito militar. Se abordan las principales amenazas cibernéticas, tanto internas como externas, que inciden sobre la seguridad nacional y las capacidades del CCOCI. También se examinan las políticas, estrategias y acciones implementadas por el Gobierno colombiano y el Ministerio de Defensa para fortalecer su postura en el ciberespacio. Finalmente, con base en el análisis de capacidades tecnológicas, infraestructura y talento humano, se propone una estrategia integral orientada a mejorar la resiliencia, la coordinación interinstitucional y la respuesta operativa del CCOCI frente a amenazas actuales y emergentes. El capítulo combina revisión documental y entrevistas estratégicas con actores clave del sector defensa con el propósito de aportar recomendaciones prácticas para fortalecer la ciberdefensa nacional desde una perspectiva conjunta y prospectiva.

Palabras clave: capacidades cibernéticas; ciberamenazas; ciberdefensa; ciberseguridad; Estrategia Nacional de Ciberseguridad; infraestructuras críticas; Mando Conjunto Cibernético.

* Capítulo de libro resultado del proyecto de investigación "La gobernanza del ciberespacio a nivel global, regional y nacional: desafíos, oportunidades y estrategias para la soberanía digital", del grupo de investigación "Ciberespacio, Tecnología e Innovación", de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado en 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 al autor y no reflejan necesariamente los de las instituciones participantes.

Cristian Mauricio Toro Mora
Sargento Segundo del Ejército Nacional de Colombia. Administrador de Empresas. Magíster en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Integra el Departamento de Operaciones del Comando Conjunto Cibernético. Contribuyó a la construcción del Plan de Ciberseguridad y Ciberdefensa Arkano 2024–2026. **https://orcid.org/0009-0002-4664-4808** - Contacto: **cristian.toro@esdeg.edu.co**

Citación APA: Toro-Mora, C. M. (2026). Ciberseguridad en el Comando Conjunto Cibernético de Colombia: Desafíos y oportunidades. En M. E. Realpe-Díaz & A. M. González-González (Eds.), *Transformación digital y ciberseguridad en Colombia: Desafíos estratégicos para sectores de infraestructura crítica* (pp. 119-150). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818644.04

TRANSFORMACIÓN DIGITAL Y CIBERSEGURIDAD EN COLOMBIA: DESAFÍOS ESTRATÉGICOS PARA SECTORES DE INFRAESTRUCTURA CRÍTICA
ISBN impreso: 978-628-7818-63-7
ISBN digital: 978-628-7818-64-4
DOI: https://doi.org/10.25062/9786287818644

Colección Ciberseguridad y Ciberdefensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2026

Introducción

En el contexto actual, marcado por el volátil avance de las tecnologías de la información y las comunicaciones (TIC), el ciberespacio es un nuevo dominio estratégico para la seguridad y la defensa de las naciones. Colombia no es ajena a esta realidad. Durante la última década, el país ha evidenciado un crecimiento sostenido en el uso de plataformas digitales en todos los sectores, lo que ha traído enormes beneficios, pero también múltiples riesgos en varios aspectos. Las amenazas cibernéticas no solo comprometen la privacidad de los ciudadanos o la seguridad de las infraestructuras críticas, sino que tienen el potencial de afectar la soberanía, la estabilidad institucional y el funcionamiento de las capacidades militares.

En este teatro, el Comando Conjunto Cibernético (CCOCI) se establece como la unidad encargada de liderar las operaciones militares en el ciberespacio, con el objetivo de proteger los intereses estratégicos de la nación frente a ataques cibernéticos dirigidos a estructuras de defensa y activos tecnológicos del Estado. Desde su creación, consolidación y operación, estas han sido etapas esenciales dentro de la Política de Ciberdefensa del Ministerio de Defensa Nacional, la cual sigue los lineamientos establecidos por el Documento CONPES 3701 de 2011 y la Estrategia Nacional de Ciberseguridad, que ha servido como referente regional en materia de ciberseguridad.

No obstante, a pesar de los avances institucionales y operativos desde su creación, el CCOCI afronta hoy una serie de retos que limitan su capacidad de respuesta frente a Amenazas de Naturaleza Cibernética (ANC) cada vez más sofisticadas. Estos desafíos están relacionados con la rápida evolución de los vectores de ataque, la dependencia tecnológica, la escasez de talento humano especializado, las brechas en interoperabilidad entre las Fuerzas y la necesidad de fortalecer la conjuntez y la cooperación interinstitucional. Además, las dinámicas

geopolíticas actuales exigen que las Fuerzas Militares estén preparadas para actuar en un entorno híbrido, donde los ciberataques pueden acompañar o preceder conflictos armados convencionales, o incluso constituir por sí mismos agresiones estratégicas en este nuevo teatro de operaciones.

Por ello, resulta crucial analizar en profundidad el entorno cibernético del país, identificar las principales amenazas que inciden sobre las Fuerzas Militares y evaluar las capacidades actuales del CCOCI. Esta evaluación debe considerar tanto la infraestructura tecnológica como la doctrina operativa, los recursos humanos y la articulación con el sistema de defensa nacional. Asimismo, se hace necesario revisar las políticas y estrategias vigentes para determinar si responden de manera efectiva a las amenazas emergentes o si requieren ajustes estructurales que garanticen la seguridad digital de sus Fuerzas Armadas.

Este capítulo tiene como objetivo principal proponer una estrategia que permita afrontar los desafíos de ciberseguridad que enfrenta el CCOCI, con un enfoque integral que considere tanto los factores internos de desarrollo institucional como los riesgos externos provenientes de actores estatales y no estatales. Para ello, se desarrollan tres objetivos específicos: 1) analizar las principales amenazas cibernéticas y los desafíos de ciberseguridad que afectan al CCOCI, considerando tanto actores internos como externos; 2) examinar las políticas, estrategias y acciones específicas que el CCOCI y el Gobierno colombiano han implementado para fortalecer la ciberseguridad y la ciberdefensa en el ámbito militar, y 3) proponer una estrategia que responda de manera realista y proactiva a las necesidades de fortalecimiento del CCOCI frente al panorama actual y futuro.

La importancia de este capítulo radica en que aporta una visión estratégica y prospectiva sobre el papel del CCOCI como pilar de la defensa nacional en el ciberespacio. Asimismo, busca contribuir con propuestas concretas a la formulación de una estrategia institucional que articule capacidades, optimice recursos, fortalezca la formación del talento humano y consolide al CCOCI como un referente regional en la defensa cibernética. En un mundo cada vez más interconectado, no basta con tener estructuras operativas, sino que se requiere visión, liderazgo y una capacidad adaptativa permanente para enfrentar amenazas invisibles pero letales.

En conclusión, esta introducción no solo contextualiza el papel del CCOCI en el sistema de defensa nacional, sino que también evidencia la necesidad de revisar y proponer mejoras estratégicas para su gestión. Ante el incremento de las ANC, resulta urgente pensar soluciones viables, integrales y sostenibles que garanticen la defensa de la nación en este nuevo campo de batalla digital.

Amenazas cibernéticas y desafíos de ciberseguridad que enfrenta el Comando Conjunto Cibernético de Colombia

El ciberespacio se ha consolidado como un dominio estratégico de confrontación al mismo nivel que la tierra, el mar, el aire y el espacio exterior. Las operaciones militares modernas se desarrollan simultáneamente en todos estos dominios, donde la información y la tecnología se convierten en armas decisivas (NATO CCDCOE, 2022). En este escenario, el CCOCI de las Fuerzas Militares de Colombia cumple una misión esencial: ejercer la ciberseguridad y la ciberdefensa para conducir operaciones militares cibernéticas a nivel estratégico. Específicamente, su objetivo es garantizar la seguridad y la defensa de la Nación en el ciberespacio de acuerdo con la Disposición 013/18.

En este contexto, el apartado analiza y estudia las principales amenazas y los desafíos de ciberseguridad que enfrenta el CCOCI en la actualidad. Su propósito es comprender cómo la evolución de las ANC ha transformado la forma en que las Fuerzas Militares planean, operan y defienden el dominio digital. Para ello, se adopta un enfoque descriptivo y analítico que se fundamenta en la triangulación de fuentes doctrinales, normativas y técnicas, e incorpora evidencias de organismos internacionales como la Agencia de la Unión Europea para la Ciberseguridad (ENISA, 2023), el Foro Económico Mundial (2024), IRM (2025) y Armis (2025), así como información institucional proveniente del propio CCOCI.

Del poder cibernético a la Defensa Nacional

El siglo XXI ha transformado la naturaleza del poder. Específicamente, Nye (2021) define el poder cibernético como la capacidad estatal para cumplir sus objetivos mediante el control del ciberespacio y la influencia sobre la información. En este contexto, Rid (2013) sostiene que los conflictos cibernéticos se caracterizan no por la destrucción física, sino por la disrupción y el espionaje prolongado. Esta perspectiva es complementada por Healey (2019), quien subraya que una defensa efectiva en este ámbito solo es posible si existe una cooperación sostenida entre los sectores público, privado y académico.

En Colombia, el poder cibernético se materializa en la capacidad del CCOCI para anticipar, detectar y responder a las agresiones que amenazan la soberanía digital. No obstante, este poder no se ejerce de manera aislada pues la ciberdefensa debe ser colaborativa, de manera que constituye una responsabilidad

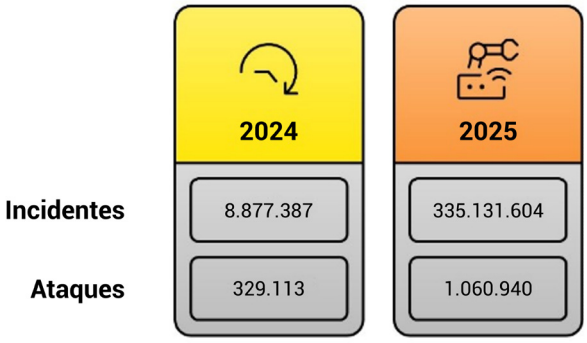
compartida entre el CCOCI, los proveedores tecnológicos y los responsables de las Infraestructuras Críticas Cibernéticas Nacionales y Militares (ICCN/ICCM). Su éxito depende de la sinergia permanente entre todos los actores, del intercambio de inteligencia y de la coordinación táctica en tiempo real.

Ahora bien, la protección del ciberespacio requiere mantener un equilibrio entre tres pilares fundamentales: la doctrina, que establece los lineamientos de actuación; el talento humano, encargado de llevar a cabo las operaciones; y la tecnología, la cual brinda las herramientas necesarias para la detección y la respuesta ante amenazas. Esta integración, enmarcada dentro del Plan Arkano Plus 2024-2026, guía al CCOCI hacia un modelo de defensa integral, proactiva y flexible, orientado al cumplimiento de su misión institucional.

Tendencias y aumento de la actividad cibernética

Entre 2023 y 2025, el entorno digital militar colombiano registró una expansión sin precedentes, con un crecimiento que superó el 3.700 %. Este fenómeno se manifestó en cifras significativas, pues en 2024 el CCOCI procesó 8,8 millones de incidentes y 329.000 ataques no materializados, mientras que para el 31 de octubre de 2025 se contabilizaban más de 335 millones de eventos y cerca de un millón de ataques mitigados (figura 1). Dicho incremento refleja tanto la intensificación de las actividades hostiles como la mejora en la capacidad de monitoreo del Comando.

Figura 1. *Comparación de incidentes y ataques 2024-2025*



Fuente: CCOCI (2025).

Por su parte, el Foro Económico Mundial (2024) y ENISA (2023) también señalan un incremento en las amenazas contra las infraestructuras críticas, un fenómeno impulsado por el uso de inteligencia artificial con fines ofensivos, el auge del

espionaje digital y la creciente sofisticación del *ransomware*. De hecho, en el contexto latinoamericano, Colombia figura entre los países con mayor nivel de actividad maliciosa dirigida al sector defensa (IBM X-Force, 2024). Entre los principales vectores identificados se encuentran los escaneos automatizados, la explotación de vulnerabilidades conocidas, los ataques de denegación de servicio distribuido (DDoS) y las campañas de ingeniería social de alto nivel.

Para el CCOCI, esta evolución significa enfrentar un entorno operacional más denso y tecnológicamente complejo, donde la capacidad de correlacionar eventos, automatizar respuestas y mantener la resiliencia de los sistemas se ha convertido en un requisito estratégico.

Vectores de ataque: el frente de entrada de la amenaza

Los vectores de ataque representan las vías de acceso que utilizan los adversarios para infiltrarse en los sistemas. De acuerdo con los informes de Mandiant (2024) e IRM (2025), los principales son:

- Escaneo y explotación de servicios expuestos: los atacantes recurren a herramientas automatizadas para detectar debilidades en servidores, bases de datos o dispositivos con configuraciones inadecuadas.
- Compromiso de credenciales: el robo o filtración de contraseñas sigue siendo el método más habitual para lograr acceso inicial a los sistemas.
- Explotación de vulnerabilidades conocidas (CVE): la falta de actualización oportuna de parches aumenta significativamente el riesgo, sobre todo en entornos operacionales (OT) y sistemas de mando y control.

Los datos registrados del 1 de enero al 31 de octubre de 2025 en el CCOCI muestran una realidad similar a la de los datos analizados por Mandiant (2024) e IRM (2025) (tabla 1).

Tabla 1. *Estadísticas de incidentes y ataques*

N°	Taxonomía	Total de incidentes	Total de ataques
1	Contenido dañino	336 736	9 199
2	Disponibilidad	237 644 788	668
3	Obtención de información	31 204 854	3 603
4	Intento de intrusión	39 631 857	127
5	Intrusión	194 633	103
6	Fraude	637 139	263 169

N°	Taxonomía	Total de incidentes	Total de ataques
7	Vulnerable	57 438	394
8	Compromiso de información	19 285 236	13
9	Contenido abusivo	1 096 532	780 867
10	Otros	5 042 393	286
	Total Fuerzas Militares	335 131 604	1 060 940

Fuente: CCOCI (2025).

Ante este panorama, el CCOCI ha respondido reforzando la segmentación de redes, la autenticación multifactor (MFA) y los controles PAM, con lo cual se ha alineado con el marco Zero Trust y las directrices del NIST (2022). Estas medidas reducen la superficie de ataque y limitan los movimientos laterales dentro de las redes militares.

Actores de amenaza: internos y externos

El panorama de riesgos incluye actores internos y externos. Los primeros comprenden personal militar, contratistas o terceros con acceso legítimo a los sistemas, cuyo riesgo proviene de la negligencia operativa, el error humano o la manipulación externa. Por otro lado, los actores externos abarcan a los grupos de Amenazas Persistentes Avanzadas (APT), el crimen organizado y el *hacktivismo* político.

Al respecto, Armis (2025) destaca que los grupos de APT orientan sus ataques hacia el espionaje estratégico y la obtención de información militar sensible. De igual forma, IRM (2025) advierte que los ataques de *ransomware* y la comercialización de accesos iniciales (Initial Access Brokers) se han convertido en un negocio muy rentable en la región. Ante este panorama, el CCOCI considera que es necesario fortalecer la contrainteligencia digital y la gestión de identidades privilegiadas.

Como se señaló antes, la ciberdefensa colaborativa es esencial frente a esta diversidad de actores, pues cada proveedor o entidad con acceso a infraestructura crítica comparte la responsabilidad de proteger los sistemas. Por esta razón, la cooperación efectiva entre el CCOCI, los proveedores y los administradores de ICCM/ICCN permite una detección más temprana y una respuesta más eficiente, lo cual consolida una verdadera defensa colectiva.

Relación entre vectores y métodos

Los ataques rara vez emplean una sola técnica. El marco MITRE ATT&CK (2024) demuestra que las campañas exitosas combinan fases de reconocimiento, acceso inicial, escalamiento de privilegios, persistencia y exfiltración de información.

Particularmente en las Fuerzas Militares, estas secuencias suelen iniciar con escaneos externos, continúan con ataques de *phishing* y culminan con movimientos laterales hacia sistemas de mando y control.

Por esta razón, el CCOCI ha institucionalizado ejercicios de *red teaming* y *purple teaming* para evaluar sus defensas y entrenar a sus analistas en entornos simulados de guerra digital. Estos ejercicios, basados en escenarios reales, permiten medir tiempos medios de detección (MTTD) y de respuesta (MTTR), así como validar la coordinación entre unidades cibernéticas. En este contexto, se destaca su esfuerzo colaborativo con las ICCN y las ICCM, mediante la realización de ejercicios tanto técnicos como para los tomadores de decisión.

Riesgos de cadena de suministro y terceros

El 60 % de los incidentes cibernéticos graves en el mundo se originan en vulnerabilidades de terceros o en la cadena de suministro (IRM, 2025). Esta situación impacta de manera directa al sector defensa, que depende de una amplia red de proveedores de software, hardware y servicios especializados. Entre los ataques más frecuentes se encuentran la inserción de código malicioso en actualizaciones, la manipulación de certificados digitales y el uso indebido de herramientas de administración remota.

Para el CCOCI, estos riesgos resultan especialmente críticos, ya que gran parte de sus operaciones depende de proveedores externos que manejan componentes esenciales como software de seguridad, servicios en la nube, equipos de comunicación y sistemas de monitoreo. Esta dependencia amplía significativamente la superficie de ataque, pues una vulnerabilidad en cualquiera de los eslabones puede comprometer la integridad de las operaciones militares. Según el informe *The State of Cyberwarfare 2025,* los actores hostiles han empezado a utilizar a los proveedores como verdaderos "caballos de Troya" para infiltrarse en ecosistemas más protegidos introduciendo fallas en componentes aparentemente legítimos o alterando procesos de actualización sin ser detectados (Armis, 2025).

En el caso colombiano, este panorama se complica aún más por la diversidad de contratistas y de plataformas que emplean las Fuerzas Militares. De hecho, el CCOCI ha identificado que los ataques dirigidos a la cadena de suministro no solo buscan afectar la disponibilidad de los sistemas, sino también infiltrar operaciones con fines de espionaje o sabotaje estratégico. Por ello, la gestión de terceros se ha convertido en un eje prioritario dentro de la institución. En los últimos años, el CCOCI ha impulsado la adopción de mecanismos de verificación y monitoreo permanente sobre los proveedores con acceso remoto a sus sistemas, a lo cual se suma la

implementación de auditorías periódicas a los contratos tecnológicos. Estas acciones buscan reforzar la confianza y asegurar que los aliados tecnológicos cumplan con los mismos estándares de seguridad exigidos dentro del sector defensa.

Impacto operacional y organizacional

Las amenazas cibernéticas no solo comprometen la infraestructura tecnológica, sino que también afectan la moral del personal, la toma de decisiones y la imagen institucional. Los ataques de desinformación, *deepfakes* y manipulación cognitiva buscan erosionar la confianza en las instituciones militares (WEF, 2024). En este sentido, el CCOCI no solo enfrenta una guerra técnica, sino también psicológica e informativa.

Finalmente, es importante señalar que el impacto operacional se mide por la capacidad de mantener la continuidad de la misión bajo ataque, pues un incidente que paraliza un sistema de mando o que interrumpe la comunicación entre unidades puede tener consecuencias estratégicas. Por esta razón, el entrenamiento constante del personal y la simulación de escenarios de crisis son componentes esenciales de la preparación militar en el dominio cibernético.

Proyección prospectiva 2035-2040

El informe Global Trends 2040 (ODNI, 2021) proyecta que la competencia tecnológica mundial incrementará la exposición de los Estados a ataques híbridos cada vez más sofisticados, una tendencia que, en el contexto colombiano, convierte la defensa del ciberespacio en un componente esencial de la seguridad nacional. Por ello, el CCOCI debe avanzar hacia un modelo de defensa predictiva, sustentado en el uso de inteligencia artificial, análisis de grandes volúmenes de datos y procesos automatizados de respuesta.

De igual manera, resulta fundamental fortalecer la cooperación regional con socios estratégicos y mantener la participación activa en ejercicios multinacionales, tales como Locked Shields o Resolute Sentinel, en los cuales las Fuerzas Militares de Colombia han demostrado un desempeño destacado. Estos escenarios contribuyen a validar doctrinas, compartir experiencias y consolidar la interoperabilidad ante amenazas de carácter complejo.

Dimensión ética y legitimidad de la ciberdefensa

La defensa del ciberespacio plantea profundos desafíos éticos y jurídicos. Al respecto, Kello (2017) subraya que la efectividad operacional debe mantenerse en equilibrio con el cumplimiento del Derecho Internacional Humanitario (DIH). Específicamente, en el contexto colombiano, la Disposición 002 de 2022 establece las reglas de enfrentamiento en el ciberespacio, las cuales garantizan que

las acciones militares se rijan por los principios de proporcionalidad, necesidad y trazabilidad. De este modo, la transparencia institucional y una comunicación estratégica efectiva son los pilares fundamentales para fortalecer la legitimidad del CCOCI ante la sociedad y la comunidad internacional.

Durante el periodo 2023-2025, el ciberespacio militar colombiano se ha consolidado como un entorno de confrontación constante, pues las amenazas dejaron de ser escenarios hipotéticos para convertirse en realidades persistentes y organizadas. Frente a este escenario, el CCOCI ha mostrado una notable capacidad de adaptación al fortalecer sus procesos de vigilancia, detección y respuesta. Sin embargo, el incremento sostenido en el número de incidentes confirma que la superficie de ataque continúa expandiéndose, lo cual exige estrategias más integrales y colaborativas.

En síntesis, el análisis realizado permite concluir que la eficacia de la defensa digital no radica exclusivamente en la tecnología, sino en la articulación entre doctrina, talento humano especializado y cooperación interinstitucional. En este sentido, la ciberdefensa colaborativa entre el CCOCI, los proveedores tecnológicos y los responsables de las ICCN/ICCM constituye el eje central de la resiliencia nacional frente a adversarios cada vez más sofisticados. Este examen de las amenazas y los desafíos que enfrenta el CCOCI sienta las bases para abordar, en el siguiente objetivo, el marco doctrinal y jurídico que orienta las operaciones de ciberseguridad y ciberdefensa militar en Colombia, así como las políticas que trazan su proyección estratégica hacia el horizonte 2042.

Políticas, estrategias y acciones institucionales en ciberseguridad y ciberdefensa militar

El avance del ciberespacio como dominio estratégico de confrontación ha transformado profundamente las dinámicas de la seguridad nacional. Las operaciones militares ya no se limitan al control territorial, aéreo o marítimo, pues hoy incluyen la protección del entorno digital, ámbito en el cual la información, la infraestructura tecnológica y la toma de decisiones se han convertido en objetivos prioritarios de actores estatales y no estatales (NATO CCDCOE, 2022). En Colombia, el liderazgo del CCOCI del Comando General de las Fuerzas Militares (CGFM) ha sido decisivo para consolidar una defensa digital institucional, basada en doctrina, gobernanza y capacidades conjuntas.

Esta sección analiza las políticas, los planes y las acciones que el CCOCI ha desarrollado entre 2023 y 2025 para fortalecer la ciberseguridad y la ciberdefensa del país, con el propósito de mostrar cómo la política pública nacional y la estrategia militar se complementan en la cimentación de un ecosistema cibernético articulado, interoperable y resiliente, en línea con los objetivos del Plan Arkano Plus 2024-2026, el Plan Ayacucho Plus y la visión PEMT 2042.

Marco normativo y doctrinal

La base normativa que respalda la acción cibernética en el sector defensa colombiano se ha desarrollado de manera progresiva y en consonancia con la política pública nacional. Específicamente, el CONPES 3701 de 2011 marcó el punto de partida al definir los lineamientos de la Política Nacional de Ciberseguridad y Ciberdefensa, acción que propició la creación del CCOCI, el COLCERT y el Centro Cibernético Policial. Más adelante, el CONPES 3854 de 2016 introdujo un enfoque orientado a la gestión del riesgo digital, mientras que el CONPES 3995 de 2020 amplió el alcance hacia la construcción de confianza digital y la protección de la información en todos los sectores del Estado colombiano.

En el ámbito jurídico, la Ley 1273 de 2009 modificó el Código Penal al incorporar la protección de la información como bien jurídico, mientras que la Ley 1581 de 2012 estableció las normas sobre protección de datos personales. Por su parte, la Ley 1621 de 2013 reguló las actividades de inteligencia y contrainteligencia, lo cual permitió configurar un marco legal para la actuación legítima del Estado frente a amenazas cibernéticas. A su vez, el Decreto 338 de 2022 fortaleció la gobernanza de la seguridad digital al establecer las instancias de coordinación nacional, los procedimientos para la gestión de incidentes y los lineamientos para identificar las ICCN. Este marco fue complementado por la Resolución 7870 de 2022 del Ministerio de Defensa Nacional, que formalizó la Política de Seguridad Digital del Sector Defensa, y por la Disposición 002 de 2022, que estableció las reglas de enfrentamiento en operaciones cibernéticas, alineadas con los principios del DIH.

Desde la perspectiva doctrinal, la Directiva Permanente N.º 140 de 2013 permitió la activación del Centro de Operaciones de Seguridad (SOC) del CCOCI, mientras que los Manuales Fundamentales Conjuntos (MFC) 1.0, 3-0 y 5-0 del CGFM integraron el dominio cibernético dentro de la doctrina operacional conjunta. No obstante, persiste una brecha importante: la ausencia de un manual conjunto actualizado de ciberseguridad y ciberdefensa que unifique los procedimientos, defina los estándares y establezca las métricas claras de desempeño. No obstante, cabe señalar que el CCOCI está actualizando este documento, en cuya elaboración

se integran lecciones aprendidas de ejercicios multinacionales como Resolute Sentinel 2024 y Locked Shields 2023, así como buenas prácticas derivadas de la OTAN (2023) y de la Organización de los Estados Americanos (OEA, 2022).

Finalmente, la Estrategia Nacional de Seguridad Digital 2025-2027 (ENSD) refuerza este entramado normativo porque actualiza las responsabilidades institucionales, prioriza la protección de las infraestructuras críticas y promueve la cooperación multisectorial. Para el CCOCI, esta estrategia representa un punto de convergencia entre la doctrina militar y la política pública nacional, pues demanda una mayor gobernanza, interoperabilidad y transparencia en las operaciones de ciberseguridad del Estado colombiano.

El Plan Arkano Plus 2024-2026: pilar de la defensa digital militar

El Plan Arkano Plus 2024-2026 representa la herramienta estratégica más consolidada del CCOCI y sintetiza más de una década de madurez doctrinal en materia de defensa digital. Este plan da continuidad a los programas Binario, Domo Virtual y Arkano, y se orienta a fortalecer una defensa cibernética integral articulada con el Plan de Campaña Estratégico Conjunto Ayacucho Plus y con la visión proyectiva del Plan Estratégico Militar de Transformación (PEMT) 2042.

A diferencia de sus predecesores, Arkano Plus trasciende la mera coordinación técnica para establecer una arquitectura multidominio sustentada en tres pilares interdependientes: protección cibernética, resiliencia cibernética y defensa cibernética nacional.

La protección cibernética es un componente que se orienta a anticipar, prevenir y neutralizar amenazas antes de que afecten los activos estratégicos. Su enfoque se basa en la gestión de riesgos, el control de accesos, la segmentación de redes y la corrección de vulnerabilidades, todo ello bajo el principio de defensa en profundidad. El objetivo primordial es fortalecer la seguridad desde el diseño mismo de la infraestructura tecnológica, lo que garantiza una protección estructural y proactiva (Ministerio de Defensa Nacional, 2024).

La resiliencia cibernética, al reconocer la inevitabilidad de los ciberataques, busca garantizar la continuidad de las operaciones militares y constitucionales incluso en condiciones adversas. Asimismo, abarca la gestión integral de incidentes, el análisis forense digital, la restauración de servicios críticos y la mejora continua, la cual se materializa mediante auditorías, lecciones aprendidas y ejercicios de simulación.

Finalmente, la defensa cibernética nacional sitúa al CCOCI en una postura estratégica, desde la cual articula la inteligencia, la vigilancia táctica, el desarrollo doctrinal y la cooperación internacional. Comprende tanto operaciones defensivas

como acciones de carácter ofensivo controlado, e incluye el intercambio de inteligencia con aliados y la participación en ejercicios multinacionales, todos ellos destinados a fortalecer la preparación frente a amenazas híbridas o grupos de APT.

En conjunto, el Plan Arkano Plus consolida la visión de conjuntez entre las Fuerzas, integrando doctrina, talento humano e innovación tecnológica. De acuerdo con entrevistas institucionales (CCOCI, 2025), su implementación ha permitido homogeneizar los procesos de detección de incidentes, reducir los tiempos de contención y mejorar la interoperabilidad doctrinal entre el Ejército Nacional, la Armada, la Fuerza Aeroespacial y las Direcciones Conjuntas de Inteligencia, Operaciones y Comunicaciones. Todo ello contribuye de manera decisiva al fortalecimiento de la seguridad y defensa cibernética nacional.

Gobernanza y marco de gestión interinstitucional

El CCOCI se articula con instancias de seguridad digital, tanto nacionales como internacionales, conforme al modelo de Gobernanza del Decreto 338 de 2022. Este decreto establece una coordinación en tres niveles: estratégico (Consejo Nacional de Seguridad Digital), operativo (CSIRT Gobierno y COLCERT) y táctico (equipos sectoriales como el CSIRT Defensa). Dicha estructura garantiza que las operaciones cibernéticas del sector defensa se integren con la respuesta estatal y eviten duplicidades.

Además, la Resolución 02277 de 2025, que actualiza el Modelo de Seguridad y Privacidad de la Información (MSPI), alineó los controles de seguridad con la norma internacional ISO/IEC 27001:2022, con lo que reforzó las auditorías, la trazabilidad de incidentes y la gestión del riesgo institucional. Para el CCOCI, esta convergencia normativa significa fortalecer la interoperabilidad con el Estado, mejorar la transparencia y elevar la madurez cibernética.

La gobernanza militar cibernética del CCOCI no solo depende de sus capacidades internas, sino también de la cooperación externa. Por eso, mantiene una red de trabajo constante con entidades como el COLCERT, el CSIRT Gobierno, la Policía Nacional (C4) y la Dirección Nacional de Inteligencia (DNI), a las que se suman organismos aliados de carácter internacional, entre los que destacan SOUTHCOM, la OTAN y la OEA (CICTE, 2023). Dichas alianzas son cruciales para fortalecer la prevención, la detección y la respuesta ante amenazas transnacionales.

Capacidades operativas y conjuntez

El CCOCI lidera las labores de detección y respuesta ante incidentes cibernéticos. Para ello, se apoya en sistemas de gestión de información y eventos de seguridad (SIEM), así como en plataformas avanzadas de inteligencia de amenazas, las cuales

son capaces de procesar millones de eventos diariamente. En 2025, las estadísticas institucionales reportaron más de 159 000 millones de eventos procesados, un volumen que representa un crecimiento del 42 % respecto al año 2024 (CCOCI, 2025). Este incremento refleja tanto la creciente actividad de los actores hostiles como el fortalecimiento y la madurez de las capacidades de monitoreo del sistema.

Específicamente, la conjuntez operacional entre las Fuerzas Militares se evidencia en la coordinación constante del CCOCI con el CAOCC, la BRICC, el BACCI, la DICAE y el COCIB. Este modelo de trabajo, fundamentado en la interoperabilidad, permite que las capacidades técnicas y humanas de las distintas unidades se complementen, se compartan alertas de manera oportuna y se mantenga una trazabilidad efectiva de los incidentes. Desde el plano doctrinal, la conjuntez se materializa en la homogeneización de procedimientos, la adopción de taxonomías comunes y el fortalecimiento de la cultura de seguridad digital en todas las Fuerzas.

En este escenario, el talento humano se consolida como un pilar esencial de la capacidad cibernética. Según entrevistas institucionales, los comandantes de las unidades coinciden en que, si bien el CCOCI ha logrado avances significativos en la formación y profesionalización del personal técnico, persisten desafíos en la retención y la renovación de talento especializado. En este sentido, la alta rotación del personal, motivada por las diferencias salariales frente al sector privado, constituye una vulnerabilidad estructural que afecta la continuidad y acumulación del conocimiento operativo.

Integración de percepciones en entrevistas institucionales

Las entrevistas realizadas al Comandante del CCOCI y a los comandantes de las unidades cibernéticas evidencian una visión compartida: el CCOCI es percibido como el eje articulador de la defensa digital militar, cuyo rol debe evolucionar de un enfoque meramente técnico hacia un centro de convergencia estratégica en materia cibernética.

No obstante, los entrevistados también resaltan la necesidad de incrementar la frecuencia de los ejercicios conjuntos, mantener una actualización doctrinal constante y establecer una política sostenida de fortalecimiento del talento humano. Según el Comandante del CCOCI (2025), las prioridades institucionales se centran en la consolidación de un sistema unificado de indicadores de desempeño, la garantía de interoperabilidad entre las Fuerzas y la formalización de la conjuntez doctrinal mediante la elaboración del nuevo Manual Conjunto de Ciberseguridad y Ciberdefensa.

De este proceso de entrevistas se desprenden tres conclusiones clave:

- Los objetivos estratégicos del CCOCI se alinean claramente con la Política Nacional de Seguridad Digital (ENSD, MSPI, Decreto 338 de 2022).
- Persisten diferencias operativas entre las Fuerzas Militares, las cuales demandan una mayor homogeneización doctrinal y un entrenamiento conjunto.
- El fortalecimiento de la ciberdefensa colaborativa, que debe darse entre el CCOCI, los proveedores tecnológicos y los responsables de las ICCN/ICCM, se reconoce de manera unánime como el camino más efectivo para garantizar la continuidad operativa y la resiliencia nacional frente a las amenazas del ciberespacio.

Tabla 2. *Comparativo de percepciones entre el Comandante del CCOCI y los Comandantes de las Unidades Cibernéticas*

Categoría de análisis	Comandante del CCOCI	Comandantes de Unidades Cibernéticas (Ejército, Armada, FAC)
Desafíos principales	Consolidar la capacidad conjunta, fortalecer la gobernanza y la sensibilización institucional. Enfrentar retos tecnológicos emergentes como la inteligencia artificial y la criptografía poscuántica.	Falta liderazgo y estrategia operacional clara; no existe una hoja de ruta definida ni manual doctrinal actualizado (vigente desde 2016).
Impacto en la seguridad nacional	Considera que el CCOCI es el núcleo central de las operaciones de ciberdefensa, fortaleciendo las capacidades humanas, técnicas y de respuesta ante incidentes.	Reconocen el papel estratégico del CCOCI, pero perciben una madurez doctrinal y operativa insuficiente, con apoyo táctico más que estratégico.
Interoperabilidad y articulación	Señala que existe integración de capacidades y roles entre las Fuerzas, con avances en coordinación y anticipación ante vectores hostiles.	La coordinación es limitada; no hay ejercicios regulares ni estrategia común. Se requiere entrenamiento conjunto periódico.
Capacidades críticas y en desarrollo	Identifica como críticas las de fuego y mando y control, y en desarrollo las de inteligencia, soporte y protección.	Consideran necesaria una reingeniería doctrinal y desarrollo de capacidades de inteligencia e investigación aplicada.
Gestión de incidentes cibernéticos	Se ha avanzado en la estandarización de procesos y la reacción inmediata ante incidentes.	La respuesta es más reactiva que proactiva, sin análisis completo de vectores APT ni del ciclo de inteligencia.

Categoría de análisis	Comandante del CCOCI	Comandantes de Unidades Cibernéticas (Ejército, Armada, FAC)
Lecciones aprendidas	Destaca la importancia del liderazgo coordinado, la identificación de vectores y el diseño de controles anticipatorios.	Señalan falta de retroalimentación, seguimiento y motivación posterior a los ejercicios cibernéticos.
Brechas identificadas	Limitaciones presupuestales y alta rotación de personal especializado.	Deficiencias en inteligencia, doctrina desactualizada y estructura organizacional poco adecuada.
Acciones estratégicas a futuro (2025–2030)	Modernización de la ICCN e ICCM, fortalecimiento de alianzas internacionales y desarrollo de capacidades cognitivas, IA y computación cuántica.	Crear una hoja de ruta definida, integrar la inteligencia al marco legal, potenciar I+D+i y participar en ejercicios estratégicos.
Percepción general de evolución del CCOCI	Evalúa la evolución como positiva, con consolidación progresiva del liderazgo cibernético nacional.	Perciben estancamiento: el CCOCI perdió liderazgo regional por falta de innovación y enfoque estratégico.

Fuente: Elaboración propia con base en entrevistas institucionales al Comandante del CCOCI y a los Comandantes de las Unidades Cibernéticas de las Fuerzas Militares de Colombia (2025).

Cooperación internacional y ciberdiplomacia

La dimensión internacional se ha convertido en un pilar estructural del CCOCI. La cooperación técnica con aliados como SOUTHCOM, OTAN, Francia y Brasil ha permitido fortalecer doctrinas conjuntas y estandarizar procedimientos. Esta colaboración también ha posibilitado la participación en ejercicios de alta complejidad, entre los que destaca Locked Shields, organizado por el Centro de Excelencia en Ciberdefensa Cooperativa (CCDCOE).

A nivel hemisférico, la participación activa de Colombia en las iniciativas de la OEA-CICTE (2023) ha favorecido la transferencia de capacidades y la adopción de buenas prácticas regionales. Dicha colaboración no solo se circunscribe al intercambio técnico, sino que también fortalece la ciberdiplomacia, concebida como la proyección internacional de las capacidades nacionales en el ciberespacio (WEF, 2024).

Logros, vacíos y oportunidades

Entre los logros más importantes destacan:

- La madurez alcanzada por el CCOCI como actor conjunto y especializado.
- La implementación efectiva del Plan Arkano Plus 2024–2026.
- La alineación con la ENSD 2025-2027 y con estándares internacionales.

- La consolidación de un ecosistema nacional de cooperación técnica con CSIRT sectoriales.

No obstante, persisten vacíos, entre los cuales se destacan la falta de un manual conjunto vigente, la ausencia de un modelo de madurez cibernética militar medible y la necesidad de reducir las brechas tecnológicas entre las Fuerzas. Asimismo, la incorporación de inteligencia artificial, automatización y analítica avanzada sigue en fase de desarrollo (IRM, 2025).

Las oportunidades estratégicas se centran en fortalecer la gobernanza conjunta, mejorar la retención del talento técnico, impulsar programas de investigación aplicada y consolidar un ecosistema nacional de innovación cibernética que se vincule con universidades y el sector privado.

Gobernanza, conjuntez y ciberdefensa colaborativa

La ciberdefensa colaborativa se asume como un principio esencial. Esta no constituye una función aislada del CCOCI, sino una responsabilidad compartida entre los proveedores tecnológicos y los responsables de las ICCN/ICCM. Su éxito, por ende, depende de la sinergia operativa, la interoperabilidad doctrinal y la confianza institucional.

La conjuntez, en este contexto, representa el medio a través del cual la colaboración se traduce en resultados operacionales, ya que permite coordinar capacidades, compartir inteligencia de amenazas e integrar respuestas ante incidentes críticos. Los entrevistados coinciden en que la consolidación de esta cultura colaborativa ha reducido los tiempos de detección y mejorado la trazabilidad de las decisiones en escenarios de crisis.

Alineación estratégica: Arkano Plus – Ayacucho – PEMT 2042 – ENSD

Existe coherencia vertical y horizontal entre las estrategias. De manera vertical, el Plan Arkano Plus aterriza los objetivos del Plan Ayacucho Plus y del PEMT 2042, lo cual garantiza preparación, disuasión, respuesta y mejora continua. De manera horizontal, integra la ENSD 2025-2027, el Decreto 338 de 2022 y el MSPI actualizado, lo que genera un marco de acción armónico que unifica la política pública y la doctrina militar.

Esta alineación ofrece al CCOCI un marco de legitimidad y consistencia estratégica, puesto que el Comando deja de ser un actor puramente técnico para convertirse en un gestor de política pública en el dominio cibernético militar. En síntesis, Colombia cuenta hoy con un andamiaje normativo y doctrinal robusto

que sustenta su defensa digital. El CCOCI ha pasado de ser un centro de respuesta técnica a convertirse en el eje estratégico de la ciberdefensa nacional, que integra las políticas públicas, la doctrina militar y la cooperación internacional.

En este sentido, el Plan Arkano Plus 2024-2026 se consolida como la base operativa que articula la protección, la resiliencia y la defensa activa del sector defensa. Esta iniciativa se alinea, además, con la ENSD 2025-2027 y la visión PEMT 2042. Al respecto, las entrevistas confirman avances reales, pero también la necesidad de actualizar la doctrina, fortalecer la conjuntez y asegurar la continuidad del talento especializado.

El éxito de la ciberdefensa colaborativa, concebida como una responsabilidad compartida entre el CCOCI, los proveedores y los dueños de infraestructuras críticas, dependerá de mantener la sinergia interinstitucional y la cooperación con aliados, lo que permitirá al CCOCI enfrentar con eficacia los desafíos futuros del ciberespacio.

Con esta base consolidada de doctrina, políticas y capacidades, el siguiente objetivo presentará la estrategia integral para fortalecer la capacidad del CCOCI frente a los desafíos actuales de ciberseguridad, la cual establecerá metas medibles, fases de ejecución y criterios de sostenibilidad hacia 2042.

Estrategia para fortalecer la capacidad del CCOCI frente a los desafíos actuales de ciberseguridad

Propósito y enfoque

Tras identificar las amenazas, los vectores y las brechas estructurales en los objetivos anteriores, este tercer componente formula una estrategia integral de fortalecimiento institucional del CCOCI, cuyo objetivo es robustecer su capacidad de conducción y respuesta frente a un entorno de riesgo dinámico, híbrido y persistente, en el cual convergen la guerra de información, el espionaje digital, los ciberataques y las operaciones cognitivas.

La estrategia se alinea con el Plan Arkano Plus 2024-2026, el Plan de Campaña Estratégico Conjunto Ayacucho Plus y el PEMT 2042, de tal manera que constituye una hoja de ruta para evolucionar de un esquema de reacción técnica hacia un modelo de gestión anticipatoria, integral y medible. Este modelo está sustentado en cuatro pilares gerenciales: doctrina, talento, tecnología y cooperación, bajo el principio de que la ciberdefensa es una responsabilidad colaborativa entre el CCOCI, los proveedores tecnológicos y los administradores de las ICCN/ICCM.

Por lo tanto, el éxito del CCOCI no radica exclusivamente en su infraestructura técnica, sino en su capacidad de generar sinergia institucional entre las Fuerzas, las agencias estatales y los aliados estratégicos. Así, esta estrategia busca proyectar al CCOCI como el centro gravitacional del poder cibernético militar colombiano con una gobernanza madura, personal especializado y una arquitectura tecnológica resiliente que asegure la continuidad de su misión constitucional, incluso en condiciones de ataque sostenido.

Principios rectores

Los principios que guían esta estrategia responden a un enfoque integral de liderazgo, gobernanza y sostenibilidad institucional:

1. **Conjuntez efectiva**. La planeación, ejecución y evaluación deben ser integradas entre Fuerzas, con doctrina unificada y estándares interoperables.
2. **Resiliencia operacional.** La continuidad de la misión es el criterio superior, el cual articula personas, procesos, tecnología y logística en un solo sistema.
3. **Defensa basada en inteligencia.** La priorización de esfuerzos debe responder al riesgo y al impacto sobre la misión, con base en inteligencia táctica y estratégica (IT/OT/ICS).
4. **Mejora continua (PHVA).** Cada incidente, auditoría y ejercicio debe traducirse en lecciones aprendidas institucionalizadas.
5. **Legalidad y legitimidad.** Toda acción en el ciberespacio debe ajustarse al DIH, los Derechos Humanos y la legislación colombiana.
6. **Innovación aplicada.** Adopción prudente de IA, la automatización y el desarrollo local de soluciones, con vigilancia tecnológica y soberanía digital.
7. I**nteroperabilidad y cooperación.** La defensa del ciberespacio requiere articulación permanente entre el sector defensa, el sector privado, la academia y los aliados internacionales.

Transformación institucional del CCOCI

En la última década, el CCOCI ha pasado de ser un centro técnico de monitoreo a convertirse en un comando estratégico con alcance nacional, responsable de la seguridad digital militar y de la articulación con el ecosistema nacional de ciberseguridad. Sin embargo, la naturaleza intrínseca del ciberespacio, marcada por su asimetría, anonimato y velocidad, exige un salto cualitativo: pasar de ser un actor operativo a ser el arquitecto del sistema de defensa digital militar colombiano.

La estrategia plantea al CCOCI como un gestor del conocimiento cibernético, cuya capacidad radica en anticipar, integrar y coordinar acciones conjuntas entre

el Ejército, la Armada y la Fuerza Aeroespacial. Dicha gestión se fundamenta en un enfoque de liderazgo estratégico y pensamiento sistémico. Específicamente, este modelo se inspira en el concepto de C4ISR+Cyber de la OTAN (NATO CCDCOE, 2023), que combina mando, control, comunicaciones, inteligencia, vigilancia y ciberdefensa en un solo marco de gobernanza.

La finalidad es que el CCOCI no solo reaccione ante amenazas, sino que administre el riesgo cibernético como una función de mando y control, en lugar de una tarea técnica subordinada. Esta perspectiva lo convierte en un instrumento de decisión del Comando General, y no únicamente en un componente operativo.

Ejes estratégicos de fortalecimiento

Eje 1. Gobernanza, doctrina y estandarización conjunta

La gobernanza debe institucionalizarse mediante la publicación y adopción del Manual Conjunto de Ciberseguridad y Ciberdefensa, el cual deberá establecer roles, flujos de decisión, métricas, taxonomías y procedimientos unificados, y que, consecuentemente, constituirá la base para la interoperabilidad entre Fuerzas y con organismos civiles.

La estrategia también plantea consolidar un Consejo de Gobernanza Cibernética (CGC) que estará liderado por el Comandante del CCOCI e integrado por las jefaturas J2, J3 y J6, además de un enlace doctrinal y jurídico. Este Consejo tendrá como misión fijar prioridades anuales, aprobar proyectos, definir indicadores de madurez y supervisar la ejecución de la estrategia.

En paralelo, se formaliza la PMO Arkano (Oficina de Proyectos de Ciberdefensa), encargada de traducir las directrices del CGC en planes, presupuestos y métricas, lo que asegura la continuidad institucional y el control de avance.

Eje 2. Operaciones inteligentes y automatización

El CCOCI debe consolidar una operación centrada en datos e inteligencia, capaz de orquestar alertas, correlacionar eventos y generar información táctica para la toma de decisiones. En este sentido, se prioriza la automatización de casos de uso con herramientas SOAR y UEBA para reducir los tiempos de detección (MTTD) y respuesta (MTTR) en al menos 40 % durante los primeros doce meses.

La automatización no busca reemplazar al analista, sino liberarlo de tareas repetitivas para que se concentre en la interpretación táctica. De esta manera, la combinación de IA supervisada y análisis humano fortalecerá la capacidad del SOC para operar en escenarios de alta carga sin degradar su efectividad.

Eje 3. Protección de ICCN e ICCM con enfoque diferencial

Las infraestructuras críticas son el corazón operativo de la defensa nacional, por ello, la estrategia propone fortalecer su seguridad mediante segmentación macro/micro, gestión de vulnerabilidades basada en el impacto de la misión, políticas Zero Trust y pruebas periódicas de recuperación.

Con este propósito, se establecerán acuerdos de nivel de servicio (SLA) con los dueños de las ICCN/ICCM y proveedores estratégicos, los cuales definirán responsabilidades compartidas en monitoreo, contingencia y evidencia digital.

Eje 4. Talento, cultura y liderazgo técnico

El eje humano es el núcleo estratégico. Actualmente, la principal vulnerabilidad del sistema cibernético militar no radica en aspectos tecnológicos, sino estructurales, concretamente en la carencia de personal especializado, cuyo déficit de analistas T2 y T3 limita la capacidad del CCOCI para sostener operaciones continuas y desarrollar nuevas capacidades.

El Comando reconoce que la profesionalización cibernética no puede seguir dependiendo de capacitaciones externas. Por tanto, se plantea la creación formal de la especialidad cibernética dentro de las Fuerzas Militares, proyectada como una carrera de servicio, con escuelas y certificaciones propias.

Este desafío enfrenta una barrera constitucional: el artículo 217 de la Constitución Política de 1991, que reconoce únicamente tres Fuerzas (Ejército, Armada y Fuerza Aérea). Sin embargo, la evolución del conflicto global, sumada al reconocimiento internacional del ciberespacio como dominio de guerra (OTAN, 2016), justifican la necesidad de una especialidad cibernética transversal. Dicha especialidad no implicaría crear una "cuarta fuerza", sino dotar a las Fuerzas existentes de un componente especializado en ciberdefensa, articulado bajo el CCOCI.

Específicamente, el fortalecimiento del talento humano se abordará mediante cuatro líneas:

1. Priorizar suboficiales con entre 6 y 10 años de servicio proyectado y oficiales jóvenes con vocación técnica, para asegurar su permanencia poscertificación durante 24-36 meses.
2. **Incentivos diferenciados:** bonos por rol crítico, certificación o disponibilidad operativa 24/7.
3. **Formación y rotación inter-Fuerzas:** convenios con universidades y aliados (OTAN, SOUTHCOM, academia nacional), con el fin de desarrollar un programa de certificaciones conjuntas.

4. **Reserva cibernética:** incorporar personal retirado o civil experto a través de mecanismos de reingreso temporal, una medida que fortalece la continuidad de la misión y asegura la disponibilidad de una reserva técnica y operativa esencial para momentos de necesidad.

En síntesis, el CCOCI debe convertirse en el centro de excelencia en talento cibernético de las Fuerzas Militares, no solo un operador de seguridad.

Modelo de indicadores (KPI y KRI)

Los Indicadores Clave de Desempeño (KPI) y los Indicadores Clave de Riesgo (KRI) son los mecanismos de gobierno que permiten transformar la estrategia en resultados verificables. En esta caso específico se dividen en cuatro niveles, como se describe a continuación.

1. Indicadores de desempeño operacional

- MTTD (Mean Time to Detect): tiempo promedio de detección de incidentes. **Meta:** reducción del 40 % en 12 meses y del 60 % en 24 meses.
- MTTR (Mean Time to Respond): tiempo promedio de contención y mitigación. **Meta:** reducción del 35 % en 12 meses y del 55 % en 24 meses.
- Contención temprana (≤ 24 h): **meta** de 75 % de incidentes críticos controlados en menos de un día.
- Casos de uso automatizados: **incremento gradual** de 10 a 50 casos priorizados según criticidad.

Estos indicadores miden la eficiencia de los procesos operativos del SOC/CSIRT y reflejan la capacidad de resiliencia técnica del CCOCI.

2. Indicadores de talento y sostenibilidad

- Tasa de fuga de personal técnico: **meta** de ≤ 12 % anual, bajando a ≤ 8 % en 24 meses.
- Retención poscertificación: **al menos** 80 % del personal formado debe permanecer 24 meses tras su certificación.
- Cobertura de roles críticos: **alcanzar** el 90 % de los puestos técnicos ocupados.
- Horas de mentoría: **mínimo** 6 h mensuales por analista senior.
- Tasa de reposición de vacantes críticas: **menor** a 30 días hábiles.

Estos KPI aseguran que la inversión en talento se traduzca en permanencia y que el conocimiento no se pierda por rotación.

3. Indicadores de gobernanza y doctrina

- Cumplimiento de auditorías: **100 % de procesos** con seguimiento y sin hallazgos críticos.
- Porcentaje de doctrinas actualizadas: **100 % del personal** entrenado en el nuevo Manual Conjunto.
- Ejecución presupuestal estratégica: **95 % del presupuesto** de ciberdefensa ejecutado según plan anual.
- Participación interinstitucional: al menos dos ejercicios TTX y un CPX por año con aliados nacionales.

Estos indicadores miden la madurez institucional y la capacidad de liderazgo estratégico del CCOCI.

4. Indicadores de cooperación e impacto estratégico

- Participación internacional: **mínimo** un ejercicio multinacional por año.
- Tiempos de notificación TLP. **menos de 2 horas** para incidentes de alto impacto.
- Proyectos de I+D en curso: **al menos tres** iniciativas activas con universidades o industria.
- Índice de percepción de aliados (confianza): **evaluación semestral** mediante encuestas de satisfacción y desempeño.

Estos KPI consolidan la posición del CCOCI como referente regional y actor confiable en ciberdefensa.

Gobernanza, cultura organizacional y liderazgo

El éxito de la estrategia depende de una gobernanza disciplinada que sea capaz de vincular la alta dirección con la operación diaria, de ahí que la estructura organizacional se apoye en tres niveles:

1. **Nivel estratégico:** el Consejo de Gobernanza Cibernética (CGC), liderado por el Comandante del CCOCI, define prioridades, aprueba proyectos y evalúa resultados.
2. **Nivel táctico:** la PMO Arkano gestiona cronogramas, riesgos, comunicaciones y métricas.

3. **Nivel operativo:** los equipos SOC/CSIRT ejecutan acciones y generan reportes en tiempo real.

En el campo cultural, se promoverá una mentalidad de misión, donde cada integrante del CCOCI entienda que su tarea técnica tiene un propósito estratégico. Esta concepción, a su vez, implica liderazgo horizontal, mentoría constante y una cultura de aprendizaje continuo. En este sentido, el liderazgo cibernético debe concebirse como una competencia institucional, razón por la cual se propone incluir una asignatura obligatoria sobre operaciones en el ciberespacio en la formación de mandos medios y altos, la cual deberá integrar componentes éticos, legales y de gestión de crisis.

Fortalecimiento de la especialidad cibernética en las Fuerzas Militares

La Constitución Política de 1991, en su artículo 217, define que la Nación tendrá para su defensa tres Fuerzas Militares: el Ejército, la Armada y la Fuerza Aérea. Si bien este marco jurídico no contempla expresamente el ciberespacio como un dominio de guerra, la realidad operacional del siglo XXI demuestra que la defensa nacional requiere una cuarta dimensión funcional: el ciberespacio.

Como se señaló, no se trata de crear una nueva Fuerza, sino de establecer la especialidad cibernética militar como un componente transversal y permanente, dependiente del CCOCI, para lo cual debe contar con doctrina propia, plan de carrera, escuela de formación y régimen de ascensos.

El Plan Estratégico Militar de Transformación (PEMT 2042) ya reconoce la necesidad de consolidar capacidades multidominio, de ahí que la integración de la especialidad cibernética se presente como un paso natural en esta evolución. Con este fin, la estrategia plantea tres líneas de acción:

1. Creación de la Escuela Militar Cibernética Conjunta, que forme especialistas en ciberdefensa, inteligencia digital, análisis forense y respuesta a incidentes.
2. Programa de carrera técnica cibernética que permita a suboficiales y oficiales desarrollar una trayectoria de largo plazo en el dominio cibernético.
3. Sistema de incentivos vinculado a competencias certificadas, desempeño y disponibilidad operativa.

La consolidación de esta especialidad permitirá a Colombia contar con un núcleo de expertos permanentes, lo que reducirá la dependencia de contratistas externos y fortalecerá la soberanía digital del Estado.

Sostenibilidad, innovación y cooperación internacional

La sostenibilidad de la estrategia exige un equilibrio entre la inversión tecnológica, el talento humano y la cooperación. En este contexto, la automatización y el uso de inteligencia artificial deben adoptarse con una filosofía de "IA centrada en el humano", en la cual la tecnología no reemplaza el criterio táctico del analista, sino que amplía sus capacidades.

Además, la cooperación internacional seguirá siendo un eje clave, pues la participación en ejercicios de la OTAN, la OEA-CICTE y el SOUTHCOM permite medir capacidades, validar doctrina y proyectar al CCOCI como un socio confiable en la defensa hemisférica. Asimismo, se fortalecerá la diplomacia cibernética militar, que no se limita a la coordinación técnica, sino que también busca establecer marcos de confianza, protocolos de intercambio de inteligencia y una participación activa en foros multilaterales.

Proyección y cierre

El CCOCI se proyecta como el centro de excelencia en ciberdefensa militar de América Latina, con capacidades maduras, doctrina consolidada y talento especializado. Su éxito dependerá de tres condiciones:

1. Conjuntez real: integración doctrinal, entrenamiento conjunto y estandarización operativa.
2. Talento humano especializado: institucionalización de la carrera cibernética militar.
3. Gobernanza medible: decisiones basadas en evidencia y en indicadores de desempeño verificables.

La estrategia propuesta traza un camino viable, medible y sostenible. La conversión del CCOCI en un comando maduro y adaptable permitirá, en primer lugar, acortar brechas frente a amenazas avanzadas y proteger las infraestructuras críticas. Además, esta transformación fortalecerá la soberanía digital y consolidará la legitimidad de las Fuerzas Militares en el ciberespacio.

Con esta hoja de ruta gerencial, el CCOCI no solo enfrentará los desafíos actuales de la ciberseguridad, sino que también liderará la transformación del poder militar colombiano hacia la era digital, lo cual asegurará la continuidad de la misión constitucional, la defensa de la Nación y el cumplimiento de los compromisos internacionales asumidos por Colombia.

Conclusiones

El recorrido realizado en este capítulo permite comprender con mayor claridad el lugar que ocupa el ciberespacio en la defensa nacional y, en particular, el papel que desempeña el CCOCI en las Fuerzas Militares de Colombia. El análisis de sus amenazas, marcos doctrinales y estrategias demuestra que el ciberespacio se ha consolidado como un dominio de confrontación real, en el cual las operaciones no solo buscan afectar la infraestructura tecnológica, sino también influir en la información, la toma de decisiones y la legitimidad institucional del Estado.

El primer objetivo, centrado en las amenazas cibernéticas y los desafíos de seguridad que enfrenta el CCOCI, reveló un escenario operativo complejo y en expansión. Las cifras analizadas reflejan que Colombia ya no es un observador pasivo del conflicto digital, sino un blanco activo de agresiones estructuradas, lo cual se evidencia en más de 177 mil millones de eventos procesados en 2025 y un crecimiento sostenido de incidentes. Además, las ANC han encontrado en el ciberespacio militar un terreno fértil para el espionaje y la disrupción estratégica, e incluyen grupos de crimen organizado, actores patrocinados por Estados y campañas de desinformación.

Este contexto evidenció que la guerra cibernética moderna combina lo técnico con lo psicológico, y se articula en fases de reconocimiento, acceso inicial, persistencia, escalamiento de privilegios y exfiltración de información. Los ataques no se presentan de manera aislada, sino con arquitecturas multietapa que requieren defensas igualmente inteligentes y adaptativas. En ese sentido, el capítulo mostró cómo la protección del dominio cibernético militar exige no solo tecnología avanzada, sino también comprensión de los factores humanos, del comportamiento adversario y de los patrones de persistencia digital que desafían los límites tradicionales de la defensa.

Un hallazgo fundamental de este primer objetivo fue la necesidad de fortalecer la conjuntez operacional y la colaboración entre las distintas Fuerzas y dependencias del CGFM. Es decir, la ciberdefensa no puede concebirse como una acción aislada del CCOCI, sino como una responsabilidad compartida entre los administradores de las ICCN/ICCM, los proveedores tecnológicos y las autoridades estatales. Por consiguiente, solo mediante una sinergia real entre todos estos actores será posible anticipar, contener y responder a amenazas en constante evolución.

El segundo objetivo permitió analizar el marco normativo, doctrinal y estratégico que sustenta la acción del CCOCI. El estudio de los documentos CONPES 3701, 3854 y 3995, así como las disposiciones emanadas del Ministerio de Defensa

Nacional —tales como la Directiva 140 de 2013, la Disposición 002 de 2022 y la Resolución 7870 de 2022—, reveló una estructura normativa robusta, aunque todavía en proceso de maduración. En síntesis, Colombia cuenta con los cimientos legales y doctrinales necesarios para ejercer la defensa en el ciberespacio, pero aún requiere actualizar y consolidar su marco operativo conjunto.

En este apartado también se destacó el Plan Arkano Plus 2024-2026, no solo como instrumento de planeación, sino también como eje articulador de la transformación digital militar. Este plan, alineado con el PEMT 2042 y el Plan Ayacucho Plus, ha permitido ordenar las capacidades sobre tres pilares: protección cibernética, resiliencia cibernética y defensa cibernética, cada uno con una función esencial dentro del ciclo de seguridad: prevenir, resistir y responder. Sin embargo, el análisis también mostró que estos avances normativos y doctrinales deben traducirse en capacidades sostenibles, indicadores verificables y un modelo de gobernanza. Este último es crucial para asegurar la continuidad a largo plazo.

De igual forma, el capítulo resaltó que la doctrina debe adaptarse a la velocidad del entorno digital. Aún existe una brecha crítica por la ausencia de un Manual Conjunto actualizado de Ciberseguridad y Ciberdefensa, instrumento que permitiría estandarizar conceptos, reglas de enfrentamiento y procedimientos técnicos entre las Fuerzas. Este vacío no solo genera fragmentación operativa, sino que también limita la interoperabilidad con socios internacionales. Por ello, la actualización doctrinal se identifica como un imperativo estratégico.

El tercer objetivo, enfocado en el diseño de una estrategia para fortalecer la capacidad del CCOCI, consolidó los hallazgos previos en un marco de acción integral. La estrategia propuesta no se limita al ámbito técnico, sino que está diseñada bajo una lógica gerencial y de transformación institucional, que coloca al CCOCI como eje articulador del poder cibernético militar colombiano.

Uno de los componentes más relevantes de esta estrategia es el fortalecimiento del talento humano especializado. El documento argumenta que la brecha más significativa del sistema no es tecnológica, sino humana, manifestada por la escasez de personal técnico con formación avanzada, la alta rotación y la dependencia de contratistas, factores que debilitan la sostenibilidad de la defensa digital. Por consiguiente, la creación de la especialidad cibernética militar se propone como una necesidad inaplazable.

Ahora bien, este punto adquiere relevancia constitucional y estratégica, pues aunque el artículo 217 de la Constitución Política de 1991 reconoce solo tres Fuerzas (Ejército, Armada y Fuerza Aérea), la evolución del conflicto moderno demanda una dimensión transversal cibernética dentro de ellas, la cual, lejos de

implicar una nueva Fuerza, constituye una capacidad permanente y multidominio articulada bajo el CCOCI. Específicamente, su implementación apoyaría con continuidad institucional, profesionalización del talento y soberanía tecnológica.

Asimismo, la estrategia plantea que la defensa cibernética debe sustentarse en indicadores de desempeño (KPI) y riesgo (KRI) que permitan evaluar de manera objetiva la eficacia de las acciones emprendidas. La reducción del tiempo promedio de detección y respuesta (MTTD/MTTR), la tasa de contención temprana, la retención poscertificación, la cobertura de roles críticos y la participación en ejercicios interinstitucionales se proponen como métricas de gobierno que convierten la ciberdefensa en un proceso medible, no intuitivo.

El capítulo también resaltó la importancia de una gobernanza disciplinada, razón por la cual la creación del Consejo de Gobernanza Cibernética y de la PMO Arkano permitirá institucionalizar la planeación, el seguimiento y la rendición de cuentas. Esta estructura de mando es esencial para pasar de una defensa reactiva a una gestión estratégica del riesgo cibernético, alineada con los estándares internacionales de la OTAN y la OEA.

En el plano cultural, también se reconoció que el liderazgo cibernético debe ser una competencia esencial de los mandos militares, de tal manera que formar líderes capaces de comprender las implicaciones tácticas, jurídicas y políticas del ciberespacio resultará determinante para consolidar la legitimidad y la eficacia de la defensa. En este sentido, el CCOCI no solo debe operar redes, sino además construir cultura estratégica y conciencia situacional digital en todos los niveles de la Fuerza.

El cierre del capítulo subraya que la ciberdefensa, entendida como responsabilidad compartida entre el CCOCI, los administradores de las ICCN/ICCM y los proveedores tecnológicos, solo alcanzará su eficacia plena si se articula bajo principios de conjuntez, cooperación y soberanía tecnológica. La seguridad del ciberespacio militar colombiano dependerá, en última instancia, de la capacidad del Estado para alinear su doctrina, su talento y su infraestructura hacia un mismo propósito: la continuidad de la misión constitucional en el ámbito digital.

En suma, este capítulo demuestra que la defensa en el ciberespacio no es un desafío técnico, sino estratégico y humano. Colombia ha avanzado en el fortalecimiento de su gobernanza digital, en la consolidación de su marco normativo y en la profesionalización del CCOCI. No obstante, el ritmo de las amenazas impone la necesidad de acelerar la madurez institucional y doctrinal.

Referencias

Agencia de la Unión Europea para la Ciberseguridad [ENISA]. (2023). *ENISA threat landscape 2023: Emerging threats*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Armis. (2025). *The state of cyberwarfare 2025*. Armis Security.

C4 – Centro de Capacidades para la Ciberseguridad de la Policía Nacional. (2024). *Informe nacional sobre amenazas cibernéticas al sector defensa*. Policía Nacional de Colombia.

Centro Cibernético Policial. (2023). *Informe anual de incidentes cibernéticos en Colombia*. Policía Nacional de Colombia. https://caivirtual.policia.gov.co/observatorio/analisis-cibercrimen

Comando Conjunto Cibernético de Colombia [CCOCI]. (2023). *Resumen estadístico anual del Comando Conjunto Cibernético – Año 2023* [Documento interno]. Departamento de Operaciones del CCOCI.

Comando Conjunto Cibernético de Colombia [CCOCI]. (2024). *Resumen estadístico del 28 de noviembre al 04 de diciembre de 2024* [Documento interno]. Departamento de Operaciones del CCOCI.

Comando Conjunto Cibernético de Colombia [CCOCI]. (2025a). *Estrategia cibernética militar 2025* [Documento interno]. Comando General de las Fuerzas Militares.

Comando Conjunto Cibernético de Colombia [CCOCI]. (2025b). *Plan de ciberseguridad y ciberdefensa Arkano Plus 2024–2026* [Documento interno]. Comando General de las Fuerzas Militares.

Comando Conjunto Cibernético de Colombia [CCOCI]. (2025c). *Resumen estadístico del 16 al 22 de mayo de 2025* [Documento interno]. Departamento de Operaciones del CCOCI.

Comando Conjunto Cibernético de Colombia [CCOCI]. (2025d). *Resumen estadístico del 20 al 26 de junio de 2025* [Documento interno]. Departamento de Operaciones del CCOCI.

Comando General de las Fuerzas Militares [CGFM]. (2018). *Manual Fundamental Conjunto MFC 1.0: Doctrina conjunta*. Comando General de las Fuerzas Militares. https://esdegue.edu.co/sites/default/files/2024-09/MFC%201.0%20DOCTRINA%20CONJUNTA.pdf

Comando General de las Fuerzas Militares [CGFM]. (2023). *Manual Fundamental Conjunto MFC 3-0: Operaciones conjuntas*. Comando General de las Fuerzas Militares. https://esdegue.edu.co/sites/default/files/2024-05/MFC%203-0%20OPERACIONES%20CONJUNTAS.pdf

Comando General de las Fuerzas Militares [CGFM]. (2024). *Manual Fundamental Conjunto MFC 5-0: Planeamiento conjunto*. Comando General de las Fuerzas Militares. https://esdegue.edu.co/sites/default/files/2024-06/MFC%205-0%20PLANEAMIENTO%20CONJUNTO-4.pdf

Comando General de las Fuerzas Militares [CGFM]. (2024). *Plan de Campaña Estratégico Conjunto Ayacucho Plus* [Documento institucional]. Comando General de las Fuerzas Militares.

Comando General de las Fuerzas Militares. (s. f.). P*lan Estratégico Militar de Transformación (PEMT) 2042* [Documento institucional]. Comando General de las Fuerzas Militares.

Consejo Nacional de Política Económica y Social. (2011). *CONPES 3701: Lineamientos de política para la ciberseguridad y la ciberdefensa.* Departamento Nacional de Planeación (DNP). https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Consejo Nacional de Política Económica y Social. (2016). *CONPES 3854: Política nacional de seguridad digital.* Departamento Nacional de Planeación (DNP). https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Consejo Nacional de Política Económica y Social. (2020). *CONPES 3995: Política nacional de confianza y seguridad digital.* Departamento Nacional de Planeación (DNP). https://colaboracion.dnp.gov.co/cdt/Conpes/Econ%C3%B3micos/3995.pdf

Constitución Política de Colombia. (1991). *Artículo 217.* Diario Oficial de la República de Colombia.

Decreto 338 de 2022. Por el cual se adiciona el Título 21 al Decreto Único 1078 de 2015 (gobernanza de la seguridad digital, ICCN y coordinación de incidentes). Presidencia de la República de Colombia D. O. 52271, 22 de marzo de 2022. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866

Departamento Nacional de Planeación. (2023). P*lan Nacional de Desarrollo 2022–2026: Colombia potencia mundial de la vida.* DNP. https://www.dnp.gov.co/plan-nacional-desarrollo/pnd-2022-2026

Dirección Nacional de Inteligencia. (2023). *Informe técnico de riesgo cibernético sectorial 2023–2024* [Documento clasificado].

Escuela Superior de Guerra [ESDEG]. (2023). *Manual de doctrina conjunta sobre operaciones cibernéticas en las Fuerzas Militares de Colombia* [Documento interno]. ESDEGUE.

Escuela Superior de Guerra. (2024). *Manual de ciberdefensa para las Fuerzas Militares Colombianas (FF.MM. 3-38).* ESDEGUE.

Foro Económico Mundial. (2024). *The global cybersecurity outlook 2024.* World Economic Forum. https://www.weforum.org/reports/global-cybersecurity-outlook-2024

IBM X-Force. (2024). *Threat intelligence index: Latin America highlights.* International Business Machines Corporation. https://www.ibm.com/security/data-breach/threat-intelligence

Institute of Risk Management (IRM). (2025). *Risk trends 2025.* IRM Global. https://www.theirm.org/news/irm-risk-trends-2025-report/

Ley 1273 de 2009. *Por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos*. Congreso de la República. *D.O.* 47239, 5 de enero de 2009. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Ley 1581 de 2012. *Por la cual se dictan disposiciones generales para la protección de datos personales.* Congreso de la República. *D. O.* 48587, 18 de octubre de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Ley 1621 de 2013. *Por la cual se expiden normas para fortalecer el marco jurídico de inteligencia y contrainteligencia*. Congreso de la República. D. O. 48740, 17 de abril de 2013. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=52706

Mandiant. (2022). *Threat actor profiles and UNC classification system.* https://www.mandiant.com/resources/apt-groups

Ministerio de Defensa Nacional [MDN]. (2013). *Directiva Permanente No. 140: Activación del Centro de Operaciones de Seguridad del CCOCI.* MDN.

Ministerio de Defensa Nacional [MDN]. (2020). *Política de Seguridad y Defensa para el Ciberespacio* [Documento institucional]. MDN.

Ministerio de Defensa Nacional [MDN]. (2022). *Disposición No. 002: Reglas de enfrentamiento para operaciones militares cibernéticas.* MDN.

Ministerio de Defensa Nacional [MDN]. (2022). *Resolución 7870: Política general de seguridad digital del sector defensa.* MDN.

Ministerio de Defensa Nacional [MDN]. (2024). *Informe de implementación del Plan ARKANO PLUS* [Documento institucional]. CCOCI/MDN.

Ministerio de Tecnologías de la Información y las Comunicaciones [MinTic]. (2018). *Manual de Gobierno Digital* (versión 6). MinTIC. https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/Manual-de-Gobierno-Digital/

Ministerio de Tecnologías de la Información y las Comunicaciones [MinTic]. (2025). *Estrategia Nacional de Seguridad Digital 2025–2027.* MinTIC. https://www.mintic.gov.co/portal/715/articles-403023_recurso_2.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones [MinTic]. (2025, 25 de junio). *Resolución 02277 de 2025: Actualización del Modelo de Seguridad y Privacidad de la Información (MSPI) alineado con ISO/IEC 27001:2022.* MinTIC.

MITRE Corporation. (2024). *ATT&CK framework for enterprise.* https://attack.mitre.org/

NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE]. (2023). *Locked Shields technical report.* OTAN.

NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE]. (2023). *Cyber defence framework and C4ISR integration.* OTAN.

Organización de los Estados Americanos [OEA] – Comité Interamericano contra el Terrorismo [CICTE]. (2022). E*stado de la ciberseguridad en América Latina y el Caribe.* OEA.

Organización de los Estados Americanos [OEA]. (2022). *Guía de capacidades de ciberseguridad en América Latina y el Caribe.* OEA.

Resolute Sentinel. (2024). Ejercicio conjunto cibernético multinacional. SOUTHCOM – Fuerza Aérea Colombiana.

U.S. Cybersecurity and Infrastructure Security Agency [CISA]. (2023). *MITRE ATT&CK: Adversarial tactics, techniques, and common knowledge.* https://attack.mitre.org/

U.S. Southern Command [Southcom]. (2023). *Cyber defense cooperation and exercises report.* U.S. Department of Defense.

World Economic Forum. (2024). *Global cybersecurity outlook 2024.* WEF. https://www.weforum.org/reports/global-cybersecurity-outlook-2024

Capítulo 5

Ciberseguridad en el sector universitario colombiano: diagnóstico, desafíos y recomendaciones para un entorno digital seguro*

DOI: https://doi.org/10.25062/9786287818644.05

Jeison Stiven Melo Mendoza
Universidad Militar Nueva Granada

Resumen: La creciente digitalización de las instituciones de educación superior (IES) en Colombia ha revelado importantes desafíos en materia de ciberseguridad, especialmente frente al incremento de ataques cibernéticos dirigidos a entornos educativos. Este capítulo tiene como propósito proponer estrategias de mitigación ajustadas a las capacidades tecnológicas, normativas y organizacionales de las IES en Colombia, considerando sus niveles de madurez digital y sus condiciones operativas. Para ello, se basa en la aplicación de un enfoque metodológico cualitativo que parte del análisis bibliográfico para evaluar el estado actual de la ciberseguridad en las IES colombianas. A partir de este análisis, se concluye que existen brechas estructurales en gobernanza digital, la implementación de sistemas de gestión, el cumplimiento normativo y la articulación organizacional. Así, el capítulo contribuye a construir una base estratégica para reforzar la ciberresiliencia del sistema de educación superior colombiano ante amenazas digitales contemporáneas.

Palabras clave: ciberseguridad; estrategias de mitigación; gobernanza digital; instituciones de educación superior; marcos normativos.

* Capítulo de libro resultado del proyecto de investigación "La gobernanza del ciberespacio a nivel global, regional y nacional: desafíos, oportunidades y estrategias para la soberanía digital", del grupo de investigación "Ciberespacio, Tecnología e Innovación", de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado en 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 al autor y no reflejan necesariamente los de las instituciones participantes.

Jeison Stiven Melo Mendoza

Ingeniero en Telecomunicaciones, con maestría en Ciberseguridad y Ciberdefensa y certificación internacional en ISO 27001. Cuento con más de cinco años de experiencia en el sector educativo desde el ámbito administrativo, impulsando la transformación digital con visión estratégica, liderazgo colaborativo y compromiso con la protección de la información. **https://orcid.org/0009-0003-1999-0251** - Contacto: **jeison.melo@esdeg.edu.co**

Citación APA: Melo-Mendoza, J. S. (2026). Ciberseguridad en el sector universitario colombiano: Diagnóstico, desafíos y recomendaciones para un entorno digital seguro. En M. E. Realpe-Díaz & A. M. González-González (Eds.), *Transformación digital y ciberseguridad en Colombia: Desafíos estratégicos para sectores de infraestructura crítica* (pp. 151-182). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818644.05

TRANSFORMACIÓN DIGITAL Y CIBERSEGURIDAD EN COLOMBIA: DESAFÍOS ESTRATÉGICOS PARA SECTORES DE INFRAESTRUCTURA CRÍTICA
ISBN impreso: 978-628-7818-63-7
ISBN digital: 978-628-7818-64-4
DOI: https://doi.org/10.25062/9786287818644

Colección Ciberseguridad y Ciberdefensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2026

Introducción

La transformación digital de los sectores estratégicos de un Estado ha redefinido las dinámicas de producción, circulación y protección de la información, lo cual ha configurado un entorno en el que los activos digitales adquieren valor económico, científico y geopolítico. En este escenario, las instituciones de educación superior (IES) emergen como infraestructuras críticas de conocimiento, no solo por su función formativa, sino por su papel como centros de investigación, transferencia tecnológica, gestión de datos sensibles y articulación interinstitucional. La digitalización progresiva de sus procesos, incluyendo plataformas de gestión académica, sistemas administrativos integrados, entornos virtuales de aprendizaje, repositorios científicos, servicios en la nube y redes distribuida, ha fortalecido la eficiencia operativa y ampliado la cobertura educativa. Sin embargo, esta expansión tecnológica ha incrementado proporcionalmente la superficie de ataque y ha complejizado la matriz de riesgos cibernéticos.

La evidencia internacional confirma que el sector educativo se encuentra entre los más impactados por incidentes de seguridad digital. De hecho, el IBM X-Force Threat Intelligence Index (2024) ubica a la educación en el tercer lugar global entre los sectores más atacados, con un incremento del 46 % en campañas de *ransomware* y *phishing* dirigidos a universidades y centros de investigación. Este comportamiento no es circunstancial, sino estructural. Las IES no solo concentran datos personales, financieros, académicos y científicos de alto valor estratégico, sino que además operan con infraestructuras tecnológicas heterogéneas que, con frecuencia, combinan sistemas legados con arquitecturas cloud. A esto se suma que mantienen modelos de gobernanza descentralizados, los cuales dificultan la estandarización de controles. A diferencia de sectores regulados con marcos estrictos de cumplimiento, la universidad funciona con principios de autonomía,

apertura y colaboración, situación que introduce tensiones permanentes entre disponibilidad, accesibilidad y confidencialidad. Desde la perspectiva de la gestión del riesgo, esta configuración produce una exposición sistémica. La multiplicidad de usuarios —estudiantes, docentes, investigadores, contratistas, visitantes y aliados externos— amplía la superficie de interacción con los sistemas institucionales. Así, plataformas de gestión del aprendizaje (LMS), redes inalámbricas abiertas, portales administrativos, sistemas financieros, bibliotecas digitales y bases de datos de investigación constituyen vectores críticos de vulnerabilidad cuando no se integran en un marco coherente de seguridad de la información (SI). Al respecto, la Agencia de la Unión Europea para la Ciberseguridad (ENISA, 2023) ha señalado que los entornos académicos presentan condiciones propicias para amenazas persistentes avanzadas (APT), exfiltración de información y ataques de denegación de servicio (DDoS), especialmente cuando la gobernanza tecnológica carece de estructuras formales de supervisión.

En el contexto colombiano, los desafíos en ciberseguridad presentan características particulares asociadas a niveles desiguales de madurez digital. El *Estudio de la evolución de los incidentes de seguridad informática* (Cano & Almanza, 2020) identifica incrementos relevantes en *phishing* (23 %), *ransomware* (18 %) y uso no autorizado de software (38 %), los cuales son tendencias coherentes con entornos institucionales en proceso de transformación digital acelerada. Aunque el estudio no se limita al sector educativo, sus hallazgos resultan extrapolables a numerosas IES, donde la expansión de la conectividad, la descentralización tecnológica y el trabajo remoto han ampliado la superficie de exposición. Estos resultados se articulan con el CONPES 3854 y la Estrategia Nacional Digital, que enfatizan el fortalecimiento de capacidades más allá del cumplimiento normativo.

Ahora bien, es importante señalar que la problemática trasciende la dimensión técnica. De hecho, la literatura en gobernanza digital señala que la resiliencia depende de la integración entre liderazgo institucional, cultura organizacional, recursos adecuados y la adopción efectiva de estándares como ISO/IEC 27001 o NIST, cuya implementación en Colombia continúa siendo parcial y fragmentada. Con frecuencia, la ciberseguridad se concibe como función operativa del área TIC, y no como eje transversal de la gestión del riesgo.

Este capítulo propone lineamientos estratégicos sustentados en dos hipótesis: la existencia de una brecha entre norma e implementación y la disponibilidad de modelos replicables cuya eficacia depende de su adaptación contextual. Dada la heterogeneidad institucional, se plantea un marco flexible que promueva una transición progresiva hacia una gobernanza digital resiliente y sostenible.

Metodología y diseño de la revisión sistemática de literatura

El presente capítulo adopta un enfoque metodológico predominantemente cualitativo, el cual se complementa con herramientas analíticas de carácter mixto orientadas a fortalecer la consistencia interpretativa, la trazabilidad y la robustez del análisis. Esta elección responde a la naturaleza compleja, multidimensional y contextual del fenómeno estudiado: la gobernanza digital y la ciberseguridad en las IES colombianas. De acuerdo con Hernández et al. (2021), el enfoque cualitativo resulta apropiado cuando el objetivo es comprender fenómenos organizacionales complejos en interacción con su entorno normativo e institucional, priorizando la profundidad analítica sobre la generalización estadística.

El estudio no busca validar hipótesis mediante inferencia cuantitativa ni producir estimaciones poblacionales, sino identificar patrones estructurales, brechas sistémicas, marcos normativos predominantes y prácticas transferibles, todo ello a partir de un análisis crítico, comparado e inductivo de la literatura especializada. Con esta lógica, se adoptó como método central una revisión sistemática de literatura (RSL), complementada con análisis temático, análisis de contenido dirigido y bibliometría descriptiva.

Estrategia metodológica y criterios de selección

La estrategia de búsqueda se desarrolló mediante consultas sistemáticas en bases de datos indexadas de alto impacto, como IEEE Xplore, Scopus y SpringerLink, seleccionadas por su amplia cobertura en ingeniería, ciencias computacionales y estudios organizacionales. Adicionalmente, se utilizó Google Scholar para verificar la exhaustividad y detectar literatura relevante complementaria. Las cadenas de búsqueda combinaron términos en español e inglés mediante operadores booleanos, lo que permitió integrar conceptos asociados a educación superior, ciberseguridad, gobernanza digital y marcos normativos (ISO/IEC 27001, NIST CSF, SGSI, MFA, CSIRT). Asimismo, se aplicaron filtros por periodo (2015–2024), idioma (español e inglés), áreas temáticas y tipo documental, incluyendo artículos científicos, capítulos de libro, informes técnicos y documentos de política pública. Para la inclusión, se consideraron estudios que abordaran explícitamente IES, analizaran marcos, políticas o controles de ciberseguridad, presentaran trazabilidad metodológica y estuvieran disponibles en texto completo. Por el contrario, se excluyeron investigaciones centradas exclusivamente en educación básica (K–12), entornos corporativos sin transferibilidad al ámbito universitario, documentos de opinión y trabajos puramente técnicos sin una dimensión organizacional aplicable.

Tras la depuración y eliminación de duplicados, se consolidó un corpus de 58 documentos, de los cuales 40 conformaron el núcleo analítico por su profundidad y pertinencia contextual. Para garantizar la comparabilidad, se diseñó una matriz de extracción que registró variables normativas, técnicas, organizacionales y formativas, así como resultados medibles y el grado de replicabilidad para IES colombianas. El análisis combinó enfoque temático, análisis de contenido dirigido y bibliometría descriptiva, e incluyó doble codificación parcial ($\kappa \geq 0{,}75$) y triangulación metodológica. De tal forma, esta arquitectura metodológica asegura rigor, trazabilidad y validez interna, lo cual permite generar conocimiento estructurado y transferible para la formulación de lineamientos estratégicos en ciberseguridad universitaria.

Políticas de ciberseguridad en IES colombianas, una revisión sistemática de literatura

Las IES en Colombia registraron un incremento sostenido en los incidentes de ciberseguridad, con predominio de ataques de DDoS, *phishing* académico y exfiltración de bases de datos institucionales. Estos eventos reflejan una tendencia creciente hacia la explotación de vulnerabilidades propias del ecosistema universitario, tales como el uso de redes WiFi abiertas, sistemas de autenticación débiles, plataformas de gestión académica desactualizadas y repositorios de datos sin cifrado. Esta tendencia confirma lo observado por Cano y Almanza (2020), quienes ya advertían que los incidentes de seguridad en Colombia mostraban un crecimiento sostenido durante la última década, un fenómeno impulsado por la expansión de los servicios digitales sin un correlato equivalente en políticas de protección y monitoreo.

La revisión documental permitió identificar que estas amenazas no se manifiestan de forma aislada: responden a la combinación de brechas normativas, debilidades organizacionales y carencias técnicas estructurales. En particular, los entornos académicos resultan muy atractivos para los atacantes, dada su alta conectividad, la heterogeneidad de sus usuarios, la disponibilidad de datos personales y científicos valiosos, así como la frecuente ausencia de políticas unificadas de seguridad. Según el IBM X-Force Threat Intelligence Index (2024), el sector educativo ocupó el tercer lugar global entre los más atacados, con un aumento del 46 % en incidentes de *ransomware* y *phishing* dirigidos a universidades y centros de investigación.

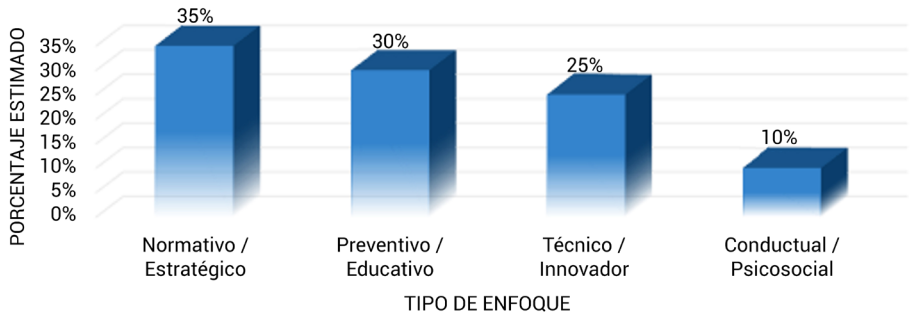
Específicamente, el desarrollo del objetivo se presenta con una mirada directa al panorama, donde se mapea cómo las IES en Colombia están concibiendo y ejecutando actualmente la ciberseguridad. El proceso comienza con la identificación de los enfoques predominantes, tales como el normativo/estratégico, preventivo/

educativo, técnico/operativo y conductual/organizacional, así como su manifestación práctica en los documentos analizados. Posteriormente, se muestran las brechas principales por dimensión (normativa, organizacional, técnico/operativa, formativa y de cooperación) y los niveles emergentes de madurez institucional. Finalmente, se destacan las implicaciones de estos hallazgos para la gobernanza digital universitaria, con el fin de orientar decisiones estratégicas sobre la priorización de controles, la estandarización de procesos y el fortalecimiento de capacidades institucionales.

Análisis inicial de hallazgos

Uno de los primeros hallazgos relevantes fue la identificación de cuatro tipos de enfoque predominantes en las estrategias de ciberseguridad, documentados por características clave, como se observa en la figura 1. Estos enfoques son: el normativo/estratégico, que comprende el desarrollo de marcos regulatorios, políticas internas y diagnósticos. Por su parte, el enfoque preventivo/educativo se centra en campañas de concienciación, formación técnica y cultura digital. Asimismo, el enfoque técnico/innovador integra el uso de inteligencia artificial (IA), biometría y herramientas de análisis predictivo. Finalmente, el enfoque conductual/psicosocial aborda los modelos de percepción de riesgo y la motivación de protección.

Figura 1. *Distribución de los documentos analizados según su enfoque.*



Nota: Se presenta el porcentaje de documentos clasificados por su enfoque predominante (normativo, preventivo, técnico-operativo, formativo/cultural). Esta clasificación se obtuvo mediante un análisis de contenido dirigido, y los porcentajes resultantes son relativos a una muestra de n = 40.

Fuente: Elaboración propia con base en la matriz de extracción.

Uno de los ejes centrales para comprender el estado de la ciberseguridad en las IES en Colombia es el análisis del uso y la implementación de marcos normativos y estándares internacionales. Aunque la revisión de los 40 documentos

seleccionados en la RSL evidencia una tendencia reiterada hacia la adopción declarativa de referentes globales, esta apropiación no siempre se traduce en institucionalización operativa ni en transformación estructural de la gestión del riesgo.

El estándar ISO/IEC 27001 es el marco más citado, principalmente en relación con el diseño de políticas, identificación de activos y definición preliminar de controles asociados a Sistemas de Gestión de Seguridad de la Información (SGSI). No obstante, la implementación integral —que implica análisis sistemático de riesgos, auditorías internas, mejora continua y certificación— se concentra en un número reducido de IES con mayor capacidad técnica y financiera. En la mayoría de los casos, el SGSI permanece en fases parciales, lo cual limita su impacto organizacional. Una situación similar se observa con marcos como COBIT e ITIL, frecuentemente mencionados como referentes para fortalecer la gobernanza y la gestión de servicios TI, pero aplicados de forma fragmentada y sin integración sistémica. En el plano nacional, aunque la Ley 1581 de 2012 sobre protección de datos es ampliamente referenciada, persisten debilidades en auditoría, definición de responsabilidades y trazabilidad del consentimiento digital.

En particular, la evidencia sugiere que la brecha no radica en desconocimiento normativo, sino en limitaciones para institucionalizar estándares de manera sostenida, lo cual configura brechas estructurales en gobernanza y madurez digital.

Dimensión técnica

Se evidencian carencias significativas en herramientas avanzadas de monitoreo y respuesta. Estas se manifiestan en la ausencia o en la implementación incipiente de sistemas SIEM (Security Information and Event Management), centros de operaciones de seguridad (SOC), monitoreo continuo de vulnerabilidades, segmentación de redes y auditorías técnicas periódicas, situación que reduce la capacidad de anticipación y contención frente a incidentes. Asimismo, se identifican debilidades en autenticación multifactor, cifrado robusto y gestión de accesos privilegiados. Tales limitaciones no solo incrementan la probabilidad de incidentes, sino que también dificultan la recuperación oportuna.

Dimensión normativa

Aunque existe referencia frecuente a estándares internacionales y leyes nacionales, el seguimiento sistemático y la evaluación de cumplimiento son irregulares, una situación que se agrava por la frecuente carencia de indicadores de desempeño (KPI), cronogramas de actualización y mecanismos de revisión independiente en las políticas, una brecha que afecta la consolidación de una cultura de cumplimiento y mejora continua.

Dimensión organizacional

La gobernanza digital presenta un carácter fragmentado. En muchas IES, la ciberseguridad depende exclusivamente del área de tecnologías de la información, lo cual impide su articulación con rectoría, planeación estratégica, jurídica o gestión del talento humano. Además, la ausencia de comités institucionales de seguridad o de figuras equivalentes a un CISO limita la capacidad de integración transversal del riesgo digital en la toma de decisiones estratégicas.

Dimensión formativa

Las iniciativas de concientización y capacitación son generalmente esporádicas, voluntarias y sin continuidad presupuestal, razón por la cual, aunque existen campañas y talleres, pocos programas se integran formalmente al currículo académico o a procesos obligatorios de inducción institucional. En conclusión, la cultura organizacional en torno a la seguridad digital no se encuentra plenamente consolidada.

Dimensión de articulación multisectorial

A pesar de la existencia del CONPES 3854 y de la Estrategia Nacional Digital 2023-2026, la conexión entre estos instrumentos y los planes estratégicos universitarios es débil. Esta debilidad se manifiesta en la ausencia de programas sistemáticos que traduzcan los lineamientos macro en acciones específicas para el sector educativo, así como en la falta de esquemas robustos de acompañamiento técnico o financiamiento diferenciado. Como consecuencia, esta desconexión amplía la desigualdad entre universidades con alta capacidad operativa y aquellas ubicadas en regiones con menor infraestructura. Específicamente, el análisis de superficies de ataque revela que los vectores más frecuentes incluyen portales académicos, correo institucional, redes inalámbricas abiertas y aplicaciones en la nube. Las vulnerabilidades más recurrentes se relacionan con autenticación débil, ausencia de segmentación de red y configuraciones inseguras derivadas de la descentralización tecnológica. Además, la alta rotación de usuarios incrementa la probabilidad de incidentes asociados a error humano.

A partir de la información consolidada, los niveles de madurez organizacional estimados revelan que aproximadamente el 25 % de las IES exhibe un nivel alto, caracterizado por políticas formalizadas, roles definidos, monitoreo continuo y procesos de mejora estructurados, lo que a menudo se refleja en su participación en redes internacionales o procesos de acreditación. Por otra parte, mientras el 50 % se ubica en un nivel medio, con iniciativas parcialmente implementadas y sin integración transversal completa, el 25 % restante presenta un nivel bajo, con acciones reactivas y la ausencia de una estructura formal de gobernanza digital.

En cuanto a las buenas prácticas identificadas, estas incluyen la implementación progresiva de SGSI basados en ISO/IEC 27001, el desarrollo de modelos integrados de gobernanza que combinan COBIT, ITIL y NIST, la adopción incipiente de inteligencia artificial para la detección de anomalías, así como el fortalecimiento de políticas internas de protección de datos que superan los mínimos legales. De estas, las prácticas más sostenibles comparten características comunes, tales como el liderazgo desde la alta dirección, la alineación estratégica, una asignación presupuestal dedicada y mecanismos de evaluación formal.

En contraste, las iniciativas aisladas dependen del liderazgo individual y carecen de institucionalización. En particular, la triangulación de resultados confirma un patrón de fragmentación estratégica y una limitada integración de la ciberseguridad en los marcos de aseguramiento de la calidad universitaria. En síntesis, el diagnóstico evidencia que para consolidar una postura robusta de ciberseguridad en las IES colombianas, se requiere una arquitectura multinivel que articule políticas públicas, gobernanza institucional, capacidades técnicas y cultura organizacional. Sin esta integración, los marcos normativos continuarán siendo referencias declarativas más que instrumentos efectivos de transformación estructural.

Brechas por dimensión

Para clarificar dónde se concentran los déficits, la tabla 1 presenta una estimación comparada de las brechas por dimensión. Además, la visualización tipo radar permite apreciar de forma inmediata el perfil de rezagos relativos y su peso específico en el conjunto de evidencias figura 2).

Tabla 1. *Dimensiones de la brecha institucional en IES colombianas (Escala 1-5)*

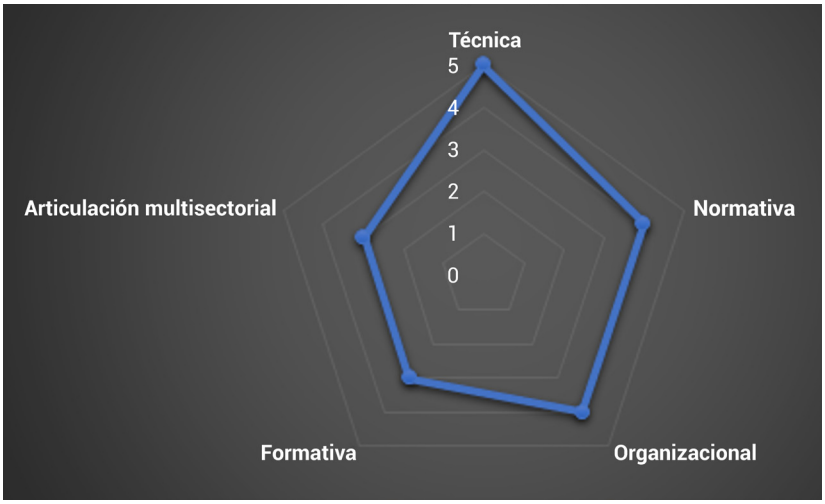
Dimensión de brecha	Valores	Descripción sintetizada
Técnica	5	Carencia de SIEM, SOC, monitoreo, segmentación de red y auditorías internas.
Normativa	4	Bajo cumplimiento de ISO 27001, NIST, Ley 1581 y políticas nacionales.
Organizacional	4	Gobernanza digital fragmentada, roles difusos y escasa articulación institucional.
Formativa	3	Falta de capacitación continua, además de acciones aisladas y sin sostenibilidad.
Articulación multisectorial	3	Escasa conexión con CONPES, Estrategia Nacional Digital y redes externas de cooperación.

SIEM: Security Information and Event Management; **SOC:** centros de operaciones de seguridad.

Nota: Valores estimados a partir de codificación temática y análisis de contenido de 40 documentos (2015-2024). La escala (1-5) expresa magnitud de brecha (1 = baja, 5 = alta). Los ejemplos técnicos incluyen SIEM ,SOC y ISO/IEC 27001.

Fuente: elaboración propia con base en la matriz de extracción de la RSL.

Figura 2. *Brechas institucionales*



Fuente: Elaboración propia con base en la RSL (n = 40).

La consolidación de capacidades institucionales para enfrentar amenazas cibernéticas complejas exige el estudio y el análisis de estrategias que hayan demostrado eficacia en escenarios comparables. Con base en los 40 documentos analizados en la RSL, se han identificado un conjunto de buenas prácticas en ciberseguridad que ofrecen un alto valor de replicabilidad en el contexto colombiano, dadas sus características estructurales, normativas, tecnológicas y organizativas. En síntesis, la RSL permitió confirmar que el ecosistema universitario colombiano presenta vulnerabilidades específicas derivadas de su estructura digital abierta, la diversidad de usuarios y la limitada institucionalización de la ciberseguridad como política transversal. Si bien existen marcos regulatorios y buenas prácticas documentadas, su implementación efectiva continúa siendo desigual entre las instituciones. Los resultados también evidencian la necesidad de tener un enfoque diferenciado que considere los niveles de madurez tecnológica y organizacional de cada institución, y que permita traducir la normativa vigente en mecanismos operativos de protección, detección y respuesta sostenibles.

En este sentido, tras evaluar el estado actual del ecosistema de ciberseguridad en las IES colombianas, el siguiente paso consiste en identificar, interpretar y sistematizar aquellas prácticas exitosas, tanto de origen nacional como internacional, que puedan ser adaptadas para fortalecer las capacidades institucionales de las IES, entendidas como la articulación entre sus estructuras académicas, administrativas y tecnológicas.

Específicamente, la premisa central de este análisis radica en que la eficacia de una estrategia de ciberseguridad no depende únicamente de la sofisticación tecnológica que incorpora, sino del grado de articulación institucional, de la sostenibilidad presupuestal y de la coherencia con el entorno normativo local.

Criterios y trazabilidad de prácticas

Para garantizar la validez metodológica del proceso de selección, se definieron cinco criterios que permitieron evaluar y priorizar las buenas prácticas identificadas en la revisión documental (tabla 2). Estos criterios, además, consideran tanto la robustez de la evidencia como la viabilidad de implementación en el contexto colombiano.

Tabla 2. *Dimensiones de brechas institucionales*

Criterio	Descripción
Evidencia empírica	La práctica debe estar documentada en fuentes verificables, con descripción clara de su implementación.
Resultados medibles	Debe haber datos que evidencien el impacto en la reducción de riesgos, incidentes o mejoras de madurez.
Costo y viabilidad	Evaluación preliminar del costo relativo frente a los beneficios, considerando recursos típicos de las IES colombianas.
Auditabilidad y monitoreo	Debe permitir que se haga seguimiento a través de indicadores o reportes internos.
Replicabilidad contextual	La práctica puede ser adaptada al ecosistema colombiano con ajustes normativos, técnicos o institucionales.

Fuente: Elaboración propia.

Prácticas priorizadas de ciberseguridad con alta adaptabilidad en las IES colombianas

La trazabilidad entre los hallazgos de la RSL y la selección final de prácticas priorizadas constituye un componente metodológico central para garantizar la validez interna, la coherencia analítica y la replicabilidad del estudio. La RSL permitió identificar 18 buenas prácticas documentadas en experiencias institucionales verificables (12 de origen internacional y 6 nacionales), las cuales se clasificaron inicialmente en cinco categorías analíticas: normativas, técnicas, formativas, colaborativas e innovadoras. Esta categorización no solo respondió a criterios descriptivos, sino también a una lógica de diferenciación funcional orientada a mapear los distintos niveles de intervención institucional en ciberseguridad.

Criterios de priorización y matriz comparativa

La priorización se realizó mediante una matriz comparativa multicriterio diseñada para evaluar cada práctica de acuerdo con cinco dimensiones estratégicas previamente definidas: 1) grado de evidencia empírica reportada, 2) impacto demostrado en indicadores de desempeño (por ejemplo, MTTD, MTTR o reducción de incidentes), 3) factibilidad presupuestaria y operativa en contextos con recursos limitados, 4) nivel de adopción global o regional, y 5) grado de transferibilidad contextual al ecosistema colombiano de educación superior.

El uso de esta matriz permitió reducir sesgos de selección y evitar priorizaciones basadas únicamente en innovación tecnológica o visibilidad internacional. Las prácticas fueron ponderadas de manera equilibrada, con un énfasis particular en aquellas que presentaban resultados cuantificables y replicables en contextos con heterogeneidad institucional. Asimismo, se incorporó el criterio de reiteración en múltiples fuentes independientes, lo cual fortaleció la robustez de la evidencia. Como resultado de este proceso analítico, se seleccionaron cinco prácticas con un alto grado de transferibilidad contextual, es decir, con la capacidad de adaptarse a diferentes niveles de madurez organizacional sin requerir transformaciones estructurales inviables. Estas prácticas no solo demostraron un impacto tangible, sino que también evidenciaron coherencia con el marco normativo colombiano y con las condiciones presupuestales promedio de las IES públicas y privadas.

Prácticas priorizadas

La implementación progresiva de SGSI basados en ISO/IEC 27001 constituye la práctica con mayor consistencia metodológica y normativa en el conjunto analizado. El enfoque por fases —diagnóstico inicial, análisis de riesgos, definición de controles, auditoría interna y mejora continua— permite una institucionalización gradual, adaptable a distintos niveles de madurez. En particular, la experiencia internacional de la Universidad de Reading demuestra que la adopción estructurada de un SGSI puede reducir significativamente el tiempo medio de detección de incidentes (MTTD), lo cual impacta directamente en la resiliencia organizacional. En el ámbito nacional, la Universidad Nacional de Colombia ha avanzado en la estructuración de políticas, designación de responsables y ejecución de auditorías internas, aun sin certificación formal.

Desde una perspectiva técnica y normativa, esta práctica es altamente compatible con la Ley 1581 de 2012 y el Decreto 1377, puesto que fortalece los principios de responsabilidad demostrada y gestión del riesgo. Asimismo, su intrínseca modularidad facilita a las instituciones con capacidad presupuestaria más

limitada la implementación de procesos piloto en áreas críticas, previo a la expansión del sistema a nivel institucional.

Programas obligatorios de concientización y formación continua

El factor humano continúa siendo uno de los principales vectores de riesgo en entornos universitarios abiertos y altamente descentralizados. La evidencia recopilada indica que los programas obligatorios de formación continua reducen significativamente la vulnerabilidad frente a *phishing,* ingeniería social y *malware.* Al respecto, la Universidad de Málaga logró incrementar en 60 % la detección de intentos de *phishing* mediante microcursos, simulacros y contenidos diferenciados por perfil. En Colombia, la Universidad de los Andes implementó campañas con *phishing* simulado, lo cual resultó en una cobertura superior al 80 % de su comunidad académica.

Creación de comités institucionales de ciberseguridad

La gobernanza fragmentada fue identificada como una de las principales brechas en las IES colombianas, de manera que la creación de comités multidisciplinarios permanentes constituye una respuesta estructural a esta problemática. Estos comités integran áreas TIC, jurídica, planeación, académica y administrativa, lo cual genera una arquitectura transversal de toma de decisiones.

En este contexto, la experiencia de la Universidad Nacional de Colombia muestra que la formalización de un comité institucional redujo 36 % el tiempo medio de respuesta ante incidentes (MTTR) y permitió la aprobación de nuevas políticas internas. De manera complementaria, la Universidad del Cauca fortaleció su capacidad de reacción mediante simulacros interdepartamentales periódicos. Esta práctica rompe con el paradigma según el cual la ciberseguridad es responsabilidad exclusiva del área tecnológica y promueve la corresponsabilidad institucional. Además, facilita el reporte estructurado a rectoría y órganos de control, al tiempo que se alinea con principios de gobernanza y control interno.

Participación en redes nacionales de ciberseguridad

La vinculación a redes como RENATA, ColCERT y CSIRT regionales emerge como una estrategia de alto impacto y bajo costo, por cuanto estas permiten el intercambio de alertas tempranas, el acceso a reportes de vulnerabilidades y la coordinación de simulacros.

Según reportes del MinTIC (2023), universidades vinculadas a RENATA han mejorado sustancialmente sus MTTR. El caso de la Universidad del Norte, por

ejemplo, evidencia beneficios concretos, ya que redujo su MTTR de 72 a 24 horas mediante la integración con protocolos de ColCERT. Por lo tanto, esta práctica fortalece la ciberdefensa colaborativa y reduce asimetrías entre instituciones con diferentes niveles de capacidad técnica, además de contribuir al fortalecimiento del ecosistema nacional de seguridad digital educativa.

Implementación de autenticación multifactor (MFA)

Constituye una medida técnica muy efectiva contra accesos no autorizados, cuya implementación en servicios críticos como correo institucional, LMS y sistemas académicos reduce de forma significativa la probabilidad de compromiso de credenciales.

Al respecto, la Universidad de Toronto reportó una reducción del 76 % en accesos ilegítimos tras implementar MFA. En Colombia, la Universidad del Rosario alcanzó una cobertura del 95 % en cuentas estudiantiles y docentes, lo cual redundó en una mejora de los resultados en auditorías internas. Desde una perspectiva técnica, el MFA puede implementarse mediante soluciones *open-source* o servicios en la nube de bajo costo, lo cual favorece su escalabilidad progresiva.

En síntesis, existen cinco prácticas priorizadas que ofrecen un marco estratégico robusto para orientar acciones institucionales (tabla 3), por lo cual es fundamental considerar el conjunto más amplio de experiencias documentadas en el ámbito nacional e internacional. Estas evidencias no solo permiten contrastar, validar y ampliar las perspectivas sobre la adaptabilidad y la eficacia de las estrategias en contextos reales, sino que también aportan insumos para construir una clasificación sistemática y contextualizada.

Tabla 3. *Prácticas priorizadas en IES de Colombia*

Práctica priorizada	Justificación técnica	Adaptabilidad al contexto colombiano	Costo relativo	Indicadores sugeridos	Ejemplo institucional
1. Implementación progresiva de SGSI (ISO/IEC 27001)	Estandariza la gestión de sistemas de información, facilita las auditorías y promueve la mejora continua.	Alta (requiere liderazgo y fases).	Alto (inicial) a moderado (mantenimiento).	Porcentajes de controles ISO implementados y tiempo de cierre de hallazgos.	Universidad de Reading (Reino Unido) y Universidad Nacional de Colombia.
2. Formación obligatoria en ciberseguridad	Fortalece la cultura digital, reduce el riesgo humano y es fácil de integrar en procesos académicos.	Muy alta.	Bajo.	Porcentaje de participación anual y tasa de detección en simulacros.	Universidad de Málaga (España) y Universidad de los Andes (Colombia).

Práctica priorizada	Justificación técnica	Adaptabilidad al contexto colombiano	Costo relativo	Indicadores sugeridos	Ejemplo institucional
3. Comité institucional de ciberseguridad	Mejora la gobernanza digital, articula áreas clave y genera políticas internas.	Muy alta.	Bajo.	Número de reuniones/año, políticas generadas y MTTR.	Universidad Nacional de Colombia y Universidad del Cauca (Colombia).
4. Participación en redes de ciberseguridad (RENATA y ColCERT)	Fortalece respuesta a incidentes y permite acceso a inteligencia compartida y alertas tempranas.	Muy alta.	Bajo (en algunos casos, subvencionado).	Número de alertas gestionadas, MTTR y participación en simulacros.	Universidad del Norte (Colombia), RENATA y ColCERT.
5. Autenticación multifactor (MFA)	Reduce los accesos no autorizados, fortalece la identidad digital y tiene alto impacto técnico.	Alta.	Medio a bajo (*open-source* o *cloud*).	Porcentaje de cuentas con MFA activa y reducción de accesos indebidos.	Universidad de Toronto (Canadá) y Universidad del Rosario (Colombia).

SGSI: Sistema de Gestión de Seguridad de la Información; MTTR: tiempo medio de respuesta ante incidentes.

Fuente: Elaboración propia.

Evidencia documental de experiencias nacionales e internacionales en ciberseguridad universitaria

Experiencias nacionales en IES colombianas

En el contexto colombiano, la evidencia documental revela un proceso progresivo aunque heterogéneo de fortalecimiento de capacidades en ciberseguridad dentro de las IES. Prueba de ello son las diversas experiencias sistematizadas en estudios técnicos y académicos, entre los cuales se incluyen los trabajos de Calderón Aguirre y Trujillo-Bohórquez (2023), Moreno-Valencia & Mejía-Cardona (2024), Gurumendi-Párraga (2023), Carreño-Ospina (2024), Guerrero-Sumalave (2023), Molina- Oviedo (2020), Cheng y Wang (2022) y Alexei (2021). Estos trabajos permiten identificar patrones de adopción normativa, consolidación organizacional y transformación cultural en torno a la seguridad digital.

Una de las tendencias más consistentes corresponde a la adopción progresiva de SGSI basados en ISO/IEC 27001, aun sin certificación formal. La documentación de casos, como la presentada por Orosco-Fabian (2024), Carreño Ospina (2024) y Cheng y Wang (2022), revela cómo distintas IES han empleado este estándar como marco orientador para estructurar diagnósticos de riesgo, inventarios de activos críticos, definición de roles y realización de auditorías internas. Aunque estos procesos no culminan necesariamente en certificaciones internacionales, sí han permitido fortalecer la conciencia institucional sobre la gestión del riesgo digital y mejorar la articulación entre áreas técnicas, jurídicas y directivas.

En paralelo, la literatura evidencia el surgimiento de estructuras internas de respuesta a incidentes, incluso en instituciones que no cuentan con SOC formales. Así lo confirman Guerrero-Sumalave (2023) y Molina-Oviedo (2020), quienes documentan que varias universidades han conformado comités o unidades funcionales dedicadas al monitoreo y la documentación de eventos de seguridad. Estas estructuras representan un avance significativo en términos de gobernanza, pues trasladan la ciberseguridad desde un enfoque reactivo y exclusivamente técnico hacia una dimensión estratégica y transversal.

En el plano normativo, algunas IES han avanzado más allá del cumplimiento mínimo de la Ley 1581 de 2012. En este sentido, los estudios de Calderón-Aguirre y Trujillo-Bohórquez (2023), y Alexei (2021) documentan la implementación de protocolos internos de notificación de incidentes, controles de acceso lógico y mecanismos estructurados de gestión de consentimientos informados. Estas prácticas suelen complementarse con reglamentos institucionales y cursos obligatorios de inducción, aunque persisten diferencias en su actualización y cobertura. Por otro lado, desde la perspectiva organizacional, el caso de la Universidad Popular del Cesar, descrito en Molina -Oviedo (2020) resulta particularmente ilustrativo, pues la ciberseguridad fue integrada al plan estratégico institucional como componente del modelo de gobernanza y gestión del riesgo tecnológico.

Finalmente, en el ámbito cultural y formativo, múltiples universidades han implementado campañas sostenidas de sensibilización. Según Gurumendi-Párraga (2023), Cayón-Peña y García-Segura (2014), y Cheng y Wang (2022), estas iniciativas incluyen boletines electrónicos, charlas periódicas y estrategias de gamificación, todas ellas orientadas a reducir riesgos asociados al factor humano. En particular, su bajo costo relativo y alta adaptabilidad las convierten en prácticas particularmente viables en contextos regionales con recursos limitados.

Referentes internacionales de ciberseguridad en educación superior

En el ámbito internacional, la literatura identifica modelos más avanzados de institucionalización de la ciberseguridad. Estos modelos están documentados en fuentes como National Cyber Security Centre (2019), Alwahaibi et al., (2022), Oroni et al. (2025), Ragab et al. (2025), Ambali-Parambil et al. (2024) y Kumar et al. (2024), que constituyen referentes estratégicos para el diseño de políticas adaptativas en Colombia.

Una de las prácticas más consolidadas es la implementación de arquitecturas integradas que combinan ISO/IEC 27001, NIST y COBIT. Según el National Cyber Security Centre (2019) y Alwahaibi et al. (2022), universidades de Reino Unido y Australia han adoptado modelos que integran auditorías externas periódicas, monitoreo automatizado de cumplimiento y evaluación continua de riesgos.

Asimismo, el uso de inteligencia artificial para la detección de amenazas en entornos virtuales de aprendizaje representa una innovación relevante. Los estudios de Ragab et al. (2025) y Ambali-Parambil et al. (2024) reportan la integración de sistemas de inteligencia artificial en plataformas como Moodle para identificar comportamientos anómalos y generar alertas tempranas. También cabe señalar que si bien en Colombia su implementación es incipiente, esta tecnología podría escalar mediante alianzas interinstitucionales.

En conjunto, la evidencia internacional confirma que la sostenibilidad de la ciberseguridad universitaria depende de la integración entre gobernanza, tecnología, cultura organizacional y evaluación sistemática del riesgo, elementos que pueden ser progresivamente adaptados al contexto colombiano.

Matriz de transferencia y adaptabilidad institucional (GAP & FIT)

La identificación y caracterización de buenas prácticas en ciberseguridad, tanto en el ámbito nacional como internacional, permite establecer un marco referencial valioso. Con este propósito, se desarrolló una matriz de transferencia y adaptabilidad institucional (GAP & FIT), la cual se sintetiza en la tabla 4. Específicamente, este instrumento permite estimar el grado de alineación entre las condiciones requeridas por una práctica —tales como requerimientos mínimos de infraestructura, capacidades técnicas, estructura organizativa y normatividad vigente, entre otros— y las capacidades reales de una institución determinada.

Asimismo, este enfoque parte de reconocer que la adopción eficiente de una estrategia no depende exclusivamente de su efectividad técnica o normativa, sino también de la compatibilidad entre los factores internos de la organización y los elementos habilitantes de cada práctica.

Tabla 4. *Matriz de transferencia y adaptabilidad institucional (GAP & FIT)*

Práctica	Requisitos (Normativos / organizacionales / técnicos)	Costo relativo	Riesgos	Ajustes para IES colombianas	KPI
1. SGSI basado en ISO/IEC 27001	Adopción de ISO/IEC 27001.	Alto (inicial) / Moderado (sostenible).	Resistencia al cambio.	Escalar por fases.	Porcentaje de controles ISO 27001 implementados.
	Comité de seguridad.		Ausencia de cultura de auditoría.	Formación de líderes internos.	Número de auditorías internas/año.
	Personal con competencias en gestión de riesgos.			Adaptación al Decreto 1377 y a la Ley 1581.	
	Infraestructura TIC organizada.				
2. Programas de formación obligatoria en ciberseguridad	Diseño curricular institucional.	Bajo.	Baja participación.	Gamificación.	Porcentaje de población capacitada/año.
	Coordinación entre TIC y Bienestar Universitario.		Fatiga informativa.	Integración con bienestar y currículo.	Porcentaje de usuarios que detectan ataques simulados.
	Plataformas LMS activas.			Evaluación por niveles.	
3. Comité institucional de ciberseguridad multidisciplinar	Estructura organizativa clara.	Bajo / medio.	Falta de continuidad.	Inclusión en reglamento interno.	Número de reuniones al año.
	Roles definidos (TIC, Jurídica y Planeación).		Falta de empoderamiento real.	Reuniones obligatorias y reportes a rectoría.	Número de decisiones implementadas.
	Apoyo directivo.				
4. Participación en redes (RENATA, ColCERT y CSIRT)	Conectividad robusta.	Bajo / apoyo estatal.	Falta de respuesta rápida.	Convenios formales.	Número de alertas compartidas al semestre.
	Personal técnico con acceso a nodos.		Brechas regionales.	Capacitación continua en protocolos CERT.	MTTR.
	Protocolos de intercambio de alertas.				

Práctica	Requisitos (Normativos / organizacionales / técnicos)	Costo relativo	Riesgos	Ajustes para IES colombianas	KPI
5. Autenticación multifactor (MFA) en sistemas críticos	Plataformas de autenticación integrables.	Medio / bajo (con soluciones open-source).	Fricción con el usuario.	Pilotos por unidades.	Porcentaje de usuarios activos con MFA.
	Infraestructura *cloud* o híbrida.		Falta de soporte técnico inicial.	Inclusión en reglamentos de uso TIC.	Número de accesos no autorizados detectados.
	Gestión de identidad centralizada.				

LMS: plataformas de gestión de aprendizaje: MTTR: tiempo medio de respuesta ante incidentes.

Fuente: Elaboración propia

Una vez identificadas y priorizadas las prácticas de ciberseguridad aplicables a las IES en Colombia, se avanzó hacia su sistematización conceptual mediante una clasificación analítica que facilita su comparación, la evaluación de madurez y la proyección de adaptabilidad institucional. Específicamente, la tipología se construyó a partir de un análisis cualitativo con codificación temática de fuentes nacionales e internacionales, el cual permitió organizar las estrategias según cuatro criterios: origen (nacional o internacional), nivel de implementación (básico, intermedio, avanzado), dimensión de impacto (normativa, organizacional, técnica, formativa o mixta) y grado de replicabilidad (alta, media, baja). De este proceso emergieron cinco categorías: normativas, organizacionales, técnicas, formativas e híbridas. Así, esta clasificación permite diseñar lineamientos diferenciados y ajustados a la realidad estructural y tecnológica de cada institución.

Adaptabilidad de estrategias al contexto colombiano

Para completar el proceso de clasificación y evaluación de las estrategias identificadas, se ha elaborado la tabla 5, donde se comparan y cruzan las principales iniciativas que se encontraron en los documentos analizados con su dimensión estratégica, contexto geográfico, ejemplos institucionales y nivel de adaptabilidad estimado para IES en Colombia.

Tabla 5. *Iniciativas clasificadas según los documentos*

Estrategia	Dimensión	Contexto	Ejemplo de institución	Nivel de adaptabilidad
Política de seguridad institucional (ISO adaptado)	Normativa	Nacional	Universidad Nacional y Universidad del Valle.	Alta

Estrategia	Dimensión	Contexto	Ejemplo de institución	Nivel de adaptabilidad
Gobierno TI y riesgos institucionales	Organizacional	Nacional	Universidad Popular del Cesar.	Alta
Gestión de incidentes sin SOC	Técnica	Nacional	Universidad Distrital y Universidad Pedagógica Nacional.	Media
Campañas de concien-ciación y gamificación	Formativa	Nacional	Universidad de la Amazonía y Universidad Tecnológica de Pereira.	Alta
Marcos integrados ISO–NIST–COBIT	Normativa-técnica	Internacional	Universidad de Oxford y Universidad de Melbourne.	Media
Inteligencia artificial aplicada a detección de amenazas	Técnica	Internacional	Universidad Tecnológica de Malasia y Stanford University.	Baja
Evaluación de la ma-durez institucional en ciberseguridad	Organizacional	Internacional	Red Europea de -Universidades Digitales (EDUCAUSE)	Alta
Programas educati-vos con evaluación motivacional	Formativa	Internacional	University Teknologi MARA (Malasia), Corea del Sur	Alta

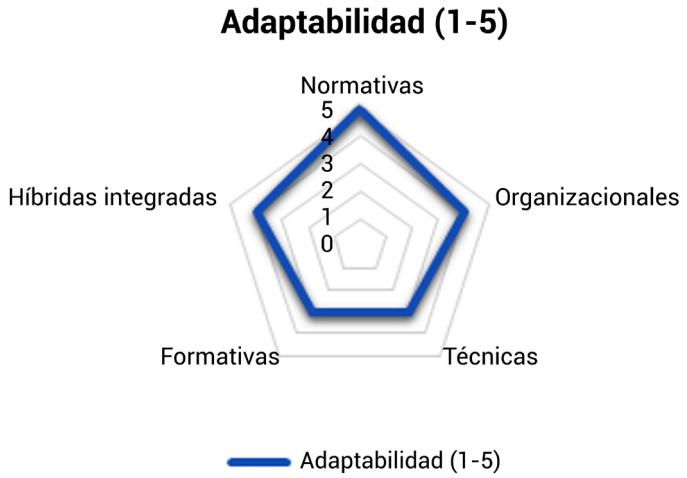
SOC: centros de operaciones de seguridad.

Fuente: Elaboración propia.

La tabla 5 permite observar que las estrategias con mayor potencial de transferencia y escalabilidad son aquellas de naturaleza normativa y organizacional, particularmente cuando se originan en contextos nacionales. Ejemplos como la adaptación de políticas ISO en universidades colombianas o los modelos de gobernanza TI y gestión de riesgos demuestran una alta adaptabilidad. En particular, esta adaptabilidad se fundamenta en su bajo requerimiento tecnológico, su alineación con marcos regulatorios nacionales (como la Ley 1581 y el Decreto 1377) y su sostenibilidad operativa. En contraste, las estrategias de origen internacional, basadas en tecnologías emergentes como la inteligencia artificial para la detección de amenazas o en marcos integrados ISO-NIST-COBIT, muestran una adaptabilidad media o baja. En este caso, dicha adaptabilidad reducida se atribuye a sus elevadas exigencias técnicas, los costos de implementación y la significativa brecha de infraestructura presente en muchas IES.

Para visualizar de forma integral esta evaluación, se construyó una gráfica tipo radar (figura 3), la cual representa el nivel de adaptabilidad de cada categoría estratégica según cinco criterios. Como se observa, las estrategias normativas alcanzan el mayor nivel de adaptabilidad (5/5), a las que siguen las organizacionales y formativas. Las técnicas y híbridas, si bien aportan alto valor, requieren mayores capacidades institucionales para su aplicación exitosa.

Figura 3. *Prioridades realistas para el diseño de políticas institucionales de ciberseguridad en IES colombianas*



Nota: Escala de 1 = baja adaptabilidad; 5 = alta adaptabilidad

Fuente: Elaboración propia

Lineamientos estratégicos para políticas institucionales de ciberseguridad

El análisis comparado evidencia que las estrategias normativas y formativas presentan mayor facilidad de adopción en las IES colombianas, puesto que su implementación depende principalmente de voluntad institucional, alineación regulatoria y fortalecimiento organizacional, más que de inversiones tecnológicas complejas. No obstante, esta facilidad no menoscaba la relevancia de las estrategias técnicas, las cuales son estructuralmente indispensables, pero cuya implementación exige mayor madurez digital, capacidades especializadas y sostenibilidad financiera. Por consiguiente, resulta metodológicamente pertinente un modelo de adopción escalonado.

La evidencia también muestra que la replicabilidad efectiva no consiste en transferir mecánicamente buenas prácticas, sino en adaptarlas progresivamente según su viabilidad y contexto. Específicamente, las acciones normativas y formativas pueden consolidar la base cultural y organizativa, mientras que las soluciones técnicas avanzadas se implementan en fases posteriores. De esta manera, este enfoque permite responder a la creciente exposición al riesgo derivada de la digitalización universitaria, a través de lineamientos estratégicos que se ajustan a la heterogeneidad institucional colombiana.

Alineamiento normativo institucional

El primer eje estratégico es el alineamiento normativo institucional: la formalización de políticas internas de SI y protección de datos debe concebirse como componente estructural de la gobernanza universitaria y no como respuesta reactiva ante incidentes.

En este sentido, se recomienda adoptar ISO/IEC 27001:2022 como marco metodológico de referencia, incluso sin aspiración inmediata a certificación. Su estructura basada en ciclo PHVA (Planificar/Hacer/Verificar/Actuar) permite organizar procesos de identificación de activos, evaluación de riesgos, implementación de controles y mejora continua. De hecho, la experiencia comparada demuestra que las instituciones que adoptan este estándar como guía estructural avanzan con mayor coherencia hacia la institucionalización.

No obstante, este alineamiento debe complementarse con la creación obligatoria de un Comité Institucional de SI, el cual deberá contar con representación multidisciplinaria (tecnología, planeación, jurídica, académica y administrativa) y una vinculación jerárquica directa a rectoría o vicerrectoría general. Finalmente, es importante señalar que la efectividad de este comité dependerá de su capacidad de seguimiento y evaluación periódica.

Gobernanza digital interdependiente

El segundo eje corresponde al fortalecimiento de la gobernanza digital interdependiente: la evidencia internacional demuestra que la ciberseguridad no puede depender exclusivamente del área TIC, sino que debe integrarse transversalmente en la planeación institucional. Por ello, se propone que cada IES diseñe formalmente un Modelo de Gobernanza Digital, en el cual se definan roles, líneas de reporte, matrices de responsabilidad (RACI) y protocolos de gestión del riesgo digital.

Además, este modelo debe articularse con el Plan de Desarrollo Institucional (PDI) para asegurar la coherencia estratégica, así como designar un responsable Institucional de Seguridad de la Información (CISO), lo cual es fundamental. Este perfil debe combinar competencias técnicas y estratégicas, entre las cuales se incluyen conocimientos en auditoría de sistemas, normativas internacionales, gestión de riesgos y liderazgo organizacional. Cabe aclarar que su rol no se debe limitar a la operación tecnológica, sino que abarca la mediación institucional y la representación en redes de cooperación.

Modelo de escalabilidad técnica y operativa

El modelo de escalabilidad técnica y operativa se estructura en tres fases progresivas: básica, intermedia y avanzada, diseñadas para adaptarse a la heterogeneidad

institucional del sistema universitario colombiano. La fase básica establece los controles mínimos indispensables para reducir los riesgos inmediatos y garantizar la continuidad operativa. La fase intermedia introduce capacidades de monitoreo activo y formalización de procesos de respuesta, lo cual fortalece la coordinación interna y la detección temprana. Finalmente, la fase avanzada consolida un enfoque proactivo basado en análisis inteligente de amenazas, automatización y cooperación internacional. Con esta estructura, el esquema evita imponer estándares técnicamente inalcanzables para instituciones con menor capacidad instalada y promueve una progresión gradual, sostenible y contextualizada hacia niveles superiores de madurez en ciberseguridad.

Formación continua y cultura digital

Dado que la formación estructurada es clave para la sostenibilidad institucional en ciberseguridad, se propone un plan institucional segmentado por perfiles, con cursos obligatorios, simulacros de *phishing,* evaluaciones periódicas e integración curricular estratégica. Complementado con alertas y campañas, el plan institucional no solo busca informar, sino también transformar conductas y fortalecer la cultura digital.

Integración en sistemas de calidad y autoevaluación

La ciberseguridad debe incorporarse a los sistemas de aseguramiento de la calidad y a los procesos de acreditación. En este sentido, incluir indicadores de seguridad digital en auditorías internas y modelos de excelencia institucional genera incentivos de sostenibilidad.

Redes de cooperación y participación internacional

La participación en redes como RENATA, ColCERT, FIRST o EDUCAUSE fortalece el aprendizaje colaborativo y el acceso a alertas tempranas. Para ello, cada IES debería designar un punto focal técnico que mantenga una interacción permanente.

Integración curricular y extensión

La inclusión de contenidos de ciberseguridad en programas académicos debe abarcar dimensiones técnicas, éticas y jurídicas. Complementariamente, diplomados y programas de extensión abiertos a la comunidad amplían el impacto social y posicionan a la universidad como referente en seguridad digital.

En síntesis, la construcción de un ecosistema robusto de ciberseguridad universitaria no depende exclusivamente de la sofisticación tecnológica, sino de la integración estratégica, el liderazgo institucional, la sostenibilidad financiera y la

cultura organizacional. En este sentido, un enfoque escalonado, articulado y contextualizado permitirá avanzar hacia una gobernanza digital resiliente, proactiva y alineada con las exigencias del entorno digital contemporáneo.

Lineamientos estratégicos y recomendaciones para su implementación en Colombia

El presente objetivo no formula recetas genéricas ni modelos prescriptivos rígidos. Por el contrario, traduce la evidencia empírica obtenida en la RSL y las buenas prácticas priorizadas en una arquitectura operativa que se compone de principios rectores, dominios de intervención, fases progresivas de implementación y mecanismos verificables de seguimiento. Así, su propósito es que cada IES, conforme a su nivel de madurez tecnológica y organizacional, disponga de una ruta escalable, medible y verificable que le permita transformar declaraciones normativas en resultados concretos de protección, continuidad académica y resiliencia institucional.

El alcance de estos lineamientos abarca los dominios críticos identificados en la RSL: 1) gobernanza y normativa institucional; 2) gestión técnica y operativa; 3) identidad y control de accesos; 4) monitoreo y respuesta a incidentes; 5) protección de datos y aplicaciones; 6) gestión de proveedores tecnológicos; y 7) formación y concientización continua. Esta estructura es clave, pues la evidencia demuestra que si bien las intervenciones aisladas —limitadas a herramientas técnicas o a campañas formativas ocasionales— producen mejoras puntuales, en realidad no logran consolidar un ecosistema seguro. En consecuencia, se propone una aproximación sistémica en la cual la política institucional, la gobernanza estratégica y los controles técnicos mínimos operen de manera sinérgica y articulada.

Específicamente, los lineamientos se estructuran en siete principios rectores que orientan la priorización y el diseño de las acciones institucionales. Primero, la orientación por riesgo, que implica priorizar activos críticos y procesos misionales. Segundo, la progresividad y la modularidad, que avanza por fases (básico, intermedio y avanzado) con entregables verificables. Tercero, la trazabilidad y generación de evidencia, donde cada acción produzca artefactos comprobables (actas, registros, bitácoras, informes técnicos). Cuarto, la transversalidad de la gobernanza, que reconoce que la seguridad es una responsabilidad institucional y no exclusiva del área TIC. Quinto, la defensa en profundidad, que combina controles organizacionales, técnicos y formativos. Sexto, la interoperabilidad y la cooperación, que integra redes nacionales como RENATA y ColCERT, al tiempo que alinea

estándares internacionales. Finalmente, la mejora continua, sustentada en auditorías periódicas, indicadores de desempeño (KPI) y reportes directos a la rectoría.

Esta propuesta considera el análisis desarrollado en los objetivos previos, el cual evidenció que las IES colombianas enfrentan desafíos estructurales de carácter normativo, organizacional y cultural, los cuales explican la fragmentación de su gobernanza digital. No obstante, la misma revisión identificó rutas viables hacia un modelo de madurez institucional que combine estandarización con flexibilidad operativa. Sobre esta base, los lineamientos propuestos constituyen una hoja de ruta adaptable, diseñada para integrar la ciberseguridad a la misión académica y administrativa de las universidades.

Eje de gobernanza institucional

El primer eje estratégico plantea la institucionalización de la ciberseguridad como política universitaria transversal, lo cual supone integrarla a los procesos de planeación estratégica y aseguramiento de la calidad, al tiempo que se evita confinarla al ámbito técnico. En este sentido, se recomienda la creación de comités de ciberseguridad interdisciplinarios, integrados por representantes directivos, académicos, jurídicos y administrativos, con funciones claras de priorización, asignación de recursos y evaluación de resultados.

Ahora bien, es importante tener en cuenta que la formalización de estos comités mediante resoluciones rectorales o acuerdos de consejo superior otorga legitimidad y capacidad decisoria, elementos que la evidencia empírica asocia con mayores niveles de implementación efectiva. Complementariamente, se propone la designación de un *Chief Information Security Officer* (CISO) o figura equivalente, con dependencia jerárquica directa de la rectoría o vicerrectoría administrativa, lo cual garantizaría continuidad estratégica y evitaría la dilución de responsabilidades en dinámicas operativas de corto plazo.

Eje de gestión técnica y operativa

El segundo eje se orienta a la consolidación de infraestructuras seguras mediante la adopción progresiva de estándares internacionales, específicamente los SGSI alineados con ISO/IEC 27001. Específicamente, su implementación debe iniciar con diagnósticos institucionales y la priorización de controles críticos, ajustados a los niveles de madurez existentes.

Con este propósito, se recomienda la implementación obligatoria de autenticación multifactor (MFA) en sistemas académicos y administrativos que gestionen datos sensibles, dado su impacto comprobado en la reducción de accesos no

autorizados. Asimismo, resulta estratégico fortalecer capacidades de monitoreo interno mediante equipos de respuesta a incidentes (CSIRT universitarios), los cuales, incluso en modalidades básicas, deben estar articulados con redes nacionales para el intercambio de alertas y protocolos actualizados.

Eje de formación y cultura institucional

El tercer eje reconoce que la tecnología por sí sola no garantiza seguridad. Por ello, se propone la incorporación obligatoria de formación en ciberseguridad para toda la comunidad universitaria, la cual incluirá módulos diferenciados según perfiles y evaluaciones periódicas destinadas a medir los cambios en los conocimientos y las conductas. Al respecto es importante señalar que, según la evidencia, la capacitación sistemática reduce los incidentes asociados a *phishing* y al uso indebido de credenciales, además de que fortalece la cultura organizacional de prevención.

Eje de cooperación e innovación

El cuarto eje enfatiza la cooperación interinstitucional y la integración activa en redes nacionales e internacionales. Como se ha mencionado, la participación sistemática en RENATA y ColCERT facilita el acceso a alertas tempranas y buenas prácticas, con lo cual se reducen los tiempos de respuesta ante incidentes y se fortalece la resiliencia colectiva del sistema universitario.

Finalmente, el quinto eje propone la adopción progresiva de tecnologías emergentes, como inteligencia artificial y análisis predictivo, a través de proyectos piloto articulados con programas de investigación y posgrado. Esta estrategia permite generar evidencia local sobre desempeño, tasas de falsos positivos e impacto operativo, lo cual facilita una transición controlada hacia soluciones avanzadas. En conjunto, estos lineamientos configuran una arquitectura escalable y verificable que permite a las IES colombianas avanzar hacia un modelo de madurez institucional en ciberseguridad, basado en evidencia, gobernanza efectiva y mejora continua.

Conclusiones

En conjunto, los hallazgos sugieren que la ciberseguridad en las IES colombianas se encuentra en una fase inicial de madurez institucional, condicionada por la dispersión normativa, la débil articulación organizacional y la insuficiente inversión en capacidades técnicas y formativas. Más que confirmar una realidad cerrada, este análisis delimita un punto de partida empírico que permitirá avanzar hacia

estrategias sostenibles de madurez, gobernanza y cooperación digital, orientadas al fortalecimiento integral del sistema universitario colombiano.

Al integrar la RSL con el análisis comparado de prácticas nacionales e internacionales, se demostró que es posible transitar hacia un modelo de madurez institucional que combina estandarización y adaptación contextual. El aporte central del trabajo es convertir la evidencia en arquitectura operativa: comités interdependenciales con mandato claro, rol formal de CISO, adopción progresiva de un SGSI guiado por ISO/IEC 27001, controles de "rápido impacto" (MFA, *backups* verificados, canal de incidentes), cooperación efectiva con RENATA/ColCERT y uso responsable de analítica avanzada (pilotos IA/ML). Todo ello se ancla en métricas accionables (MTTD, MTTR, porcentaje de MFA y de controles, gestión de alertas) y en artefactos auditables (actas, bitácoras, informes), lo cual garantiza la trazabilidad entre decisiones y resultados. En síntesis, el capítulo pasa de describir el problema a ofrecer una ruta escalable, medible y sostenible para fortalecer la resiliencia digital universitaria.

Más allá de cada institución, el trabajo propone un marco replicable para el sistema de educación superior: lineamientos escalonados por fases (preparación, *quick wins,* consolidación, integración colaborativa y optimización, responsabilidades RACI, un cronograma con tiempos y un tablero de KPI alineado con ciclos de auditoría y mejora. Esta arquitectura permite armonizar políticas internas con estándares internacionales y el marco regulatorio nacional, lo cual fomenta economías de escala mediante redes y alianzas, al tiempo que habilita decisiones basadas en evidencia. De este modo, las recomendaciones sientan las bases para una política universitaria y pública: institucionalizar la ciberseguridad como eje estratégico, asegurar la continuidad presupuestal y de talento, fortalecer la cooperación interinstitucional y promover la investigación aplicada que alimente pilotos y escalamiento tecnológico. El resultado es una agenda de transformación con sentido de país: proteger la infraestructura crítica del conocimiento, blindar procesos misionales y consolidar una cultura de seguridad que evoluciona por datos y no por inercia, con metas verificables y responsabilidad compartida entre la dirección, las áreas técnicas y la comunidad académica.

Referencias

Aguilar Ojeda, C. E., Hernández Omaña, T. H., & Soto Ortíz, S. I. (2024). Buenas prácticas de ciberseguridad en educación superior. *South Florida Journal of Development, 5*(12), 1–10. https://doi.org/10.46932/sfjdv5n12-080

Alexei, A. (2021). Cyber security strategies for higher education institutions. *Journal of Engineering Science, XXVIII*(4), 74–92. https://doi.org/10.52326/jes.utm.2021.28(4).07

Alwahaibi, A. M., Wan Hassa, W. A. B. W., Wan Ismail, W. B., & Almamari, M. (2022). A systematic literature review on IT security standards for higher education institution. *Journal of Tianjin University Science and Technology, 55*(7). https://doi.org/10.17605/OSF.IO/F935H

Amazon Web Services [AWS]. (2024). G*uía estratégica para mejorar la postura de ciberseguridad de Colombia.* https://d1.awsstatic.com/whitepapers/colombia-cybersecurity-guide-2024.pdf

Ambali Parambil, M. M., Rustamov, J., Ahmed, S. G., Rustamov, Z., Awad, A. I., Zaki, N., & Alnajjar, F. (2024). Integrating AI-based and conventional cybersecurity measures into online higher education settings: Challenges, opportunities, and prospects. *Computers and Education: Artificial Intelligence, 7,* 100327. https://doi.org/10.1016/j.caeai.2024.100327

Bonilla Bonilla, E. V. (2019). *Propuesta de mejoramiento continuo de la seguridad informática y de la información en las instituciones de educación superior* [Monografía de pregrado, Universidad Santo Tomás].

Cajamarca Mendez, G., Ron Gavi, M. G., Chamorro Ruiz, P. T., & Genovez Tobar, C. A. (2023). Evaluación del nivel de seguridad informática desplegado en los institutos de educación superior de la red RIT II. *Revista Conectividad, 4*(1), 38–49. https://doi.org/10.37431/conectividad.v4i1.49

Cano, J., & Almanza, M. (2020). *Estudio de la evolución de los incidentes de seguridad informática en Colombia 2010–2020. ISLA 2020 Proceedings, 11,* 1–11. https://aisel.aisnet.org/isla2020/11/?utm_source=aisel.aisnet.org%2Fisla2020%2F11&utm_medium=PDF&utm_campaign=PDFCoverPages

Cárdenas, H., Rubiano, S., & Cabra, L. (2023). Liderazgo, gobernanza y transformación digital en el diseño organizacional de la educación superior colombiana. Una revisión sistémica. *Revista Miradas, 18*(2), 164–189. https://doi.org/10.22517/25393812.25468

Castro-Maldonado, J. J., Villar-Vega, H. F., Marín-Ayala, K., Duarte-Herrera, K., & Giraldo-García, V. (2022). *Análisis de riesgos y vulnerabilidades de seguridad informática aplicando técnicas de inteligencia artificial orientado a instituciones de educación superior.* Servicio Nacional de Aprendizaje (SENA). https://www.researchgate.net/publication/359379099

Cayón Peña, J., & García Segura, L. A. (2014). La importancia del componente educativo en toda estrategia de ciberseguridad. *Estudios en Seguridad y Defensa, 9*(18), 5–13. https://doi.org/10.25062/1900-8325.9

Cheng, E. C. K., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information, 13*(4), 192. https://doi.org/10.3390/info13040192

Correa Zabala, M. M., Cano Fresneda, M. V., & Rivera Cuervo, N. (2024, 15 de enero). Universidad del Rosario: Una mirada integral a la seguridad y privacidad de los datos personales en las instituciones de educación superior. *Revista Nova et Vetera, 10*(91). https://urosario.edu.co/revista-nova-et-vetera/volumen-10-no-91

Deepika, B., & Srinivasan, M. (2023). Enhancing cybersecurity in higher education institutions using optimal deep learning-based biometric verification. *Journal of Intelligent & Fuzzy Systems, 44*(5), 6357–6369. https://doi.org/10.1016/j.aej.2025.01.012

Departamento Nacional de Planeación [DNP]. (2016). *Documento CONPES 3854: Política nacional de seguridad digital en Colombia.* Consejo Nacional de Política Económica y Social. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

European Union Agency for Cybersecurity [ENISA]. (2023). *Cybersecurity for higher education: Recommendations for universities and research centers.* ENISA. https://www.enisa.europa.eu/sites/default/files/publications/ENISA_Cybersecurity%20education%20initiatives%20in%20MS.pdf

Guerrero Sumalave, D. F. (2023). *Modelo de gestión de ciberseguridad para resolver incidentes en instituciones de educación superior* [Tesis de maestría, Universidad Francisco de Paula Santander Ocaña]. Facultad de Ingenierías.

Gurumendi Párraga, D. J. (2023). La importancia de tener instituciones educativas ciberseguras post pandemia. *Journal of Alternative Perspectives in the Social Sciences, 11*(4), 543–550.

IBM Security. (2024). *X-Force threat intelligence index 2024.* IBM Corporation. https://www.ibm.com/reports/threat-intelligence

ISO/IEC. (2022). *ISO/IEC 27001:2022 - Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos* (3.ª ed., octubre). Consultores B&C S.A.S.

Kumar, A., Mishra, K., Kumar Mahto, R., & Kumar Mishra, B. (2024). A framework for institution to enhancing cybersecurity in higher education: A review. *LatIA, 2*(94), 1–8. https://doi.org/10.62486/latia202494

Ley estatutaria 1581 de 2012. *Por la cual se dictan disposiciones generales para la protección de datos personales.* Congreso de la República. *D. O.* 48587, 18 de octubre de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sánchez, F., López-Fonseca, G., & Quiroz, D. (2020). Information security management frameworks and strategies in higher education institutions: A systematic review. *Annals of Telecommunications, 75*(9), 515–531. https://doi.org/10.1007/s12243-020-00783-2

Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]. (2023). *Estrategia nacional digital 2023–2026.* MinTic. https://www.mintic.gov.co/portal/715/articles-334120_recurso_1.pdf

Molina Oviedo, A. (2020). *Modelo de gobierno y gestión de riesgos TI para las universidades públicas de Colombia: Caso de estudio Universidad Popular del Cesar* [Tesis de maestría, Fundación Universidad del Norte]. Repositorio Uninorte. https://manglar.uninorte.edu.co/handle/10584/10394

Montilla Malaver, L. (2024). *Estado actual de la seguridad informática en las instituciones de educación superior en Colombia* [Trabajo de especialización, Universidad Abierta y a Distancia] Repositorio UNAD. https://repository.unad.edu.co/handle/10596/34638

Morales Carrillo, J. J., Avellán Zambrano, N., Mera Cantos, J. S., & Zambrano Bravo, M. (2019). *Ciberseguridad y su aplicación en las instituciones de educación superior públicas de Manabí* [Tesis, Escuela Superior Politécnica Agropecuaria de Manabí]. Repositorio ESPAM. https://repositorio.espam.edu.ec/items/3c004ff6-3968-42b4-ae32-6fbb354b5538/full

Morales Sáenz, F. I., Medina Quintero, J. M., & Abrego Almazan, D. (2025). Ciberseguridad en instituciones de educación superior: Un análisis desde la perspectiva de la teoría de la motivación de protección. *Revista de Investigación Educativa de la Rediech, 16,* e2271. https://doi.org/10.33010/ie_rie_rediech.v16i0.2271

Moreno Valencia, E. F., & Mejía Cardona, G. A. (2024). *Guía de ciberseguridad orientada a la comunidad educativa* [Monografía de especialización, Universidad Católica de Manizales]. Repositorio UCM. https://repositorio.ucm.edu.co/entities/publication/58318b9b-1f9b-4e83-9d51-5ec8b492f82c

Orosco-Fabian, J. (2024). Ciberseguridad en educación superior: Una revisión bibliométrica. *Revista Digital de Investigación en Docencia Universitaria, 18*(2), e1933. https://doi.org/10.19083/ridu.2024.1933

Ospina, H. F. (2024). Modelo de ciberseguridad para la protección de información crítica en las universidades públicas de Colombia. *Ciberespacio, Tecnología e Innovación, 3*(5), 33–56. https://doi.org/10.25062/2955-0270.4872

Piazza, A., Vasudevan, S., & Carr, M. (2023). Cybersecurity in UK universities: Mapping (or managing) threat intelligence sharing within the higher education sector. *Journal of Cybersecurity, 9*(1), 1–15. https://doi.org/10.1093/cybsec/tyad019

Pinda Román, N. J., & Moya Martínez, L. A. (2024). Ciberseguridad enfocada en el futuro digital de los estudiantes. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, 5*(2), 701–714. https://doi.org/10.56712/latam.v5i2.1910

Ragab, M., Alghamdi, B. M., Alakhtar, R., Alsobhi, H., Maghrabi, L. A., Alghamdi, G., Nooh, S., & AL-Malaise AL-Ghamdi, A. (2025). Enhancing cybersecurity in higher education institutions using optimal deep learning-based biometric verification. *Alexandria Engineering Journal, 117,* 340–351. https://doi.org/10.1016/j.aej.2025.01.012

Said-Hung, E., Cousido-González, M.-P., & Berlanga-Fernández, I. (2018). Transparencia en las instituciones de educación superior en Colombia. *El Profesional de la Información, 27*(1), 162–171. https://doi.org/10.3145/epi.2018.ene.15

Salman, A., & Alexandron, G. (2024). The digital fingerprint of learner behavior: Empirical evidence for individuality in learning using deep learning. *Computers and Education: Artificial Intelligence, 7,* 100322. https://doi.org/10.1016/j.caeai.2024.100322

Torres-Reyes, A.-M. (2024). Caracterización de ciberataques en universidades: Análisis de una muestra por conglomerados de cobertura mediática. *Cultura, Educación y Sociedad, 15*(2), e34465393. http://doi.org/10.17981/culteduso c.15.2.2024.5393

Vaca Orellana, C. F., Rosero, C. X., Vaca, A. J., & Valle, M. F. (2022). Privacidad de la información en internet: Un análisis sobre preocupaciones, acciones y razones en estudiantes universitarios. *Revista Ibérica de Sistemas e Tecnologias de Informação, (E53),* 531–544. https://www.risti.xyz/issues/ristie53.pdf

Valenzuela, L. A., Collantes, Z. M., & Durand, E. E. (2020). Sobre la gobernanza digital, política digital y educación. *Revista Eleuthera, 22*(2), 88–103. https://doi.org/10.17151/eleu.2020.22.2.6

Capítulo 6

Firewall humano y la protección de infraestructura crítica: modelo marco de formación en ciberseguridad*

DOI: https://doi.org/10.25062/9786287818644.06

Erika Tatiana Sánchez Gómez
Bulwark

Resumen: En Colombia, la ciberseguridad en las organizaciones de infraestructura crítica exige mucho más que esfuerzos formativos aislados, requiere arquitecturas de aprendizaje diseñadas intencionalmente para desarrollar capacidades reales y sostenibles. Este capítulo propone un modelo marco de formación en ciberseguridad adaptado a las necesidades de la infraestructura crítica, basado en estándares internacionales y apoyado en tecnologías innovadoras y emergentes. El objetivo es superar los enfoques reactivos y construir sistemas de aprendizaje estratégicos, medibles y contextualizados, que posicionen a las personas como pilar fundamental de la resiliencia digital.

Palabras clave: arquitecturas de aprendizaje; ciberseguridad; Colombia; infraestructura crítica; tecnologías innovadoras y emergentes.

* Capítulo de libro resultado del proyecto de investigación "La gobernanza del ciberespacio a nivel global, regional y nacional: desafíos, oportunidades y estrategias para la soberanía digital", del grupo de investigación "Ciberespacio, Tecnología e Innovación", de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado en 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 la autora y no reflejan necesariamente los de las instituciones participantes.

Erika Tatiana Sánchez Gómez
Ejecutiva colombiana especializada en estrategia empresarial, transformación digital y ciberseguridad. Iniciativa en estrategias de negocio y tecnología para fortalecer la madurez y las capacidades del entorno digital en organizaciones públicas y privadas. Enfoque en la convergencia entre el factor humano, la inteligencia estratégica y el ecosistema digital, bajo una visión que amplía la ciberseguridad hacia un enfoque sistémico e integral. **https://orcid.org/0009-0001-2594-8063** - Contacto: **tatiana@bulwark.la**

Citación APA: Sánchez-Gómez, E. T. (2026). *Firewall* humano y la protección de infraestructura crítica: Modelo marco de formación en ciberseguridad. M. E. Realpe-Díaz & A. M. González-González (Eds.), *Transformación digital y ciberseguridad en Colombia: Desafíos estratégicos para sectores de infraestructura crítica* (pp. 183-238). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818644.06

TRANSFORMACIÓN DIGITAL Y CIBERSEGURIDAD EN COLOMBIA: DESAFÍOS ESTRATÉGICOS PARA SECTORES DE INFRAESTRUCTURA CRÍTICA
ISBN impreso: 978-628-7818-63-7
ISBN digital: 978-628-7818-64-4
DOI: https://doi.org/10.25062/9786287818644

Colección Ciberseguridad y Ciberdefensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2026

CC BY NC ND

Introducción

"Las organizaciones no necesitan más cursos. Necesitan arquitecturas de aprendizaje que generen habilidades reales". Esta premisa debería ser una regla para las organizaciones. Así pues, en Colombia, las empresas de infraestructura crítica, por no decir todas, enfrentan un entorno cibernético cada vez más complejo, donde la continuidad operativa y la protección de servicios esenciales dependen tanto de la tecnología como del conocimiento aplicado de las personas. De hecho, el 95 % de las brechas de seguridad tienen origen en "errores" humanos, lo cual evidencia una falla estructural en los procesos de formación y en la construcción de cultura digital dentro de las organizaciones.

Según el Global Cybersecurity Outlook 2025 del Foro Económico Mundial, el entorno cibernético actual está marcado por una creciente complejidad, el uso ofensivo de tecnologías emergentes como la inteligencia artificial, y una alarmante escasez de talento especializado. En este contexto, y de acuerdo con la Estrategia Nacional de Seguridad Digital 2025-2027, Colombia enfrenta vulnerabilidades críticas en sus servicios esenciales, derivadas de debilidades institucionales, brechas de formación y una limitada articulación sectorial.

En el ámbito global, la escasez de expertos supera los cuatro millones, mientras que en América Latina y el Caribe la brecha alcanza 1,3 millones de profesionales (Forbes Centroamérica, 2024). Esta carencia expone a las empresas a riesgos severos, que van desde interrupciones operativas hasta pérdidas económicas y daños reputacionales. En Colombia, las causas de este vacío son múltiples y se retroalimentan entre sí: formación poco accesible en muchas regiones, baja concientización social y empresarial sobre la ciberseguridad, transformación digital acelerada sin estrategias de protección adecuadas y fuga de talento hacia el extranjero.

Ante esta realidad, resulta fundamental reconocer que la tecnología por sí sola no puede contener el avance de las amenazas digitales. La verdadera defensa comienza en las personas: en su criterio, su capacidad de respuesta y su comprensión del entorno. Específicamente, el *firewall* humano, ese escudo que cada colaborador representa cuando está bien formado, se convierte en un elemento clave en la protección de las organizaciones, especialmente cuando se trata de infraestructura crítica.

Sin embargo, este *firewall* no surge por inercia ni por voluntad, sino que requiere de modelos de formación diseñados con intención, pertinencia y sostenibilidad. Estos modelos deben integrar tecnologías emergentes y metodologías activas, además de adaptarse a la diversidad de roles, niveles de madurez y contextos operativos existentes dentro de las organizaciones. Por ello, la pregunta clave no es solo cómo formar, sino cómo lograr que el aprendizaje se traduzca en una capacidad real de protección y resiliencia.

En este sentido, a partir del entendimiento de las teorías y las metodologías de aprendizaje, así como del análisis de la construcción y el desarrollo del conocimiento humano, este saber debe abordarse hoy como una extensión al mundo digital y como una capacidad intelectual, una visión que emerge con el advenimiento del internet y la ciberseguridad, los cuales han propiciado nuevos modelos, escenarios y tecnologías que permiten la interconexión de lo físico y lo virtual. Estas tecnologías forman parte de un ecosistema que evoluciona al ritmo de las amenazas y que demanda estrategias de formación igualmente dinámicas, personalizadas y sostenibles.

Aunque algunas empresas ya han dado pasos hacia la formación de equipos especializados y la sensibilización de sus colaboradores, a menudo lo han hecho desde la urgencia, con entrenamientos fragmentados, campañas de concientización aisladas o espacios que no garantizan una transferencia efectiva del aprendizaje a la acción. A ello se suma una profunda desconexión entre la oferta formativa de muchas instituciones y las necesidades reales del sector productivo, particularmente en los sectores de infraestructura crítica, para responder a un entorno de amenazas dinámicas y persistentes. Por lo tanto, se vuelve indispensable preguntarse: ¿Son estas acciones suficientes y sostenibles? ¿Están alineadas con las necesidades reales de protección que exige una organización crítica? ¿Qué tipo de modelo formativo permitiría desarrollar verdaderas capacidades de defensa en todos los niveles de una empresa? ¿Qué tecnologías, metodologías y frecuencias de entrenamiento se deben implementar para construir un verdadero *firewall* humano, capaz de adaptarse al riesgo y actuar con criterio, según su rol y nivel de responsabilidad?

Metodología

La construcción del modelo marco de formación en ciberseguridad para empresas de infraestructura crítica en Colombia se desarrolló con una metodología de investigación cualitativa de tipo estratégico y deductivo. Esta se fundamentó en los postulados de Hernández et al. (2014), quienes plantean este enfoque como una vía idónea para interpretar fenómenos complejos, especialmente cuando se busca comprender los significados y las relaciones subyacentes en los procesos organizacionales y sociales. A diferencia de la recolección empírica de datos cuantificables, esta metodología se basa en la revisión crítica, sistemática y argumentada de fuentes documentales, normativas y técnicas de alta relevancia, con el propósito de construir un modelo teórico-práctico que responda a una problemática contextual concreta.

Así, el desarrollo del modelo C-TOET (Cyber Technology Organizational Environment Training) se fundamentó en la articulación de múltiples fuentes primarias y secundarias. Para ello, se realizó una revisión sistemática de literatura especializada, que abarcó marcos de referencia internacionales (como NIST NICE, ISO/IEC 27001:2022, MITRE ATT&CK) e informes prospectivos y técnicos de alto impacto (como el *Global Cybersecurity Outlook 2025,* del Foro Económico Mundial, y el *Threat Landscape Report* de ENISA). Asimismo, se analizaron documentos estratégicos del contexto colombiano, entre ellos la Estrategia Nacional de Seguridad Digital 2023-2027 y el CONPES 3995. Esta revisión permitió identificar brechas estructurales, desafíos de gobernanza, vacíos en capacidades humanas y la falta de alineación entre la formación existente y los riesgos que enfrentan los sectores de infraestructura crítica.

De forma complementaria, se desarrolló un análisis comparativo de tecnologías formativas, que incluyó la evaluación de plataformas especializadas como Cyberbit, Hack The Box, HackRocks, Immersive Labs y TryHackMe, entre otras. Cabe señalar que este ejercicio no buscó comparar características superficiales, sino analizar el valor pedagógico y operativo de estas herramientas en función de criterios como realismo, adaptabilidad, nivel de inmersión, personalización por rol y alineación con estándares de certificación internacional. A su vez, se incorporó el estudio de metodologías activas de aprendizaje ampliamente validadas, como el aprendizaje basado en problemas (ABP), *microlearning*, simulaciones tipo CTF, gamificación y *flipped classroom,* seleccionadas por su capacidad de generar apropiación significativa del conocimiento y fomentar la transferencia efectiva del aprendizaje a contextos reales.

El modelo se concibió a partir de la integración conceptual del marco TOE (Technology–Organization–Environment), específicamente adaptado al contexto de formación, y se enriqueció con elementos del modelo VSM (Viable System Model). Esta combinación teórica tuvo como propósito asegurar la coherencia entre las dimensiones tecnológicas, organizacionales y de entorno, factores clave que condicionan la adopción de programas de entrenamiento en ciberseguridad. Gracias a esta sólida base teórica, fue posible construir una arquitectura formativa modular, escalable y aplicable a múltiples roles dentro de las organizaciones.

De este modo, el modelo C-TOET se construye no como una propuesta aislada, sino como el resultado de un proceso metodológico riguroso que entrelaza fundamentos teóricos, revisión normativa, análisis técnico de plataformas y principios pedagógicos activos. Así, esta base no solo otorga validez académica y estratégica al modelo, sino que lo convierte en una herramienta adaptable a los distintos niveles, roles y contextos de las organizaciones protectoras del corazón digital del país.

Tecnologías internacionales aplicables a los programas de formación en ciberseguridad para empresas en Colombia

En un entorno marcado por la aceleración de la transformación digital, entendida como la adopción estratégica de tecnologías digitales para redefinir procesos, modelos de negocio y servicios públicos (MinTIC, 2020), la ciberseguridad ha pasado de ser un componente técnico a convertirse en una capacidad organizacional crítica. Este nuevo panorama, caracterizado por amenazas cibernéticas cada vez más sofisticadas, ha evidenciado las limitaciones de los modelos formativos tradicionales, centrados en la teoría o en ejercicios desarticulados de la realidad operativa.

En especial para las organizaciones que gestionan infraestructura crítica, la necesidad de entrenamientos más realistas, adaptativos y basados en el contexto se ha vuelto inaplazable. No se trata solo de "enseñar" ciberseguridad, sino de desarrollar competencias prácticas, situadas y medibles que permitan a los equipos responder de manera eficaz y oportuna frente a escenarios complejos. Esto plantea una pregunta esencial para el diseño de programas de formación en el país: ¿Qué tecnologías disponibles a nivel internacional permiten, hoy y en el futuro, construir capacidades humanas en ciberseguridad que sean escalables, contextualizadas y alineadas con los riesgos reales que enfrentan las empresas en Colombia?

Responder a esta pregunta exige ir más allá de identificar herramientas que simplemente "enseñan"; implica reconocer plataformas y entornos capaces de

desarrollar capacidades que sean medibles, escalables y sostenibles en el tiempo. En este contexto, las tecnologías emergentes y las innovadoras tienen un papel clave como habilitadores de aprendizajes significativos en el ámbito de la ciberseguridad. Las primeras son definidas por la Organización para la Cooperación y el Desarrollo Económicos (OECD) como aquellas que aún no están plenamente desarrolladas o comercializadas, pero que tienen el potencial de generar disrupciones o nuevas oportunidades económicas y sociales, mientras que las segundas, según Rogers (2003), son aquellas ya adoptadas con éxito que demuestran mejoras sustanciales en procesos, productos o servicios.

Con el fin de garantizar la rigurosidad en la identificación de tecnologías aplicables a la formación en este campo, se establecieron cinco criterios fundamentales, los cuales fueron definidos a partir de una triangulación metodológica entre tres fuentes principales (tabla 1).

Tabla 1. *Fuentes principales para definir los criterios*

Fuente	Rol en el análisis
Literatura académica y marcos pedagógicos (OECD, Tobón, Piaget, Vygotsky, Kolb y Bandura).	Fundamentan las *dimensiones clave del aprendizaje,* como aplicabilidad, personalización, evaluación continua, etc.
Referentes sectoriales y técnicos internacionales (NIST, ENISA, WEF, NICE, ISO/IEC 27001 y MITRE ATT&CK).	Fundamentan los *criterios de pertinencia,* como resiliencia, cumplimiento normativo, y segmentación por roles.
Estudios de mercado e impacto (Forrester Wave, Gartner, casos de uso y validaciones de impacto)	Respaldan los *criterios de madurez tecnológica,* como validación, escalabilidad e innovación continua.

Fuente: Elaboración propia.

La construcción de los cinco criterios de evaluación tecnológica se deriva de una articulación intencionada entre tres fuentes clave, cada una con un rol específico en el análisis. En primer lugar, a partir de los aportes de autores como Tobón, Piaget, Vygotsky, Kolb y Bandura, y de las orientaciones de organismos como la OECD, la literatura académica y los marcos pedagógicos permitieron identificar las dimensiones esenciales del aprendizaje significativo, situado y por competencias. Esta identificación fundamenta el primer criterio, centrado en las dimensiones clave del aprendizaje, el cual incorpora aspectos como aplicabilidad práctica, simulación realista, personalización por rol, interacción significativa y evaluación continua.

En segundo lugar, los marcos técnicos y normativos internacionales aportaron los elementos necesarios para comprender los desafíos específicos del sector

de infraestructura crítica, como NIST, ENISA, ISO/IEC 27001, NICE Framework y MITRE ATT&CK. Esta fuente respalda el segundo criterio, el cual evalúa la pertinencia sectorial en función de su capacidad para enfrentar amenazas persistentes, cumplir normativas, escalar entre perfiles y compensar brechas de talento.

En tercer lugar, los estudios de mercado e impacto, que abarcaban *rankings* como Forrester Wave y Gartner, casos de uso documentados y validaciones académicas o institucionales, sirvieron para definir el tercer criterio, el cual se orientó a la validación de impacto y madurez tecnológica. Este criterio incluye la evidencia de efectividad, la escalabilidad de las soluciones y su capacidad de innovación continua.

A partir del análisis transversal de estas tres fuentes, surgieron además dos criterios complementarios que fortalecen la aplicabilidad real de las tecnologías en contextos organizacionales: el cuarto criterio —relacionado con la alineación con certificaciones internacionales (como CISSP, CISM, CEH, CompTIA, entre otras)— garantiza la conexión entre los contenidos formativos y los estándares globales de talento en ciberseguridad, mientras que el quinto criterio responde a la necesidad de segmentar la oferta según el público objetivo o "*firewall* humano", la cual debe considerar a empleados generales, directivos estratégicos y expertos técnicos, cada uno con niveles de exposición y responsabilidad diferenciados frente al riesgo cibernético.

Esta matriz de cinco criterios (tabla 2), resultado de la integración de teorías del aprendizaje, estándares técnicos y evidencia de mercado, permite evaluar de forma rigurosa, estratégica y contextualizada las tecnologías emergentes e innovadoras aplicadas a la formación en ciberseguridad en sectores de infraestructura crítica.

Tabla 2. *Criterios de análisis de tecnologías para formación en ciberseguridad*

Criterio principal	Subcriterios	Aspectos clave de evaluación
Dimensiones clave del aprendizaje (Basadas en teorías del aprendizaje significativo, situado y por competencias)	Aplicabilidad práctica	¿La tecnología permite aplicar lo aprendido en situaciones reales del entorno operativo? ¿Facilita el traslado del conocimiento al desempeño laboral?
	Simulación realista	¿Qué grado de inmersión y fidelidad tiene frente a escenarios reales de amenaza? ¿Reproduce condiciones de presión y toma de decisiones críticas?
	Interacción significativa	¿Promueve la toma de decisiones, ensayo-error, retroalimentación inmediata, colaboración o pensamiento crítico?
	Personalización por rol	¿Permite adaptar la experiencia formativa a diferentes perfiles (operativos, tácticos, estratégicos)? ¿Ofrece rutas de aprendizaje diferenciadas?
	Evaluación continua	¿Incorpora mecanismos para medir progreso, desempeño, brechas de aprendizaje y evolución del talento? ¿Ofrece *dashboards* o analítica integrada?

Criterio principal	Subcriterios	Aspectos clave de evaluación
Pertinencia para el sector de infraestructura crítica (Basado en los desafíos específicos del sector)	Resiliencia ante amenazas persistentes	¿La tecnología permite preparar a los usuarios frente a amenazas avanzadas y ataques dirigidos? ¿Incluye escenarios de ataque sofisticado?
	Margen de error cero	¿Contribuye al entrenamiento en toma de decisiones bajo presión y escenarios donde el error no es opción? ¿Simula entornos de misión crítica?
	Multinivel y multiperfil	¿Es útil para formar desde técnicos de campo hasta líderes de nivel CISO o directivos? ¿Escala entre roles y niveles de responsabilidad?
	Cumplimiento normativo	¿Está alineada con marcos como NIST, ISO 27001, MITRE ATT&CK? ¿Incorpora controles, simulaciones o contenidos vinculados a estándares internacionales?
	Déficit de talento	¿Compensa la falta de expertos mediante automatización del entrenamiento, inteligencia artificial adaptativa o aprendizaje autodirigido? ¿Permite acelerar la curva de desarrollo?
Validación de impacto y madurez (Basado en evidencia, informes y casos reales)	Validación en el mercado	¿Está reconocida en *rankings* como el Forrester Wave, Gartner u otras consultoras? ¿Es usada por entidades de defensa, banca o infraestructura crítica?
	Evidencia de efectividad	¿Hay estudios de impacto que demuestren mejora en habilidades o reducción de incidentes posentrenamiento? ¿Cuenta con validaciones independientes o académicas?
	Escalabilidad y adaptabilidad	¿Funciona en diferentes contextos (nacional, regional, remoto, híbrido)? ¿Se adapta fácilmente a distintos sectores y niveles de madurez digital?
	Innovación continua	¿Tiene ciclos frecuentes de actualización? ¿Integra nuevas tecnologías como IA, RV, RA, *data analytics*, CTF automatizados, etc.?
Alineación con certificaciones internacionales Público objetivo	Certificaciones y estándares reconocidos	¿La tecnología prepara o se integra con certificaciones como CISSP, CISM, CEH, CompTIA Security+, etc.?
	Adaptabilidad por perfil de usuario	¿La tecnología contempla diferentes niveles de usuario: empleados, directivos y expertos técnicos; y adapta el contenido, la complejidad y los escenarios de acuerdo con su rol, responsabilidad y nivel de exposición al riesgo cibernético? ¿Facilita la creación de un "*firewall* humano" integral mediante rutas formativas diferenciadas y complementarias?

Fuente: Elaboración propia según fuentes.

Una vez definidos los criterios de análisis y las dimensiones clave del aprendizaje en ciberseguridad para empresas de infraestructura crítica, el siguiente paso fue identificar y seleccionar tecnologías representativas en el ámbito internacional que pudieran evaluarse de forma comparativa y rigurosa. Este proceso no buscó una lista exhaustiva, sino una muestra estratégica de soluciones que, aplicadas ya en contextos reales, han demostrado tener impacto, adopción o innovación relevante en el entrenamiento de talento en ciberseguridad. La tabla 3 presenta las plataformas y tecnologías que son consideradas más sólidas y reconocidas internacionalmente para entrenamiento en ciberseguridad.

Tabla 3. *Tecnologías para formación en ciberseguridad*

Tipo de tecnología	Plataformas referentes	Justificación
Simulación avanzada / Cyber Range	Cyberbit, SimSpace, Circadence, RangeForce, SANS Cyber Aces y InmerseLbas.	Simulan entornos hiperrealistas, ataques tipo APT, con dashboards en tiempo real y alineación con marcos como NIST/MITRE.
Gamificación y retos técnicos (CTF)	Hack The Box, TryHackMe, HackRocks, PentesterLab, VulnHub, OverTheWire, Root Me y PortSwigger Academy.	Formatos interactivos y escalables para talento joven y técnico. Entrenan habilidades ofensivas y defensivas mediante retos progresivos.
Concientización y comportamiento humano	KnowBe4, Lucy Security, Cybrary, Infosec IQ, Terranova Security, Living Security, Cofense PhishMe, Wombat Security, Mimecast y Security Mentor.	Diseñadas para modificar el comportamiento humano frente al riesgo. Incluyen simulaciones de phishing, campañas automatizadas y métricas individuales.
E-learning general con cursos en ciberseguridad	Coursera, edX, Udemy, Khan Academy, Pluralsight, Skillshare, FutureLearn, Domestika y MasterClass.	Accesibles globalmente, permiten iniciar procesos de formación en ciberseguridad con respaldo académico. Útiles para fundamentos generales.
Certificaciones profesionales y vendors	CompTIA, (ISC)², ISACA, Cisco Networking Academy, EC-Council, Offensive Security (OffSec), SANS Institute / GIAC, Microsoft Learn, Google Cloud Training y AWS Training & Certification.	Otorgan certificaciones reconocidas internacionalmente, esenciales para roles técnicos y estratégicos en ciberseguridad.

Fuente: Elaboración propia con base en las fuentes consultadas.

Con base en esta selección, el siguiente paso fue traducir cualitativamente los criterios establecidos en una escala ordinal. Esta transformación permite no solo estandarizar la evaluación de cada herramienta, sino también generar una matriz de análisis robusta que puede utilizarse en estudios cuantitativos posteriores. Cada subcriterio fue calificado en una escala del 1 al 5, donde 1 representa un nivel bajo o ausente de cumplimiento y 5 representa un cumplimiento óptimo o validado por evidencia.

En cuanto a la construcción de la escala de medición, para cuantificar el análisis cualitativo y comparativo entre tecnologías se propone una escala ordinal tipo Likert de 5 niveles, la cual asigna valores numéricos a los grados de cumplimiento observados en cada criterio. (tabla 4).

Tabla 4. *Escala ordinal tipo Likert de 5 niveles*

Nivel	Valor numérico	Descripción operativa
Muy bajo / no aplica	1	No evidencia cumplimiento del criterio / no es aplicable para el contexto crítico.

Nivel	Valor numérico	Descripción operativa
Bajo	2	Evidencia limitada, cumplimiento parcial o no validado en entornos reales.
Moderado	3	Cumple parcialmente el criterio, con limitaciones o sin validación sectorial.
Alto	4	Cumplimiento claro del criterio, con validaciones parciales o indirectas.
Muy alto / avanzado	5	Cumple totalmente, validado, reconocido por terceros y aplicable directamente a infraestructura crítica.

Fuente: Elaboración propia.

El criterio relacionado con el público objetivo o perfil de entrenamiento no representa un nivel de calidad o desempeño, sino una variable de cobertura y adaptabilidad poblacional. Por esta razón, se propuso una escala ordinal de amplitud, en la que el valor 1 indica tecnologías enfocadas en un solo tipo de perfil (como talento joven o usuarios finales). En contraste, el valor 5 refleja tecnologías que permiten entrenar a múltiples perfiles (empleados, técnicos, directivos) de forma diferenciada según su nivel de madurez y responsabilidad frente al riesgo (tabla 5).

Tabla 5. *Cobertura y descripción del público objetivo por tecnología de entrenamiento en Ciberseguridad*

	Empleados	Directivos	Técnicos
Cyberbit (RangeForce)			
Immersive Labs			
Hack The Box			
Coursera / Platzi /edX			
HackRocks			
Lucy ThriveDX			
Try HackMe			
KnowBe4			
RangeForce			
SimSpace			
Cybrary			

Fuente: Elaboración propia.

Por otro lado, se incorporó una columna cualitativa que describe de forma explícita los tipos de usuario objetivo que cada tecnología aborda. Esto permite a las organizaciones identificar fácilmente qué soluciones formativas son más adecuadas según el perfil de sus equipos y los desafíos específicos de su infraestructura crítica (tabla 6).

Tabla 6. *Evaluación de las tecnologías de formación en ciberseguridad*

Criterio	Subcriterio	Cyberbit (Range-Force)	Immersive Labs	Hack The Box	Coursera / Platzi / edX	Hack-Rocks	Lucy ThriveDX	Try HackMe	KnowBe4	Range-Force	SimSpace	Cybrary
Dimensiones clave del aprendizaje	Aplicabilidad práctica	5	4	4	2	4	4	4	3	5	4	3
	Simulación hiperrealista	5	4	4	1	3	5	4	4	5	4	3
	Interacción significativa	5	5	5	2	4	5	4	3	4	4	3
	Personali-zación por rol	5	5	5	2	5	4	3	4	5	4	3
	Evaluación continua	5	5	5	3	5	5	4	5	5	4	2
Pertinencia para el sector de infraestructura crítica	Resiliencia ante amenazas persistentes	5	4	4	1	5	5	4	5	4	4	3
	Margen de error cero	5	4	4	1	4	3	3	3	4	4	2
	Multinivel y multiperfil	5	5	5	1	5	5	3	4	5	5	3
	Cumplimiento normativo	5	5	5	1	3	4	3	5	5	5	3
	Déficit de talento	5	4	4	1	5	4	3	3	5	4	2
Validación de impacto y madurez	Validación en el mercado	5	4	4	2	5	5	4	5	4	4	3
	Evidencia de efectividad	5	4	4	2	4	5	4	4	4	4	4
	Escalabilidad y adaptabilidad	5	4	4	3	4	5	5	5	4	4	3
	Innovación continua	5	4	4	2	5	5	4	5	5	4	3
Alineación con certificaciones internacionales	Certificaciones y estándares reconocidos	5	4	3	1	4	3	2	2	5	4	3
Público Objetivo	Audiencia ideal	3	3	3	1	4	4	3	4	3	4	2

Fuente: Elaboración propia según fuentes (*Forrester*).

El análisis comparativo de tecnologías evidencia una clara diferenciación entre las plataformas en términos de profundidad pedagógica, aplicabilidad en contextos críticos y alineación con estándares internacionales. Tecnologías como Cyberbit, InmerseLabs y HackTheBox se posicionan como las más robustas y completas, puesto que alcanzan puntuaciones máximas en criterios clave como simulación hiperrealista, personalización por rol, cumplimiento normativo y evaluación continua. Esta capacidad las convierte en opciones muy pertinentes para empresas de infraestructura crítica que requieren entrenamientos avanzados y sostenibles, un hecho que se corrobora en Forrester Wave Q4 2023 (figura 1).

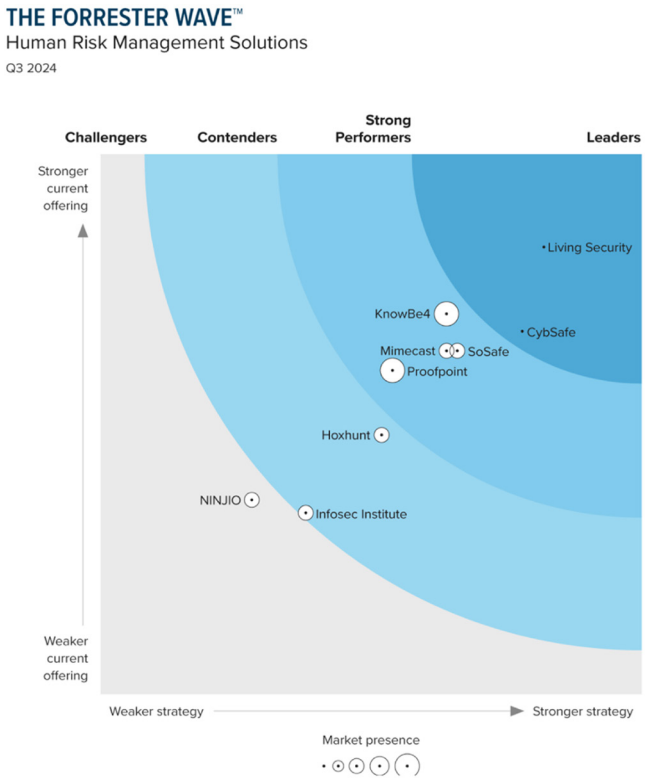
Figura 1. *Cuadrante Forrester Wave Q4 2023*

Fuente: Forrester Wave Q4 2023.

Por otro lado, herramientas como RangeForce (adquirida recientemente por Cyberbit), Pluralsight y SimSpace destacan por su marcado enfoque, si bien presentan limitaciones en áreas como la validación de impacto o la cobertura multinivel. Además, plataformas como Living Security, CybSafe y KnowBe4 se orientan claramente al entrenamiento masivo en conciencia cibernética y usuarios finales, lo cual las hace muy efectivas en la reducción de errores humanos comunes. De hecho, entre 2022 y 2024 se evidenció un cambio notable en el liderazgo de las

plataformas de concientización, según el informe Forrester Wave. KnowBe4, que lideraba ampliamente en 2022, descendió en la evaluación de 2024 porque fue percibida como menos innovadora y centrada en contenido genérico. En contraste, Living Security ascendió al primer lugar gracias a su enfoque en la gestión del riesgo humano, el uso de experiencias inmersivas y su capacidad para generar analítica individualizada del comportamiento, lo cual le permitió alinearse mejor con las necesidades emergentes de ciberseguridad organizacional (figura 2).

Figura 2. *Cuadrante Forrester Wave Q3 2024*



Fuente: Cuadrante Forrester Wave Q3 2024.

Finalmente, tecnologías como Coursera, Platzi o Cybrary, si bien ofrecen una amplia cobertura de contenidos, muestran una menor capacidad de simulación realista y aplicación directa. Por esta razón, son más adecuadas como complemento conceptual que como herramienta principal de entrenamiento táctico. Esta caracterización permite a las organizaciones tomar decisiones más estratégicas y

basadas en evidencia al momento de definir qué tecnología utilizar según su perfil de riesgo, madurez digital y públicos objetivo.

Ahora bien, más que establecer soluciones definitivas, este análisis permite identificar tecnologías formativas que cumplen funciones específicas dentro del ecosistema de entrenamiento en ciberseguridad. Cada una de ellas representa una pieza valiosa, ya sea por su capacidad de simular entornos reales, de adaptarse a diferentes perfiles, de desarrollar competencias técnicas o de facilitar la evaluación continua. Estas piezas podrán integrarse, de manera estratégica, en un modelo más amplio, lo cual permitirá evidenciar su utilidad para diseñar programas formativos escalables, medibles y alineados con los objetivos de resiliencia y continuidad del negocio en las organizaciones de infraestructura crítica en Colombia.

Con las tecnologías ya mapeadas, el foco ahora se traslada al terreno donde realmente importan las empresas de infraestructura crítica en Colombia. En este contexto, es crucial determinar su nivel de preparación y sus necesidades para cerrar la brecha entre riesgo y resiliencia., por cuanto entender estos desafíos es clave para diseñar estrategias de formación que no solo suenen bien en teoría, sino que funcionen en la realidad.

Necesidades y desafíos de las empresas de infraestructura crítica en Colombia

Toda transformación profunda en las organizaciones comienza con la identificación clara de dos elementos: lo que se necesita y lo que se interpone en el camino para lograrlo. En el contexto de la ciberseguridad, estas dos nociones —necesidades y desafíos— adquieren un carácter estratégico y urgente, particularmente en sectores considerados críticos para la estabilidad nacional.

Las necesidades pueden entenderse como aquellas condiciones, recursos o capacidades esenciales para lograr un estado deseado de protección, resiliencia o sostenibilidad en seguridad digital. En contraste, los desafíos representan los obstáculos técnicos, humanos, financieros o estructurales que impiden alcanzar tal estado y que, por tanto, deben ser abordados con decisión y enfoque estratégico.

En Colombia, las empresas de infraestructura crítica —definidas como "aquellos activos, servicios y sistemas físicos y virtuales cuya afectación comprometería gravemente la seguridad nacional, la salud pública, la economía o el bienestar de la población" (CONPES 3701 de 2011, ampliada por el CONPES 3995 de

2020)— abarcan sectores esenciales como energía, hidrocarburos, agua potable, transporte, telecomunicaciones, salud, finanzas, defensa y seguridad, y gobierno digital. Por consiguiente, abordar las necesidades y desafíos en formación en ciberseguridad para estas entidades trasciende una simple discusión técnica o pedagógica. Se trata, en efecto, de una cuestión de seguridad nacional, de la continuidad de servicios esenciales y de la preservación del bienestar ciudadano. Sobre todo si se tiene en cuenta que sectores como la energía, el agua, la salud o las telecomunicaciones operan con una alta exposición a amenazas cibernéticas cada vez más sofisticadas, que exigen no solo tecnologías robustas, sino sobre todo talento humano preparado, actualizado y resiliente.

En este escenario, comprender las necesidades y desafíos formativos implica ir más allá del inventario de cursos disponibles o de la medición de certificaciones obtenidas. Requiere adoptar una mirada estructural, apoyada en teorías del conocimiento y el aprendizaje, que permita diseñar arquitecturas de formación alineadas con los riesgos reales del entorno, con los marcos normativos internacionales y con las capacidades humanas necesarias para enfrentarlos.

Al respecto, se debe señalar que las primeras teorías del saber, desde el racionalismo clásico de Platón, que plantea que el conocimiento surge de las ideas innatas y el pensamiento abstracto, hasta el empirismo de Aristóteles, que lo ubica en la experiencia sensorial, la observación y la clasificación del mundo físico, nos muestran dos fuentes fundamentales del conocimiento: la razón y la experiencia. Más adelante, el racionalismo moderno (Descartes, Spinoza, Leibniz) refuerza el poder del pensamiento lógico, la imaginación y la percepción interna como caminos hacia el conocimiento, mientras que el empirismo moderno (Locke, Hume) incorpora la experiencia externa e interna como base para conectar ideas y generar saberes útiles. Kant, con su criticismo, propone una síntesis: el conocimiento se construye al integrar percepciones sensoriales con estructuras lógicas propias de la mente. Luego, el positivismo (Comte) enfatiza la observación empírica y el pragmatismo (Dewey, James, Pierce) introduce la adaptabilidad y la utilidad práctica del conocimiento en contextos reales. Además, corrientes como la fenomenología y el constructivismo resaltan la experiencia vivida, la interpretación del fenómeno y la interacción social como elementos clave para construir conocimiento significativo. Finalmente, la epistemología genética de Piaget muestra cómo el conocimiento evoluciona desde la infancia mediante procesos de desequilibrio, adaptación y reorganización cognitiva. Estas visiones convergen en una idea central: el aprendizaje es más efectivo cuando es activo, contextualizado, basado en la experiencia y ajustado al desarrollo del individuo (tabla 7).

Las teorías del conocimiento y del aprendizaje no solo han marcado la evolución del pensamiento humano, sino que hoy encuentran su máxima expresión en el uso de tecnologías emergentes aplicadas a la formación. Esta convergencia permite fundamentar un modelo de formación que integre aprendizaje basado en problemas, simulaciones y aprendizaje adaptativo. Dicho modelo resulta especialmente pertinente en el entrenamiento en ciberseguridad, ámbito en el cual el conocimiento debe ser construido, aplicado y fortalecido en escenarios críticos, reales y cambiantes a través de tecnologías innovadoras y emergentes.

Tabla 7. *Teorías de conocimiento y metodologías de aprendizaje*

Corriente filosófica	**Metodología de aprendizaje**	**Aplicación en ciberseguridad**
Constructivismo (Bruner, Husel)	Aprendizaje basado en problemas (ABP)	Resolver un ataque *ransomware* simulado en un laboratorio.
Pragmatismo (Dewey, Constructivismo)	Aprendizaje basado en proyectos	Diseñar una estrategia de protección de datos para una Pyme.
Empirismo (Hume) y aprendizaje experiencial (Kolb)	Aprendizaje experiencial	Analizar una intrusión real en un entorno virtual para aprender de los errores.
Constructivismo social (Vygotsky y Bandura)	Aprendizaje colaborativo	Trabajo en grupo para resolver un caso cibernético desde varios roles
Conductismo y psicología del comportamiento	Gamificación	Competencias CTF para entrenar equipos SOC.
Epistemología genética (Piaget) y realismo crítico	Aprendizaje adaptativo	Ruta personalizada de formación según evaluación de habilidades.
Racionalismo y constructivismo	*Flipped classroom* ('aula invertida').	Ver fundamentos teóricos y luego aplicar en simuladores prácticos.
Criticismo y competencias (Tuning, Deusto)	Aprendizaje basado en competencias.	Ejercicios de detección y respuesta aplicados a casos reales.
Fenomenología y aprendizaje social (Bandura)	Aprendizaje social	Aprender sobre inteligencia social mediante observación y práctica.
Constructivismo, aprendizaje experiencial y realismo crítico	Simulaciones y aprendizaje inmersivo (VR/AR)	Simulaciones de incidentes en entornos como Cyber Range o con realidad virtual.

CTF: capturar la bandera; SOC: centros de operaciones de seguridad

Fuente: Elaboración propia.

De los conceptos a la necesidad real: una lectura aplicada a la arquitectura formativa

Si bien las teorías del conocimiento y del aprendizaje permiten estructurar modelos formativos coherentes y técnicamente sólidos, las verdaderas urgencias emergen

en el terreno de las operaciones. En este ámbito, las empresas responsables de infraestructuras críticas —como energía, salud, telecomunicaciones o transporte— enfrentan amenazas cibernéticas en constante evolución, cuya velocidad, en muchos casos, supera la capacidad de respuesta institucional.

Frente a esta realidad, el talento humano capacitado se constituye como el activo más estratégico en la defensa adaptativa. Sin embargo, en Colombia persiste una brecha formativa estructural que se manifiesta en la "escasez de talento especializado" y una "débil cultura de seguridad digital", ambos obstáculos críticos para consolidar capacidades de ciberdefensa sostenibles, tal como lo indica la Estrategia Nacional de Seguridad Digital 2025-2027. Esta situación obliga a las organizaciones a dejar de pensar en la formación como un componente periférico y a empezar a verla como parte estructural de su arquitectura de seguridad.

Para ello, fue necesario identificar y mapear las principales necesidades transversales de formación mediante un análisis documental comparativo, la referenciación normativa (NIST, NICE, OCDE, WEF) y estudios de caso. Estas necesidades se explicitan a continuación (tabla 8), no solo desde una perspectiva teórica, sino también desde su manifestación práctica y su impacto directo en la madurez de los programas de formación.

Tabla 8. *Codificación de necesidades con soporte documental.*

Necesidad	Fragmento textual/documento	Fuente
1. Visión sistémica	"La mayoría de los líderes consultados (59 %) indica que sus organizaciones no cuentan con programas de desarrollo profesional específicos en ciberseguridad".	World Economic Forum. (2025, p. 21).
	"Las organizaciones deben desarrollar y mantener una fuerza laboral con las competencias adecuadas [...] mediante entrenamiento continuo, certificaciones y planes de carrera".	NIST (2024, p. 16).
2. Seguimiento continuo e integración con la matriz de riesgos	"El marco CSF 2.0 refuerza la integración de la gestión del riesgo con el desarrollo del talento humano".	NIST. (2024, p. 9).
	"Las capacidades de entrenamiento deben ser trazables en las funciones organizacionales clave y en los dominios de riesgo".	NIST (2024, p. 9).
3. Identificación proactiva de brechas por área	"Las evaluaciones diagnósticas por rol siguen siendo una gran ausencia en las estrategias formativas de América Latina".	OECD (2023, pp. 23-24).
	"No se realiza un análisis de brechas de habilidades basado en funciones específicas".	WEF (2025, p. 21).

Necesidad	Fragmento textual/documento	Fuente
4. Formación práctica sectorial	"La mayoría de los programas carecen de simulaciones prácticas y formación contextualizada por sector".	OECD (2023, pp. 23-24).
	"La formación generalista no contempla entrenamiento práctico ni por roles" (sector salud en Colombia).	Universidad Cooperativa de Colombia. (2024, s. p.).
5. Acceso y presupuesto	"Solo el 35 % de las organizaciones reporta haber incrementado su inversión en talento especializado en ciberseguridad".	WEF (2025, p. 22).
	"El acceso a certificaciones y programas internacionales está limitado por barreras de idioma, costo y conectividad".	OECD (2023, pp. 23-24).

Fuente: Elaboración propia.

Necesidades de las empresas de infraestructura crítica

A continuación, se presentan las principales necesidades de las empresas de infraestructura crítica:

1. Visión sistémica: ¿existe realmente una arquitectura formativa? La primera necesidad identificada corresponde a la ausencia de una visión sistémica en la arquitectura de formación. Muchas organizaciones abordan la capacitación como un conjunto de actividades aisladas, sin conexión con los objetivos del negocio ni con las funciones críticas. Precisamente, el World Economic Forum (2025) alerta que el 59 % de los expertos entrevistados reconoce que sus organizaciones no cuentan con un plan de desarrollo profesional en ciberseguridad alineado a los riesgos del negocio. De forma similar, el NIST CSF 2.0 establece que una organización madura debe integrar la formación como parte fundamental de su sistema de gobernanza. En este sentido, se asigna un puntaje de 6.5 a esta necesidad, lo cual refleja una presencia parcial y aún no estructural en el país, dado que, si bien existen programas formativos, estos no se configuran como un sistema con cobertura transversal ni alineación estratégica.
2. Seguimiento e integración con la matriz de riesgos: la debilidad del vínculo. Una segunda necesidad crítica es la falta de seguimiento continuo de la formación y su escasa integración con la gestión del riesgo. A pesar de que el NIST CSF 2.0 (2024, p. 16) recomienda explícitamente alinear las competencias del personal con los dominios de riesgo cibernético, muchas organizaciones en Colombia carecen de indicadores (KPI) que evalúen la efectividad del entrenamiento o de mecanismos que conecten los

programas de formación con las matrices de riesgo organizacional. Esta brecha justifica una calificación de 5.5, lo cual indica una implementación incipiente, caracterizada por algunos esfuerzos dispersos, pero sin una articulación formal ni mecanismos institucionalizados de monitoreo.

3. Identificación proactiva de brechas: ¿sabemos qué perfiles faltan? El tercer eje se relaciona con la capacidad de las organizaciones para identificar de forma proactiva las brechas de conocimiento y las habilidades por áreas funcionales clave. En su informe sobre Latinoamérica, la OCDE (2023) señaló que las evaluaciones diagnósticas por rol siguen siendo una gran ausencia en las estrategias formativas, mientras que el WEF (2025) advierte que "no se realiza un análisis de brechas basado en funciones específicas". Con base en esta evidencia, se asigna un puntaje de 6, lo cual indica que, si bien hay conciencia sobre la necesidad de mapeo de habilidades (*skill mapping*), la aplicación práctica es limitada y carece de herramientas estructuradas por función.
4. Soluciones prácticas y sectoriales: un entrenamiento genérico no basta. Otra necesidad estructural tiene que ver con la escasez de formación práctica adaptada a los sectores. En un entorno donde los riesgos varían según la industria, los programas generalistas resultan insuficientes, una realidad que confirman tanto la Universidad Cooperativa de Colombia (2024) en su análisis del sector salud, como el Centro de Ciberseguridad Industrial (CCI, 2022) respecto a entornos OT, pues ambos informes coinciden en que los programas actuales carecen de simulaciones contextualizadas y de entrenamiento realista por sector. En función de esto, se otorga un puntaje de 4.5, uno de los más bajos en el radar, lo cual refleja una brecha crítica que limita la efectividad del aprendizaje situado y reduce la preparación de los equipos ante amenazas específicas del entorno operativo.
5. Acceso y presupuesto disponible: no todas las empresas pueden formar. Finalmente, debe considerarse una necesidad transversal que afecta especialmente a empresas medianas y entidades públicas: la limitada disponibilidad presupuestal y las barreras de acceso a formación especializada. El WEF (2025) indica que solo el 35 % de las organizaciones reporta un incremento en su inversión en formación en ciberseguridad, mientras que la OCDE (2023) resalta obstáculos como el idioma, el costo y la conectividad. Con base en esta información, se asigna un puntaje de 5, lo cual representa una condición restrictiva persistente que limita la democratización del entrenamiento, especialmente en sectores clave para la seguridad nacional.

Visualizando la brecha: construcción del radar

La integración de estos cinco ejes se representa gráficamente en un radar de necesidades (figura 3), donde cada dimensión fue evaluada con una escala de 1 a 10, siguiendo criterios de traducción cualitativa de contenido (presencia, madurez, limitaciones y articulación normativa). Además del estado actual, se incluyen dos líneas adicionales: una de evolución esperada (según tendencias sectoriales) y otra de nivel ideal (marco de referencia global). Esta representación no solo permite identificar las prioridades de intervención, sino también revela cuáles dimensiones presentan mayor estancamiento relativo y, por tanto, requieren de soluciones más urgentes o innovadoras.

Codificación de indicadores cualitativos por fuente

Se realizó una lectura estructurada de informes relevantes (NIST CSF 2.0, WEF 2025, OCDE 2023, CCI 2022, entre otros) con el objetivo de identificar fragmentos textuales que aludieran al grado de implementación, a la frecuencia, a la cobertura o a la prioridad de cada necesidad en contextos empresariales. Posteriormente, estos fragmentos se categorizaron con etiquetas como:

a. Presencia alta / moderada / baja.
b. Ausencia explícita de mecanismos.
c. Limitaciones o barreras recurrentes.
d. Existencia de buenas prácticas, pero sin cobertura nacional.
e. Percepción de avance, pero sin evaluación formal.

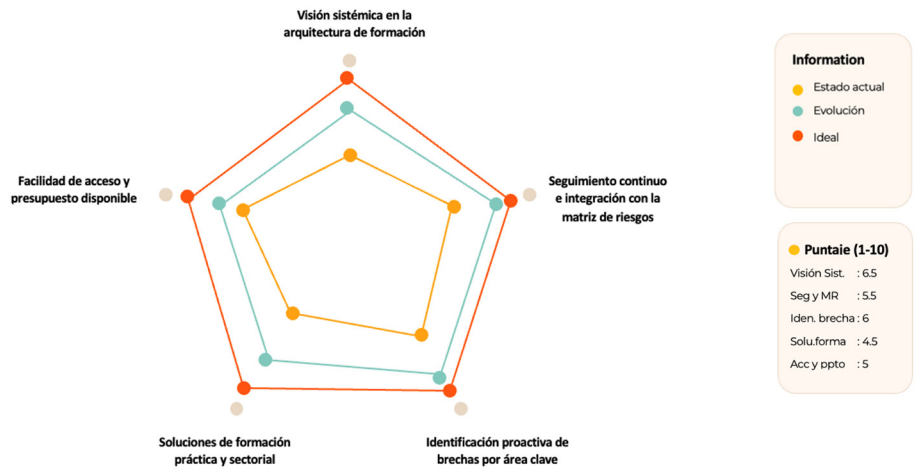
Respecto a la traducción cualitativa a escala ordinal (1-10), se debe señalar que una vez codificados los fragmentos, se aplicó un criterio de traducción cualitativa a valor numérico, como se muestra en la tabla 9.

Tabla 9. *Traducción cualitativa a escala ordinal de necesidades*

Indicador textual	Traducción en escala
"Escasa oferta", "bajo uso", "limitado acceso".	4-5
"Avance parcial" o "implementación inicial".	6-6.5
"Presencia significativa pero no estructural".	7-8
"Cobertura plena, con mecanismos formales".	9-10
"Ausencia total o crítica".	1-3

Fuente: Elaboración propia.

Figura 3. *Radar de necesidades de las empresas*



Fuente: Elaboración propia.

Desafíos estructurales para cerrar las brechas formativas

Si bien las necesidades identificadas permiten trazar un mapa claro de los aspectos que deben ser fortalecidos, su abordaje no es lineal ni está exento de obstáculos. Las empresas de infraestructura crítica enfrentan una serie de desafíos estructurales, culturales y operativos que limitan la adopción efectiva de estrategias de formación en ciberseguridad. Dichos obstáculos operan, en efecto, como barreras sistémicas que impiden pasar del diagnóstico a la acción y, por tanto, deben ser comprendidos desde una perspectiva multidimensional.

1. Fragmentación institucional y desarticulación intersectorial. Aunque existen políticas nacionales y lineamientos como el CONPES 3995 o la Estrategia Nacional de Seguridad Digital 2025-2027, la fragmentación institucional y la desarticulación intersectorial se evidencian en una aplicación sectorial dispareja. Muchas empresas no cuentan con equipos especializados o desconocen los lineamientos actuales, lo cual les impide consolidar una visión compartida sobre los estándares formativos que deberían implementar. Esta fragmentación se agrava por la falta de coordinación entre los sectores público, privado y académico, lo cual además limita la creación de rutas de formación integradas y sostenibles.
2. Limitada cultura organizacional en torno a la ciberseguridad. Según el informe del Foro Económico Mundial (WEF, 2025), solo el 37 % de los líderes

considera que su organización cuenta con el equipo adecuado para responder a incidentes cibernéticos, y más del 50 % no ha integrado la ciberseguridad en su cultura de liderazgo. Esta realidad genera un desinterés por invertir en formación continua, particularmente en los niveles directivos, que son precisamente donde se toman las decisiones críticas de inversión y gestión de riesgos.

3. Escasa articulación entre formación y roles estratégicos. A pesar del reconocimiento de marcos como NICE o NIST CSF 2.0, muchas organizaciones no mapean sus funciones críticas ni diseñan rutas formativas diferenciadas por perfil. Esta situación genera entrenamientos generalistas, sin alineación a las verdaderas necesidades del negocio, como lo señalan estudios de la OCDE (2023) y la CCI (2022). En consecuencia, se perpetúan las brechas entre lo que se enseña y lo que realmente se necesita en campo, especialmente en entornos OT/ICS.
4. Limitaciones presupuestales y falta de modelos sostenibles. De acuerdo con el WEF (2025), solo el 35 % de las empresas a nivel global reporta estar aumentando su inversión en formación de talento, y en América Latina el porcentaje es incluso menor. Este escenario plantea un gran reto para las infraestructuras críticas en Colombia, las cuales deben asumir costos operativos crecientes mientras compiten por talento con el sector financiero o tecnológico, que suelen ofrecer mejores condiciones. Además, muchas iniciativas formativas se estructuran como eventos puntuales sin continuidad ni impacto sostenido.
5. Débil monitoreo y evaluación del impacto formativo. La ausencia de indicadores (KPI) que permitan evaluar el impacto real de la formación en términos de reducción de riesgo, mejora en tiempos de respuesta o madurez organizacional, impide demostrar el retorno de la inversión. Según NIST CSF 2.0, el monitoreo de la eficacia del entrenamiento es un pilar de gobernanza, aunque en el contexto colombiano, estos mecanismos son aún incipientes o inexistentes (NIST, 2024). Esta carencia debilita la justificación técnica y financiera de programas de formación continuada.

De la comprensión al diseño: hacia un modelo marco de formación

Los hallazgos presentados en esta sección permiten evidenciar vacíos estructurales, retos comunes y patrones que requieren una respuesta transformadora. En este contexto, las necesidades identificadas, junto con los desafíos organizacionales,

ponen de manifiesto la urgencia de contar con una estrategia integral y sostenible que trascienda las intervenciones aisladas. Entre estas necesidades se destacan la falta de una arquitectura de formación sistémica, la débil integración con la matriz de riesgos o la escasa oferta práctica sectorial.

En este marco, las teorías del conocimiento y del aprendizaje analizadas cobran relevancia no solo como fundamento conceptual, sino también como guía para la acción. Enfoques como el constructivismo social, el aprendizaje experiencial y el aprendizaje situado ofrecen herramientas para diseñar soluciones formativas adaptadas al contexto real, participativas y orientadas al desarrollo de competencias. Asimismo, modelos de formación basada en roles, competencias y simulaciones, inspirados en marcos como NICE y MITRE ATT&CK, permiten construir rutas diferenciadas y efectivas según el perfil y la función dentro de la organización.

Así, este conjunto de elementos —diagnóstico, teoría y desafíos— constituye el punto de partida para la formulación del modelo C-TOET (Cyber Technology Organizational Environment Training). El modelo no surge de una recolección empírica tradicional, sino de una construcción teórico-práctica basada en una lógica deductiva que parte de las siguientes premisas fundamentales:

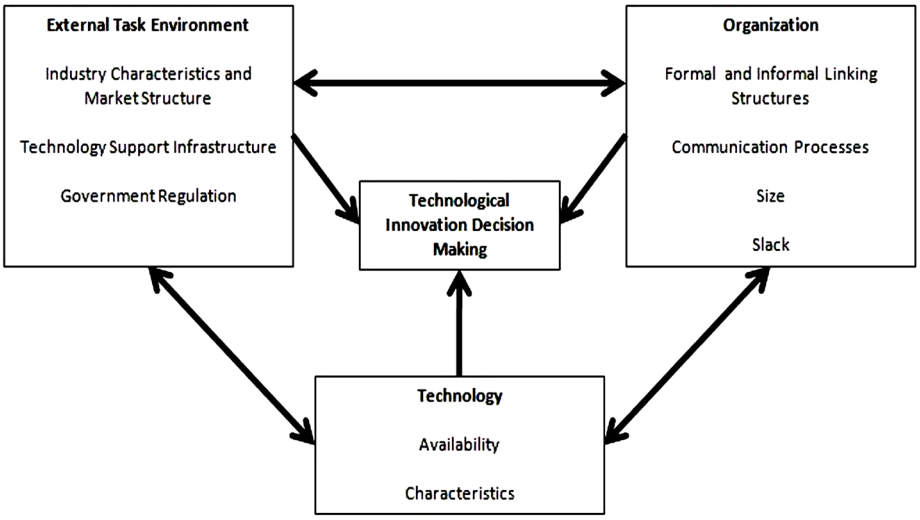
- La adopción efectiva de tecnologías formativas está condicionada por la interacción entre tres dimensiones: el entorno externo (regulación, amenazas y gobernanza), la estructura organizacional (cultura, procesos y liderazgo) y las capacidades tecnológicas (plataformas, recursos y madurez digital), tal como lo plantea el modelo TOE (Tornatzky & Fleischer, 1990).
- La formación en ciberseguridad exige enfoques activos, significativos y por competencias, capaces de generar transferencia efectiva al entorno laboral, fundamento que se halla en teorías como el aprendizaje significativo (Ausubel, 1983), el aprendizaje basado en problemas (ABP), la gamificación y las simulaciones aplicadas (Ruiz et al., 2019; Kolb, 1984).
- Las tecnologías emergentes (OCDE, 2021), aún en fase de adopción, y las tecnologías innovadoras (Rogers, 2003), ya probadas y escaladas, tienen el potencial de actuar como catalizadores del aprendizaje si se integran con intención pedagógica.
- Marcos internacionales como el NICE Framework (NIST, 2020) y ENISA, además de reportes como el Global Cybersecurity Outlook (WEF, 2025) evidencian la necesidad urgente de contar con modelos formativos adaptables y alineados con los roles críticos, las brechas del sector y los escenarios de amenaza persistente.

Con base en estas premisas se estructura el modelo propositivo, concebido como una arquitectura modular de entrenamiento en ciberseguridad que responde a la necesidad de construir capacidades en todos los niveles de una organización crítica, mediante la integración de teoría, práctica, tecnologías, normativas y experiencia del sector.

Diseño del modelo marco para la creación de programas de formación

El modelo TOE (Technology–Organization–Environment), desarrollado por Tornatzky y Fleischer (1990), ha sido uno de los marcos teóricos más utilizados para explicar los procesos de adopción tecnológica en las organizaciones (figura 4).

Figura 4. *Características del modelo TOE desarrollado por Tornatzky y Fleischer*



Fuente: Tornatzky y Fleischer (1990).

Específicamente, este modelo plantea que la decisión de adoptar una tecnología se fundamenta en tres dimensiones interrelacionadas, como se describe en la tabla 10.

Tabla 10. *Dimensiones del modelo TOE*

Dimensión	Descripción	Enfoque original
Tecnología (T)	Considera la disponibilidad, complejidad y ventajas percibidas de las tecnologías que se van a incorporar.	Determina la **capacidad técnica** de adopción.
Organización (O)	Se refiere a los recursos humanos, la cultura, la estructura y los procesos internos que facilitan o limitan el cambio.	Determina la **capacidad institucional y cultural.**
Entorno (E)	Representa los factores externos, como la regulación, el mercado o la competencia que impulsan o restringen la innovación.	Determina la **presión ambiental o contextual.**

Fuente: Elaboración propia con base en el modelo TOE.

Como se evidencia, el TOE ofrece una visión estructural del proceso de innovación tecnológica. Sin embargo, el fenómeno de la formación en ciberseguridad plantea un desafío adicional: no basta con adoptar tecnología, sino que es imprescindible integrarla en procesos de aprendizaje continuo que sean medibles y sostenibles en el tiempo. De acuerdo con lo anterior, surge el modelo Cyber–Technology–Organizational–Environment–Training (C-TOET), que adapta el enfoque TOE al campo de la adopción de tecnologías y metodologías de formación en ciberseguridad.

Concepción del modelo C-TOET

El modelo C-TOET analiza cómo las organizaciones adoptan, integran y sostienen tecnologías de formación orientadas al desarrollo de competencias en ciberseguridad. Asimismo, se enfoca en la madurez formativa, entendida como la capacidad de aprendizaje, práctica y consolidación del talento humano dentro del ecosistema cibernético. En síntesis, su propósito es explicar las condiciones internas y externas que determinan la adopción efectiva de tecnologías de entrenamiento, como plataformas de simulación, ejercicios tipo CTF, *microlearning,* gamificación o inteligencia artificial educativa, así como su traducción en cultura, práctica y desempeño organizacional.

El C-TOET amplía el TOE original al incorporar dos dimensiones transversales que son esenciales para comprender la evolución del aprendizaje organizacional en ciberseguridad: la frecuencia (Z), que representa la sostenibilidad del entrenamiento, y la madurez formativa (W), que simboliza el resultado de esa interacción dinámica.

Dimensiones

La Dimensión Organizacional (Eje X) refleja la capacidad interna de la organización para integrar la ciberseguridad como cultura y competencia institucional. Incluye tres subniveles interdependientes:

- Cultural: sensibilización, hábitos digitales y liderazgo visible.
- Estratégico: alineación entre los objetivos de negocio y las políticas de seguridad.
- Técnico: competencias operativas, roles definidos y respuesta a incidentes.

Esta dimensión, que determina la base estructural del modelo, se nutre de indicadores como la existencia de políticas formativas, planes de carrera, el respaldo de la alta dirección o métricas de participación.

Por su parte, la Dimensión Tecnológica (Eje Y) evalúa la naturaleza, la diversidad y la profundidad de las herramientas y entornos de entrenamiento utilizados. Específicamente, se estructura en un continuo que abarca desde lo teórico-informativo hasta lo experiencial-simulativo, representado por diferentes tipos de tecnologías:

1. E-learning y contenidos básicos.
2. Campañas de concientización y *microlearning*.
3. Gamificación y ejercicios tipo Capture The Flag (CTF).
4. Plataformas hiperrealistas de entrenamiento, como Cyber Range y la inteligencia artificial adaptativa.

El avance tecnológico no se mide solo por su complejidad técnica, sino también por su capacidad para generar aprendizaje significativo, analítica de desempeño y transferencia de conocimiento a la operación real.

La Dimensión de Frecuencia (Eje Z). La frecuencia representa el pulso vital del modelo, es decir, la regularidad con la que se ejecutan y repiten las acciones de formación y simulación, de manera que es el elemento que convierte el conocimiento en hábito. Su medición se basa en indicadores observables, tales como la periodicidad de las capacitaciones, la recurrencia de simulaciones o la actualización continua de contenidos. Así, una frecuencia alta refleja un aprendizaje sostenido y una cultura consolidada, mientras que una frecuencia baja indica un modelo reactivo o episódico.

El Nivel de Madurez (Eje W), por su parte, no se representa como una coordenada adicional dentro del cubo, sino como una capa topográfica de color y relieve que emerge de la interacción entre los tres ejes estructurales del sistema: la organización (X), la tecnología (Y) y la frecuencia (Z) de los procesos de formación en ciberseguridad. Mientras los ejes X, Y y Z definen el espacio tridimensional del modelo, el eje W introduce una cuarta dimensión analítica (4D): el nivel de madurez formativa alcanzado por la organización. Específicamente, esta madurez no es un valor estático, sino una manifestación visible del equilibrio y coherencia entre cultura, tecnología y práctica.

En otras palabras, el eje W simboliza la capacidad institucional para convertir la formación en competencia sostenida, lo cual implica que mide no solo cuántas acciones de entrenamiento existen, sino también su efectividad, integración y permanencia a lo largo del tiempo.

Ahora bien, en cuanto a la variable Entorno como deformador sistémico se debe precisar que el Entorno constituye la dimensión transversal que diferencia al C-TOET de otros modelos de madurez. No se representa como un eje adicional, sino como una fuerza de deformación que incide sobre los tres anteriores, lo cual altera la altura (frecuencia) y el color (madurez) de la superficie topográfica. Por lo tanto, en la visualización el entorno se manifiesta como un campo dinámico capaz de elevar, hundir o inclinar la capa de madurez en función de su intensidad. A continuación, la tabla 11 sintetiza las dimensiones del modelo C-TOET propuesto.

Tabla 11. *Dimensiones del modelo C-TOET propuesto*

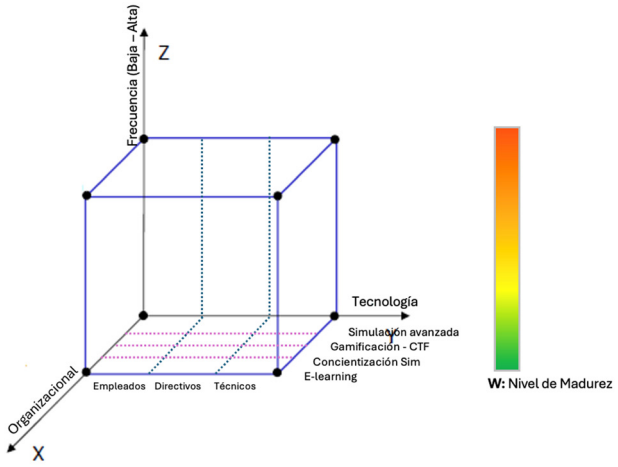
Dimensión	Símbolo	Descripción	Representación
Organizacional	X	Evalúa la cultura, la estructura y la gobernanza que soportan los procesos de formación. Mide el nivel de liderazgo y la alineación estratégica del aprendizaje en ciberseguridad.	Eje horizontal
Tecnología	Y	Representa el nivel de adopción, diversidad y profundidad de las herramientas y metodologías formativas.	Eje de profundidad
Frecuencia	Z	Mide la periodicidad y continuidad de las acciones formativas. Representa el grado de sostenibilidad del aprendizaje.	Eje vertical
Madurez formativa	W	Es el resultado emergente de la interacción entre X, Y y Z. Expresa la consolidación de competencias y hábitos cibernéticos.	Color y relieve de la superficie
Entorno	—	Actúa como un campo de gravedad que deforma el equilibrio entre las variables internas. Incluye presiones regulatorias, amenazas y exigencias del sector.	Capa superior (tensor o campo ambiental)

Fuente: Elaboración propia.

Análisis estructural del modelo: una arquitectura 4D de adopción y aprendizaje [T2]

El modelo C-TOET opera como un sistema de interacción cuatridimensional en el cual las variables organizacional (X), tecnológica (Y) y de frecuencia (Z) se combinan para generar un nivel de madurez formativa (W) (figura 5).

Figura 5. *Estructura de la arquitectura 4D del modelo C-TOET*



Fuente: Elaboración propia.

A diferencia de un enfoque lineal, el C-TOET plantea una estructura sistémica y relacional, en la cual ninguna dimensión puede analizarse de manera aislada y en la que el entorno actúa como fuerza deformadora que altera el equilibrio interno del sistema.

Interacción de dimensiones

Cada eje del modelo cumple un rol estructural que se potencia al interactuar con los demás:

- El eje organizacional (X) define la capacidad interna de la empresa para sostener la cultura formativa.
- El eje tecnológico (Y) habilita los medios y las metodologías mediante los cuales la teoría se transforma en experiencia.
- El eje de frecuencia (Z) otorga el ritmo que propicia la transformación del conocimiento en hábito.

Cuando estos tres ejes se sincronizan, emerge el eje W, el cual constituye la expresión visual de la madurez formativa. Cabe resaltar que dicha topografía no representa únicamente el estado actual, sino que es el resultado dinámico de las interacciones entre estructura, medios y práctica. Además, el eje W, concebido como un resultado emergente, representa el nivel de madurez que sintetiza el grado de equilibrio entre cultura, tecnología y sostenibilidad del aprendizaje. Por lo tanto, no es una variable independiente, sino que, más bien, se presenta como una emergencia visual y analítica que se materializa en una superficie de color y relieve

que revela la coherencia del sistema. De este modo, el eje W traduce un fenómeno intangible —el aprendizaje organizacional— en una forma medible y observable:

- Color: indica la calidad de la madurez formativa (de rojo a verde)
- Altura: refleja la frecuencia con que se ejercitan las competencias.
- Curvatura: expresa la coherencia o tensión entre las dimensiones.

En cuanto al entorno como deformador sistémico, se debe enfatizar que si bien el entorno (E) se comporta como un campo de gravedad que afecta el equilibrio del sistema, no se mide como un eje adicional, sino como una fuerza vectorial que modifica la superficie topográfica. Por lo tanto:

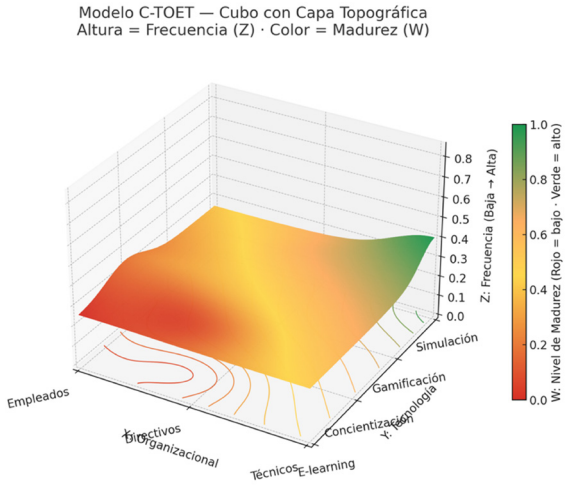
- Puede elevar zonas de alta presión regulatoria.
- Inclinar regiones de cambio tecnológico.
- Hundir sectores donde la amenaza es menor.

En esta dinámica, entonces, se dan las siguientes relaciones:

- Un entorno regulatorio o de riesgo elevado aumenta la madurez aparente, pues impulsa acciones sostenidas de formación.
- Un entorno de baja presión relaja la curva de aprendizaje, lo cual genera declives en la superficie.

Así, el C-TOET introduce la idea de una madurez no lineal, dependiente tanto de los factores internos como de las condiciones externas que la deforman (figura 6).

Figura 6. *Representación del modelo C-TOET*



Fuente: Elaboración propia.

Aplicabilidad del modelo C-TOET

El modelo C-TOET está diseñado no solo como un modelo de análisis, sino también como una metodología práctica que permite a las organizaciones diagnosticar, planificar y sostener su madurez formativa en ciberseguridad de manera estructurada y continua. Por lo tanto, su aplicabilidad consiste en un proceso reflexivo y progresivo, basado en la observación, el diálogo interfuncional y la toma de decisiones estratégica.

Propósito de la aplicación

El propósito del C-TOET es convertir el aprendizaje en un sistema organizacional vivo que sea capaz de evolucionar junto con las amenazas, la regulación y la tecnología, para lo cual ofrece una ruta que le permite a cada organización identificar los siguientes aspectos:

- Qué fuerzas del entorno la están impulsando o presionando.
- Cómo su estructura interna responde y aprende.
- Qué tecnologías habilitan y sostienen esa evolución.

El resultado no es solo una puntuación numérica, sino sobre todo un mapa de madurez narrativa que muestra el estado actual y las posibles trayectorias de avance.

Herramienta para su aplicación: Matriz de Diagnóstico C-TOET

La evaluación y la aplicación del modelo C-TOET se vuelve operativa a través de la Matriz de Diagnóstico C-TOET, una herramienta diseñada para medir y analizar el nivel de madurez formativa de la organización en las cinco dimensiones estructurales del modelo (entorno, organización, tecnología y frecuencia, y madurez). Como se presenta en detalle en el Anexo 1, la matriz incluye los bloques temáticos, objetivos, preguntas y justificaciones que permiten realizar un diagnóstico integral y reflexivo de la madurez organizacional en ciberseguridad.

Específicamente, la Matriz de Diagnóstico C-TOET constituye el instrumento operativo que traduce su arquitectura conceptual en una herramienta de diagnóstico, planificación y mejora continua. Su propósito es permitir que las organizaciones identifiquen, evalúen y fortalezcan su madurez formativa en ciberseguridad desde una perspectiva sistémica que integra factores humanos, tecnológicos y contextuales.

Más que un cuestionario, este instrumento se concibe como un dispositivo reflexivo y estratégico, pues combina la medición cuantitativa (escala tipo Likert) con la observación cualitativa (evidencias y comentarios), gracias a lo cual es posible comprender tanto el nivel de madurez actual como las causas que lo explican.

Estructura de la matriz

Como se mencionó, la Matriz de Diagnóstico C-TOET se compone de cinco dimensiones estructurales —entorno, organización, tecnología y frecuencia, y madurez—, las cuales representan las fuerzas del modelo C-TOET. Así mismo, incorpora bloques por dimensión que agrupan las variables observables, cada uno de los cuales está diseñado para explorar un aspecto esencial de la madurez formativa y se compone de tres elementos:

- Objetivo del bloque: define qué se busca comprender en esa parte de la evaluación. Es decir, permite que el usuario sitúe la intención subyacente a las preguntas y conecte el ejercicio con los ejes del modelo.
- Preguntas o ítems de medición: constituyen la evidencia práctica del modelo. Se formulan en lenguaje operativo, cercano a la realidad de la organización, y se responden en una escala tipo Likert de 1 a 5, donde 1 significa "no implementado" y 5 "plenamente implementado y sostenido en el tiempo"
- Justificación: acompaña a cada pregunta e indica por qué es importante formularla, de manera que no solo explica el sentido del ítem, sino que además orienta la interpretación del resultado. De esta manera, la justificación convierte cada pregunta en una guía de reflexión estratégica, lo cual ayuda a la organización a comprender qué implica estar en un nivel fundacional, intermedio o avanzado.

El diseño de bloques, que incorpora objetivos, preguntas y justificaciones, cumple tres propósitos clave:

1. Favorecer la comprensión integral del modelo: cada bloque conecta directamente con las variables teóricas del C-TOET, lo cual facilita la lectura transversal entre entorno, organización y tecnología.
2. Estimular la autoevaluación reflexiva: la justificación convierte cada pregunta en un punto de diálogo entre las áreas de la organización. Más que llenar un formulario, la matriz invita a revisar prácticas, identificar brechas y descubrir oportunidades.
3. Fortalecer la trazabilidad y la evidencia: al acompañar cada respuesta con su justificación y evidencia documental, la matriz proporciona información verificable. Esta característica la hace útil tanto para procesos de auditoría interna como para seguimiento estratégico.

Proceso de uso y aplicación de la Matriz de Diagnóstico C-TOET

La aplicación de la Matriz de Diagnóstico C-TOET combina el análisis cuantitativo de resultados con la interpretación cualitativa de evidencias. En particular, este proceso busca garantizar que la herramienta no se limite a la medición, sino que se convierta en un instrumento de aprendizaje organizacional y una guía para la toma de decisiones estratégicas en materia de ciberseguridad. A continuación, se describe el paso a paso de la aplicación:

1. Planeación y preparación de la evaluación

El primer paso consiste en definir el alcance y los actores involucrados. La matriz debe ser aplicada de forma transversal, involucrando las áreas responsables de tecnología, gestión del talento humano, riesgos, cumplimiento y liderazgo directivo. Durante esta fase se identifican los responsables de proveer la información, se explican los objetivos del modelo y se establecen los criterios de evidencia documental que acompañarán las respuestas. Asimismo, se recomienda realizar una sesión inicial de socialización con los equipos, en la cual se exponga la estructura del modelo C-TOET, su escala de valoración y los beneficios del diagnóstico. Cabe enfatizar que esta prepara a los participantes para una evaluación más consciente y alineada con la realidad institucional.

2. Recolección de información y diligenciamiento

Cada bloque de la matriz se aborda siguiendo su orden temático: entorno, organización, tecnología, frecuencia y madurez. Específicamente, los responsables deben revisar las preguntas o ítems de cada bloque y asignar un valor en la escala tipo Likert de 1 a 5, de acuerdo con el grado de implementación observado. Simultáneamente, se debe adjuntar evidencia que respalde cada valoración, como documentos, registros, políticas, reportes o ejemplos de actividades formativas. Este enfoque dual, numérico y documental permite garantizar la trazabilidad del diagnóstico y la credibilidad de los resultados. En esta fase, la matriz puede aplicarse:

- De manera individual, por cada área o segmento de la organización.
- De forma colectiva, mediante talleres o sesiones de autoevaluación guiadas. Esta modalidad es la más recomendable, puesto que promueve la reflexión y el diálogo interdepartamental, los cuales constituyen principios esenciales del modelo C-TOET.

3. Consolidación y análisis de resultados

Una vez completado el diligenciamiento, los valores obtenidos se promedian por bloque y por dimensión, lo cual genera tres tipos de resultados:

- Promedio por bloque: identifica fortalezas y brechas en variables específicas (por ejemplo, gobernanza, cooperación sectorial o infraestructura).
- Promedio por dimensión: resume el nivel de madurez del entorno, la organización y la tecnología.
- Promedio global: refleja la madurez formativa total de la organización.

Posteriormente, los resultados se clasifican en tres niveles de desarrollo:

- Fundacional (1,0–2,4): procesos incipientes, formación reactiva o fragmentada.
- Intermedio (2,5–3,4): prácticas definidas, pero sin integración plena ni evaluación sistemática.
- Avanzado (3,5–5,0): cultura consolidada, aprendizaje continuo y tecnología integrada a la estrategia.

No obstante, el análisis no se limita a los valores numéricos, sino que exige la interpretación de la coherencia entre las dimensiones. Por ejemplo, una organización madura presentará promedios equilibrados, mientras que diferencias marcadas entre ellas indicarán desequilibrio sistémico o dependencia excesiva de uno de los componentes del modelo.

4. Visualización mediante la dimensión de frecuencia y madurez formativa

La etapa de visualización de resultados se desarrolla a partir de la dimensión frecuencia y madurez formativa, que permite integrar los hallazgos en las tres dimensiones principales del modelo (entorno, organización y tecnología). Esta dimensión combina los niveles de aplicación (frecuencia) y de consolidación (madurez) de las metodologías tecnológicas utilizadas en la formación y se representa a través de una matriz cruzada que relaciona los segmentos organizacionales con los tipos de metodologías o tecnologías formativas.

La tabla 12 ilustra el tipo de información que se obtiene de este cruce: en ella, cada celda representa la valoración Likert (1 a 5) correspondiente al grado de aplicación de una metodología en un grupo específico, donde:

1 indica una práctica inexistente o incipiente.

3 refleja una aplicación ocasional o intermitente.

5 representa una aplicación que se distingue por ser continua, institucionalizada y madura.

Tabla 12. *Visualización de la dimensión de frecuencia y madurez formativa*

Tipo de metodología formativa	Empleados	Directivos	Técnicos
E-learning	1	1	1
Concientización	3	3	5
Gamificación	4	1	1
Simulación	1	2	5

Fuente: Elaboración propia.

La lectura conjunta de esta matriz permite observar la distribución de la madurez formativa en toda la organización, pues los valores se representan luego en un gráfico topográfico en el que:

- El eje X corresponde a los tipos de formación (tecnologías o metodologías).
- El eje Y representa los segmentos organizacionales (empleados, directivos y técnicos).
- El eje Z muestra el nivel de madurez o la frecuencia que se ha alcanzado.

Así, la superficie del gráfico refleja la intensidad, el equilibrio y la coherencia en la aplicación de las tecnologías formativas a lo largo de los distintos niveles organizacionales. Los picos o elevaciones señalan áreas de alto desarrollo o metodologías institucionalizadas, como, por ejemplo, simulaciones o campañas de concientización dirigidas al equipo técnico. En contraste, los valles o zonas planas evidencian prácticas aisladas, de baja frecuencia o con ausencia de integración transversal, tales como el *E-learning* para empleados y directivos.

Esta representación visual complementa la Matriz de Diagnóstico C-TOET, lo cual permite una interpretación sistémica del aprendizaje organizacional, pues gracias a la combinación de los ejes de frecuencia y madurez, la organización puede identificar dónde se concentran sus esfuerzos formativos, qué segmentos están menos expuestos a metodologías activas y cuán alineadas están las prácticas con las demandas del entorno. Además, el gráfico de radar permite visualizar la interacción práctica entre los ejes de la dimensión de frecuencia y madurez formativa del modelo C-TOET conectando directamente los elementos más observables de cada una de sus dimensiones estructurales. Finalmente, la tabla 13 complementa la interpretación del radar detallando la correspondencia entre las metodologías tecnológicas de formación (*E-learning,* concientización, gamificación y simulación) y los segmentos organizacionales que participan en ellas.

Tabla 13. *Herramienta de interacción entre las dimensiones radar del modelo C-TOET*

Dimensión	**Organización**		
Tecnología	**Empleados**	**Directivos**	**Técnicos**
***E-learning* / cursos virtuales**	¿Se realizan cursos virtuales o tienen plataforma de *E-learning* para formar a los empleados sobre ciberseguridad?	¿Se ofrecen módulos virtuales específicos para directivos (por ejemplo, sobre gestión del riesgo o toma de decisiones)?	¿El equipo técnico recibe formación virtual orientada a actualizaciones normativas o certificaciones técnicas?
Concientización / campañas o *microlearning*	¿Se implementan campañas de concientización para empleados sobre prácticas seguras (campañas de *phishing,* contraseñas, redes, *endomarketing*)?	¿Los directivos participan en sesiones de concientización enfocadas en responsabilidad y liderazgo en ciberseguridad?	¿El personal técnico recibe contenidos de concientización relacionados con cumplimiento normativo y reporte de incidentes?
Gamificación / competencias y retos (CTF y simulaciones lúdicas)	¿Se promueven actividades de gamificación o retos prácticos (por ejemplo: *paintball* de equipos de ciber, talleres presenciales, etc.) entre los empleados?	¿Existen ejercicios de gamificación para directivos (por ejemplo, desafíos de toma de decisiones o gestión de crisis)?	¿El equipo técnico participa en competencias CTF o entornos gamificados para fortalecer habilidades prácticas?
Simulación / ejercicios prácticos o crisis controladas	¿Se realizan ejercicios de simulación de *phishing,* dominios ficticios, *smishing,* entre otros, como campañas de ataque para los empleados?	¿Se han desarrollado simulaciones de crisis ejecutivos 360 y ejercicios "tabletop" para directivos?	¿Se realizan ejercicios de simulación técnica para los empleados (por ejemplo, laboratorios, simulaciones de ataque tipo *ransomware,* talleres de simulación de crisis)?

Fuente: Elaboración propia.

Cada celda plantea una pregunta orientadora que invita al evaluador a valorar, mediante una escala tipo Likert de 1 a 5, el nivel de implementación y madurez alcanzado en cada combinación específica (tabla 14).

Tabla 14. *Escala tipo Likert 1-5 de las dimensión aplicación y frecuencia*

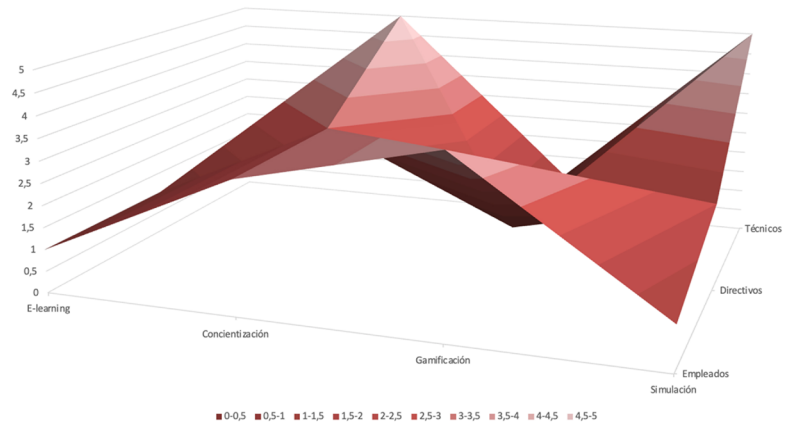
Valor	**Descripción**	**Interpretación cualitativa**
1 – No se ha realizado	La metodología **no se aplica** a este segmento o no existe registro de actividades formativas.	Ausencia total o desconocimiento.
2 – Se ha realizado de forma puntual	Se han llevado a cabo **acciones aisladas o pilotos** sin continuidad.	Iniciativas esporádicas, no sistemáticas.
3 – Se aplica ocasionalmente	La metodología se utiliza **una o dos veces al año,** sin un plan formal de seguimiento.	Uso intermitente, aún dependiente de factores externos (presupuesto, requerimientos o auditorías).

Valor	Descripción	Interpretación cualitativa
4 – Se aplica de manera regular	La metodología se implementa **con planificación semestral o trimestral,** con registro y seguimiento básico.	Práctica institucionalizada, pero sin evaluación sistemática de impacto.
5 – Se aplica de forma continua y madura	La metodología está **plenamente integrada** al plan formativo institucional y adaptada al rol o segmento.	Práctica sostenida, con monitoreo, mejora continua y retroalimentación.

Fuente: Elaboración propia.

Esta estructura permite reconocer no solo si una práctica existe, sino también con qué frecuencia y profundidad se ejecuta. Así, los resultados ofrecen una visión del aprendizaje en la organización. Ahora bien, como se ha indicado, los valores resultantes se pueden representar en el gráfico de radar o en un mapa topográfico, en el cual las áreas más amplias o elevadas reflejan mayor integración tecnológica y madurez formativa, mientras que las zonas más bajas evidencian brechas de aplicación o baja frecuencia.

Figura 7. *Gráfico de radar de la dimensión frecuencia y madurez formativa*



	Empleados	Directivos	Técnicos
E-learning	1	1	1
Concientización	3	3	5
Gamificación	4	1	1
Simulación	1	2	5

Fuente: Elaboración propia.

Para construir el gráfico topográfico del modelo C-TOET, se partió de la información recopilada en la tabla de interacción entre segmentos organizacionales y tipos de tecnologías de formación. Como se ha insistido, dicha información permite valorar el nivel de implementación y madurez de las metodologías tecnológicas empleadas en los procesos de capacitación en ciberseguridad, pues estas valoraciones reflejan tanto la presencia como la frecuencia y madurez de uso de cada metodología en los distintos niveles de la organización. En el ejemplo presentado, las calificaciones de referencia, las cuales se muestran en la tabla que aparece en la parte inferior de la figura 7, fueron las siguientes:

- *E-learning:* baja aplicación general (valor 1 en los tres segmentos), lo cual evidencia que hay escasa integración de plataformas virtuales formales.
- Concientización: aplicación intermedia (3 en empleados y directivos, 5 en técnicos), lo cual muestra un esfuerzo continuo por sensibilizar al personal técnico, aunque con menor énfasis en otros grupos.
- Gamificación: nivel alto en empleados (4) y bajo en directivos y técnicos (1), lo cual señala que existen prácticas puntuales con potencial de expansión.
- Simulación: madurez alta en técnicos (5), intermedia en directivos (2) y baja en empleados (1), lo que indica una especialización avanzada pero no transversalizada.

La superficie resultante evidencia diferencias significativas en la aplicación tecnológica entre segmentos, las cuales se manifiestan en picos pronunciados en la formación técnica, especialmente en concientización y simulación, así como en valles en los espacios donde la formación es menos frecuente o no está institucionalizada, como el *E-learning* para empleados y directivos. Además, esta superficie describe una concentración de madurez en los segmentos técnicos, especialmente en las metodologías de concientización y simulación, lo cual refleja que la organización ha orientado sus esfuerzos formativos hacia la respuesta operativa y la especialización técnica.

Este comportamiento es coherente con las demandas del entorno, donde las regulaciones, los incidentes y las tendencias del mercado presionan para fortalecer las capacidades tácticas del personal que enfrenta directamente los riesgos cibernéticos. Sin embargo, la presencia de valles o zonas planas en la formación de empleados y directivos revela una brecha estructural en la cultura de seguridad organizacional, particularmente en metodologías como el *E-learning* o la gamificación. Es decir, mientras los equipos técnicos avanzan en competencias

específicas, los demás segmentos mantienen niveles de participación más bajos o intermitentes, situación que puede limitar la sostenibilidad de la estrategia global de ciberseguridad.

En términos de gestión, este resultado sugiere que la empresa se encuentra en una etapa de madurez intermedia: ha logrado consolidar el componente tecnológico del modelo, pero aún requiere ampliar la cobertura cultural y estratégica. Desde la perspectiva del modelo C-TOET, esta asimetría refleja una desalineación parcial entre las dimensiones de entorno, organización y tecnología: el entorno impulsa exigencias normativas y técnicas (ISO, NIST, ENS), que la empresa traduce eficazmente en prácticas de entrenamiento técnico. La organización, sin embargo, no ha institucionalizado del todo la formación como práctica transversal, lo cual se traduce en baja frecuencia en los niveles directivo y operativo general. Es decir, la tecnología actúa como habilitador focalizado, pero no como un sistema integral de aprendizaje.

En consecuencia, la empresa evidencia la necesidad de evolucionar desde un enfoque reactivo y especializado hacia un modelo cultural y sostenible, de tal manera que la ciberseguridad se incorpore en todos los niveles de decisión y desempeño. Esto implica, por un lado, fortalecer la dimensión organizacional del C-TOET, con especial atención al liderazgo, la gobernanza y la cultura. Por otro lado, también supone ampliar el uso estratégico de las tecnologías de formación, con el fin de alcanzar un equilibrio maduro entre técnica, gestión y conciencia institucional.

5. Interpretación estratégica y uso de los resultados

La interpretación de los resultados de la dimensión de frecuencia y madurez formativa constituye la fase analítica y estratégica del proceso de aplicación del modelo C-TOET. En esta etapa, la organización no solo observa valores o gráficos, sino que traduce los hallazgos visuales en conocimiento accionable, lo cual le permite identificar las causas estructurales que explican las diferencias entre segmentos, metodologías y niveles de madurez. Específicamente, el análisis se debe centrar en tres niveles complementarios:

1. Nivel micro – análisis operativo: se revisan los valores individuales de la matriz para identificar metodologías subutilizadas o ausentes en ciertos segmentos. Por ejemplo, un valor bajo en *E-learning* para empleados y directivos evidencia la necesidad de fortalecer la accesibilidad a contenidos formativos y crear rutas básicas de aprendizaje digital. De manera similar, una alta valoración en Simulación para técnicos indica una madurez focalizada, pero también subraya la necesidad de transferir ese aprendizaje práctico hacia otros grupos.

2. Nivel meso – coherencia organizacional: se comparan los resultados entre segmentos y metodologías para identificar simetrías o desequilibrios. Una superficie topográfica equilibrada refleja coherencia formativa y madurez institucional, en tanto que las áreas con valles pronunciados señalan brechas culturales o estructurales en la gestión del conocimiento. Estas asimetrías suelen derivarse de la falta de alineación entre la estrategia de capacitación, la priorización de recursos y la comprensión de los riesgos cibernéticos en cada nivel jerárquico.
3. Nivel macro – lectura sistémica y contextual: finalmente, los resultados se contrastan con las exigencias del entorno (regulación, normativas, tendencias y amenazas). Por ejemplo, un patrón de concentración en lo técnico puede evidenciar una organización que responde reactivamente a la presión del entorno, pero que todavía no logra integrar la ciberseguridad como un componente transversal de su cultura. En cambio, una distribución homogénea y sostenida de valores altos en todos los segmentos indica un ecosistema organizacional alineado, resiliente y adaptativo, capaz de anticipar y aprender del cambio.

La interpretación estratégica convierte así la visualización de datos en una hoja de ruta para la mejora continua, cuyos resultados orientan la formulación de un plan de acción institucional que debe incluir:

1. Fortalecimiento de metodologías con baja frecuencia o alcance limitado.
2. Ampliación de la cobertura formativa hacia segmentos subatendidos, tales como líderes o empleados.
3. Incorporación de métricas de impacto y seguimiento continuo.
4. Integración de la formación en ciberseguridad dentro de la estrategia general de gestión del talento y del riesgo organizacional.

En conjunto, este punto permite que el modelo C-TOET trascienda el diagnóstico y se convierta en un sistema de gobernanza formativa en el cual la organización analiza, prioriza y mejora continuamente su capacidad de aprendizaje. De esta manera, la lectura visual de la madurez formativa, cuando se interpreta bajo los principios del modelo, se convierte en un instrumento estratégico para la toma de decisiones, capaz de guiar la inversión, la planeación y la evolución cultural hacia una ciberseguridad sostenible.

6. Retroalimentación y evolución continua del modelo

La última etapa del proceso corresponde a la retroalimentación y evolución continua, principio esencial del modelo C-TOET. En particular, esta fase asegura que la aplicación de la herramienta no se limite a un diagnóstico estático, sino que se transforme en un mecanismo dinámico de aprendizaje organizacional y de mejora permanente. Con este propósito, los resultados —tanto los de la matriz como los de las visualizaciones de frecuencia y madurez— deben ser integrados a los procesos institucionales de planeación, gestión del talento, evaluación de riesgos y estrategia tecnológica, de tal forma que cada ciclo de aplicación alimenta un nuevo nivel de madurez, lo cual genera un proceso iterativo en el que la organización aprende, ajusta y se adapta a las condiciones cambiantes del entorno digital.

Ahora bien, la retroalimentación debe realizarse en tres planos complementarios:

1. Retroalimentación táctica (operativa): los equipos responsables de formación y ciberseguridad revisan los hallazgos para ajustar programas, contenidos y metodologías, priorizando las áreas con menor madurez o baja frecuencia. Esta revisión conlleva, por tanto, la actualización de los calendarios de formación, la incorporación de nuevas herramientas tecnológicas o el diseño de actividades específicas para segmentos que requieren mayor cobertura.
2. Retroalimentación estratégica (institucional): los resultados agregados se presentan a la alta dirección y a los comités de riesgo o seguridad, con el fin de vincular la madurez formativa con los objetivos corporativos. Esta conexión asegura que la formación deje de ser un esfuerzo aislado y se convierta en una política transversal de desarrollo organizacional que apoye la cultura de seguridad y la sostenibilidad digital.
3. Retroalimentación contextual (entorno): el modelo invita a comparar los avances internos con las tendencias y regulaciones externas, lo cual permite anticipar nuevos requerimientos del entorno —como actualizaciones normativas o cambios en el panorama de amenazas— y ajustar los programas de formación antes de que las brechas se amplíen. De este modo, la organización no solo reacciona al entorno, sino que evoluciona junto a él.

La periodicidad de aplicación recomendada es anual o semestral, con el propósito de que la Matriz de Diagnóstico C-TOET funcione como un termómetro continuo de madurez formativa. Además, cada nueva medición debe comparar los resultados con períodos anteriores, lo cual genera líneas de tendencia que reflejan

el progreso institucional y la efectividad de las acciones implementadas. El valor agregado de este ciclo reside en que la herramienta retroalimenta su propio modelo, puesto que los resultados cuantitativos fortalecen la dimensión tecnológica, los aprendizajes cualitativos nutren la dimensión organizacional y las adaptaciones frente al contexto enriquecen la dimensión del entorno. Así, el C-TOET opera como un sistema vivo, donde cada aplicación impulsa una nueva iteración del aprendizaje corporativo.

Validación empírica y proyección de aplicación del modelo

El modelo marco de formación en ciberseguridad propuesto busca fortalecer las competencias del talento humano en empresas de infraestructura crítica, con el fin de promover una cultura de seguridad que consolide el denominado *"firewall* humano".

Como fase inicial de validación empírica, se plantea la aplicación piloto del modelo en una organización cliente de la maestrante, la cual pertenece al sector de infraestructura crítica nacional. El propósito de esta iniciativa es evaluar la pertinencia, la aplicabilidad y la percepción de la efectividad del modelo en un entorno real. Cabe señalar, sin embargo, que si bien esta aproximación permitirá observar resultados medibles en diversos aspectos, entre los cuales destacan el nivel de conocimiento, la adopción de buenas prácticas y la madurez en la cultura de ciberseguridad, se recomienda que en etapas posteriores el modelo sea ampliado y validado en otras organizaciones de infraestructura crítica con el propósito de contrastar los resultados y verificar su escalabilidad.

Este proceso de validación progresiva se alinea con los objetivos de la Estrategia Nacional de Seguridad Digital de Colombia 2025-2027, particularmente en las líneas orientadas a mejorar la ciberresiliencia nacional y a desarrollar la fuerza laboral de seguridad digital. Asimismo, se vincula con los principios del NIST Cybersecurity Framework 2.0, el cual promueve la gestión adaptativa de riesgos.

Conclusiones

El desarrollo del modelo marco de formación en ciberseguridad para las empresas de infraestructura crítica de Colombia permitió comprobar que la sostenibilidad de la ciberresiliencia empresarial depende directamente de la integración armónica entre las tres dimensiones fundamentales: entorno, tecnológica y organizacional.

Consideradas dentro del modelo C-TOET (Cyber–Technology–Organization–Environment Training Framework) y junto con las dimensiones de frecuencia y

madurez, estas dimensiones configuran una arquitectura sistémica que vincula la adopción tecnológica, la cultura organizacional y las presiones del entorno en un mismo proceso formativo, flexible y evolutivo. Además, el modelo propuesto articula dichas dimensiones a través de una arquitectura de aprendizaje adaptable, sustentada en tecnologías emergentes y metodologías activas, que permiten diseñar programas de formación coherentes con el contexto, el riesgo y la madurez de cada organización.

Por otra parte, este enfoque confirma que la formación en ciberseguridad debe ser entendida como un sistema vivo dentro de la gestión del riesgo organizacional, y no como un conjunto aislado de cursos o actividades puntuales. Consecuentemente, al integrar las metodologías de aprendizaje, las tecnologías y las competencias organizacionales, el modelo establece una correspondencia directa entre los roles de los colaboradores y los objetivos estratégicos de la seguridad digital. De esta manera, se garantiza que haya coherencia entre el entrenamiento técnico, la cultura de seguridad y la continuidad del negocio, lo cual consolida la formación como un eje estratégico de la resiliencia corporativa.

Con este propósito, la Matriz de Diagnóstico C-TOET, desarrollada como instrumento operativo del modelo, traduce estos principios en una herramienta de análisis y mejora continua. A través de sus bloques temáticos, objetivos y justificaciones, la matriz permite a las organizaciones identificar su nivel de madurez formativa, detectar brechas y construir planes de evolución basados en evidencia. Su estructura flexible integra tanto indicadores cuantitativos (valoración en escala tipo Likert) como cualitativos (observación y evidencia documental), lo cual transforma la medición en un proceso reflexivo y colaborativo.

En este contexto, la incorporación de la dimensión de frecuencia y madurez formativa, junto con su representación gráfica tridimensional, aporta una lectura visual y estratégica del aprendizaje organizacional. En particular, el mapa topográfico del modelo C-TOET revela cómo las metodologías formativas se distribuyen entre los distintos segmentos de la organización, lo cual permite identificar las zonas de mayor desarrollo o las brechas en cobertura y continuidad: las superficies elevadas indican madurez institucional y aplicación sostenida, mientras que las zonas planas reflejan la necesidad de fortalecer la transversalidad y la gobernanza de la formación.

En el contexto colombiano, el modelo demuestra que las empresas de infraestructura crítica requieren una gobernanza formativa compartida entre el Estado, la academia y el sector privado, la cual debe asegurar la actualización permanente de los contenidos frente al cambiante panorama de amenazas. Este principio de coevolución institucional se alinea con la Estrategia Nacional de Seguridad Digital

2025-2027, que promueve el fortalecimiento de las capacidades humanas y tecnológicas mediante alianzas multisectoriales y programas de formación sostenibles.

Asimismo, la incorporación de tecnologías emergentes, como la inteligencia artificial para la analítica de desempeño, la realidad aumentada para simulaciones y los entornos inmersivos tipo Cyber Range, reafirma que la tecnología no solo mejora la eficiencia del aprendizaje, sino que personaliza y contextualiza la formación, lo cual optimiza recursos y fortalece competencias críticas. De igual forma, este enfoque potencia el desarrollo de un "*firewall* humano", donde el conocimiento, la conciencia situacional y la responsabilidad digital de cada colaborador actúan como la primera línea de defensa ante incidentes.

El modelo también confirma la relevancia de las metodologías activas, como el aprendizaje basado en problemas (ABP), la gamificación y las simulaciones prácticas (Capture The Flag, ejercicios de crisis e ingeniería social), las cuales favorecen el pensamiento crítico, la resiliencia y la colaboración. De este modo, dichos enfoques transforman la formación en una experiencia inmersiva y significativa que fortalece tanto las capacidades técnicas como las habilidades blandas necesarias para gestionar la seguridad en entornos de alta complejidad.

Finalmente, el modelo C-TOET demuestra ser replicable y escalable, pues su estructura modular permite implementarlo en diferentes niveles de madurez organizacional, lo que facilita la adaptación de sus componentes a las necesidades de empresas de distinto tamaño o sector. Al integrar competencias técnicas (protección, detección y respuesta) con *power skills* (liderazgo, comunicación, pensamiento crítico y resiliencia emocional), el modelo trasciende la formación técnica para convertirse en un marco integral de transformación cultural.

Se concluye entonces que el modelo C-TOET no solo responde la pregunta de investigación, sino que además ofrece a las organizaciones un marco de referencia metodológico y evolutivo para diseñar, evaluar y sostener sus programas de formación en ciberseguridad. Así, más que un instrumento de medición, el C-TOET se consolida como una estrategia de madurez y gobernanza del aprendizaje, alineada con las exigencias del entorno y capaz de fortalecer la sostenibilidad, la resiliencia y la cultura digital de las organizaciones.

Referencias

Burn, J., Blankenship, J., Born, F., & Belden, M. (2023, 12 de diciembre). The cybersecurity skills and training platforms landscape, Q4 2023. https://www.forrester.com/report/the-forrester-wave-tm-cybersecurity-skills-and-training-platforms-q4-2023/RES178480

Cyber4Dev. (2024). *Creating a career path in cybersecurity program (2017-2024).* OAS; CICTE.. https://www.oas.org/ext/DesktopModules/MVC/OASDnnModules/Views/Item/Download.aspx?type=1&id=1173&lang=1

European Union Agency for Cybersecurity [ENISA]. (2022). *European cybersecurity skills framework (ECSF).* ENISA. https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf

Foro Económico Mundial. (2024). *Global cybersecurity outlook 2025.* WEF. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

Foro Económico Mundial. (2025). *Future of jobs report 2025.* WEF.

Fortinet. (2025). G*lobal Threat landscape report.* Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-landscape-report-2025.pdf

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación.* MacGrawHill.

Kolb, D. A. (1984). *Experiential learning: Experience as the source of learning development.* Prentice Hall.

Ministerio de las Tecnologías de la Información y las Comunicaciones [MinTic] . (2025). *Estrategia nacional de seguridad digital de Colombia 2025–2027.* https://www.mintic.gov.co/portal/715/articles-403023_recurso_2.pdf

National Initiative for Cyber Security Education [NICE]. (2020). Cybersecurity workforce framework. https://niccs.cisa.gov/tools/nice-framework

National Institute of Standards and Technology [NIST]. (2023). *Framework for improving critical infrastructure cybersecurity.* NIST. https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology [NIST]. (2024). *The NIST Cybersecurity Framework (CSF) 2.0.* NIST. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Organisation for Economic Co-operation and Development [OECD]. (2023). *Building a skilled cybersecurity workforce in Latin America.* OECD. https://doi.org/10.1787/9400ab5c-en

Restrepo Gómez. (2005). *Aprendizaje basado en problemas (ABP). Educación y Educadores, 8*, 9–19. https://www.redalyc.org/pdf/834/83400803.pdf

Universidad Cooperativa de Colombia. (2024). *Guía de buenas prácticas de ciberseguridad en salud* [Tesis de pregrado, Universidad Cooperativa de Colombia]. Repositorio UCC. https://repository.ucc.edu.co/server/api/core/bitstreams/faa7b57e-4268-4c5a-839e-4f4185a3ebf5/content

Anexo 1. Matriz de Diagnóstico del Modelo C-TOET

(Instrumento de aplicación del modelo Cyber Technology–Organization–Environment Training Framework)

La matriz que se presenta en la tabla A1 corresponde al instrumento metodológico de aplicación del modelo C-TOET. Está compuesta por tres dimensiones principales (entorno, organización y tecnología), divididas en doce bloques y acompañadas por preguntas específicas con su respectiva justificación. El objetivo del instrumento es facilitar el diagnóstico y la planificación del desarrollo formativo en ciberseguridad, de tal manera que permita identificar brechas, buenas prácticas y oportunidades de mejora dentro de las organizaciones. De esta forma, la matriz puede ser utilizada de manera autoaplicada por las organizaciones o como base para procesos de acompañamiento y evaluación institucional.

Tabla A1. *Matriz de diagnóstico del Modelo C-TOET*

Ficha técnica del instrumento C-TOET	
Nombre:	Matriz de Diagnóstico del Modelo C-TOET.
Tipo de instrumento:	Herramienta de medición y reflexión estratégica.
Objetivo:	Evaluar la madurez formativa en ci-berseguridad según las dimensiones entorno, organización y tecnología.
Escala:	Likert 1–5 (1 = No implementado, 5 = Totalmente implementado).
Periodicidad recomendada:	Aplicación anual o semestral.
Resultados esperados:	Identificación de brechas, nivel de madurez y recomen-daciones de me-jora.

Matriz de Diagnóstico del Modelo C-TOET							
Dimensión	**Bloque**	**Objetivo**	**Nº**	**Pregunta**	**Justifi-cación**	**Respuesta (escala tipo Likert 1-5)**	**Promedio**
Entorno	**Bloque 1. Cumpli-miento y alineación normativa**	Evalúa el grado de cumplimien-to de marcos regulatorios, normativos y estándares del sector.	**1**	La organización cumple con las regulaciones nacionales e internacionales relacionadas con ciberseguridad.	Evalúa confor-midad y respon-sabilidad básica.		

Matriz de Diagnóstico del Modelo C-TOET

Dimensión	Bloque	Objetivo	Nº	Pregunta	Justificación	Respuesta (escala tipo Likert 1-5)	Promedio
Entorno	**Bloque 1. Cumplimiento y alineación normativa**	Evalúa el grado de cumplimiento de marcos regulatorios, normativos y estándares del sector.	**2**	La formación en ciberseguridad está alineada a marcos de referencia (ISO 27001, NIST CSF, ENS, NIS2, etc.).	Mide integración normativa en la formación.		
			3	Existen mecanismos para actualizar los programas formativos ante cambios regulatorios.	Indica capacidad de adaptación.		
			4	La organización audita o revisa periódicamente el cumplimiento de estas normas.	Evalúa sostenibilidad del cumplimiento.		
	Bloque 2. Participación en el ecosistema sectorial y redes de cooperación	Analiza la interacción de la organización con actores externos que fortalecen la ciberresiliencia colectiva.	**5**	La organización participa en redes, asociaciones o foros sectoriales sobre ciberseguridad.	Mide colaboración y aprendizaje interorganizacional.		
			6	Se realizan alianzas con otras entidades, proveedores o universidades para compartir buenas prácticas.	Evalúa cooperación estratégica.		
			7	Se promueven ejercicios conjuntos (simulaciones, ejercicios de crisis o *ciber-drills)* con otros actores.	Mide compromiso con la respuesta coordinada.		
			8	Se mantiene una relación activa con autoridades o reguladores del sector.	Indica alineación institucional y visibilidad.		

Matriz de Diagnóstico del Modelo C-TOET							
Dimensión	**Bloque**	**Objetivo**	**Nº**	**Pregunta**	**Justificación**	**Respuesta (escala tipo Likert 1-5)**	**Promedio**
Entorno	**Bloque 3. Monitoreo del entorno y análi-sis prospectivo**	Evalúa la capacidad de la organización para observar tendencias, anticipar riesgos y traducirlos en acción.	**9**	Se monitorean regularmente tendencias y amenazas emergentes en ciberseguridad.	Indica inteligencia contextual.		
			10	La organización analiza cómo los cambios del entorno (tecnológicos, sociales, regulatorios) impactan su estrategia de formación.	Evalúa pensamiento prospectivo.		
			11	Se elaboran informes o reportes de entorno que alimentan la toma de decisiones formativas.	Mide institucionalización del aprendizaje externo.		
			12	Existe un proceso formal de priorización de riesgos y tendencias detectadas en el entorno.	Indica madurez analítica.		
	Bloque 4. Reacción y capacidad de adaptación	Mide la rapidez y efectividad con que la organización responde a nuevos requerimientos externos o crisis.	**13**	Ante cambios regulatorios o incidentes sectoriales, la organización ajusta rápidamente su formación o políticas internas.	Mide agilidad de respuesta.		
			14	Se dispone de protocolos o planes de contingencia que contemplan formación inmediata ante eventos críticos.	Evalúa preparación reactiva y aprendizaje en crisis.		
			15	La organización aprende de incidentes propios o ajenos, actualizando sus procesos formativos.	Indica madurez adaptativa.		

Matriz de Diagnóstico del Modelo C-TOET							
Dimensión	**Bloque**	**Objetivo**	**Nº**	**Pregunta**	**Justificación**	**Respuesta (escala tipo Likert 1-5)**	**Promedio**
Organización	**Bloque 1. Gobernanza y liderazgo de la formación**	Evalúa el compromiso, la estructura formal y la alineación estratégica de la formación en ciberseguridad	**16**	Existe una política institucional que regula la formación continua en ciberseguridad.	Indica formalización del proceso.		
			17	La alta dirección respalda activamente la estrategia de formación.	Mide patrocinio y liderazgo ejecutivo.		
			18	La formación en ciberseguridad está alineada a los riesgos corporativos y a los objetivos estratégicos.	Evalúa integración estratégica		
			19	Existe un presupuesto específico destinado a formación en ciberseguridad.	Indica sostenibilidad y prioridad.		
			20	Hay un comité o responsable formal que coordina los programas de capacitación en ciberseguridad.	Refleja gobernanza y seguimiento.		
	Bloque 2. Cultura, perfiles y competencias	Analiza cómo la organización desarrolla el talento, diferencia roles y fomenta la cultura de seguridad.	**21**	Se han definido perfiles de puesto con competencias específicas en ciberseguridad.	Mide claridad de responsabilidades.		
			22	Las competencias se encuentran segmentadas por niveles (básico, intermedio, avanzado).	Indica progresividad y madurez formativa.		
			23	Existen rutas de aprendizaje o planes de carrera para los distintos roles (técnico, estratégico y cultural).	Evalúa desarrollo continuo.		

Matriz de Diagnóstico del Modelo C-TOET							
Dimensión	**Bloque**	**Objetivo**	**Nº**	**Pregunta**	**Justificación**	**Respuesta (escala tipo Likert 1-5)**	**Promedio**
Organización	**Bloque 2. Cultura, perfiles y competencias**	Analiza cómo la organización desarrolla el talento, diferencia roles y fomenta la cultura de seguridad.	**24**	Se utilizan marcos de referencia internacionales (NIST NICE, ENISA, etc.) para definir competencias.	Alinea formación con buenas prácticas.		
			25	La organización promueve comportamientos seguros y cultura de reporte frente a incidentes.	Mide adopción cultural.		
	Bloque 3. Coordinación y comunicación interna	Evalúa la integración transversal entre áreas y segmentos de la organiza-ción.	**26**	Los equipos técnicos, directivos y empleados participan conjuntamente en actividades de formación.	Mide transversalidad y colaboración.		
			27	Se realiza comunicación regular sobre avances, logros y aprendizajes en ciberseguridad.	Indica gestión del conocimiento y visibilidad.		
			28	Los resultados de formación se presentan y revisan en los comités de dirección o gestión de riesgos.	Evalúa apropiación por la alta dirección.		
	Bloque 4. Evaluación, seguimiento y mejora continua	Mide la capacidad de la organización para evaluar la efectividad del aprendizaje y cerrar brechas.	**29**	Se evalúan conocimientos y habilidades antes y después de cada proceso formativo.	Mide aprendizaje medible.		
			30	Se mide el impacto de la formación en el comportamiento y desempeño laboral.	Evalúa transferencia de conocimiento.		

Matriz de Diagnóstico del Modelo C-TOET							
Dimensión	**Bloque**	**Objetivo**	**Nº**	**Pregunta**	**Justificación**	**Respuesta (escala tipo Likert 1-5)**	**Promedio**
Organización	**Bloque 4. Evaluación, seguimiento y mejora continua**	Mide la capacidad de la organización para evaluar la efectividad del aprendizaje y cerrar brechas.	**31**	Se realiza seguimiento al cierre de brechas detectadas en las evaluaciones.	Indica mejora continua.		
			32	Se utilizan indicadores o tableros para monitorear el progreso del aprendizaje.	Mide analítica de desempeño formativo.		
			33	Los resultados de la evaluación se usan para ajustar y rediseñar los programas de formación.	Mide retroalimentación organizacional.		

Matriz de Diagnóstico del Modelo C-TOET							
Dimensión	**Bloque**	**Objetivo**	**Nº**	**Pregunta**	**Justificación**	**Respuesta (escala tipo Likert 1-5)**	**Promedio**
Tecnología	**Bloque 1. Infraestructura y plataformas formativas**	Evalúa la disponibilidad, variedad e integración de tecnologías dedicadas a la formación en ciberseguridad.	**34**	La organización cuenta con una plataforma de gestión del aprendizaje (LMS) para centralizar la formación.	Mide existencia de infraestructura base.		
			35	Se utilizan laboratorios técnicos o entornos simulados para la práctica de habilidades de ciberseguridad.	Evalúa el aprendizaje experiencial.		
			36	Se emplean plataformas de gamificación o CTF para entrenamientos prácticos.	Indica innovación y motivación del aprendizaje.		

Matriz de Diagnóstico del Modelo C-TOET							
Dimensión	**Bloque**	**Objetivo**	**Nº**	**Pregunta**	**Justificación**	**Respuesta (escala tipo Likert 1-5)**	**Promedio**
Tecnología	**Bloque 1. Infraestructura y plataformas formativas**	Evalúa la disponibilidad, variedad e integración de tecnologías dedicadas a la formación en ciberseguridad.	**37**	Existen entornos de simulación de crisis dirigidos a líderes o directivos.	Mide preparación estratégica y realismo organizacional.		
			38	Las plataformas tecnológicas están interconectadas con otros sistemas (evaluación, desempeño, recursos humanos, analítica).	Evalúa madurez de integración digital.		
	Bloque 2. Diversidad de metodologías y frecuencia de uso	Analiza cómo la tecnología amplía los métodos de aprendizaje y su continuidad en el tiempo.	**39**	Se utilizan metodologías variadas (cursos, *microlearning,* simulaciones, talleres).	Evalúa diversidad pedagógica.		
			40	Las actividades tecnológicas de formación se realizan de manera frecuente o continua durante el año.	Mide sostenibilidad del aprendizaje.		
			41	La tecnología permite combinar aprendizaje sincrónico y asincrónico de forma efectiva.	Evalúa flexibilidad y alcance.		
			42	Se aprovechan contenidos digitales externos (Coursera, edX, etc.) integrados al ecosistema interno.	Mide apertura y colaboración digital.		

Matriz de Diagnóstico del Modelo C-TOET

Dimensión	Bloque	Objetivo	Nº	Pregunta	Justificación	Respuesta (escala tipo Likert 1-5)	Promedio
Tecnología	**Bloque 3. Analítica, personalización e innovación**	Revisa el grado en que la organización usa tecnología avanzada para medir, personalizar y evolucionar su formación.	**43**	Se aplican evaluaciones automatizadas antes, durante y después de los procesos formativos.	Mide madurez en seguimiento.		
			44	Se utiliza analítica de datos o tableros para medir el progreso individual y colectivo.	Indica gestión basada en evidencia.		
			45	La organización emplea tecnologías adaptativas o inteligencia artificial en la formación.	Evalúa innovación y personalización.		
			46	Los resultados de la analítica se usan para ajustar programas y contenidos.	Mide retroalimentación tecnológica.		
			47	La tecnología contribuye a simular escenarios realistas de ataque o crisis.	Mide uso de innovación para resiliencia.		
	Bloque 4. Integración tecnológica con la estrategia institucional	Analiza si la infraestructura y las herramientas tecnológicas están alineadas con los objetivos organizacionales.	**48**	Las tecnologías utilizadas para la formación están alineadas con la estrategia de ciberseguridad corporativa.	Evalúa coherencia estratégica.		
			49	Existe un plan de actualización tecnológica para mantener las plataformas vigentes y seguras.	Mide sostenibilidad del ecosistema digital.		
			50	Los resultados obtenidos mediante tecnología se reportan a los líderes o comités de dirección.	Mide integración vertical de la información.		

Matriz de Diagnóstico del Modelo C-TOET							
Dimensión	**Bloque**	**Objetivo**	**Nº**	**Pregunta**	**Justificación**	**Respuesta (escala tipo Likert 1-5)**	**Promedio**
Frecuencia y madurez en formación	**Bloque 1. Implementación de *E-learning***	Fortalecer la formación continua mediante plataformas virtuales que garanticen acceso y cobertura en ciberseguridad	**51**	¿Se realizan cursos virtuales o tienen plataforma de *E-learning* para formar a los empleados sobre ciberseguridad?	Mide nivel tecnológico para formación.		
			52	¿Se ofrecen módulos virtuales específicos para directivos (por ejemplo, sobre gestión del riesgo o toma de decisiones)?	Indica fortalecimiento estratégico en ciberseguridad.		
			53	¿El equipo técnico recibe formación virtual orientada a actualizaciones normativas o certificaciones técnicas?	Evalúa cumplimiento.		
	Bloque 2. Implementación de concientización y campañas de *microlearning*	Promover la cultura de ciberseguridad a través de acciones breves y periódicas de sensibilización.	**54**	¿Se implementan campañas de concientización para empleados sobre prácticas seguras (campañas de *phishing,* contraseñas, redes, *endomarketing*)?	Mide cobertura y cultura en ciberseguridad.		
			55	¿Los directivos participan en sesiones de concientización enfocadas en responsabilidad y liderazgo en ciberseguridad?	Mide cobertura y cultura en ciberseguridad.		
			56	¿El personal técnico recibe contenidos de concientización relacionados con cumplimiento normativo y reporte de incidentes?	Mide cobertura y cultura en ciberseguridad.		

Matriz de Diagnóstico del Modelo C-TOET							
Dimensión	**Bloque**	**Objetivo**	**Nº**	**Pregunta**	**Justificación**	**Respuesta (escala tipo Likert 1-5)**	**Promedio**
Frecuencia y madurez en formación	**Bloque 3. Implementación de gamificación, competencias, retos y simulaciones lúdicas**	Desarrollar habilidades técnicas y conductuales mediante metodologías lúdicas y ejercicios prácticos.	**57**	¿Se promueven actividades de gamificación o retos prácticos (por ejemplo: paintball de equipos de ciber, talleres presenciales, etc) entre los empleados?	Indica innovación.		
			58	¿Existen ejercicios de gamificación para directivos (por ejemplo, desafíos de toma de decisiones o gestión de crisis)?	Indica innovación.		
			59	¿El equipo técnico participa en competencias CTF o entornos gamificados para fortalecer habilidades prácticas?	Indica innovación.		
	Bloque 4. Implementación de simulaciones hiperrealistas	Consolidar la capacidad de respuesta ante incidentes mediante ejercicios técnicos y de crisis simuladas.	**60**	¿Se realizan ejercicios de simulación de *phishing*, dominios ficticios, *smishing*, entre otros; como campañas de ataque para los empleados?	Indica alto nivel de conciencia cibernética.		
			61	¿Se han desarrollado simulaciones de crisis ejecutivos o 360 y ejercicios "tabletop" para directivos?	Indica fortalecimiento estratégico en ciberseguridad.		
			62	¿Se realizan ejercicios de simulación técnica para los empleados (por ejemplo, laboratorios, simulaciones de ataque tipo *ransomware*, talleres de simulación de crisis)?	Indica dominio y profundidad técnica.		

EDITORIAL ESDEG

Capítulo 7

Madurez de la implementación de la inteligencia artificial en ciberseguridad en el sector salud en Colombia*

DOI: https://doi.org/10.25062/9786287818644.07

Miguel Anderson Amaya Piracoca
Smart Cloud

Resumen: El sector salud en Colombia enfrenta importantes desafíos en ciberseguridad debido a la acelerada digitalización, el aumento de ataques a infraestructuras críticas y la limitada inversión en tecnologías de protección. Factores como la obsolescencia de sistemas, la falta de normativas robustas y la escasez de personal especializado han convertido a las instituciones de salud en objetivos prioritarios para los ciberdelincuentes. El ataque de *ransomware* a IFX Networks en 2023 evidenció la vulnerabilidad del sector y el impacto potencial sobre la prestación de servicios médicos. Además, la baja adopción de inteligencia artificial y el incumplimiento de estándares internacionales agravan la exposición a riesgos. Este trabajo analiza los principales incidentes de ciberseguridad en los últimos cinco años, evalúa el nivel de implementación de la inteligencia artificial en la protección de infraestructuras críticas y propone medidas para fortalecer la resiliencia y la seguridad digital en el sector salud colombiano.

Palabras clave: cibercrimen; ciberseguridad; digitalización; inteligencia artificial; sector salud; visualización.

* Capítulo de libro resultado del proyecto de investigación "La gobernanza del ciberespacio a nivel global, regional y nacional: desafíos, oportunidades y estrategias para la soberanía digital", del grupo de investigación "Ciberespacio, Tecnología e Innovación", de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado en 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 al autor y no reflejan necesariamente los de las instituciones participantes.

Miguel Anderson Amaya Piracoca
Ingeniero de Sistemas de la Universidad Central, Candidato a Magister en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto"
https://orcid.org/0009-0004-8459-3831 - Contacto: **miguel.amaya@esdeg.co**

Citación APA: Amaya-Piracoca, M. A. (2026). Madurez de la implementación de la inteligencia artificial en ciberseguridad en el sector salud en Colombia. En M. E. Realpe-Díaz & A. M. González-González (Eds.), *Transformación digital y ciberseguridad en Colombia: Desafíos estratégicos para sectores de infraestructura crítica* (pp. 239-268). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818644.07

TRANSFORMACIÓN DIGITAL Y CIBERSEGURIDAD EN COLOMBIA: DESAFÍOS ESTRATÉGICOS PARA SECTORES DE INFRAESTRUCTURA CRÍTICA
ISBN impreso: 978-628-7818-63-7
ISBN digital: 978-628-7818-64-4
DOI: https://doi.org/10.25062/9786287818644

Colección Ciberseguridad y Ciberdefensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2026

CC BY NC ND

Introducción

La transformación digital ha revolucionado el sector salud en Colombia, lo cual ha generado cambios profundos en la forma como se gestionan los servicios, la información y la atención a los pacientes. La adopción de tecnologías digitales ha permitido optimizar procesos administrativos, mejorar la calidad de la atención y facilitar el acceso a servicios médicos, incluso en regiones apartadas. Sin embargo, este avance también ha traído consigo nuevos desafíos, especialmente en materia de ciberseguridad, ya que la creciente dependencia de sistemas digitales ha expuesto a las instituciones sanitarias a riesgos cada vez más sofisticados y persistentes.

En los últimos años, el sector salud colombiano se ha convertido en un objetivo prioritario para los ciberdelincuentes, quienes buscan explotar las vulnerabilidades inherentes a los sistemas hospitalarios y a la infraestructura crítica. El incremento de ciberataques, como el *ransomware,* ha sido notorio, especialmente durante y después de la pandemia de COVID-19, un periodo caracterizado por una significativa aceleración de la digitalización. Incidentes recientes han puesto de manifiesto la fragilidad de la infraestructura digital del sector salud y la necesidad urgente de fortalecer las capacidades de ciberseguridad, tanto a nivel técnico como organizacional. Además, la falta de inversión en tecnologías modernas y la persistencia en el uso de software heredado han contribuido a la existencia de brechas significativas, que son aprovechadas por actores maliciosos para llevar a cabo ataques dirigidos.

A pesar de los avances en la adopción de nuevas tecnologías, el sector salud en Colombia enfrenta retos estructurales en materia de ciberseguridad. Entre los principales desafíos se encuentran la insuficiente inversión en soluciones avanzadas, la escasez de talento especializado y la falta de una cultura organizacional orientada a la seguridad digital. Muchas instituciones continúan operando con

sistemas desactualizados, arquitecturas heredadas y dispositivos médicos conectados que carecen de mecanismos de protección adecuados. Esta situación se agrava por la ausencia de normativas estrictas y la falta de integración de estándares internacionales, circunstancia que deja a discreción de cada entidad la adopción de medidas de seguridad.

La protección de los datos de salud es un aspecto crítico, ya que la información médica es altamente sensible y su exposición puede tener consecuencias graves para la privacidad y la seguridad de los pacientes. La falta de controles robustos y de políticas claras para el endurecimiento de infraestructuras críticas ha generado un entorno propicio para la explotación de vulnerabilidades, lo que afecta la integridad, la confidencialidad y la disponibilidad de la información. Además, la carencia de programas de concientización y capacitación en ciberseguridad para el personal sanitario incrementa el riesgo de ataques de ingeniería social, como el *phishing,* que siguen siendo muy efectivos en este sector.

En este contexto, la inteligencia artificial (IA) emerge como una herramienta prometedora para fortalecer la ciberseguridad en el sector salud. Específicamente, la IA tiene el potencial de identificar vulnerabilidades, detectar amenazas en tiempo real y automatizar respuestas ante incidentes, lo cual se traduce en mejoras significativas para la protección de los sistemas críticos y la reducción de errores humanos. Sin embargo, la adopción de IA en ciberseguridad dentro del sector salud colombiano sigue siendo limitada, principalmente debido a barreras económicas, técnicas y de capacitación. Además, la falta de inversión en infraestructura tecnológica y en la formación de especialistas en IA y ciberseguridad limita la capacidad de las instituciones para implementar soluciones avanzadas y adaptarse a un entorno digital en constante evolución.

En un momento en que el país busca consolidar su transformación digital y fortalecer la confianza en el ecosistema digital nacional, el análisis de la madurez en la implementación de IA en ciberseguridad en el sector salud colombiano adquiere especial relevancia. Sobre todo si se tiene en cuenta que la existencia de políticas públicas y estrategias nacionales refleja el reconocimiento de la importancia de la ciberseguridad y la necesidad de acelerar la ejecución de acciones concretas para mitigar los riesgos asociados a la digitalización.

Específicamente, el presente capítulo busca analizar el grado de implementación de la IA en la ciberseguridad del sector salud en Colombia, con el fin de identificar las oportunidades y los desafíos para la protección de los sistemas de salud y los datos personales. La comprensión de estos aspectos es fundamental para proponer estrategias que permitan avanzar hacia un entorno digital más seguro,

resiliente y confiable, en beneficio de la sociedad colombiana y del fortalecimiento del sistema de salud nacional. Además, este análisis se enmarca en la necesidad de promover una cultura de seguridad digital, fomentar la innovación tecnológica y garantizar la protección de los derechos de los pacientes en un entorno cada vez más digitalizado.

En síntesis, la transformación digital del sector salud en Colombia, si bien representa una oportunidad única para mejorar la calidad y el acceso a los servicios médicos, también plantea retos significativos en materia de ciberseguridad. La integración de la IA en la protección de los sistemas de salud, aunque es un camino prometedor, requiere superar barreras estructurales, técnicas y humanas. Bogotá, como epicentro de la atención médica en el país, ofrece un escenario privilegiado para analizar estos desafíos y proponer soluciones innovadoras que contribuyan al desarrollo de un sistema de salud más seguro y eficiente.

Metodología

La investigación se fundamenta en un enfoque mixto que combina técnicas cuantitativas y cualitativas para ofrecer una visión integral sobre la madurez y el impacto de la IA en la ciberseguridad del sector salud colombiano. Inicialmente, el análisis cuantitativo permitió caracterizar la distribución y concentración de entidades de salud tanto públicas como privadas a partir de fuentes oficiales y bases de datos abiertas, lo cual facilitó identificar regiones con mayor exposición digital y riesgo cibernético, como Bogotá, D. C., Antioquia y Cali (CCIT, 2023; Datos Abiertos Colombia, 2025). Este mapeo estadístico se complementó con una revisión documental y normativa (CONPES 3701; CONPES 3854), con lo cual se aportó contexto sobre la estructura y los retos del sistema de salud en el país.

En la siguiente fase, el estudio profundizó en la evaluación de capacidades técnicas y operativas de la IA aplicada a la ciberseguridad. Con este propósito, se recurrió a métodos cualitativos, como el análisis de casos emblemáticos y la revisión de literatura especializada, con el fin de comprender el alcance de las técnicas de IA —que abarcan redes neuronales, sistemas de respuesta automatizada y modelos de predicción de amenazas—, así como las funcionalidades de herramientas líderes (Darktrace, Trend Micro, Vectra AI). La aplicación del modelo Capability Maturity Model (CMM) permitió medir el nivel de madurez de estas soluciones, que tomaba en cuenta dimensiones como la automatización, la integración y la capacidad de respuesta. Además, se contrastaron escenarios de mitigación de

incidentes, con base en *benchmarks* internacionales y estimaciones fundamentadas en la literatura (Ojha, 2024; Rizvi, 2023; Thapaliya & Bokani, 2024).

El análisis integrador de los resultados, apoyado en la triangulación de datos y perspectivas, permitió identificar no solo el estado actual, sino también el impacto potencial de la IA en la reducción de vulnerabilidades y riesgos cibernéticos. Se exploraron dimensiones como la prevención de incidentes, la capacidad de respuesta y la continuidad operativa, para lo cual se emplearon métricas como el tiempo medio de detección y el alcance del daño mitigado. A partir de las brechas detectadas —baja inversión, madurez intermedia en automatización, limitada integración y escasez de talento especializado— se proponen acciones concretas: programas de formación diferenciada en ciberseguridad con IA, adopción progresiva de soluciones con mayor madurez, fortalecimiento de la gobernanza digital y desarrollo de políticas públicas que incentiven la innovación en ciberdefensa. En síntesis, la reflexión estratégica que orienta este trabajo es que la IA, implementada de manera coordinada y sostenible, puede convertirse en un pilar para la resiliencia y la confianza en el sistema de salud colombiano, lo que permite anticipar amenazas, reducir el impacto de los incidentes y garantizar la continuidad de los servicios en un entorno digital cada vez más exigente (Informe LATAM CISO, 2024; Rizvi, 2023; Thapaliya & Bokani, 2024).

A pesar de los avances en ciberseguridad en otros sectores, las infraestructuras hospitalarias siguen siendo un blanco atractivo para los ciberatacantes debido a la gran cantidad de datos sensibles que manejan. En este contexto, la IA ha emergido como una herramienta prometedora para fortalecer la protección de los sistemas de salud, por cuanto permite, como se señaló, la detección temprana de amenazas, el análisis predictivo de riesgos y la automatización de respuestas ante incidentes cibernéticos. Sin embargo, la implementación de estas tecnologías en el sector salud varía según la entidad y en función de factores como la inversión en innovación, la existencia de regulaciones específicas y la preparación del talento humano en ciberseguridad. Específicamente en Colombia, surge la necesidad de evaluar el nivel de adopción de la IA en la protección de la infraestructura crítica del sector salud, lo que plantea la pregunta: ¿Cuál es el grado de implementación que tiene la IA en ciberseguridad en el sector salud en Colombia?

Entidades de salud públicas y privadas colombianas con IA en estrategias de ciberseguridad en 2024

El sistema de salud en Colombia está diseñado de acuerdo con los principios de universalidad, solidaridad, eficiencia y calidad, establecidos en la Ley 100 de 1993. Fue precisamente este marco legal el que dio origen al Sistema General de Seguridad Social en Salud (SGSSS), cuya finalidad es garantizar el acceso a servicios de salud para todos los ciudadanos, independientemente de su capacidad económica. A continuación, se describe su estructura y normatividad.

Estructura del sistema de salud en Colombia

El sistema de salud en Colombia, organizado en tres regímenes principales, cuenta con una red de entidades que garantizan la prestación de servicios y la administración de recursos.

Régimen contributivo

Este régimen va dirigido a personas con capacidad de pago, como trabajadores dependientes e independientes y sus empleadores. Se financia a través de cotizaciones obligatorias que representan un porcentaje del ingreso mensual del afiliado —actualmente, los trabajadores aportan el 4 % de su salario, mientras que los empleadores contribuyen con el 8.5 %—, y su administración recae en las Entidades Promotoras de Salud (EPS) del régimen contributivo, que son responsables de afiliar a los usuarios, de garantizar el acceso al Plan de Beneficios en Salud (PBS) y de gestionar el riesgo financiero.

Régimen subsidiado

Este régimen está diseñado para la población más vulnerable y sin capacidad de pago. Es financiado con recursos del Estado, principalmente del Sistema General de Participaciones (SGP), que proviene de los impuestos nacionales. Las EPS del régimen subsidiado administran los recursos y garantizan la prestación de servicios a los afiliados, quienes también son gestionados por estas entidades, con un enfoque en garantizar el acceso a servicios básicos de salud.

Aunque inicialmente el régimen subsidiado ofrecía un paquete de servicios más limitado, actualmente se ha equiparado al régimen contributivo, lo cual garantiza acceso a los mismos beneficios.

Régimen especial y de excepción

Este régimen aplica para grupos específicos, como las Fuerzas Militares, la Policía Nacional, el Magisterio, las Universidades Públicas y Ecopetrol. Estos regímenes poseen sus propias normas y fuentes de financiación y, adicionalmente, ofrecen acceso a servicios de salud más especializados y con menos restricciones administrativas.

Instituciones prestadoras de servicios de salud (IPS)

Las IPS son hospitales, clínicas, centros de salud y consultorios que ofrecen atención médica directa a los usuarios; estas son contratadas por las EPS para garantizar la atención de sus afiliados. Dichas instituciones pueden ser públicas o privadas.

El sistema de salud en Colombia organiza la prestación de servicios en cuatro niveles de atención, los cuales se definen según la complejidad de los servicios ofrecidos y los recursos necesarios para su ejecución, con el fin de garantizar un acceso progresivo y eficiente a los servicios de salud, desde la atención básica hasta la más especializada.

Nivel I: Atención primaria

Este es el nivel más básico y el primer punto de contacto de los usuarios con el sistema de salud. Específicamente, ofrece los siguientes servicios:

- Servicios que presta:
  - Consultas médicas generales.
  - Programas de promoción de la salud y prevención de enfermedades, que abarcan la vacunación, el control prenatal y la planificación familiar.
  - Atención básica de odontología.
  - Tratamiento de enfermedades comunes y manejo de urgencias menores.
- Infraestructura, cuenta con centros de salud, puestos de salud y consultorios médicos.
- Objetivo: resolver la mayoría de los problemas de salud de la población y, si la complejidad lo exige, derivar los casos a instancias superiores.

Nivel II: Atención secundaria

Este nivel incluye servicios especializados que no pueden ser resueltos en el primer nivel.

- Servicios ofrecidos:
  - Consultas con especialistas (pediatría, ginecología, medicina interna, entre otros).

- Procedimientos diagnósticos más avanzados, que incluyen radiografías, ecografías y análisis en laboratorios especializados.
- Cirugías de mediana complejidad.
- Hospitalización para casos que requieren un monitoreo especializado.

- Infraestructura: clínicas y hospitales de medina complejidad.
- Objetivo: brindar atención especializada y resolver los problemas de salud que demandan un conocimiento técnico y recursos superiores.

Nivel III: Atención terciaria

En este nivel, la atención se centra en la alta complejidad e integra servicios especializados y subespecializados.

- Servicios ofrecidos:
  - Cirugías de alta complejidad, que abarcan especialidades como la neurocirugía, los trasplantes y la cirugía cardiovascular.
  - Tratamientos avanzados para enfermedades crónicas y complejas, tales como el cáncer, la insuficiencia renal y las enfermedades raras.
  - Los cuidados intensivos (UCI) para pacientes críticos.
  - Diagnósticos avanzados mediante tecnología de punta, que incluye resonancias magnéticas, tomografías y estudios genéticos.
- Infraestructura: hospitales de alta complejidad y centros especializados.
- Objetivo: resolver problemas de salud que requieren tecnología avanzada y la intervención de equipos multidisciplinarios.

Nivel IV: Atención cuaternaria

En este nivel se incluyen servicios de ultra especialización y tecnologías de última generación, generalmente asociados con investigación y desarrollo.

- Servicios ofrecidos:Procedimientos experimentales o innovadores, que comprenden terapias génicas, medicina regenerativa y transplantes complejos.
- Tratamientos para enfermedades raras o de muy baja prevalencia.
- Investigación clínica avanzada y ensayos clínicos.
- Infraestructura: centros de investigación y hospitales universitarios de referencia nacional e internacional.

- Objetivo: Proveer atención de vanguardia para casos extremadamente complejos, así como contribuir al desarrollo científico y tecnológico en salud.

Entidades clave del sistema de salud en Colombia

El sistema de salud colombiano está respaldado por un conjunto de entidades que cumplen funciones específicas y complementarias para garantizar el acceso, la calidad y la sostenibilidad de los servicios de salud. Estas instituciones, tanto públicas como privadas, se encargan de la regulación, supervisión, administración de recursos, aseguramiento y prestación de servicios. Su interacción y coordinación son fundamentales para que el sistema funcione de manera eficiente y responda a las necesidades de la población, especialmente en un entorno donde la transformación digital y la ciberseguridad cobran cada vez mayor relevancia.

Ministerio de Salud y Protección Social

- Función principal: es el ente rector del sistema de salud en Colombia.
- Responsabilidades: formula políticas públicas, y dirige, coordina y evalúa los planes y el cumplimiento de los derechos en salud.
- Relevancia: lidera la transformación digital, la gestión de emergencias sanitarias y la articulación de los diferentes actores del sistema.

Superintendencia Nacional de Salud

- Función principal: es la entidad de vigilancia y control del sistema de salud.
- Responsabilidades: supervisa y controla a las EPS, las IPS y demás actores. Asimismo, protege los derechos de los usuarios, sanciona a aquellas entidades que incumplen las normas y resuelve los conflictos que se presentan entre usuarios y prestadores.
- Relevancia: garantiza la transparencia, la calidad en la atención y la protección de los usuarios frente a malas prácticas o deficiencias en el servicio.

Administradora de los Recursos del Sistema General de Seguridad Social en Salud (ADRES)

- Función principal: es la entidad encargada de administrar los recursos financieros del sistema de salud.
- Responsabilidades: centraliza y gestiona los recursos provenientes de cotizaciones y aportes estatales, realiza los pagos a las EPS e IPS, y asegura la sostenibilidad financiera del sistema.
- Relevancia: su gestión eficiente es clave para la continuidad de los servicios y la transparencia en el uso de los recursos públicos.

Entidades Promotoras de Salud (EPS)

- Función principal: prestan los servicios de salud a los afiliados.

- Responsabilidades: afiliar a los usuarios, gestionar el riesgo en salud, garantizar el acceso al Plan de Beneficios en Salud (PBS) y contratar a las IPS para la prestación de servicios.
- Relevancia: son el puente entre los usuarios y la red de prestadores, por lo cual su gestión impacta directamente en la calidad y oportunidad de la atención.

Instituciones Prestadoras de Servicios de Salud (IPS)

- Función principal: prestan los servicios de salud directamente a los usuarios.
- Responsabilidades: ofrecer atención médica en los diferentes niveles de complejidad, desde la atención primaria hasta la alta especialización, y cumplir con los estándares de calidad y seguridad del paciente.
- Relevancia: son la base operativa del sistema, ya que materializan la atención en salud a través de hospitales, clínicas, centros de salud y consultorios.

La inteligencia artificial

La inteligencia artificial (IA) es una disciplina de la informática que busca desarrollar sistemas capaces de imitar y, en algunos casos, superar las funciones cognitivas humanas, como el aprendizaje, el razonamiento y la toma de decisiones. Su principal fortaleza radica en la capacidad de procesar y analizar grandes volúmenes de datos heterogéneos, lo cual le permite identificar patrones, adaptarse a nueva información y predecir eventos con una precisión sin precedentes. En el contexto de la ciberseguridad, la IA ha revolucionado la forma en que se detectan amenazas, se gestionan vulnerabilidades y se priorizan activos, y, de este modo, supera en velocidad y exactitud a los métodos tradicionales (Kumar et al., 2023).

Específicamente, la IA constituye una rama de la informática dedicada al desarrollo de sistemas capaces de emular capacidades humanas, tales como el aprendizaje, el razonamiento, la percepción y la toma de decisiones. Sus componentes fundamentales incluyen algoritmos avanzados, aprendizaje automático (*machine learning*), aprendizaje profundo (*deep learning*) y procesamiento de lenguaje natural (NLP), la visión por computador y los sistemas expertos. El aprendizaje automático permite que los sistemas mejoren su rendimiento a partir de la experiencia, mientras que el aprendizaje profundo utiliza redes neuronales para analizar datos complejos y no estructurados. Por su parte, el procesamiento de lenguaje natural

facilita la interpretación y generación de lenguaje humano, lo cual permite que las máquinas interactúen de manera más eficiente con los usuarios y comprendan grandes volúmenes de información textual. Estos componentes trabajan de manera integrada para dotar a la IA de capacidades cognitivas avanzadas, esenciales para anticipar, identificar y prevenir amenazas en entornos digitales de diversos sectores, como la salud, la industria y la seguridad (Kumar et al., 2023).

Sin embargo, la implementación de la IA no está exenta de desafíos. En ese sentido es fundamental considerar tanto la necesidad de supervisión humana como las limitaciones inherentes a los sistemas inteligentes, entre las cuales se incluyen la dependencia de datos históricos y la posibilidad de ataques adversariales. Además, la integración de la IA en la ciberseguridad plantea importantes cuestiones éticas y de gobernanza, relacionadas con la transparencia, la privacidad y la responsabilidad en la toma de decisiones automatizadas. Por ello, se requiere un enfoque equilibrado que combine el potencial de la IA con la experiencia humana y marcos regulatorios sólidos para garantizar su uso responsable y efectivo (Kumar et al., 2023).

La IA ha transformado radicalmente el sector salud a nivel global, lo cual ha generado impactos significativos en la prevención, el diagnóstico, el tratamiento y la gestión de enfermedades. En países como Estados Unidos, Reino Unido, China y Japón, la IA se ha convertido en un aliado estratégico para mejorar la precisión diagnóstica y la eficiencia operativa. Por ejemplo, algoritmos de aprendizaje profundo han demostrado una capacidad sobresaliente para analizar imágenes médicas (radiografías, tomografías y resonancias magnéticas), lo cual posibilita la detección temprana de patologías como cáncer de mama, pulmón y piel, e incluso, en ocasiones, supera la precisión de los especialistas humanos (Kumar et al., 2023). Un caso emblemático es el uso de IA en el sistema de salud británico (NHS), donde herramientas como DeepMind Health han optimizado la interpretación de imágenes oftalmológicas, lo que acelera el diagnóstico de enfermedades oculares y reduce las listas de espera.

Además, la IA ha sido fundamental en la personalización de tratamientos. Plataformas como IBM Watson Health han integrado grandes volúmenes de literatura médica y datos clínicos para sugerir terapias personalizadas en oncología, lo cual ha permitido mejorar los resultados clínicos y reducir los efectos adversos. En Asia, hospitales en China han implementado sistemas de IA para el análisis automatizado de tomografías computarizadas durante la pandemia de COVID-19, lo que ha resultado en diagnósticos más rápidos y precisos, un aspecto crucial para la gestión de recursos hospitalarios y la contención de la enfermedad. Asimismo, la IA ha facilitado la gestión de grandes volúmenes de datos de pacientes, lo cual

optimiza la administración hospitalaria, la predicción de brotes epidemiológicos y la asignación eficiente de recursos, lo cual se traduce en una atención más oportuna y de mayor calidad (Kumar et al., 2023).

Sin embargo, la adopción de IA en salud también plantea desafíos éticos y regulatorios, como la protección de datos sensibles, la transparencia en la toma de decisiones automatizadas y la necesidad de supervisión humana. A pesar de estos retos, la evidencia internacional demuestra que, cuando es implementada de manera responsable, la IA puede contribuir significativamente a la mejora de los sistemas de salud, lo cual se traduce en una mayor equidad, eficiencia y calidad de la atención médica.

Por otra parte, en el ámbito de la ciberseguridad en salud, la IA ha emergido como una herramienta indispensable para proteger la información sensible de los pacientes y garantizar la continuidad de los servicios médicos. Los sistemas de IA pueden analizar grandes volúmenes de tráfico de red y registros de actividad en tiempo real, lo que les permite identificar patrones anómalos que podrían indicar intentos de intrusión, *malware* o ataques de *ransomware.* Por ejemplo, hospitales en Estados Unidos y Europa han implementado soluciones de IA que monitorean el acceso a historias clínicas electrónicas para detectar accesos no autorizados y prevenir filtraciones de datos antes de que se materialicen (Kumar et al., 2023).

La IA también ha permitido la automatización de respuestas ante incidentes de seguridad, lo cual reduce el tiempo de reacción y minimiza el impacto de los ataques. Algoritmos de *machine learning* pueden aprender de incidentes previos y anticipar nuevas amenazas, lo que les permite ajustar dinámicamente las políticas de seguridad y priorizar la protección de los activos más críticos. Durante la pandemia de COVID-19, la acelerada digitalización de los servicios de salud incrementó la superficie de ataque, pero también impulsó la adopción de IA para fortalecer la defensa contra amenazas cibernéticas, como el *phishing* dirigido a personal médico y la protección de dispositivos médicos conectados.

Integración de la inteligencia artificial en ciberseguridad sanitaria

La integración de IA en ciberseguridad sanitaria no está exenta de desafíos. La escasez de talento especializado, la complejidad de los sistemas hospitalarios y la necesidad de cumplir con normativas internacionales de protección de datos, como HIPAA y GDPR, requieren un enfoque integral que combine tecnología

avanzada, capacitación continua y gobernanza robusta. A pesar de estos retos, la experiencia internacional demuestra que la IA es un pilar fundamental para la resiliencia cibernética en el sector salud, pues permite anticipar, detectar y mitigar amenazas de manera proactiva y eficiente (Kumar et al., 2023).

Específicamente, los resultados de la entrevista realizada a directivos tecnológicos de una EPS y de IPS de cuarto nivel evidencian que la integración de inteligencia artificial se encuentra presente de forma transversal en procesos críticos de estas entidades, especialmente en la detección de patrones de tráfico, la identificación de comportamientos anómalos y la automatización de operaciones. Los entrevistados destacaron beneficios tangibles como la mejora en la productividad, la reducción de tiempos de respuesta frente a amenazas y la facilitación de trámites y servicios de cara a pacientes y afiliados. Sin embargo, también surgieron desafíos importantes que frenan su expansión: los altos costos de implementación, la necesidad de priorizar el uso de IA en procesos estratégicos y el reto de garantizar que estas tecnologías no comprometan la seguridad del paciente ni la continuidad de los servicios médicos. De manera prospectiva, los participantes señalaron que sus organizaciones planean fortalecer el uso de IA en detección y respuesta avanzada de incidentes, monitoreo continuo, pruebas de seguridad y adaptación a marcos regulatorios emergentes, entre los cuales se encuentran tendencias disruptivas como Zero Trust y criptografía cuántica. Este panorama revela que, si bien la IA es reconocida como una herramienta efectiva y viable para robustecer la ciberseguridad en salud, su adopción requiere un equilibrio cuidadoso entre inversión, eficiencia operativa y salvaguarda del núcleo esencial del sistema: la atención segura y confiable al paciente.

Herramientas de inteligencia artificial en ciberseguridad utilizadas para la prevención de ataques cibernéticos

La inteligencia artificial ha demostrado un impacto transformador en el sector salud a nivel global mediante la optimización de procesos clínicos, diagnósticos y administrativos. Sin embargo, este avance tecnológico también ha incrementado la superficie de exposición a riesgos digitales, lo que convierte la ciberseguridad en un pilar fundamental para la protección de la información y la continuidad de los servicios médicos. La creciente digitalización y la sofisticación de las amenazas exigen soluciones avanzadas capaces de anticipar, detectar y mitigar incidentes de manera proactiva, alineadas con las directrices emitidas por el MinTic en 2025, a través de la actualización del Modelo de Seguridad y Privacidad de la Información (MSPI), y con marcos de referencia como la ISO 27001:2022 y las buenas prácticas

de NIST. Por ello, resulta indispensable analizar el nivel de madurez de las herramientas de inteligencia artificial aplicadas a la ciberseguridad en el sector salud colombiano, con el fin de identificar fortalezas, brechas y oportunidades de mejora que permitan fortalecer la resiliencia digital de las instituciones y garantizar la confianza de los usuarios en un entorno cada vez más interconectado.

En los últimos años, el sector salud y otras infraestructuras críticas han experimentado un aumento significativo en la frecuencia y complejidad de los incidentes de ciberseguridad, lo cual ha impulsado la adopción de soluciones basadas en IA para fortalecer la capacidad de detección, respuesta y mitigación de riesgos. Evaluar la madurez de estas herramientas implica no solo revisar los incidentes registrados, sino también analizar las mejoras en los tiempos de respuesta y la efectividad de los mecanismos automatizados frente a amenazas emergentes. Este enfoque permite identificar avances, brechas y oportunidades de optimización en la protección de los activos digitales, lo cual contribuye a la construcción de un entorno más resiliente y seguro para las organizaciones colombianas en 2024.

En este sentido, la identificación y selección adecuada de herramientas de IA constituye un pilar fundamental para fortalecer la prevención de ataques cibernéticos en el sector salud colombiano. Esta necesidad se acentúa en regiones con alta incidencia de incidentes, como Bogotá D. C., Antioquia y Cali, lo cual se evidencia en la distribución geográfica de los eventos reportados. En este contexto, el uso de tecnologías avanzadas permite anticipar, detectar y mitigar amenazas de manera proactiva; estas incluyen redes neuronales convolucionales (CNN) y recurrentes (RNN), sistemas de respuesta a incidentes automatizados, modelos de predicción de amenazas y análisis de comportamiento de usuario (UBA). Dichas herramientas han demostrado ser muy efectivas en la identificación de patrones anómalos, la automatización de respuestas y la reducción de vulnerabilidades, por lo que su aplicación resulta esencial para proteger la información sensible y garantizar la continuidad de los servicios de salud (Ojha, 2024; Rizvi, 2023; Thapaliya & Bokani, 2024).

Cada una de estas soluciones de IA aporta capacidades específicas que potencian la ciberseguridad. Por ejemplo, las CNN son especializadas en la detección de *malware* y la prevención de *phishing* mediante el análisis de firmas y estructuras sospechosas, mientras que las RNN destacan en la detección de intrusiones a través del análisis de datos secuenciales. Específicamente, los sistemas de respuesta automatizada permiten mitigar ataques en tiempo real sin intervención humana, y los modelos predictivos anticipan amenazas basándose en patrones históricos. Además, el análisis de comportamiento de usuario y la inteligencia de amenazas facilitan la detección de anomalías y la identificación de riesgos

emergentes, mientras que el análisis automatizado de vulnerabilidades ayuda a identificar y corregir puntos débiles antes de que sean explotados. De esta manera, la integración de estas herramientas no solo optimiza los tiempos de respuesta ante incidentes, sino que también contribuye a la construcción de un entorno digital más resiliente y adaptativo frente a la evolución constante de las amenazas cibernéticas (Ojha, 2024; Rizvi, 2023; Thapaliya & Bokani, 2024).

A continuación, la tabla 1 relacionan diferentes técnicas de IA y su conexión con tres herramientas enfocadas en ciberseguridad. La selección de estas herramientas se basó en criterios específicos: el Cuadrante Mágico de Gartner para herramientas de detección y respuesta, del cual se eligieron dos herramientas líderes y un jugador de nicho.

Tabla 1. *Técnicas de inteligencia artificial con aplicación en ciberseguridad*

Técnica de IA	Aplicación en ciberseguridad	Funcionamiento de la técnica
Redes Neuronales Convolucionales (CNN)	Alta precisión en detección de *malware* y prevención de *phishing*.	Las CNN son redes neuronales especializadas en identificar patrones espaciales, útiles para analizar firmas de *malware* o estructuras de sitios web sospechosos.
Redes Neuronales Recurrentes (RNN)	Eficientes en detección de intrusiones gracias al análisis de datos secuenciales.	Las RNN son efectivas para analizar secuencias de datos, como paquetes de red o registros temporales, detectando comportamientos anómalos persistentes.
Redes *Feedforward* (FNN)	Modelo base usado para clasificación de ataques simples.	Las FNN son redes básicas en las que los datos fluyen hacia adelante; se utilizan para tareas simples de clasificación de amenazas conocidas.
Sistemas de Respuesta a Incidentes Automatizados	Identifican y mitigan ataques en tiempo real sin intervención humana.	Estos sistemas usan IA para ejecutar automáticamente respuestas ante amenazas, como aislar redes, bloquear las IP o generar alertas en tiempo real.
Modelos de Predicción de Amenazas	Anticipan ataques basándose en similitudes con ataques pasados.	Utilizan modelos predictivos que aprenden de ataques previos para anticipar amenazas futuras basadas en patrones similares.
Análisis de Comportamiento de Usuario (UBA)	Detecta anomalías en el comportamiento que podrían indicar un ataque interno.	Analizan patrones de comportamiento de usuarios y dispositivos para identificar accesos inusuales o potenciales ataques internos.

Técnica de IA	Aplicación en ciberseguridad	Funcionamiento de la técnica
Redes Neuronales Convolucionales (CNN)	Alta precisión en detección de *malware* y prevención de *phishing*.	Las CNN son redes neuronales especializadas en identificar patrones espaciales, útiles para analizar firmas de *malware* o estructuras de sitios web sospechosos.
Análisis de Inteligencia de Amenazas	Procesa datos de múltiples fuentes para identificar amenazas emergentes.	Procesan grandes volúmenes de datos estructurados y no estructurados para descubrir amenazas emergentes antes de que se materialicen.
Análisis de Vulnerabilidades Automatizado	Identifica puntos débiles en sistemas antes de que sean explotados.	Evalúan sistemas y redes automáticamente para identificar vulnerabilidades, proponiendo acciones preventivas antes de un ataque.

Fuente: Elaboración propia

La tabla 2 detalla la intersección de las técnicas de inteligencia artificial con las herramientas de ciberseguridad que las incorporan.

Tabla 2. *Herramientas de ciberseguridad en relación con las técnicas de inteligencia artificial*

Herramienta de IA	Técnicas de IA aplicadas (relación con la tabla 1)	Evolución de la IA en la herramienta
Darktrace	Redes Neuronales Convolucionales (CNN)	Darktrace fue pionera en el uso de IA autoaprendizaje para ciberseguridad, integrando desde 2016 algoritmos de *machine learning* no supervisado y redes neuronales para detectar amenazas desconocidas. Su plataforma ha evolucionado hacia el uso de *deep learning* y modelos híbridos, permitiendo la detección de amenazas avanzadas y la respuesta autónoma en tiempo real, adaptándose a entornos complejos y dinámicos.
	Redes Neuronales Recurrentes (RNN)	
	Análisis de Comportamiento de Usuario (UBA)	
	Sistemas de Respuesta a Incidentes Automatizados	
Trend Micro	Modelos de Predicción de Amenazas	Trend Micro, con décadas en el sector, incorporó IA avanzada en 2017, integrando *machine learning* y análisis predictivo en sus soluciones. Ha evolucionado hacia la correlación de inteligencia global, el uso de modelos supervisados y no supervisados para anticipar amenazas de día cero, y la automatización del análisis de vulnerabilidades, fortaleciendo la protección proactiva y la priorización de riesgos en grandes infraestructuras
	Análisis de Inteligencia de Amenazas	
	Análisis de Vulnerabilidades Automatizado	
	Análisis de Comportamiento de Usuario (UBA)	

Herramienta de IA	Técnicas de IA aplicadas (relación con la tabla 1)	Evolución de la IA en la herramienta
Vectra AI	Identifica puntos débiles en sistemas antes de que sean explotados	Vectra AI lanzó su plataforma Cognito en 2018, enfocada en el uso de *deep learning* y análisis de comportamiento para detectar amenazas avanzadas y movimientos laterales en la red. Su evolución ha consistido en la integración de modelos de IA que correlacionan eventos en tiempo real, automatizan la respuesta ante incidentes y priorizan amenazas emergentes, lo cual permite una defensa adaptativa y contextualizada en entornos empresariales y de salud.
	Redes Neuronales Convolucionales (CNN)	
	Redes Neuronales Recurrentes (RNN)	
	Modelos de Predicción de Amenazas	
	Análisis de Comportamiento de Usuario (UBA)	
	Sistemas de Respuesta a Incidentes Automatizados	

Fuente: Elaboración propia.

A partir de las herramientas revisadas en la tabla 2, se presentan tres incidentes de ciberseguridad relevantes ocurridos en Colombia durante 2023 y 2024 (tabla 3). Estos generaron un impacto significativo en el país y constituyen un referente esencial para la evolución de la ciberseguridad nacional. Asimismo, se examinará cómo las herramientas de ciberseguridad con IA habrían podido contribuir en la mitigación de los ataques analizados.

Tabla 3. *Herramientas de ciberseguridad en relación con las técnicas de IA empleadas en atacas recientes*

Herramienta de IA	Ataque a IFX (Sep. 2023)	Ataque al sector financiero (2024)	Ataque al sector salud (2024)
Descripción del ataque	El ataque se presenta mediante un ramsomware dirigido a la infraestructura de IFX, con un alcance aproximado de 700 entidades afectadas del sector público y privado en Latinoamérica, entre ellos Colombia siendo afectado en diferentes entidades de gobierno con un tiempo de afectación total o parcial aproximado de 5 y 10 días.	Durante el año 2024, el sector financiero enfrentó diferentes ataques. Los vectores de ataque más concurrentes fueron el ramsomware, phishing y la denegación de servicio distribuido (DDOS), los cuales afectaron la disponibilidad de las plataformas financieras y la captura de información de clientes, generando afectaciones aproximadas de 1 a 3 días.	En el sector salud se presentaron varios incidentes de seguridad que afectaron a diferentes IPS y EPS. En este caso, generaron demoras en las atenciones, problemas en los servicios administrativos y disponibilidad de la historia clínica. Los vectores de ataque más concurrentes fueron el *ramsomware* y la denegación de servicio distribuido (DDOS), lo cual causó una interrupción total aproximada de 2 a 7 días, así como interrupciones parciales de hasta 10 días.

Herramienta de IA	Ataque a IFX (Sep. 2023)	Ataque al sector financiero (2024)	Ataque al sector salud (2024)
Darktrace	Esta herramienta hubiera apoyado significativamente en el comportamiento de usuarios y esto hubiese permitido reducción en los tiempos para identificar el foco del ataque o generación de alertas de una intrusión.	Esta herramienta apoyaría en la reducción de *phishing* ya que en el sector financiero es muy común este tipo de ataques y esta herramienta fortalecería esta brecha de seguridad.	Esta herramienta en los ataques sector salud hubiese sido de gran valor en sistemas de respuesta a incidentes y en el constante monitoreo de posibles amenazas.
Trend Micro	Esta herramienta hubiese aportado en el monitoreo y la visibilidad de posibles amenazas, teniendo en cuenta el tamaño de la infraestructura de IFX.	Esta herramienta hubiese ayudado a la identificación de posibles vulnerabilidades existentes y en la predicción de posibles amenazas.	Esta herramienta hubiera permitido tener una mayor visibilidad de las posibles amenazas, así como en la inteligencia de posibles amenazas persistentes.
Vectra AI	Esta herramienta hubiera ayudado en la identificación de posibles puntos débiles y en aprendizaje de posibles nuevos vectores de ataque.	Esta herramienta fortalecería significativamente en el aprendizaje de los posibles vectores de ataques y de posibles adversarios, reduciendo los tiempos de aprendizaje de un posible nuevo ataque.	Esta herramienta fortalecería significativamente el aprendizaje sobre los posibles vectores de ataques y los posibles adversarios, reduciendo los tiempos de aprendizaje de un posible nuevo ataque.

Fuente: Elaboración propia.

La rápida digitalización del sector salud ha incrementado la exposición a ciberataques, especialmente en regiones con alta concentración de servicios médicos, como se observa en Colombia. Ante este panorama, la adopción de herramientas de IA en ciberseguridad es fundamental, pero su efectividad depende del nivel de madurez alcanzado en su implementación. Para medir de manera objetiva y estructurada este nivel, se utiliza el modelo Capability Maturity Model (CMM), que permite clasificar y comparar las capacidades de automatización, integración, aprendizaje, cobertura y respuesta de soluciones como Vectra AI, Trend Micro y Darktrace. En particular, esta metodología facilita identificar fortalezas, debilidades y áreas de mejora, lo que asegura que la inversión en IA realmente contribuya a la protección de los datos y la continuidad operativa en el sector salud.

Niveles del Capability Maturity Model (CMM) adaptado

La rápida digitalización del sector salud ha incrementado la exposición a ciberataques, especialmente en regiones con alta concentración de servicios médicos, como se observa en Colombia. Ante este panorama, la adopción de herramientas

de IA en ciberseguridad es fundamental, pero su efectividad depende del nivel de madurez alcanzado en su implementación. Para medir de manera objetiva y estructurada este nivel, se utiliza el modelo Capability Maturity Model (CMM), que permite clasificar y comparar las capacidades de automatización, integración, aprendizaje, cobertura y respuesta de soluciones como Vectra AI, Trend Micro y Darktrace. Esta metodología facilita identificar fortalezas, debilidades y áreas de mejora, lo cual asegura que la inversión en IA realmente contribuya a la protección de los datos y la continuidad operativa en el sector salud.

A continuación, se relacionan los niveles de medición del modelo CMM, adaptado para herramientas de ciberseguridad con inteligencia artificial.

- Nivel 1: Inicial. Procesos *ad hoc,* poco definidos, dependientes de usuarios expertos, sin automatización ni integración.
- Nivel 2: Repetible. Procesos definidos y documentados, cierta automatización, integración básica, respuesta reactiva.
- Nivel 3: Definido. Procesos estandarizados, integración con otros sistemas, automatización avanzada, aprendizaje supervisado.
- Nivel 4: Gestionado. Procesos medidos y controlados, adaptación dinámica, cobertura proactiva de amenazas, respuesta automatizada.
- Nivel 5: Optimizado. Mejora continua, IA para autoaprendizaje, personalización avanzada, integración total, respuesta autónoma y predictiva.

A continuación, la tabla 4 presenta la evaluación del CMM para las herramientas de IA en ciberseguridad.

Tabla 4. *Herramientas de Inteligencia Artificial en ciberseguridad, en relación con las técnicas de IA*

Criterio / Herramienta	Darktrace	Trend Micro	Vectra AI
Automatización de procesos	Nivel 5: automatización total, respuesta autónoma en tiempo real, autoaislamiento de amenazas sin intervención humana.	Nivel 3: automatización en detección y respuesta, pero requiere intervención manual en escenarios complejos.	Nivel 4: automatización avanzada en detección y respuesta, orquestación de alertas y mitigación automática de amenazas complejas.
Integración con otros sistemas	Nivel 5: integración total y dinámica con infraestructuras *on-premise, cloud* y OT, aprendizaje del entorno en tiempo real.	Nivel 4: integración con múltiples entornos (*cloud, endpoint, red*), *API* y conectores para ecosistemas híbridos.	Nivel 4: integración robusta con SIEM, SOAR, y plataformas *cloud, API* abiertas para personalización.

Criterio / Herramienta	Darktrace	Trend Micro	Vectra AI
Capacidad de aprendizaje/adaptación	Nivel 5: IA autoaprendizaje, modelos no supervisados que evolucionan con el entorno, adaptación proactiva y predictiva.	Nivel 3: *machine learning* supervisado, actualización periódica de modelos, adaptación limitada a nuevas amenazas emergentes.	Nivel 4: *machine learning* supervisado y no supervisado, adaptación dinámica a nuevas amenazas, aprendizaje continuo basado en datos de red.
Cobertura de amenazas	Nivel 5: cobertura total, detección de amenazas conocidas, desconocidas y *zero-day,* análisis de comportamiento y contexto.	Nivel 4: amplia cobertura de amenazas globales, integración de inteligencia de amenazas, protección multicapa.	Nivel 4: cobertura avanzada de amenazas conocidas y desconocidas, fuerte en detección de movimientos laterales y ataques internos.
Soporte y actualización	Nivel 5: actualizaciones en tiempo real, soporte proactivo, autoajuste de modelos y recursos de aprendizaje continuo.	Nivel 4: actualizaciones automáticas, soporte global 24/7, recursos de capacitación y comunidad de usuarios.	Nivel 4: actualizaciones frecuentes, soporte especializado, comunidad activa, documentación técnica robusta.
Usabilidad y personalización	Nivel 5: interfaz altamente intuitiva, personalización avanzada, recomendaciones automáticas y experiencia adaptativa.	Nivel 4: interfaz amigable, personalización de alertas y reportes, experiencia de usuario optimizada.	Nivel 3: interfaz intuitiva, *dashboards* personalizables; requiere capacitación para aprovechar funciones avanzadas.
Gestión de incidentes y respuesta	Nivel 5: respuesta autónoma, análisis forense automatizado, *reporting* avanzado y recomendaciones en tiempo real.	Nivel 3: respuesta semiautomatizada, requiere intervención en incidentes complejos, *reporting* estándar.	Nivel 4: respuesta automatizada, *playbooks* personalizables, análisis forense integrado, *reporting* detallado

Fuente: elaboración propia

En este contexto, los resultados del CMM evidencian que, si bien existen herramientas de IA en ciberseguridad con altos niveles de madurez tecnológica, su impacto real en Colombia depende de factores estructurales y operativos propios del país. La presencia de soluciones como Darktrace, Vectra AI o Trend Micro representa una oportunidad significativa para la anticipación y mitigación de amenazas complejas, dado que estas alcanzan niveles avanzados en automatización, integración y capacidad de aprendizaje. Sin embargo, la adopción efectiva de estas tecnologías en el entorno nacional requiere superar desafíos como la heterogeneidad de la infraestructura, la escasez de talento especializado y la necesidad de fortalecer la cultura organizacional en torno a la ciberseguridad. Así, el nivel de madurez alcanzado por estas herramientas no solo refleja el avance tecnológico disponible, sino también la urgencia de adaptar e integrar estas soluciones a las realidades y prioridades del sector salud colombiano.

Para el sector salud, estas implicaciones son especialmente relevantes, dado que se observa una alta concentración de instituciones sanitarias en regiones como Bogotá D.C., Antioquia y Cali, a lo que se suma la creciente sofisticación de los ciberataques dirigidos a servicios médicos. Por esta razón, la capacidad de automatizar la detección y respuesta ante incidentes, junto con la adaptación dinámica a nuevas amenazas, puede marcar la diferencia en la protección de datos sensibles y la continuidad de la atención médica en Colombia. No obstante, la efectividad de estas herramientas depende de su integración con los sistemas existentes, la actualización constante de infraestructuras y la capacitación del personal. En definitiva, avanzar hacia mayores niveles de madurez tecnológica en ciberseguridad no solo fortalece la defensa ante amenazas emergentes, sino que también contribuye a la sostenibilidad, integridad, disponibilidad, confianza y calidad del sistema de salud en un entorno digital cada vez más exigente.

Impacto de la IA en la resiliencia y ciberseguridad del sector salud colombiano: retos y oportunidades

El análisis realizado hasta este punto ha permitido identificar que, si bien el sector salud en Colombia ha avanzado en la adopción de tecnologías digitales y en la integración de IA en algunos procesos, persisten retos significativos en materia de ciberseguridad y protección de la infraestructura crítica. La concentración de instituciones de salud en regiones como Bogotá D.C., Antioquia y Cali resalta la necesidad de fortalecer capacidades en todo el territorio nacional para la reducción de brechas y garantizar la continuidad de los servicios médicos, lo cual se evidencia en la distribución de prestación de servicios. Además, la revisión de incidentes de gran impacto y la literatura especializada sugiere que la madurez tecnológica y la cultura organizacional en torno a la ciberseguridad son factores determinantes para enfrentar amenazas cada vez más sofisticadas.

En el contexto colombiano, los incidentes recientes de ciberseguridad, como el ataque a IFX Networks, han puesto de manifiesto la exposición y el riesgo potencial a los que están sujetas las infraestructuras tecnológicas que soportan servicios críticos, entre los cuales se cuenta el sector salud. La interrupción de servicios digitales y la afectación a plataformas de conectividad evidencian la dependencia creciente de los sistemas de salud respecto a proveedores tecnológicos, así como la necesidad de fortalecer la resiliencia digital en todo el ecosistema digital. Esta situación resalta

la importancia de contar con mecanismos avanzados de prevención y respuesta, especialmente en regiones con alta concentración de instituciones de salud.

En este escenario, la IA es una tecnología clave para transformar la gestión de la ciberseguridad en el sector salud. Herramientas basadas en IA, como las analizadas en este estudio (Darktrace, Trend Micro, Vectra AI), permiten anticipar amenazas mediante el análisis de grandes volúmenes de datos, identificar patrones anómalos en tiempo real y activar respuestas automáticas que minimizan el impacto de los incidentes. En escenarios tradicionales, sin IA, la detección de amenazas suele ser reactiva y dependiente de la intervención humana, lo que incrementa el tiempo medio de detección (MTTD) y la probabilidad de que un ataque cause interrupciones prolongadas o pérdidas de datos sensibles. Por el contrario, la literatura internacional y los *benchmarks* de la industria muestran que la adopción de IA puede reducir el MTTD de días a minutos, aumentar el número de amenazas mitigadas y limitar el alcance del daño, lo cual contribuye a la continuidad operativa y a la protección de la información crítica.

Para ilustrar este impacto, se puede comparar el desempeño de los sistemas de ciberseguridad en tres dimensiones clave: la prevención de incidentes, la capacidad de respuesta y la continuidad operativa. En la dimensión preventiva, la IA permite identificar amenazas emergentes antes de que se materialicen, lo cual es posible gracias a modelos predictivos y análisis de comportamiento. En cuanto a la capacidad de respuesta, las soluciones automatizadas pueden aislar sistemas comprometidos y contener incidentes en cuestión de minutos, mientras que en escenarios sin IA la respuesta suele ser más lenta y menos efectiva. Finalmente, en términos de continuidad operativa, la IA facilita la recuperación rápida de servicios y la protección de datos críticos, lo cual reduce el tiempo de inactividad y el impacto sobre la atención a los pacientes.

La tabla 5 sintetiza el impacto potencial de las herramientas de IA analizadas sobre incidentes documentados en el sector salud colombiano, en el cual se consideran las tres dimensiones estudiadas.

Tabla 5. *Impacto potencial de herramientas de inteligencia artificial en ciberseguridad*

Dimensión / métrica	**Sin IA (escenario tradicional)**	**Con IA (Darcktrace, Trend Micro y Vectra AI)**
Prevención de incidentes	Detección reactiva, alta tasa de falsos positivos, amenazas no anticipadas.	Detección proactiva, reducción de falsos positivos, anticipación de amenazas emergentes.

Dimensión / métrica	Sin IA (escenario tradicional)	Con IA (Darcktrace, Trend Micro y Vectra AI)
Capacidad de respuesta	Tiempo medio de detección (MTTD): 2-5 días aprox. Respuesta manual, limitada por recursos humanos.	MTTD: 5-15 minutos aprox. Respuesta automatizada, aislamiento inmediato de sistemas afectados.
Continuidad operativa	Interrupciones prolongadas (horas o días), pérdida de datos, afectación a múltiples sedes.	Interrupciones mínimas (minutos), protección de datos críticos, rápida recuperación de servicios.

Fuente: Elaboración propia.

Este análisis evidencia que la integración de IA en la ciberseguridad del sector salud no solo mejora la capacidad de anticipar y mitigar amenazas, sino que también fortalece la resiliencia operativa y la confianza en los servicios digitales. Acompañada de una estrategia de formación y actualización constante, la adopción de estas tecnologías es fundamental para enfrentar los desafíos actuales y futuros en un entorno cada vez más digitalizado y expuesto a riesgos cibernéticos.

En este sentido, la formación en ciberseguridad con enfoque en IA debe ser una prioridad transversal para el sector salud. No basta con capacitar únicamente al personal técnico; por el contrario, es fundamental diseñar programas diferenciados para los niveles gerencial, clínico, administrativo y operativo. Para los directivos, la formación debe centrarse en la gestión del riesgo digital, la toma de decisiones informadas sobre inversión en tecnologías emergentes y la comprensión de los marcos regulatorios nacionales e internacionales, como la Ley 1581 de 2012 y el marco NIST. El personal clínico y administrativo, por su parte, requiere entrenamiento práctico en la identificación de amenazas como el *phishing,* la manipulación de dispositivos médicos conectados y la protección de datos sensibles de los pacientes. Finalmente, los equipos técnicos deben recibir capacitación avanzada en el uso, integración y gestión de herramientas de IA para la detección, respuesta y recuperación ante incidentes, así como en la aplicación de estándares internacionales como ISO 27001 y el NIST CSF. La creación de alianzas con universidades, centros de investigación y proveedores tecnológicos puede acelerar la transferencia de conocimiento y el desarrollo de talento especializado, lo cual permitiría cerrar la brecha crítica de capital humano que hoy limita la madurez del sector.

Ahora bien, la adopción progresiva de herramientas de ciberseguridad potenciadas por IA puede guiarse por una hoja de ruta basada en el CMM. Desde esta perspectiva, las entidades de salud deben priorizar la adquisición e integración de soluciones que permitan avanzar desde niveles intermedios de madurez

—caracterizados por automatización parcial y respuestas reactivas— hacia niveles superiores, donde la automatización avanzada, la integración 360 y la respuesta autónoma sean capacidades de gran valor. Esto implica invertir en plataformas que permitan la orquestación de alertas, la correlación de eventos en tiempo real y la integración con sistemas clínicos, administrativos y de gestión de datos. Además, es clave asegurar la interoperabilidad entre las nuevas herramientas y los sistemas legados, para evitar vacíos de información y maximizar el retorno de la inversión. La experiencia internacional muestra que la adopción de soluciones con IA, como sistemas de detección de amenazas basados en *machine learning* y plataformas de respuesta automatizada, reduce significativamente el tiempo de detección y contención de incidentes, al tiempo que mejora la continuidad operativa y la protección de los datos sensibles (Ojha, 2024; Rizvi, 2023).

Frente a este panorama, el fortalecimiento de la gobernanza digital en salud es indispensable para articular los esfuerzos de ciberseguridad y garantizar la sostenibilidad de las acciones implementadas. Actualmente, la ausencia de una estructura de gobernanza robusta dificulta la coordinación interinstitucional, la asignación eficiente de recursos y la rendición de cuentas. Por lo tanto, se recomienda la creación de comités de ciberseguridad en cada entidad, con representación de todas las áreas críticas, y la definición de roles y responsabilidades claras en la gestión del riesgo digital. Asimismo, es necesario establecer protocolos de actuación ante incidentes, mecanismos de reporte y monitoreo continuo, y canales de comunicación efectivos con entidades regulatorias, como el Ministerio de Salud y MinTIC, además de considerar la creación de una Agencia Nacional de Seguridad Digital. Con este propósito, la gobernanza digital se debe basar en los lineamientos del CONPES 3995 y el Decreto 338 de 2022, de tal manera que cuente con los instrumentos para promover la adopción de mejores prácticas y la colaboración público-privada para fortalecer la resiliencia del sector.

Finalmente, el desarrollo y la implementación de políticas públicas que incentiven la adopción de IA en ciberdefensa resultan fundamentales para acelerar la transformación digital segura del sector salud. Aunque el reciente CONPES 4144 de 2025 establece lineamientos estratégicos para la promoción de la IA en Colombia, es necesario traducir estos lineamientos en incentivos concretos, tales como beneficios fiscales, líneas de financiación específicas y requisitos de ciberseguridad e IA en los procesos de habilitación y acreditación de las entidades de salud. Además, la articulación con iniciativas internacionales y la adopción de estándares globales permitirá a Colombia posicionarse como un referente regional en la protección de infraestructuras críticas de salud. La colaboración con organismos

multilaterales, la academia y el sector privado será clave para acceder a recursos, asistencia técnica y mejores prácticas que aceleren la madurez digital del sector.

En síntesis, la aplicación coordinada de estas acciones permitirá que la inteligencia artificial se convierta en un pilar estratégico para la resiliencia del sistema de salud colombiano. Para ello, es crucial avanzar en la formación de talento, la adopción de tecnologías maduras, la consolidación de la gobernanza digital y el desarrollo de políticas públicas robustas. De este modo, la IA no solo fortalecerá la capacidad de anticipar y mitigar amenazas, sino que también garantizará la continuidad operativa, la protección de los datos y la confianza de los usuarios en un entorno cada vez más digitalizado y desafiante.

Conclusiones

Si bien la IA es un habilitador estratégico para la resiliencia cibernética del sector salud colombiano, su impacto depende de la madurez tecnológica y la integración organizacional. Específicamente, el análisis realizado evidencia que la IA, aplicada a la ciberseguridad, permite anticipar, detectar y mitigar amenazas con mayor eficacia que los métodos tradicionales, lo cual reduce el tiempo medio de detección y el alcance de los incidentes. Sin embargo, la efectividad de estas soluciones está condicionada por el nivel de automatización, integración y capacidad de aprendizaje alcanzado, así como por la alineación con los procesos y la cultura organizacional de las entidades de salud. Por tanto, se recomienda que las instituciones de cualquier nivel avancen progresivamente en la adopción de herramientas de IA, y que prioricen aquellas que permitan una integración escalable y una respuesta autónoma ante incidentes, de acuerdo con el modelo CMM.

La escasez de talento especializado y la limitada inversión en innovación constituyen los principales obstáculos para la consolidación de la IA en la ciberseguridad dentro del sector salud. A pesar de la disponibilidad de tecnologías avanzadas, la falta de personal capacitado y la baja inversión en investigación y desarrollo restringen su adopción efectiva. Esta brecha se manifiesta en una madurez intermedia de las soluciones implementadas y en una dependencia de proveedores externos. Por ello, es fundamental que el país impulse programas de formación diferenciada en ciberseguridad con enfoque en IA, dirigidos tanto a perfiles técnicos como a directivos y personal clínico. Asimismo, debe fomentar la colaboración entre el sector público, la academia y la industria para fortalecer el ecosistema de talento digital.

La gobernanza digital y la articulación interinstitucional son condiciones necesarias para una ciberdefensa sostenible y efectiva en salud. La ausencia de estructuras robustas de gobernanza dificulta la coordinación de esfuerzos, la asignación eficiente de recursos y la respuesta integral ante incidentes. Por esta razón, se recomienda la creación de comités de ciberseguridad en cada entidad, la definición de roles y responsabilidades claras y la adopción de protocolos de actuación alineados con los marcos regulatorios nacionales (MSPI MinTic 2025) e internacionales. Además, la creación de una Agencia Nacional de Seguridad Digital, como se discute en la política pública, puede ser un catalizador para la consolidación de una estrategia nacional de ciberdefensa en salud.

Asimismo, la adopción de IA en ciberseguridad debe estar acompañada de políticas públicas que incentiven la innovación y garanticen la protección de los datos sensibles. El reciente CONPES 4144 establece lineamientos estratégicos para la promoción de la IA en Colombia. No obstante, es necesario traducir estos lineamientos en incentivos concretos, como beneficios fiscales, líneas de financiación específicas y requisitos de ciberseguridad e IA en los procesos de habilitación y acreditación de las entidades de salud. De igual forma, la articulación con estándares internacionales y la colaboración con organismos multilaterales permitirá acelerar la madurez digital del sector y posicionar a Colombia como referente regional en la protección de infraestructuras críticas de salud.

En síntesis, la transformación digital segura del sector salud requiere una visión integral que combine tecnología, talento, gobernanza y políticas públicas. En este sentido, la evidencia recopilada demuestra que la IA puede convertirse en un pilar para la resiliencia y la confianza en el sistema de salud colombiano, siempre que su implementación sea coordinada, sostenible, incluyente (especialmente para entidades con recursos limitados o sin ellos) y adaptada a las realidades del país. Avanzar en la formación de talento, la adopción de tecnologías maduras, la consolidación de la gobernanza digital y el desarrollo de políticas públicas robustas permitirá no solo anticipar y mitigar amenazas, sino también garantizar la continuidad operativa, la protección de los datos y la confianza de los usuarios en un entorno cada vez más digitalizado y desafiante.

Referencias

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: Current state of research. *International Journal of Internet and Enterprise Management, 6*(4), 279–314. https://doi.org/10.1504/IJIEM.2010.035624

Arctic Wolf. (2023). *The top 15 healthcare industry cyber attacks of the past decade*.

Cámara Colombiana de Informática y Telecomunicaciones [CCIT], & Tanque de Análisis y Creatividad de las TIC [TicTAc]. (2023). Estado de la ciberseguridad y la inteligen-cia artificial en Colombia. CCIT. TIC; TicTac. https://www.ccit.org.co/estudios/esta-do-de-la-ciberseguridad-y-la-inteligencia-artificial-en-colombia/

Canavos, G. C. (1988). *Probabilidad y estadística: Aplicaciones y métodos.* McGraw-Hill.

Chatfield, A. T., & Reddick, C. G. (2019). A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in US federal government. *Government Information Quarterly, 36*(2), 346–357. https://doi.org/10.1016/j.giq.2018.09.007

Damar, M., Özen, A., & Yılmaz, A. (2024). Cybersecurity in the health sector in the reality of artificial intelligence, and information security conceptually. *Journal of AI, 8*(1), 61–82. https://doi.org/10.61969/jai.1466340

Decreto 1377 de 2013. *Por el cual se reglamenta parcialmente la Ley 1581 de 2012.* Ministerio de Salud y Protección Social. *D. O.* 48834, 27 de junio de 2013. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Decreto 338 de 2022. *Por el cual se establecen lineamientos generales para fortalecer la gobernanza de la seguridad digital en Colombia.* Ministerio de Tecnologías de la Información y las Comunicaciones. https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%20338%20DEL%2001%20DE%20MARZO%20DE%202022.pdf

Decreto 620 de 2020. *Por el cual se reglamenta la Ley 1273 de 2009 y se dictan otras disposiciones. Presidencia de la República.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=137753

Departamento Nacional de Planeación [DNP]. (2025). *Documento CONPES 4144: Política nacional para el desarrollo y adopción de la inteligencia artificial en Colombia.* https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4144.pdf

Global Center on AI Governance. (2024). *Informe sobre talento en ciberseguridad e IA.* https://globalcenteraigovernance.org/informe-talento-ciberseguridad-ia-2024

Goutam, R. K. (2015). Importance of cyber security. *International Journal of Computer Applications, 111*(7), 14–15. https://doi.org/10.5120/19550-1250

Häyrinen, K., Saranto, K., & Nykänen, P. (2008). Definition, structure, content, use and impacts of electronic health records: A review of the research literature. *International Journal of Medical Informatics, 77*(5), 291–304. https://doi.org/10.1016/j.ijmedinf.2007.09.001

International Telecommunication Union [ITU]. (2020). *Global cybersecurity index 2020.* ITU. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Khan, B., Fatima, H., Qureshi, A., Kumar, S., Hanan, A., Hussain, J., & Abdullah, S. (2023). Drawbacks of artificial intelligence and their potential solutions in the healthcare sector. *Biomedical Materials & Devices, 1*(2), 731–738. https://doi.org/10.1007/s44174-023-00063-2

Ley 100 de 1993. *Por la cual se crea el sistema de seguridad social integral y se dictan otras disposiciones.* Congreso de la República de Colombia. D. O. 41148, 23 de diciembre de 1993. http://www.secretariasenado.gov.co/senado/basedoc/ley_0100_1993.html

Ley 1273 de 2009. *Por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado: la protección de la información y de los datos.* Congreso de la República de Colombia. *D. O.* 47223 del 5 de enero de 2009. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Ley 1581 de 2012. *Por la cual se dictan disposiciones generales para la protección de datos personales.* Congreso de la República. *D. O.* 48587, 18 de octubre de 2012

Ley 1751 de 2015. *Por la cual se regula el derecho fundamental a la salud y se dictan otras disposiciones*. Congreso de la República de Colombia. Congreso de la República. D. O. 49427, 16 de febrero de 2015. http://www.secretariasenado.gov.co/senado/basedoc/ley_1751_2015.html

López Ardila, G., Lesmes Patiño, J., & Díaz Parra, V. (2025). *Estado de la ciberseguridad y la inteligencia artificial en Colombia.* Cámara Colombiana de Informática y Telecomunicaciones (CCIT) & TicTac. https://www.ccit.org.co/estudios/estado-de-la-ciberseguridad-y-la-inteligencia-artificial-en-colombia/

Ojha, D. R. (2024). Use of artificial neural networks to detect and prevent cybersecurity threats. *NPRC Journal, 1*(6), 132–141. https://doi.org/10.3126/nprcjmr.v1i6.71754

Pawar, J., Kulkarni, D., & Dhanwate, V. (2024). Understanding cyber security in health sector. *Journal of Advanced Zoology, 45,* 55–64. https://doi.org/10.53555/jaz.v45iS4.4149

Rizvi, M. (2023). Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. *International Journal of Advanced Engineering Research and Science (IJAERS), 10*(5), 55–59. https://dx.doi.org/10.22161/ijaers.105.8

Schwartz, A., Contreras, B., Steffaro, A., Jordan-Zoob, I., Hoffman, D., Herrera, C., Bermúdez, L., Pereira Salas, D., Kotz, A., Gross, L., Park, D., Martínez, A., & González Castellanos, H. (2024). *Informe LATAM CISO 2024: Cybersecurity insights from industry leaders.* Centro de Política y Derecho de Ciberseguridad.

Upguard. (2024). 14 biggest healthcare data breaches. https://www.upguard.com/blog/biggest-data-breaches-in-healthcare

EDITORIAL ESDEG

Capítulo 8

Cooperación internacional en ciberseguridad y gobernanza digital*

DOI: https://doi.org/10.25062/9786287818644.08

Mónica Lissette Flórez Cáceres
Universidad Militar Nueva Granada

Resumen: El capítulo examina la cooperación internacional como eje estratégico de la ciberseguridad y la gobernanza digital. En un contexto de creciente interdependencia tecnológica global, se subraya que la seguridad cibernética demanda enfoques colaborativos fundamentados en la confianza, la interoperabilidad y el fortalecimiento de capacidades. En este marco, se analizan los avances institucionales en Colombia, así como su articulación con organismos multilaterales y los principales mecanismos de cooperación, tales como el intercambio de información, las operaciones conjuntas y el desarrollo de capacidades. Asimismo, se abordan los desafíos derivados de la fragmentación normativa, la desconfianza geopolítica y las amenazas emergentes asociadas con la inteligencia artificial y las cadenas de suministro. Se concluye que la cooperación internacional constituye un pilar esencial para la estabilidad global, la protección de infraestructuras críticas y la consolidación de un ciberespacio seguro, inclusivo y sostenible.

Palabras clave: ciberdiplomacia; ciberseguridad internacional; cooperación multilateral; gobernanza digital; resiliencia cibernética.

* Capítulo de libro resultado del proyecto de investigación "La gobernanza del ciberespacio a nivel global, regional y nacional: desafíos, oportunidades y estrategias para la soberanía digital", del grupo de investigación "Ciberespacio, Tecnología e Innovación", de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado en 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 la autora y no reflejan necesariamente los de las insti-tuciones participantes.

Mónica Lissette Flórez Cáceres
Profesional en Relaciones Internacionales y Estudios Políticos, Universidad Militar Nueva Granada, Colombia. Especialista en Gerencia de Comercio Internacional y magíster en Acción Política, Fortalecimiento Institucional y Participación Ciudadana en el Estado de Derecho, Universidad Francisco de Vitoria, España. Ph. D. Honoris Causa en Cooperación Internacional y Relaciones Internacionales. Contacto: **monica.florez@unimilitar.edu.co**

Citación APA: Flórez-Cáceres, M. L. (2026). Cooperación internacional en ciberseguridad y gobernanza digital. En M. E. Realpe-Díaz & A. M. González-González (Eds.), *Transformación digital y ciberseguridad en Colombia: Desafíos estratégicos para sectores de infraestructura crítica* (pp. 269-294). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818644.08

TRANSFORMACIÓN DIGITAL Y CIBERSEGURIDAD EN COLOMBIA: DESAFÍOS ESTRATÉGICOS PARA SECTORES DE INFRAESTRUCTURA CRÍTICA
ISBN impreso: 978-628-7818-63-7
ISBN digital: 978-628-7818-64-4
DOI: https://doi.org/10.25062/9786287818644

Colección Ciberseguridad y Ciberdefensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2026

Introducción

La acelerada transformación digital de las dos últimas décadas ha configurado un ecosistema global caracterizado por la hiperconectividad, la interdependencia tecnológica y la vulnerabilidad sistémica. En este contexto, la ciberseguridad y la gobernanza digital emergen como pilares estratégicos para garantizar la estabilidad política, económica y social de los Estados, así como la integridad del ciberespacio como dominio común global (Nye, 2021; DeNardis, 2020). El incremento exponencial de las amenazas cibernéticas —que abarcan desde el espionaje industrial y la desinformación hasta los ciberataques a infraestructuras críticas— ha impulsado un cambio de paradigma en el que la seguridad ya no puede concebirse exclusivamente como una responsabilidad estatal aislada, sino como un esfuerzo de cooperación multinivel que involucra actores públicos, privados y multilaterales (Clarke & Knake, 2020; Maurer, 2022).

A medida que los ciberconflictos adquieren dimensiones geopolíticas, la cooperación internacional en ciberseguridad se convierte en un componente esencial de la seguridad colectiva y la defensa digital. Formulada por Nye (2022) y desarrollada por Betz y Stevens (2018), la noción de "poder cibernético" (*cyber power*) se fundamenta en la capacidad de los Estados y sus aliados para proteger sus activos digitales, disuadir agresiones y proyectar estabilidad en el ciberespacio mediante marcos de gobernanza compartidos. No obstante, esta cooperación enfrenta importantes desafíos estructurales, tales como las asimetrías o brechas tecnológicas, la falta de confianza estratégica, las divergencias normativas y la fragmentación de los regímenes de gobernanza global (Finnemore & Hollis, 2020).

El concepto de gobernanza digital se articula, en consecuencia, como una respuesta integral a la complejidad del entorno digital contemporáneo. Este enfoque

abarca la regulación de los flujos de datos, la gestión ética de la inteligencia artificial, la protección de infraestructuras críticas y la preservación de la soberanía tecnológica, enmarcada dentro de principios de transparencia, cooperación y responsabilidad compartida (Floridi, 2020). Al respecto, la Organización de las Naciones Unidas (UNODA, 2021) y la Unión Europea (European Commission, 2021, 2023) han avanzado en la formulación de marcos normativos e iniciativas multilaterales que buscan establecer estándares comunes de seguridad, confianza digital y resiliencia, lo cual evidencia la interdependencia entre la ciberseguridad y la gobernanza global.

Sin embargo, el desarrollo de dinámicas propias del panorama cibernético ha demostrado que los esfuerzos unilaterales resultan insuficientes para contrarrestar amenazas globales de alta sofisticación: campañas de desinformación patrocinadas por Estados, el *ransomware* transnacional, vulnerabilidades en la cadena de suministro digital y operaciones encubiertas en la denominada "zona gris" del ciberespacio (Buchanan & Rid, 2021; Hsu & Lin, 2022; NCSC UK, 2021). En este sentido, autores como Klimburg (2019) y Libicki (2020) destacan la necesidad de establecer mecanismos de interoperabilidad estratégica que fortalezcan la cooperación técnica, el intercambio de inteligencia y la coordinación de respuestas ante incidentes cibernéticos, en un marco de confianza mutua y respeto por la soberanía digital.

La cooperación internacional en ciberseguridad va más allá del ámbito militar o gubernamental. En la práctica, involucra un ecosistema amplio en el que convergen instituciones multilaterales, organizaciones regionales, empresas tecnológicas, centros de investigación y sociedad civil (Healey, 2021). La Organización de los Estados Americanos, por ejemplo, ha promovido programas de fortalecimiento de capacidades y marcos de respuesta coordinada en América Latina. Por su parte, la OTAN, a través del CCDCOE, impulsa ejercicios como Locked Shields para fomentar la preparación conjunta ante ciberincidentes (NATO CCDCOE, 2023). Estas iniciativas reflejan el tránsito desde modelos de defensa nacional hacia una seguridad cooperativa y adaptativa, en la que la inteligencia compartida y la respuesta colectiva son componentes centrales del poder cibernético contemporáneo (Singer & Friedman, 2020).

Por otra parte, el avance de tecnologías disruptivas como la inteligencia artificial, el internet de las cosas (IoT), la computación cuántica y las arquitecturas de confianza cero (*Zero Trust*) ha ampliado tanto las oportunidades como los riesgos asociados al ciberespacio (Garde & Dorr, 2022; Microsoft, 2023). Además, la digitalización masiva incrementa la superficie de ataque y complejiza la atribución de

responsabilidades, lo cual genera nuevas brechas regulatorias que exigen marcos de gobernanza adaptativos y colaborativos.

En este escenario, la gobernanza digital se consolida como un ámbito multidimensional que trasciende la seguridad técnica y abarca cuestiones éticas, jurídicas y geopolíticas. En línea con esta perspectiva, Floridi (2020) sostiene que la ética de la información debe ser la base de una gobernanza responsable del ciberespacio, orientada al bienestar social y la sostenibilidad. Por ello, la cooperación internacional en ciberseguridad requiere integrar principios de transparencia, responsabilidad y proporcionalidad, de modo que la defensa de los sistemas digitales no comprometa los valores democráticos ni la confianza pública.

En el plano estratégico, la interdependencia digital redefine los conceptos tradicionales de poder y seguridad. Al respecto, Nye (2014) plantea que el ciberespacio constituye un dominio donde el poder blando basado en la cooperación y la legitimidad normativa puede ser tan influyente como el poder duro. Desde esta perspectiva, la cooperación internacional en ciberseguridad se convierte en una estrategia de defensa para la construcción de confianza y la proyección de estabilidad internacional. Por tanto, las políticas de ciberdefensa deben articularse con los principios de la gobernanza digital para garantizar un equilibrio entre la seguridad, la libertad y la innovación tecnológica (Floridi, 2020; Singer & Friedman, 2020).

En síntesis, la ciberseguridad y la gobernanza digital constituyen dimensiones interdependientes de un mismo desafío global en el que se debe preservar la seguridad colectiva y la confianza en el entorno digital mediante la cooperación internacional. A través de mecanismos de coordinación técnica, marcos normativos compartidos y esfuerzos conjuntos de construcción de capacidades, los Estados y actores no estatales pueden contribuir al fortalecimiento de un orden digital sostenible y resiliente. Este capítulo desarrolla, por tanto, un análisis de los fundamentos, mecanismos y desafíos de la cooperación internacional en ciberseguridad, en el que se exploran sus implicaciones para la gobernanza digital contemporánea y las perspectivas futuras de la seguridad global.

Fundamentos de la cooperación internacional en ciberseguridad y gobernanza digital

La cooperación internacional en materia de ciberseguridad surge como una respuesta estructural ante la interdependencia tecnológica global y la naturaleza transnacional de las amenazas digitales. En la medida en que los sistemas políticos, económicos y

sociales se digitalizan, las fronteras tradicionales del poder y la seguridad se desdibujan, lo cual da lugar a un escenario de vulnerabilidad compartida (Nye, 2014). El ciberespacio, concebido inicialmente como un dominio abierto y descentralizado, se ha transformado en un entorno estratégico donde convergen intereses estatales, corporativos y sociales, lo cual exige una gobernanza colectiva que combine capacidades técnicas, marcos jurídicos y mecanismos de confianza (Klimburg, 2019).

Desde la perspectiva de la teoría de las relaciones internacionales, la cooperación en ciberseguridad se inserta en la lógica de la interdependencia compleja formulada por Keohane y Nye (2012), según la cual los Estados, aunque persiguen sus propios intereses, se ven obligados a colaborar para enfrentar amenazas comunes que ningún actor puede mitigar por sí solo. En este sentido, la ciberseguridad debe dejar de ser concebida únicamente como un asunto de defensa nacional. Por el contrario, se debe incluir como un bien público global, cuya preservación demanda coordinación transnacional y gobernanza compartida (Deibert, 2020).

El reconocimiento del ciberespacio como un dominio operativo en los escenarios de seguridad nacional y defensa internacional marcó un punto de inflexión. La OTAN, en su Cumbre de Varsovia de 2016, declaró el ciberespacio como el "quinto dominio" de operaciones militares, junto con tierra, mar, aire y espacio (NATO, 2016). Esta conceptualización amplió las responsabilidades de los Estados en materia de protección digital, a la vez que impulsó la creación de estructuras multinacionales para la cooperación técnica y estratégica. De manera complementaria, la Unión Europea, mediante su Estrategia de Ciberseguridad de 2020, reafirmó la necesidad de un enfoque coordinado entre gobiernos, sector privado y sociedad civil para fortalecer la resiliencia digital del bloque (European Commission, 2020).

Históricamente, los primeros mecanismos de cooperación internacional en ciberseguridad surgieron a partir de la necesidad de responder al cibercrimen transfronterizo. La Convención de Budapest sobre Ciberdelincuencia (2001), auspiciada por el Consejo de Europa, estableció el primer marco jurídico internacional para la cooperación judicial y la estandarización de procedimientos de investigación digital (Council of Europe, 2022). Este instrumento sentó las bases de la colaboración interestatal en persecución penal y de la asistencia mutua en materia de evidencia electrónica. Sin embargo, su alcance sigue siendo limitado por la falta de adhesión de potencias clave como China y Rusia, circunstancia que evidencia las tensiones geopolíticas en torno a la definición de normas globales del ciberespacio (Maurer, 2018).

En el ámbito político-estratégico, la cooperación cibernética se articula bajo el concepto de seguridad colectiva digital. Derivado del principio de seguridad colectiva de la Carta de las Naciones Unidas, este paradigma postula que un ataque

cibernético contra un Estado puede tener repercusiones globales y, por tanto, exige una respuesta coordinada (UNODA, 2021). De acuerdo con Healey (2020), la seguridad cibernética colectiva depende de la capacidad de los Estados para compartir información de amenazas, establecer protocolos comunes de defensa y generar confianza mutua mediante medidas de transparencia.

El intercambio de información, sin embargo, requiere un delicado equilibrio entre la protección de la soberanía nacional y la necesidad de cooperación técnica. Dunn Cavelty (2008) advierte que, en ausencia de confianza institucionalizada, los Estados tienden a mantener una postura defensiva y restrictiva respecto al flujo de inteligencia cibernética. De ahí que organismos como la European Union Agency for Cybersecurity (ENISA) y el Forum of Incident Response and Security Teams (FIRST) promuevan la creación de redes de confianza y estándares compartidos que faciliten la gestión de incidentes, la interoperabilidad y la comunicación segura (ENISA, 2023; FIRST, 2022).

Por otro lado, la expansión del poder digital de las grandes corporaciones tecnológicas ha introducido nuevos actores en el escenario de la cooperación cibernética, entre los cuales se cuentan empresas como Microsoft, Google o IBM, las cuales operan infraestructuras críticas y gestionan vastos volúmenes de datos estratégicos que impactan directamente en la seguridad nacional y global. Deibert (2021) sostiene que esta privatización de la ciberseguridad plantea un desafío de gobernanza, ya que las decisiones tomadas por actores corporativos pueden tener implicaciones geopolíticas sin pasar por mecanismos de rendición de cuentas democráticos. En consecuencia, la cooperación internacional debe integrar a los actores privados dentro de un marco regulatorio transparente que garantice tanto la seguridad como los derechos digitales.

En paralelo, la proliferación de acuerdos bilaterales y regionales en materia de ciberseguridad evidencia la fragmentación de la gobernanza global. Mientras la Unión Europea impulsa modelos de cooperación basados en la normativa del Reglamento General de Protección de Datos (GDPR), potencias como Estados Unidos y China adoptan estrategias centradas en la soberanía digital y la supremacía tecnológica (Segal, 2021). Esta divergencia normativa genera tensiones que obstaculizan la creación de estándares universales. Según Rid y Buchanan (2021), la falta de consenso sobre principios básicos —como la atribución de ataques o el uso legítimo de la fuerza en el ciberespacio— limita el alcance de la cooperación internacional y aumenta el riesgo de malentendidos estratégicos.

En el plano técnico-operativo, los equipos nacionales de respuesta a incidentes de seguridad informática (CSIRT) han evolucionado como nodos esenciales de cooperación práctica. Su función trasciende la gestión de incidentes domésticos para convertirse en puntos de enlace internacional que facilitan el intercambio de alertas tempranas, indicadores de compromiso (IoC) y tácticas de ataque. En este sentido, la experiencia del CERT-EU y del NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) demuestra que la cooperación técnica puede fortalecer la ciberresiliencia regional y consolidar la confianza entre aliados (CCDCOE, 2023).

Sin embargo, la cooperación no puede limitarse al ámbito técnico, pues requiere también una dimensión política y normativa que garantice la coherencia estratégica entre los Estados. Al respecto, Maurer y Morgus (2021) destacan que la institucionalización de la cooperación a través de mecanismos como el Cyber Diplomacy Toolbox de la UE o las Confidence-Building Measures (CBMs) de la OSCE constituye un avance significativo hacia una gobernanza cibernética basada en la transparencia y la rendición de cuentas. Estos instrumentos buscan establecer canales diplomáticos permanentes, protocolos de comunicación en crisis y acuerdos sobre el comportamiento responsable de los Estados en el ciberespacio.

En este marco, la cooperación internacional en ciberseguridad debe concebirse como un proceso dinámico, evolutivo y multidimensional que, más allá de los marcos jurídicos y técnicos, implica la convergencia de voluntades políticas, capacidades institucionales y confianza recíproca. En palabras de Mueller (2017), la gobernanza del ciberespacio debe entenderse como un sistema policéntrico, en el cual los Estados, las organizaciones internacionales, el sector privado y la sociedad civil interactúan bajo principios compartidos, lo cual hace posible evitar la hegemonía de un solo actor o bloque geopolítico. Este enfoque pluralista busca preservar la apertura y la interoperabilidad del entorno digital, pilares esenciales para el funcionamiento del internet global.

Asimismo, el desarrollo de capacidades constituye otro componente esencial de la cooperación internacional. Más allá de los aspectos técnicos, el fortalecimiento de capacidades abarca la formación de talento humano, la investigación aplicada, la creación de marcos normativos y la consolidación de ecosistemas de innovación en ciberseguridad (Marinos & Sfakianakis, 2021). Las naciones con mayores niveles de madurez digital tienden a compartir conocimiento y recursos con países en desarrollo, lo cual impulsa la resiliencia global frente a amenazas como el cibercrimen, el espionaje digital o los ataques a infraestructuras críticas. En este sentido, Organismos como la Unión Internacional de Telecomunicaciones (UIT) y el Banco Mundial han desempeñado un papel clave en la promoción de

programas de capacitación y cooperación técnica en regiones de África, Asia y América Latina (ITU, 2022; World Bank, 2021).

El carácter transnacional de las amenazas cibernéticas se refleja en la sofisticación de los actores involucrados. Los grupos de ciberespionaje patrocinados por Estados, las organizaciones criminales y los grupos *hacktivistas* operan más allá de las jurisdicciones nacionales, una circunstancia que complica la atribución de responsabilidades (Rid, 2020). Este fenómeno ha impulsado la creación de mecanismos de confianza entre los Estados, como las Confidence-Building Measures (CBMs) promovidas por la Organización para la Seguridad y la Cooperación en Europa (OSCE). Estas medidas buscan fomentar la transparencia en las políticas nacionales de ciberseguridad, el intercambio de buenas prácticas y la comunicación directa en caso de incidentes (OSCE, 2019).

Desde un punto de vista estratégico, la cooperación cibernética también responde a la necesidad de evitar la militarización del ciberespacio. Diversos autores sostienen que la conjunción del incremento de las capacidades ofensivas digitales y la ausencia de mecanismos de control y verificación incrementa el riesgo de una carrera armamentista cibernética (Liff, 2022). Por ello, las iniciativas multilaterales buscan promover medidas de transparencia, intercambio de información y notificación de incidentes que contribuyan a la estabilidad estratégica (Maurer, 2020).

En este contexto, el desarrollo de la diplomacia cibernética se ha convertido en un eje central de la política exterior de numerosos Estados, en la medida en que actúa como un instrumento de disuasión y cooperación simultáneamente (Bjola & Manor, 2020). Específicamente, la diplomacia cibernética implica un conjunto de acciones orientadas a gestionar las relaciones internacionales en el ámbito digital, mediante la negociación de normas, la resolución de conflictos y la promoción de la confianza entre actores estatales y no estatales (Cornish et al., 2021). En el caso de la Unión Europea, la creación del Cyber Diplomacy Toolbox en 2017 estableció un marco común para responder de manera coordinada a incidentes cibernéticos de origen externo, el cual incluye sanciones diplomáticas y medidas de presión (European Council, 2017). De forma paralela, países como Estados Unidos, Australia y Japón han desarrollado estrategias de diplomacia cibernética enfocadas en la disuasión, la protección de infraestructuras críticas y la cooperación regional (DFAT, 2022; MOFA Japan, 2021; White House, 2023;).

En el ámbito interamericano, la OEA ha desempeñado un papel fundamental en la promoción de la cooperación hemisférica en ciberseguridad, una labor que ha concretado mediante el Programa Interamericano sobre Ciberseguridad y la creación del Centro de Ciberseguridad de las Américas (OAS, 2022). Estas iniciativas

buscan fortalecer las capacidades institucionales de los Estados miembros, mejorar la coordinación ante incidentes y fomentar una cultura de seguridad digital. En este contexto, y particularmente en el ámbito latinoamericano, donde la brecha tecnológica y las limitaciones presupuestales son significativas, la cooperación internacional se convierte en un pilar esencial para el fortalecimiento de la resiliencia digital y la soberanía tecnológica (Ramírez & Castañeda, 2021).

En este contexto, la ciberresiliencia se consolida como un objetivo estratégico de la cooperación internacional. Este concepto trasciende la mera protección de activos digitales (Linkov et al., 2018), ya que se define como la capacidad de los sistemas, organizaciones y Estados para resistir, responder y recuperarse de incidentes cibernéticos. En este sentido, implica un enfoque integral que articule políticas públicas, inversión tecnológica, educación digital y marcos normativos coherentes. Así, al facilitar el intercambio de conocimiento, la adopción de estándares y la coordinación de respuestas ante crisis, la cooperación internacional se convierte en el principal catalizador de la resiliencia cibernética global (ENISA, 2023).

En suma, la cooperación internacional en ciberseguridad y gobernanza digital se sustenta en la interdependencia, la confianza y la capacidad compartida de los Estados y actores no estatales para proteger el ecosistema digital común. La evolución del ciberespacio como dominio estratégico ha reconfigurado las dinámicas de poder, lo cual ha generado tanto nuevas oportunidades de colaboración como desafíos significativos en materia de soberanía, ética y estabilidad internacional. La construcción de una gobernanza digital inclusiva y sostenible depende, por tanto, de la voluntad política, la madurez institucional y la convergencia de intereses globales en torno a principios de transparencia, responsabilidad y cooperación mutua.

Mecanismos de cooperación y coordinación en ciberseguridad: un enfoque integral

La cooperación internacional en ciberseguridad constituye un elemento esencial dentro del marco más amplio de la gobernanza digital contemporánea. En un entorno global caracterizado por la interdependencia tecnológica, la hiperconectividad y la asimetría de las capacidades estatales, la ciberseguridad ha dejado de ser una cuestión meramente técnica para convertirse en un problema geopolítico y de gobernanza global (DeNardis, 2020). Las amenazas cibernéticas no reconocen fronteras y pueden afectar simultáneamente a actores estatales, corporaciones

privadas e infraestructuras críticas transnacionales, razón por la cual se requieren respuestas coordinadas, multilaterales y sostenidas en la confianza mutua.

La cooperación, en este contexto, se define como el proceso mediante el cual los Estados, organizaciones internacionales, empresas privadas y actores de la sociedad civil articulan esfuerzos para prevenir, detectar, mitigar y responder a incidentes cibernéticos (Maurer, 2020). Esta colaboración se materializa a través de tres dimensiones estratégicas centradas en el intercambio de información e inteligencia, las operaciones conjuntas y el desarrollo de capacidades. Dichos mecanismos conforman una arquitectura cooperativa que no solo fortalece la seguridad colectiva, sino que también promueve la confianza, la interoperabilidad y la estabilidad del ecosistema digital (ENISA, 2023).

Intercambio de información e inteligencia

El intercambio de información se erige como uno de los pilares más sólidos en la construcción de una defensa cibernética cooperativa. A nivel global, organismos como la Organización de las Naciones Unidas (ONU, 2021) y la UIT (2022) han promovido la creación de redes nacionales de respuesta a incidentes cibernéticos (CSIRT/CERT) con el fin de articular esfuerzos entre los sectores público, privado y académico para la detección, el análisis y la mitigación de amenazas.

Estos sistemas facilitan el flujo de IoC, tácticas, técnicas y procedimientos (TTP), así como la realización de análisis conjuntos de *malware* y vulnerabilidades emergentes (Barnes & Ussath, 2022). Con todo, su efectividad depende de la existencia de marcos de confianza y de estándares interoperables que garanticen la protección de la información sensible.

Al respecto, la ENISA (2023) sostiene que la consolidación de "círculos de confianza" resulta esencial para reducir el riesgo de exposición y asegurar la integridad de los datos compartidos, por cuanto estos círculos se configuran como grupos cerrados de intercambio de información entre entidades gubernamentales, militares y privadas. Además, plataformas como la Malware Information Sharing Platform (MISP) o la Cyber Threat Alliance (CTA) ejemplifican cómo el intercambio automatizado y estandarizado de indicadores de amenazas contribuye a la respuesta temprana ante ataques coordinados (ENISA, 2023).

En este sentido, los sistemas de alerta temprana (Early Warning Systems, EWS) permiten una respuesta anticipada frente a incidentes a gran escala. De acuerdo con Lindsay (2020), estos sistemas posibilitan la identificación de patrones anómalos y el despliegue de medidas preventivas antes de que las amenazas se materialicen. En este contexto de prevención y respuesta anticipada, a nivel

regional, el CERT-EU y la European Cyber Crisis Liaison Organisation Network (EU-CyCLONe) han sido reconocidos como modelos de cooperación efectiva entre Estados miembros de la Unión Europea (ENISA, 2023).

Sin embargo, los mecanismos de intercambio enfrentan importantes desafíos éticos, jurídicos y técnicos. La reticencia a compartir información sensible, la ausencia de marcos legales que definan la clasificación de datos y la falta de interoperabilidad entre sistemas nacionales son obstáculos recurrentes (Dunn-Cavelty, 2008). Además, la desconfianza entre Estados puede generar brechas en el flujo de inteligencia estratégica, lo cual debilita la efectividad de las redes internacionales. Por ello, avanzar hacia estándares internacionales unificados y marcos de gobernanza digital que promuevan la transparencia, sin comprometer la soberanía nacional, constituye una prioridad inaplazable (Raymond & Smith, 2020).

Un ejemplo emblemático de cooperación en inteligencia cibernética es el Five Eyes Alliance, que agrupa a Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda. Esta alianza, originalmente concebida para el intercambio de inteligencia militar y de señales, ha extendido su cooperación al ámbito cibernético, lo cual facilita la detección y la neutralización de amenazas avanzadas (Rid & Buchanan, 2021). No obstante, la exclusividad de tales acuerdos plantea cuestionamientos sobre la equidad en la gobernanza global del ciberespacio, especialmente respecto de países del Sur Global que carecen de acceso a información crítica (Ramírez & Castañeda, 2021).

Por su parte, iniciativas multilaterales como la Global Forum on Cyber Expertise (GFCE) buscan democratizar el acceso a la información técnica, lo cual fomenta la cooperación inclusiva entre países con distintos niveles de madurez digital. Así, estas plataformas promueven la creación de marcos colaborativos que articulan la inteligencia técnica con la diplomacia digital, lo cual propicia una gobernanza del ciberespacio más equitativa y sostenible.

Operaciones conjuntas y respuesta colaborativa

Las operaciones conjuntas en ciberseguridad y ciberdefensa representan una evolución natural de la cooperación internacional ante amenazas cada vez más complejas y persistentes. Estas operaciones, que involucran tanto a fuerzas militares como a agencias civiles, se orientan hacia la prevención, la contención y la recuperación frente a incidentes de gran escala. Asimismo, se sustentan en la coordinación multinivel entre Estados y organizaciones internacionales (CCDCOE, 2022).

El principio de interoperabilidad operacional, definido por la OTAN como la capacidad de diferentes entidades de trabajar de manera coordinada mediante

estándares técnicos, doctrinales y procedimentales comunes, es esencial para el éxito de estas operaciones (NATO, 2023). Específicamente, esta interoperabilidad garantiza que las unidades de respuesta técnica, los equipos de ciberdefensa militar y los organismos de inteligencia puedan compartir información y ejecutar acciones sincronizadas ante amenazas comunes.

De acuerdo con Libicki (2020), las operaciones conjuntas en el ciberespacio no deben concebirse únicamente como una extensión del campo de batalla tradicional, sino como un dominio operativo independiente que requiere estrategias específicas de mando, control y atribución. En este sentido, la doctrina de "ciberdefensa activa", formulada por Nye (2014), plantea la necesidad de combinar medidas defensivas reactivas con acciones preventivas de detección avanzada, un enfoque que debe enmarcarse estrictamente en el Derecho Internacional Humanitario (DIH) y en la proporcionalidad en el uso de la fuerza.

Un caso paradigmático de cooperación operativa lo constituye el Ejercicio Locked Shields, liderado anualmente por el CCDCOE, en el cual participan más de treinta países aliados y socios de la OTAN. Este ejercicio simula ataques a infraestructuras críticas y busca mejorar la coordinación técnica, legal y estratégica entre las naciones participantes (CCDCOE, 2022). Al respecto cabe señalar que la efectividad de Locked Shields radica en su enfoque integral, que abarca desde la respuesta táctica hasta la gestión política de crisis e incorpora componentes jurídicos, comunicacionales y de relaciones internacionales.

Asimismo, la Unión Europea ha fortalecido sus capacidades mediante la creación del Joint Cyber Unit (JCU), con el propósito de coordinar respuestas ante incidentes transfronterizos y apoyar a los Estados miembros en situaciones de cibercrisis (European Commission, 2021). Este modelo de respuesta colaborativa combina los principios de subsidiariedad y solidaridad, fundamentales para una gobernanza digital de carácter regional.

En el ámbito latinoamericano, la OEA ha promovido la cooperación técnica entre países de la región a través del Comité Interamericano contra el Terrorismo (CICTE), con ejercicios conjuntos, centros de capacitación y redes de respuesta coordinada ante ciberincidentes (NATO CCDCOE, 2023). Estas iniciativas han contribuido al fortalecimiento institucional y al desarrollo de marcos de confianza digital entre los Estados miembros.

Sin embargo, las operaciones conjuntas enfrentan desafíos estructurales, principalmente vinculados con la atribución de ataques, la soberanía digital y la coordinación multinivel. Según Healey (2021), el problema de la atribución —es decir, la identificación fehaciente del responsable de un ataque— sigue siendo uno de

los principales obstáculos para la respuesta colectiva, pues la ambigüedad técnica puede desencadenar tensiones diplomáticas o respuestas desproporcionadas. De ahí la necesidad de contar con mecanismos de ciberdiplomacia operativa que sean capaces de canalizar la cooperación sin vulnerar la soberanía de los Estados.

Además, el surgimiento de alianzas cibernéticas asimétricas, donde los países con mayor capacidad técnica dominan los procesos de decisión, puede generar dependencia tecnológica y desigualdad en la cooperación (Maurer, 2020). Para evitarlo, la literatura especializada propone promover modelos inclusivos basados en la responsabilidad compartida y la equidad digital (Deibert, 2020).

En este contexto, las operaciones conjuntas público-privadas adquieren relevancia estratégica. Las empresas tecnológicas, proveedores de servicios digitales y operadores de infraestructuras críticas son actores fundamentales en la defensa cibernética colectiva. Así, iniciativas como el Microsoft Digital Crimes Unit o el Cybersecurity Tech Accord ilustran la contribución de la industria al desmantelamiento de redes delictivas globales, la cual se materializa mediante la cooperación con gobiernos y organismos multilaterales (Microsoft, 2023).

Según Carr (2021), la participación del sector privado en operaciones conjuntas requiere una gobernanza híbrida que articule mecanismos de coordinación técnica y política, con el fin de evitar que los intereses comerciales prevalezcan sobre la seguridad colectiva. En esa línea, marcos como el NIST Cybersecurity Framework (2022) y los principios de la Global Commission on the Stability of Cyberspace (GCSC, 2021) ofrecen directrices para fortalecer las alianzas operativas con criterios de transparencia, rendición de cuentas y resiliencia.

Desarrollo de capacidades y fortalecimiento institucional

El tercer pilar de la cooperación internacional en ciberseguridad se relaciona con el desarrollo de capacidades. Este concepto se define como el proceso mediante el cual los Estados adquieren, consolidan y modernizan sus competencias técnicas, institucionales y normativas para prevenir y responder eficazmente a las amenazas cibernéticas (UNIDIR, 2022).

De acuerdo con Klimburg (2019), la construcción de capacidades constituye el cimiento de una gobernanza digital inclusiva y sostenible, ya que permite reducir la brecha entre naciones tecnológicamente avanzadas y aquellas con limitaciones estructurales. Para materializar este objetivo, la cooperación multilateral debe orientarse hacia la transferencia de conocimiento, la formación de talento especializado y la armonización de políticas públicas.

El Global Cybersecurity Index (UIT, 2022) identifica cinco dimensiones esenciales del desarrollo de capacidades: 1) medidas legales, 2) técnicas, 3) organizativas, 4) de creación de capacidades y 5) de cooperación internacional. Estas categorías reflejan que la madurez cibernética de un Estado no depende exclusivamente de su infraestructura tecnológica, sino también de su gobernanza, de la articulación institucional y de su compromiso con la cooperación internacional.

Al respecto cabe señalar que la Unión Europea, a través de la ENISA y el programa Digital Europe, ha impulsado estrategias de fortalecimiento de capacidades orientadas a fomentar la investigación, el desarrollo de software seguro y la estandarización de prácticas de ciberhigiene (ENISA, 2023). Paralelamente, organismos como el Banco Mundial (2022) y el Fondo Monetario Internacional (2023) han integrado la ciberseguridad como componente transversal en los proyectos de desarrollo digital, lo cual ha puesto de manifiesto su impacto en la estabilidad económica y financiera global.

Específicamente en América Latina, el Centro de Estudios para la Ciberseguridad de la OEA (CICTE, 2023) ha promovido programas de asistencia técnica, los cuales incluyen el diseño de estrategias nacionales de ciberseguridad, la capacitación de CSIRT y la formulación de marcos regulatorios adaptados a la realidad regional. Estas iniciativas fortalecen la resiliencia institucional y contribuyen a consolidar una cultura de seguridad digital compartida.

En este escenario, la formación de talento humano especializado debe incluirse como una prioridad estratégica, para la cual instituciones como la European Cybersecurity Skills Framework (ECSF, 2022) o el Cybersecurity Workforce Framework (NICE, 2022) proporcionan marcos de referencia para la educación y certificación profesional en ciberseguridad. Estas iniciativas pretenden reducir la brecha de habilidades que, según WEF (2023), supera los tres millones de profesionales en todo el mundo.

Finalmente, el fortalecimiento institucional implica la creación de marcos nacionales de gobernanza digital, centros de excelencia y mecanismos de cooperación académica y científica, aspectos fundamentales, pues, como señala Dunn-Cavelty (2008), la resiliencia digital no depende únicamente de la tecnología, sino también de la integración entre políticas públicas, diplomacia digital y cultura organizacional. En ese sentido, los esfuerzos de cooperación deben ser sostenibles, inclusivos y orientados a largo plazo.

Desafíos y perspectivas futuras en ciberseguridad y ciberdefensa

Obstáculos estructurales de la cooperación internacional en ciberseguridad

La complejidad del ecosistema digital contemporáneo ha reconfigurado la naturaleza de los conflictos, lo cual ha desplazado las confrontaciones tradicionales hacia un entorno híbrido, difuso y persistentemente interconectado. En este marco, la cooperación internacional en ciberseguridad se enfrenta a una serie de desafíos estructurales que comprometen la estabilidad del ciberespacio y la efectividad de la gobernanza digital global (Clarke & Knake, 2020; Libicki, 2020). Dichos desafíos obedecen a brechas tecnológicas, tensiones geopolíticas, divergencias normativas y asimetrías institucionales entre Estados.

La ausencia de un marco jurídico global vinculante constituye una de las principales debilidades del actual régimen de gobernanza digital. Si bien existen instrumentos relevantes, como la Convención de Budapest sobre Ciberdelincuencia (Consejo de Europa, 2001) y las recomendaciones del *Manual 2.0 de Tallin* sobre la aplicación del derecho internacional en el ciberespacio (Schmitt, 2017), su alcance sigue siendo limitado, lo cual se debe a la falta de adhesión universal y a las diferencias en los sistemas legales nacionales.

Precisamente, el BID y la OEA (2021) sostienen que la diversidad legislativa en materia de protección de datos, privacidad y persecución de delitos informáticos genera espacios de impunidad digital, que son aprovechados por actores maliciosos para evadir responsabilidades. Esta fragmentación jurídica no solo obstaculiza la cooperación judicial transfronteriza, sino que también plantea dilemas sobre soberanía digital y la extraterritorialidad, especialmente cuando los ciberataques involucran infraestructuras distribuidas en múltiples jurisdicciones (Rid, 2020).

Según Chertoff y Simon (2019), la ausencia de un consenso claro en la definición de acto hostil o uso de la fuerza en el ciberespacio restringe la capacidad de respuesta colectiva conforme al derecho internacional. Esta ambigüedad normativa se traduce en vacíos operativos y políticos que favorecen la proliferación de ataques encubiertos, operaciones de desinformación y sabotaje digital sin consecuencias jurídicas proporcionales.

A su vez, la erosión de la confianza internacional representa otro obstáculo crítico para la cooperación en ciberseguridad. En un contexto dominado por la rivalidad entre potencias tecnológicas como Estados Unidos, China y Rusia, el

ciberespacio se ha convertido en un dominio de competencia estratégica, donde la información, los algoritmos y la infraestructura digital son instrumentos de poder y coerción (Nye, 2014).

La literatura especializada describe esta dinámica como una carrera armamentista digital, caracterizada por la proliferación de capacidades ofensivas, la militarización del ciberespacio y la creciente opacidad de las operaciones cibernéticas (Healey, 2021; Libicki, 2020). De acuerdo con Jervis y Healey (2022), la ausencia de mecanismos de transparencia y comunicación directa entre potencias nucleares con capacidades cibernéticas avanzadas incrementa el riesgo de escalamiento no intencionado, situación que podría desencadenar crisis internacionales con consecuencias impredecibles.

En este contexto, la ciberdiplomacia emerge como una herramienta indispensable para restablecer la confianza y evitar el deterioro del orden digital global. Desde esta perspectiva, Nye (2021) sugiere que la creación de canales de comunicación permanentes, la implementación de medidas de fomento de confianza (Confidence-Building Measures, CBMs) y la codificación de normas de comportamiento estatal son condiciones necesarias para reducir la incertidumbre estratégica y promover la estabilidad cooperativa.

Una variable adicional, la asimetría en el desarrollo tecnológico y en las capacidades institucionales entre los Estados, constituye un obstáculo estructural que amplifica la vulnerabilidad global. Mientras que las potencias cibernéticas invierten en inteligencia artificial defensiva, análisis avanzado de amenazas y automatización de la respuesta a incidentes, los países en desarrollo carecen de recursos técnicos y humanos para implementar políticas efectivas de ciberseguridad (He, Xie & Zhao, 2021).

Por lo tanto, la brecha de capacidades incrementa el riesgo individual de los Estados menos preparados y debilita la seguridad colectiva. Como plantea Nye (2021), "la ciberseguridad global es tan fuerte como su eslabón más débil" (s. p.). Los actores maliciosos, conscientes de esta asimetría, utilizan infraestructuras ubicadas en países con menor capacidad defensiva para lanzar operaciones transnacionales, lo cual dificulta la atribución y la cooperación judicial, como se señaló anteriormente.

La transferencia tecnológica, la formación de talento especializado y la asistencia técnica multilateral constituyen, por tanto, mecanismos esenciales para equilibrar las capacidades cibernéticas y evitar la concentración de poder digital en unas pocas naciones. En este sentido, programas promovidos por la Unión Internacional de Telecomunicaciones (UIT, 2022), el Banco Mundial (2022) y la

Organización de los Estados Americanos (2023) demuestran que el fortalecimiento institucional y la cooperación regional son instrumentos efectivos para cerrar la brecha de madurez cibernética.

Por otra parte, el dinamismo tecnológico del ciberespacio impone una tensión constante entre innovación y seguridad. En este contexto, las amenazas evolucionan a un ritmo que supera la capacidad de respuesta de la mayoría de los Estados y organizaciones, lo cual genera un entorno de vulnerabilidad estructural. Por ejemplo, las modalidades de ataque basadas en *ransomware as a service*, la explotación de vulnerabilidades en la cadena de suministro y la manipulación de sistemas mediante inteligencia artificial ofensiva evidencian el carácter adaptativo de las amenazas emergentes (ENISA, 2023).

La naturaleza exponencial de estas amenazas obliga a redefinir los modelos de defensa, lo que exige la priorización de la resiliencia organizacional, la anticipación basada en inteligencia cibernética y la automatización de la detección temprana. Por lo tanto, de acuerdo con Clarke y Knake (2020), la adaptabilidad se convierte en el nuevo criterio de supervivencia en el ecosistema digital. Entendida como la capacidad de absorber, resistir y recuperarse ante perturbaciones, la resiliencia debe ser considerada entonces como un principio rector de la gobernanza cibernética global.

Amenazas emergentes y direcciones futuras de la cooperación internacional

La naturaleza evolutiva y multifacética de las amenazas cibernéticas exige que la cooperación internacional adopte un enfoque prospectivo, multidimensional y adaptable. Las dinámicas de la digitalización global, la expansión de la inteligencia artificial, la computación cuántica y la convergencia entre dominios físico-digitales amplifican los riesgos estratégicos que enfrentan los Estados y las organizaciones internacionales (Kello, 2021; Liaropoulos, 2022). En este contexto, la gobernanza digital del futuro deberá trascender los enfoques reactivos y fragmentarios para avanzar hacia una arquitectura de seguridad colectiva digital sustentada en la confianza, la interoperabilidad y la ética tecnológica.

Así, la inteligencia artificial se erige como un aspecto decisivo que se debe considerar, dado que se ha consolidado como un factor de poder determinante en la configuración del orden internacional. Su capacidad para procesar grandes volúmenes de datos, detectar patrones anómalos y ejecutar acciones automatizadas redefine los paradigmas de defensa, vigilancia e inteligencia (Taddeo & Floridi, 2018). Sin embargo, su aplicación en el ámbito cibernético plantea dilemas éticos

y estratégicos complejos que deben ser abordados de manera conjunta, transdisciplinar e interinstitucional.

Por un lado, la inteligencia artificial potencia las capacidades de ciberdefensa proactiva, al permitir la predicción de amenazas y la respuesta automatizada ante incidentes. Por otro, su uso ofensivo introduce nuevas formas de desestabilización digital, como la generación de *malware* adaptativo o ataques de ingeniería social mediante *deepfakes* (Brundage et al., 2018; Horowitz, 2019).

En este sentido, autores como Müller (2020) y Singer y Friedman (2019) destacan la urgencia de establecer regímenes internacionales de control ético y técnico sobre la inteligencia artificial aplicada a la ciberseguridad. Desde esta perspectiva, la cooperación multilateral debe promover estándares de transparencia algorítmica, certificación de seguridad y mecanismos de auditoría internacional para prevenir abusos tecnológicos. Tal como sostiene Floridi (2021), el "humanismo digital" debe guiar las decisiones políticas y estratégicas que configuren la interacción entre inteligencia artificial, ciberdefensa y derechos fundamentales.

Adicional a ello, el desarrollo de operaciones híbridas, donde convergen tácticas cibernéticas, informacionales y psicológicas, ha desplazado el epicentro de la confrontación hacia el dominio cognitivo. En este contexto, las campañas de desinformación, manipulación algorítmica y operaciones de influencia en redes sociales constituyen actualmente una de las formas más efectivas de injerencia estratégica (Singer & Brooking, 2018; Rid, 2020).

Precisamente, la OTAN (2022) ha reconocido el dominio cognitivo como un nuevo espacio operativo en el que la mente humana se convierte en el objetivo principal. Por consiguiente, la cooperación internacional en ciberseguridad debe ampliar su alcance para incluir la seguridad informacional y la alfabetización digital crítica como pilares de la defensa colectiva.

De hecho, Taddeo (2020) sostiene que el control de la información y la manipulación de narrativas constituyen amenazas tan graves como los ataques técnicos a infraestructuras críticas. Por ello, de forma similar al CCDCOE, la creación de centros multinacionales de respuesta informacional se proyecta como una estrategia necesaria para mitigar los efectos de la desinformación transnacional. Asimismo, la promoción de normas éticas sobre el uso de datos, la moderación algorítmica y la protección de la libertad de expresión en entornos digitales será clave para preservar la integridad democrática frente a la manipulación cognitiva (Morozov, 2022).

En virtud de esto, es menester mencionar la tensión entre globalización tecnológica y soberanía digital, como uno de los dilemas geopolíticos más relevantes

del siglo XXI. Específicamente, los Estados buscan garantizar el control sobre sus datos, infraestructuras críticas y flujos de información, mientras que las corporaciones tecnológicas transnacionales consolidan posiciones de poder sin precedentes (Bradshaw, DeNardis & Raymond, 2020).

Al respecto, De-Nardis (2021) advierte que la gobernanza digital se encuentra en un punto de inflexión ya que la privatización de funciones tradicionalmente estatales como la regulación del ciberespacio, la gestión de dominios o la supervisión de contenidos ha generado un régimen de poder asimétrico, donde la autoridad se ve subordinada a los intereses corporativos. En este contexto, la cooperación internacional debe reconfigurarse hacia modelos multiactor y policéntricos que integren a Estados, organizaciones internacionales, el sector privado, la academia y la sociedad civil en la definición de estándares, normas y principios de gobernanza digital (Mueller, 2019). Para evitar la fragmentación del ciberespacio en silos digitales incompatibles, será determinante la consolidación de un marco de gobernanza distribuida, el cual debe sustentarse en la transparencia, la rendición de cuentas y el respeto por los Derechos Humanos (Bendrath, 2022).

En este marco, la cooperación internacional en ciberseguridad se encuentra en una encrucijada histórica, de manera que frente a un entorno de amenazas convergentes y tecnologías exponenciales, el futuro dependerá de la capacidad colectiva para institucionalizar la confianza digital y la resiliencia global (Clarke & Knake, 2020). En esta línea, la ONU (2023) ha impulsado iniciativas como el Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG), que busca construir consensos normativos sobre el comportamiento responsable de los Estados en el ciberespacio.

Además, organismos como la OTAN, la Unión Europea y la OEA avanzan en la creación de marcos de cooperación multinivel que integran defensa, diplomacia y desarrollo tecnológico. No obstante, el desafío primordial radica en asegurar la inclusión global de los países con menor madurez cibernética, con el fin de evitar la consolidación de un orden digital excluyente.

En conclusión, la ciberseguridad se ha consolidado como una dimensión estructural de la seguridad global y del desarrollo sostenible de los Estados. En un mundo profundamente interconectado, donde los flujos de información, los sistemas críticos y las infraestructuras digitales trascienden las fronteras, la cooperación internacional ya no es una mera opción política, sino que se ha convertido en una condición indispensable para la viabilidad del orden internacional contemporáneo. La gobernanza del ciberespacio, en consecuencia, se erige como un

proyecto civilizatorio que busca equilibrar poder, soberanía, innovación y Derechos Humanos en un entorno caracterizado por la volatilidad tecnológica y la interdependencia sistémica.

Conclusiones

A lo largo del análisis, se ha evidenciado que los fundamentos de la cooperación internacional en ciberseguridad descansan en tres ejes interdependientes, como son la confianza digital, la armonización normativa y la solidaridad tecnológica. El primero de estos ejes supone el establecimiento de mecanismos transparentes para el intercambio de información y la atribución responsable de incidentes. El segundo implica la convergencia jurídica necesaria para reducir las asimetrías regulatorias que obstaculizan la persecución del cibercrimen. Por último, el tercero se centra en la reducción de la brecha de capacidades entre Estados, lo cual se logra mediante la transferencia de conocimiento, la asistencia técnica y la formación especializada.

Los mecanismos institucionales existentes, como la Convención de Budapest, el *Tallinn Manual,* los grupos de expertos gubernamentales (GGE) y el OEWG de Naciones Unidas, han constituido avances significativos hacia la construcción de un marco normativo internacional. No obstante, la eficacia de dichos instrumentos sigue condicionada por la fragmentación geopolítica y la falta de mecanismos de cumplimiento vinculante. Las tensiones entre soberanía digital y globalización tecnológica continúan, lo cual genera un escenario de competencia cibernética que amenaza la estabilidad estratégica, particularmente entre potencias emergentes y tradicionales.

El segundo eje analizado con referencia a los modelos de cooperación regional y multilateral revela que la integración de políticas y capacidades digitales entre Estados puede convertirse en un catalizador de resiliencia. La coordinación interinstitucional es un medio eficaz para gestionar amenazas compartidas, lo cual se evidencia en iniciativas como la Estrategia de Ciberseguridad de la Unión Europea, la Red Iberoamericana de Ciberseguridad (CSIRT Americas) de la OEA y la cooperación en el marco de la OTAN. Sin embargo, esta cooperación debe trascender el plano técnico y adoptar una visión integral que incorpore la diplomacia cibernética, la gobernanza ética de los datos y la sostenibilidad digital como pilares de la seguridad colectiva.

El análisis prospectivo desarrollado en la última sección destaca que la cooperación internacional enfrentará desafíos futuros en cuatro grandes dimensiones:

tecnológica, normativa, cognitiva y ambiental. La irrupción de tecnologías emergentes como la inteligencia artificial, la computación cuántica y el IoT redefine las vulnerabilidades y amplía la superficie de exposición de los sistemas globales. Frente a ello, la cooperación multilateral debe orientarse a la creación de estándares interoperables y criptografía poscuántica, así como al desarrollo de marcos de auditoría algorítmica y ética de la inteligencia artificial.

En el ámbito normativo, la consolidación de un derecho internacional del ciberespacio sigue siendo una tarea inacabada, dado que los intentos por codificar normas de comportamiento estatal enfrentan la resistencia de actores que priorizan su autonomía estratégica sobre la seguridad colectiva. Ante este escenario, la ciberdiplomacia emerge como un instrumento esencial para construir confianza mutua, prevenir conflictos y promover la cooperación operativa entre Estados, organismos internacionales y el sector privado.

La dimensión cognitiva, por su parte, refleja un cambio de paradigma, el cual implica que la seguridad ya no se limita a la protección de infraestructuras, sino que abarca la integridad informacional y psicológica de las sociedades. Las operaciones de desinformación y manipulación digital, amplificadas por algoritmos y redes sociales, constituyen un desafío a la soberanía cultural y democrática. En este escenario, la alfabetización digital crítica y la cooperación informacional internacional se vuelven herramientas indispensables para fortalecer la resiliencia cognitiva global.

Finalmente, la dimensión ambiental, con sus elementos inherentes, introduce un componente emergente en la discusión sobre ciberseguridad: la sostenibilidad digital. La infraestructura tecnológica mundial (centros de datos, redes 5G y minería de criptomonedas) tiene una huella ecológica significativa que no puede ignorarse. Incorporar criterios de eficiencia energética, economía circular y "seguridad verde" en las estrategias de ciberdefensa será fundamental para alinear la seguridad digital con los Objetivos de Desarrollo Sostenible (ODS), en particular los ODS 9 y 13.

En síntesis, la cooperación internacional en ciberseguridad y gobernanza digital debe evolucionar hacia una arquitectura global de seguridad digital inclusiva, ética y sostenible. Este modelo se construye con normas o tecnología, en el cual la voluntad política, la confianza recíproca y una visión compartida de futuro deben estar presentes. En este sentido, los Estados, las organizaciones internacionales y la sociedad civil deben converger en torno a una gobernanza cibernética basada en la corresponsabilidad, la transparencia y el respeto por los Derechos Humanos en el entorno digital.

En este escenario, la consolidación de un ciberespacio seguro, resiliente y equitativo, que contribuya al mantenimiento de la paz, la justicia y el desarrollo sostenible, solo será posible a través de la articulación de esfuerzos multilaterales y el fortalecimiento de capacidades colectivas. La ciberseguridad, entendida desde una perspectiva cooperativa y global, no es únicamente una política de defensa, sino un bien público internacional, indispensable para la estabilidad, la confianza y la prosperidad en la era digital.

Referencias

Andress, J., & Winterfeld, S. (2019). *Cyber warfare: Techniques, tactics and tools for security practitioners* (2nd ed.). Syngress.

Banco Interamericano de Desarrollo [BID], & Organización de los Estados Americanos [OEA]. (2020). *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe*. http://dx.doi.org/10.18235/0002513

Betz, D. J., & Stevens, T. (2018). *Cyberpower and national security.* Johns Hopkins University Press.

Carr, M. (2017). *Inside cyber warfare: Mapping the cyber underworld.* O'Reilly Media.

Chertoff, M., & Simon, T. (2019). *The impact of the dark web on internet governance and cybersecurity.* Center for Strategic and International Studies. https://www.cigionline.org/static/documents/gcig_paper_no6.pdf

Clarke, R. A., & Knake, R. (2020). *The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats.* Penguin Press.

Council of Europe. (2001). *Convention on cybercrime (Budapest Convention).* Council of Europe. https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf

Deibert, R. J. (2020). *Reset: Reclaiming the internet for civil society.* House of Anansi Press.

DeNardis, L. (2020). *The internet in everything: Freedom and security in a world with no off switch.* Yale University Press.

Dunn Cavelty, M. (2008). *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age.* Routledge.

European Commission. (2021). *EU cybersecurity strategy for the digital decade*. European Commission. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Commission. (2023). *Directive (EU) 2022/2555 (NIS2): Directive on measures for high common level of cybersecurity*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

European Union Agency for Cybersecurity [ENISA]. (2023). *ENISA threat landscape 2023.* ENISA. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf

Finnemore, M., & Hollis, D. (2020). Constructing norms for global cybersecurity. *American Journal of International Law, 110*(3), 425–479. https://www.iilj.org/wp-content/uploads/2017/01/Finnemore-Hollis-Constructing-Norms-for-Global-Cybersecurity.pdf

Floridi, L. (2020). *The ethics of information and digital governance.* Oxford University Press.

Foro Económico Mundial. (2022). *Global cybersecurity outlook 2022.* WEF. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

Garde, S., & Dorr, S. (2022). *Zero trust architectures for cyber resilience.* National Institute of Standards and Technology (NIST).

Global Enabling Sustainability Initiative [GeSI]. (2021). *Digital with purpose: Delivering a smarter 2030*. GeSi. https://www.gesi.org/public-resources/digital-with-purpose-report-delivering-a-smarter-2030/

Healey, J. (2021). *A fierce domain: Cyber conflict, 1986 to 2012*. Cyber Conflict Studies Association.

International Telecommunication Union [ITU]. (2022). *Global cybersecurity agenda: Building digital trust*. ITU Publications.

Janczewski, L., & Colarik, A. (2019). *Cyber warfare and cyber terrorism*. IGI Global.

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

Keohane, R. O., & Nye, J. S. (2001). *Power and interdependence* (3rd ed.). Longman.

Klimburg, A. (2019). *The darkening web: The war for cyberspace*. Penguin Books.

Libicki, M. C. (2020). *Cyberspace in peace and war* (2nd ed.). Naval Institute Press.

Maurer, T. (2022). *Cyber mercenaries: The state, hackers, and power*. Cambridge University Press.

Microsoft Security Intelligence. (2023). *Zero trust adoption report 2023*. Microsoft.

NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE]. (2023). *Locked Shields: Lessons learned 2023*. CCDCOE. https://ccdcoe.org/locked-shields/

Nye, J. S. (2014). The regime complex for managing global cyber activities. Global Com-mission on Internet Governance. https://tinyurl.com/2tuhyr4b

Office of the Director of National Intelligence [ODNI]. (2022). *Annual threat assessment of the U.S. intelligence community*. ODNI. https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2022/3597-2022-annual-threat-assessment-of-the-u-s-intelligence-community

Pomerantsev, P. (2020). *This is not propaganda: Adventures in the war against reality*. PublicAffairs.

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

Singer, P. W., & Friedman, A. (2020). *Cybersecurity and cyberwar: What everyone needs to know* (2nd ed.). Oxford University Press.

United Nations Office for Disarmament Affairs. (2021). *Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security*. United Nations.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

EDITORIAL ESDEG

Epílogo

Legado, prospectiva y llamado a la acción*

Angélica María González González[1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Una obra que nace de la urgencia nacional

Al llegar a estas páginas finales, el lector ha recorrido un itinerario intelectual de relevancia para el presente y el futuro de Colombia. En este sentido, se reitera que los capítulos que conforman esta obra no son reflexiones aisladas, sino piezas de un mismo mosaico que retrata, con franqueza y rigor, el estado de la transformación digital y la ciberseguridad en los sectores más relevantes de la nación. Desde el diagnóstico normativo de la gobernanza digital hasta las propuestas concretas de fortalecimiento institucional, esta colección es, ante todo, una respuesta académica a un imperativo estratégico. Como señala el Consejo Nacional de Política Económica y Social en el CONPES 3995 (2020), la seguridad digital dejó de ser una opción técnica para convertirse en una condición estructural del desarrollo nacional.

Colombia ocupa hoy una posición compleja en el ecosistema digital global: avanza con decisión hacia la digitalización de sus servicios públicos y privados, pero enfrenta simultáneamente un entorno de amenazas que evoluciona más rápido que sus marcos normativos y sus capacidades de respuesta. De hecho, el Global Cybersecurity Index 2024 de la Unión Internacional de Telecomunicaciones ubica a Colombia en un nivel de compromiso considerable, pero también identifica brechas estructurales en la implementación técnica y en la cultura organizacional de la ciberseguridad. Esta obra aborda precisamente esas brechas, con la convicción de que nombrarlas es el primer paso para superarlas.

[1] Gestora académica de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto". Magíster en Estrategia y Geopolítica, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Politóloga con Énfasis en Seguridad, Paz y Conflicto, Universidad del Rosario, Colombia. **https://orcid.org/0000-0003-0881-5530** - Contacto: **angelica.gonzalez@esdeg.edu.co.**

Las lecciones transversales de los capítulos

La lectura integral de esta obra revela varias conclusiones que atraviesan todos los capítulos con una coherencia reveladora; la primera es que la gobernanza digital y la ciberseguridad son inseparables. Como demostró la CR. Milena Realpe en el capítulo inaugural, sustentada en los datos del estudio sectorial de Amazon Web Services (2024), Colombia presenta disparidades significativas entre sectores en cuanto a su preparación digital: mientras algunos avanzan hacia estándares internacionales, otros (incluyendo partes del sector salud y el universitario) permanecen con vulnerabilidades críticas sin resolver.

La segunda lección transversal es que el factor humano es el determinante más subestimado de la ciberseguridad. El capítulo de Tatiana Sánchez sobre el *"firewall humano"* demostró, apoyándose en referentes internacionales de formación, que los programas de capacitación no son un lujo organizacional, sino una necesidad operativa para cualquier entidad con infraestructura crítica. Esta tesis es respaldada por el *Global Cybersecurity Outlook 2024* del Foro Económico Mundial, que identifica el error humano como el vector de entrada en más del 80 % de los incidentes cibernéticos reportados a nivel global.

La tercera lección es que ningún sector puede construir resiliencia digital en aislamiento. Los capítulos dedicados a la cooperación internacional, desarrollados por Mónica Flórez, evidenciaron que Colombia necesita profundizar su participación en los marcos multilaterales de ciberseguridad, como los promovidos por la Organización de los Estados Americanos (BID & OEA, 2020) y la Oficina de las Naciones Unidas para Asuntos de Desarme (UNODA, 2023), que han establecido normas de comportamiento responsable de los Estados en el ciberespacio. La diplomacia digital no es una opción secundaria; es una extensión natural de la política exterior de un país que aspira a ser referente regional en gobernanza digital.

Los sectores críticos: aprendizajes específicos

El análisis del sector defensa, desarrollado por Ana Catalina Cano y Cristian Mauricio Toro Mora, pone de relieve que las Fuerzas Militares colombianas enfrentan un teatro de operaciones que se ha extendido irreversiblemente al ciberespacio. El Ministerio de Defensa Nacional de Colombia reconoce en su Política Marco de Ciberseguridad y Ciberdefensa que el Comando Conjunto Cibernético requiere no solo de tecnología de punta, sino de una doctrina actualizada y de estructuras

de gobernanza que permitan respuestas ágiles y coordinadas ante amenazas híbridas. En este sentido, cabe enfatizar que los autores han contribuido a esa doctrina desde la investigación, de manera que sus hallazgos deben ser incorporados como insumo para la toma de decisiones estratégicas.

En el sector salud, Miguel Amaya demostró que la implementación de inteligencia artificial en ciberseguridad no es un horizonte lejano, sino una realidad emergente con resultados medibles. Sin embargo, la madurez de esa implementación en Colombia todavía es dispar. Si bien el Ministerio de Salud y Protección Social ha avanzado en la definición de estándares de seguridad digital para el sector, la brecha entre la norma y la práctica institucional sigue siendo significativa. En este sentido, el capítulo ofrece a los administradores hospitalarios, a los formuladores de política pública y a los investigadores una radiografía precisa de esa brecha y una hoja de ruta para reducirla.

Por su parte, el sector universitario, analizado por Jeison Melo, emerge como un caso particularmente urgente. Las instituciones de educación superior colombianas no solo custodian datos sensibles de miles de personas, sino que son el semillero del talento en ciberseguridad que el país necesita. Precisamente, la Agenda de Investigación e Innovación en Ciberseguridad 2023-2030 de MinCiencias señala que Colombia enfrenta un déficit estructural de profesionales especializados en este campo. Sin embargo, fortalecer la ciberseguridad en las universidades no es solo proteger sus redes: es proteger y potenciar el ecosistema de innovación que forjará la próxima generación de defensores del ciberespacio colombiano. Por lo tanto, se debe plantear con firmeza:

La ciberseguridad no es un destino al que se llega; es una práctica continua, colectiva y nunca acabada. Cada investigador que publica, cada profesional que se forma y cada institución que adopta una política de seguridad digital suma a la defensa de la nación.

El papel transformador de la investigación académica

Uno de los mensajes más poderosos que emerge de esta obra es que la investigación académica en ciberseguridad no es un ejercicio intelectual de gabinete: es una actividad con consecuencias directas sobre la seguridad de los ciudadanos, la continuidad de los servicios esenciales y la soberanía del Estado. De hecho, se ha documentado cómo los ataques a infraestructura crítica en Colombia han crecido

en frecuencia y sofisticación, y cómo las instituciones más vulnerables son aquellas que no cuentan con investigación actualizada que informe sus protocolos de protección.

Además, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) señala en su *Threat Landscape Report 2023* que las organizaciones con programas activos de investigación en ciberseguridad registran tiempos de detección y respuesta hasta cuatro veces menores que aquellas que no los tienen. Este dato no es menor: en el contexto de un ataque a infraestructura crítica, cada minuto de diferencia puede significar vidas humanas, continuidad de servicios o integridad de datos irreemplazables. La academia, en este sentido, no es un observador del problema de la ciberseguridad, sino uno de sus actores protagónicos.

En este contexto, aunque el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC (2022) representa un avance normativo significativo para el sector público colombiano, su efectividad depende directamente de que exista una comunidad académica y profesional capaz de interpretarlo, aplicarlo, evaluarlo y mejorarlo. Los autores de esta obra forman parte de esa comunidad, y su trabajo es una demostración de lo que es posible cuando la investigación y la práctica institucional conversan entre sí.

Una invitación activa: usted es parte de esta historia

Este epílogo no puede cerrar como un punto final, porque la transformación digital y la ciberseguridad son, por definición, procesos inacabados. Lo que este libro ha hecho es trazar coordenadas: ha identificado dónde estamos, ha señalado hacia dónde debemos ir y ha propuesto algunos de los caminos para llegar. Pero la travesía requiere muchos más viajeros comprometidos.

A los investigadores y académicos: los capítulos aquí presentados son puntos de partida, no de llegada. Cada hallazgo es una puerta abierta a nuevas preguntas. ¿Cómo evoluciona la madurez en inteligencia artificial aplicada a ciberseguridad en el sector salud en los próximos cinco años? ¿Qué nuevos modelos de cooperación internacional requiere Colombia dado el surgimiento de amenazas estatales en el ciberespacio? ¿Cuál es el impacto medible de los programas de formación del *"firewall humano"* en la reducción de incidentes? Estas son algunas de las preguntas que esta obra lanza al aire y que esperan ser recogidas por la próxima generación de investigadores. En este sentido, como argumentan diversos trabajos, Colombia

necesita con urgencia una masa crítica de investigación aplicada que informe sus políticas de gobernanza digital desde evidencia robusta y contextualizada.

A los profesionales del sector tecnológico, la seguridad y la defensa: la lectura de esta obra debe traducirse en acción. Los marcos, modelos y recomendaciones aquí propuestos no están destinados a permanecer en estantes. Están diseñados para ser implementados, piloteados, ajustados y escalados. Cada política de seguridad que adopten, cada protocolo de respuesta a incidentes que actualicen, cada programa de formación que diseñen a partir de estas páginas es una contribución directa a la resiliencia digital de Colombia.

A los tomadores de decisiones y formuladores de política pública: las recomendaciones que condensan las conclusiones de esta obra merecen ser incorporadas en los planes sectoriales, en las agendas legislativas y en los presupuestos de inversión en ciberseguridad. La actualización del CONPES 3995 y el fortalecimiento del ecosistema nacional de ciberseguridad son tareas que requieren del liderazgo político tanto como del rigor técnico.

A los estudiantes y jóvenes profesionales: ustedes son el argumento más poderoso de esta obra. La brecha de talento en ciberseguridad que documenta MinCiencias (2023) no es una amenaza abstracta: es una oportunidad extraordinaria para quienes estén dispuestos a formarse con rigor y con vocación de servicio público. El país los necesita, y los necesita ahora.

El futuro que podemos construir

Colombia tiene ante sí una ventana de oportunidad que no debe desaprovecharse, las condiciones están dadas: existe una política nacional de seguridad digital, hay una comunidad académica y profesional comprometida, el sector privado muestra una creciente conciencia sobre la importancia de la ciberseguridad y las Fuerzas Militares han dado pasos firmes hacia la consolidación del ciberdominio como eje de la defensa nacional. Lo que falta, y lo que esta obra contribuye a construir, es la articulación sostenida y sinérgica de todos esos esfuerzos en torno a una visión compartida.

Esa visión es la de una Colombia digitalmente soberana, cibernéticamente resiliente y académicamente activa en la frontera del conocimiento sobre transformación digital y ciberseguridad. No es una utopía: es el resultado lógico de mantener el ritmo y la dirección que esta obra representa. El *Informe de Ciberseguridad en América Latina y el Caribe* de la OEA (2023) señala que los países que logran articular investigación, política pública y capacidad operativa alcanzan niveles de

resiliencia digital que los posicionan como referentes regionales. Colombia puede y debe ser uno de esos países.

Que estas páginas no sean el final de su viaje, sino el mapa que lo orienta. La ciberseguridad de Colombia necesita su inteligencia, su compromiso y su acción. El momento es ahora, y el lugar es aquí.

La Escuela Superior de Guerra "General Rafel Reyes Prieto" y los autores de esta obra agradecen al lector haber llegado hasta estas líneas. Su lectura y pensamiento crítico y su disposición a actuar son el mejor fruto que este trabajo pudo haber esperado. Bienvenido a la comunidad de quienes trabajan por la seguridad digital de Colombia. El camino continúa.

Referencias

Amazon Web Services [AWS]. (2024). *Guía estratégica para mejorar la postura de ciberseguridad: Colombia.* Presidencia de la República de Colombia.

Consejo Nacional de Política Económica y Social (CONPES). (2020). Política Nacional de Confianza y Seguridad Digital. CONPES 3995. Departamento Nacional de Planeación de Colombia. https://colaboracion.dnp.gov.co/cdt/Conpes/Econ%C3%B3micos/3995.pdf

European Union Agency for Cybersecurity [ENISA]. (2023). *ENISA threat landscape 2023.* ENISA. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf

International Telecommunication Union [ITU]. (2024). *Global Cybersecurity Index 2024.* United Nations. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]. (2022). Modelo de Seguridad y Privacidad de la Información (MSPI) — versión 4.0. MinTic. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

Banco Interamericano de Desarrollo [BID] & Organización de los Estados Americanos [OEA]. (2020). Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe. https://tinyurl.com/2tw6a8at

United Nations Office for Disarmament Affairs [UNODA]. (2023). Developments in the Field of Information and Telecommunications in the Context of International Security. United Nations. https://disarmament.unoda.org/en/our-work/emerging-challenges/developments-field-information-and-telecommunications-context

World Economic Forum (WEF). (2024). Global Cybersecurity Outlook 2024. WFM. https://www.weforum.org/reports/global-cybersecurity-outlook-2024

EDITORIAL ESDEG

Transformación digital y ciberseguridad en Colombia: desafíos estratégicos para sectores de infraestructura crítica

La transformación del dominio digital ha permeado los sectores de la vida nacional del Estado colombiano generando oportunidades, pero también exponiendo vulnerabilidades que actores hostiles están dispuestos a explotar. La magnitud del desafío exige respuestas igualmente ambiciosas: políticas públicas robustas, marcos normativos actualizados, talento humano especializado y una cultura organizacional orientada a la seguridad y, en especial, a la defensa.

Este libro nace de la confluencia de distintos campos del conocimiento e investigadores multidisciplinares, como una contribución deliberada a la construcción de un ecosistema de ciberseguridad que Colombia necesita con urgencia. Desde los fundamentos de la gobernanza digital hasta la cooperación internacional; desde el análisis del sector salud hasta la formación del talento humano como primer escudo de defensa; la obra ofrece una mirada profunda sobre los retos que enfrenta el país.

EDITORIAL **ESDEG**

ISBN 978-628-7818-63-7

9 786287 818637