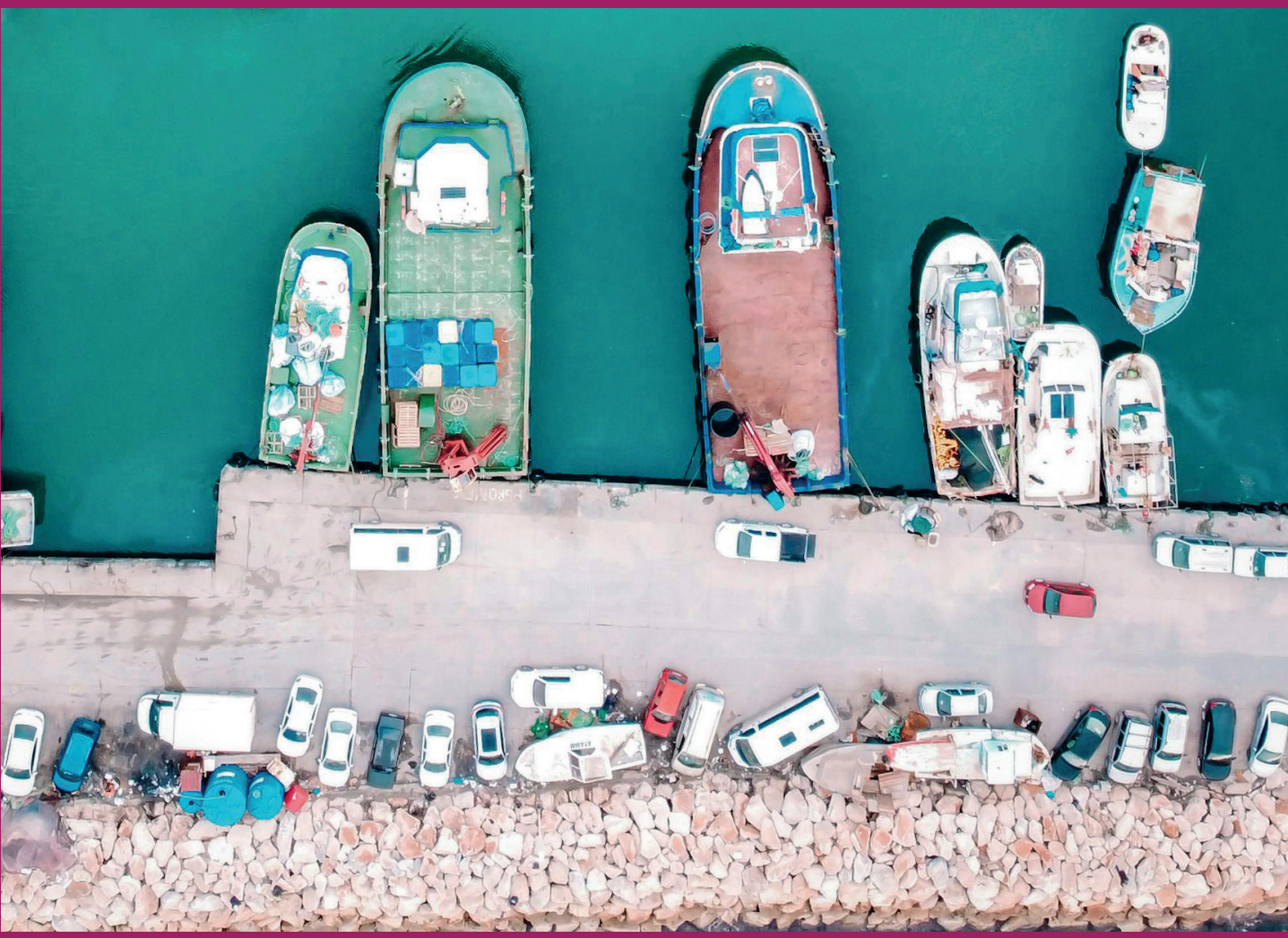


Misceláneos

doi.org/10.17141/urvio.45.2026.6456

URVIO, Revista Latinoamericana de Estudios de Seguridad, No. 45, mayo-agosto 2026
pp.99-118 • RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea) y 1390-3691

Contexto de la ciberseguridad y ciberdefensa en Latinoamérica y el Ecuador

The Context of Cybersecurity and Cyberdefense in Latin America and Ecuador

Luis-Patricio Vallejo-Rosero[1]

Recibido: 7 de enero de 2025
Aceptado: 24 de abril de 2025
Publicado: 31 de mayo de 2026

Resumen

Introducción: el trabajo contextualiza la ciberseguridad y la ciberdefensa en el ámbito latinoamericano, basándose en instrumentos proporcionados por organismos multilaterales, tendencias de algunos países e índices internacionales. **Objetivo:** contribuir al mejor entendimiento de estos temas y evidenciar los desafíos que enfrentan los Estados en el ciberespacio. Además, analizar la actuación de Ecuador en este ámbito, contrastándola brevemente con las referencias emitidas por las Naciones Unidas (ONU), la Organización de Estados Americanos (OEA) y la Junta Interamericana de Defensa (JID), para determinar su adherencia a las tendencias globales y regionales. Finalmente, identificar y analizar los niveles alcanzados por Ecuador en indicadores estandarizados como el Índice Nacional de Ciberseguridad (NCSI), el Índice Global de Ciberseguridad (GCI) y estudios de vulnerabilidades en el ciberespacio. **Metodología:** tiene un enfoque cualitativo con alcance explicativo de la política pública de ciberseguridad y ciberdefensa, complementado con un rastreo de procesos del marco normativo referencial, y la interpretación para analizar los resultados de los índices. **Conclusiones:** el trabajo permite concluir que la ciberseguridad y ciberdefensa en Ecuador cuenta con los lineamientos constitucionales, legales, organizativos y doctrinales en línea con las mejores prácticas internacionales, y que existen oportunidades de mejora técnica operativa para la ciberresiliencia ecuatoriana.

Palabras clave: ciberdefensa; ciberresiliencia; ciberseguridad; índices; información; seguridad

Abstract

Introduction: this paper provides a cybersecurity and cyberdefense in Latin America, according to multilateral organizations instruments, countries trends, and international index. Objective: the aim of this work is to contribute to the best understanding of cybersecurity and cyberdefense and highlight the challenges faced by states in the cyberspace. Furthermore, an analysis of Ecuador's actions in this field is made, and briefly contrasting them with the suggestions issued by the United Nations (UN), the Organization of American States (OAS), and the Inter-American Defense Board (IADB), in order to identify Ecuador's convergence with the global and regional trends. Finally, the levels achieved by Ecuador in standardized index such as the National Cybersecurity Index (NCSI), Global Cybersecurity Index (GCI), and vulnerability studies are identifying and analyzed. Methodology: the methodology has a qualitative approach and explanatory fucus of cybersecurity and cyber defense public policy, complemented by a process monitoring of applicable legislation and regulations; and the interpretation of indexes results. Conclusions: the findings not only allow to conclude that cybersecurity and cyber defense frameworks in Ecuador have constitutional, legal, organizational, and doctrinal are aligned with international best practices; but also, provides insights into of technical and operational opportunities for improving Ecuador's cyber resilience.

Keywords: cyberdefense; cyber resilience; cybersecurity; index; information; security

1 Fuerza Aérea Ecuatoriana, Ecuador, patriciovallejor@yahoo.com, orcid.org/0000-0002-7197-3948

Introducción

Actualmente los Estados dependen en gran medida del sector digital, y una cantidad innumerable de sus procesos se ejecuta en el ciberespacio, dimensión en la cual infraestructura física, lógica e interacciones humanas se combinan de maneras casi incalculables. La utilización cada vez mayor del internet y de las tecnologías cibernéticas es el resultado del rápido crecimiento de las tecnologías de la información y las comunicaciones (TIC), así como de la transformación digital mundial (Eriksson y Giacomello 2022). Los ciudadanos, las organizaciones y los gobiernos son los principales usuarios o actores del ciberespacio. La creciente popularidad de la computación en la nube, el internet de las cosas (IoT) y los teléfonos inteligentes ha dado lugar a un nuevo ecosistema de interacción entre humanos y tecnología (Lippert y Cloutier 2021). Este ecosistema digital incrementa la preocupación de los gobiernos y sector privado sobre qué tan seguro es su ciberespacio y los retos que deben enfrentar para mejorar sus políticas públicas frente a esta realidad.

Los ciberataques a Estonia (Carmichael 2025; McGuinness 2017), al Ministerio de Hacienda de Costa Rica (Unidad de Comunicación Institucional 2023), a la Fiscalía General de Colombia (O'Brien 2023), a servidores de correo electrónico Microsoft Exchange (Equipo de seguridad de Microsoft 2021), además de la ciberguerra entre Rusia y Ucrania (Tidy 2023) evidencian que el riesgo cibernético afecta a gobiernos y organizaciones independientemente de su ubicación geográfica, sector o tamaño (Carr 2016). En consecuencia, quienes elaboran las políticas públicas deben apoyar a las organizaciones a instaurar controles de seguridad y toma de decisiones basadas en riesgos (Woods y Seymour 2023), pues el cibercrimen puede poner en peligro la seguridad nacional debido a la progresiva frecuencia y sofisticación de los ciberataques a grupos públicos (Perera et al. 2022). En tal sentido, es fundamental asegurar y defender el ciberespacio de manera decisiva con políticas bien establecidas e identificar los riesgos críticos de la ciberseguridad, para diseñar una política integral (Mishra et al. 2022) con procedimientos *antihacking* (Georgiadou et al. 2021).

En este contexto, resulta de especial interés comprender los desafíos que enfrentan los Estados en el ciberespacio, así como analizar la actuación de Ecuador en este ámbito y contrastarla con las referencias de la Organización de las Naciones Unidas (ONU), la Organización de los Estados Americanos (OEA) y la Junta Interamericana de Defensa (JID). El objetivo es evaluar cómo se alinea con las tendencias regionales e identificar los niveles alcanzados por el país en indicadores estandarizados de ciberseguridad y estudios de vulnerabilidad.

Marco teórico

El trabajo se enmarca en un campo complejo, novedoso y de actualidad: el ciberespacio y su explotación, por lo que es necesario aportar con ciertas conceptualizaciones y definiciones fundamentales para la investigación. Primero, se puede hablar de *seguridad informática*,

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 45 • mayo-agosto 2026 • pp.99-118
ISSN 1390-4299 (en línea) y 1390-3691

definida por Duffany (2018) como los mecanismos para proteger los sistemas informáticos del acceso no autorizado, robo, daño e interrupción de los servicios. Las amenazas pueden ser internas como externas. Fallas en un programa de software o en el sistema operativo son ejemplos de amenazas internas, mientras que un acceso no autorizado o error humano son amenazas externas. Para ampliar el alcance, Nobrega, Rutkowski y Saunders (2024) proponen que, basada en la ciberseguridad y la ciencia militar, la red de ciberdefensa está compuesta de ataques, objetivos, vulnerabilidades, cargas útiles, atacantes, defensores, taxonomías/marcos y contramedidas.

Raiyn (2014) clasificó los ataques cibernéticos en cinco clases: 1) denegación de servicio (DoS), que sobrecarga la memoria de los sistemas informáticos de tal forma que los accesos autorizados no puedan ser atendidos. 2) Remoto a local (R2L), que consiste en enviar paquetes de información a un servidor local para acceder ilegalmente a un sistema aprovechando sus vulnerabilidades. 3) Usuario a raíz (U2R), que trata de acceder a la raíz a través de un usuario sin privilegios para este acceso. 4) Ataques de sondeo, que escanean la red para obtener información como direcciones IP o vulnerabilidades. 5) Amenazas persistentes avanzadas (APT), que consisten en ataques con múltiples herramientas y procesos de piratería planificados y ejecutados en un largo periodo de tiempo; exigen altos niveles de conocimiento y recursos.

El objetivo es el "objeto de un ataque como el sistema o la red" mientras que la vulnerabilidad es "una susceptibilidad del sistema o una falla en el diseño del *hardware* o *software* y puede explotarse para obtener acceso no autorizado" (Kim et al. 2020, 996). La carga útil es concebida como el *software* malicioso, entregado por un *malware*, que daña al objetivo; por otro lado, los atacantes incluyen a los propios colaboradores, piratas y terroristas informáticos y aquellos patrocinados por los estados o naciones (Duffany 2018, 3). El Instituto Nacional de Estándares y Tecnología de los Estados Unidos (National Institute of Standards and Technology 2025), entre las definiciones para las contramedidas, la concibe como las medidas de protección para cumplir con los objetivos de seguridad de un sistema de información: confidencialidad, integridad y disponibilidad. Estas medidas pueden incluir características de seguridad, controles de gestión, seguridad del personal, seguridad de estructuras, áreas y dispositivos físicos.

La importancia del ciberespacio ha generado nuevos conceptos, entre estos el *ciberpoder*, referido por Dunn (2018) como "el uso de recursos relacionados con el ciberespacio para lograr fines (políticos) específicos dentro y fuera del ciberespacio". Considera al ciberespacio como un espacio de interacción, pero también plantea que el ciberpoder permite a los actores internacionales usar este dominio para ampliar su control e influencia. Desde una visión realista, funciona como un recurso estatal que fortalece las estructuras de poder, mientras que el enfoque liberal resalta su naturaleza ambigua capaz de desafiar o reproducir estos poderes. En ambos casos, el ciberespacio se convierte en un escenario de manipulación y disputa de intereses. En este sentido, Aguilar-Antonio (2023, 72) establece que por esta preponderancia del ciberespacio y de su dominio se ha propendido a la "construcción de múltiples índices

que buscan medir el nivel de ciberpoder o el desarrollo de capacidades cibernéticas de los Estados nación", como el Global Cybersecurity Index (GCI), el National Cybersecurity Index (NCSI), el National Cyber Power Index (NCPI), y el Cyber Capabilities And National Power (CCNP). Establece que el NCPI y CCNP miden el ciberpoder de los Estados-nación e identifican a las potencias del ciberespacio; mientras que el GCI y el NCSI se centran en la visión de cooperación y de gobernanza global.

Garcés-Montalvo (2024) concluyó que la ciberdefensa es un arma de doble filo: por un lado, protege a un país en el ciberespacio, pero, por otro, genera vulnerabilidades, pues exige recursos para frenar, atacar y recuperar infraestructuras críticas a causa de ciberataques.

> Por ende, surge la necesidad de entender los desafíos a la seguridad y defensa nacional en materia de ciberdefensa; estableciendo normas, protocolos y procedimientos de seguridad asociadas a la informática, que requieren de una constante actualización para hacer frente a nuevas amenazas cibernéticas, cuyos actores pueden ser estatales como no estatales (Garcés-Montalvo 2024, 73).

Por lo expuesto, resulta de utilidad considerar que Galinec y Steingartner (2017) establecen que la ciberseguridad por sí sola no es suficiente para reducir los riesgos; hoy en día es necesaria una estrategia de prevención, defensa y respuesta. La resiliencia, como capacidad para resistir eventos cibernéticos, engloba a los preparativos relacionados con amenazas y vulnerabilidades, las defensas implementadas y los recursos para mitigar los incidentes de seguridad una vez que ocurren. Complementariamente, Možnik et al. (2023) consideran que existe una gran diferencia en una visión de ciberseguridad basada en un control de accesos a una con mentalidad estratégica más enfocada en el largo plazo.

El Centro de Estudios de Seguridad de Zürich subraya que la "ciberseguridad y la ciberdefensa son temas en constante cambio y evolución. La tecnología utilizada para llevar a cabo ataques cibernéticos y las herramientas necesarias para mitigarlos o disuadirlos se encuentra en un estado constante de desarrollo e innovación" (Dewar 2018, 6). Para Dewar (2018), la política nacional relacionada con estos temas sufre cambios periódicos, dependiendo de las prioridades nacionales; son documentos "vivos" a través de los cuales los Estados nacionales formulan sistemáticamente estrategias de ciberseguridad y ciberdefensa, para contrarrestar las ciberamenazas y los riesgos digitales percibidos. Estas políticas y estrategias están interconectadas con las estrategias de la seguridad nacional.

Simultáneamente Vargas, Recalde y Reyes (2017) perciben que los Estados, organizaciones regionales y órganos de seguridad y defensa han empezado a realizar un cambio en su estrategia, con el fin de enfrentar las amenazas en el ciberespacio o al menos disminuir su impacto. Resaltan el papel de las organizaciones internacionales que han provisto modelos o estrategias para la afrontar las amenazas de ciberdefensa y ciberseguridad a los Estados, con publicaciones o estándares como la *Guía de la ciberseguridad para los países en desarrollo* (ITU 2007) o la *Guía para la elaboración de una estrategia nacional de ciberseguridad* (ITU 2017). Adicionalmente, evidencian los aportes de las entidades de estandarización, como la

Organización Internacional de Normalización (ISO),[2] de la cual destaca la norma ISO/IEC 27000, Tecnologías para la seguridad de la Información y Técnicas de Seguridad (ISO 2012).

Para Ron et al. (2018), la ciberdelincuencia representa una amenaza de carácter transnacional que incide de forma determinante en América Latina y, de manera particular, en Ecuador. En respuesta, los Estados y el sector privado han desarrollado diagnósticos situacionales orientados a sustentar las políticas nacionales de ciberseguridad y ciberdefensa. El análisis de estos estudios proporciona insumos clave para orientar la toma de decisiones estratégicas, fortalecer la toma de conciencia de los actores públicos y privados, y definir acciones concretas para proteger la información crítica y la continuidad de las actividades que impactan en la economía nacional.

Solar (2023) caracteriza a América Latina como una región inmersa en una dualidad geopolítica en el ámbito digital. Varios Estados dependen de la cooperación tecnológica con Estados Unidos para fortalecer sus capacidades de ciberseguridad, mientras que, de forma paralela, los vínculos comerciales y tecnológicos con China se han intensificado hasta convertirla en el principal socio comercial de varios países. Esta coexistencia de alineamientos sitúa a América Latina en una posición intermedia y estructuralmente vulnerable dentro del orden digital global, caracterizada por una limitada autonomía tecnológica, una dependencia de actores externos para su seguridad cibernética y un aprovechamiento económico de la expansión tecnológica china, factores que condicionan su margen de maniobra estratégica.

Esta realidad está en sintonía con la afirmación de que el entorno actual de ciberamenazas y riesgos provenientes del ciberespacio es un reto para salvaguardar la seguridad del Estado-nación en cualquier país del mundo. No obstante, la región de América Latina y el Caribe se encuentra rezagada en la construcción de cibercapacidades para enfrentar este contexto. Según Flor-Unda et al. (2023),

> Las vulnerabilidades identificadas en los países latinoamericanos son la baja concienciación en ciberseguridad, la falta de estándares y regulaciones suficientemente implementadas, el uso de software actualizado, las brechas de seguridad en infraestructuras críticas, la capacitación y especialización inadecuadas, y la incidencia de amenazas persistentes avanzadas (ATP). Las vulnerabilidades mencionadas no son exclusivas de América Latina.

Los mismos autores, a partir de los datos de Kaspersky Lab, reportes de agencias gubernamentales y literatura científica, señalan que en América Latina los ciberataques se concentran en un grupo limitado de países. Los registros evidencian una diversidad de modalidades y una evolución constante, sin diferencias estructurales entre los Estados analizados. En este marco, Ecuador se destaca por una mayor recurrencia de incidentes vinculados al secuestro de información y al robo de identidad, mientras que las afectaciones a las comunicaciones seguras son menos frecuentes a nivel región. En términos generales, Panamá, Ecuador y Uruguay concentran el mayor volumen de eventos reportados.

2 Organización para crear estándares internacionales compuesta por diversas organizaciones nacionales de estandarización.

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 45 • mayo-agosto 2026 • pp.99-118
ISSN 1390-4299 (en línea) y 1390-3691

La investigación de López y Carrillo (2023) evidencia que, aunque existen marcos de madurez de ciberseguridad ampliamente adoptados a nivel internacional, el contexto ecuatoriano enfrenta desafíos específicos para proteger sus infraestructuras críticas. Sectores estratégicos como energía, agua, transporte y telecomunicaciones presentan una creciente dependencia de tecnologías digitales, lo que incrementa su exposición a amenazas cibernéticas. En este escenario, la principal dificultad radica en identificar de manera sistemática las brechas de seguridad y priorizar acciones correctivas. Como una respuesta a esta necesidad, propone un modelo de madurez de la capacidad de ciberseguridad (C2M2) personalizado para el Ecuador, ECUA-C2M2,[3] que permite evaluar de forma estructurada la madurez de la ciberseguridad en esos sectores. No obstante, afirma que su efectividad depende de la coordinación sostenida entre el Estado, el sector privado y las entidades responsables de proteger infraestructuras críticas.

La información expuesta evidencia la importancia de que cada Estado cuente con la capacidad para contrarrestar los riesgos del ciberespacio y la fortalezca permanentemente. El objetivo de este trabajo es establecer el contexto latinoamericano de la ciberseguridad y ciberdefensa y la situación actual del Ecuador frente a ese contexto; se considera su marco normativo, referencias de los organismos especializados, documentos de los multilaterales, índices y tendencias en otros países. Así mismo, se busca cuantificar los niveles alcanzados en los índices internacionales para identificar potenciales áreas de mejora.

A continuación, se expone la metodología que soporta el trabajo, seguida de una sección de discusión y resultados. Se presenta la visión de los organismos multilaterales para la ciberseguridad y ciberdefensa, el marco normativo de Ecuador para estos campos, y se analizan las tendencias en materia de ciberseguridad y ciberdefensa en otros países, para contrastarlas con el caso ecuatoriano. Esto permite establecer las conclusiones del trabajo; para finalizar, se reconocen los aportes de los diferentes autores con las referencias bibliográficas.

Metodología

La metodología se basará en un enfoque cualitativo, con alcance descriptivo (Hernández, Fernández y Baptista 2014) de estándares y política pública de ciberseguridad y ciberdefensa. Se utilizan técnicas de revisión documental de textos emitidos por organismos internacionales con recomendaciones, lineamientos y guías sobre estos temas. A través de prácticas interpretativas, se caracterizan las referencias internacionalmente aceptadas, se las analiza y se identifica la situación de la seguridad en el ciberespacio de los países de interés. Este enfoque y alcance se fundamenta en lo establecido por Hernández, Fernández y Baptista (2014, 92) de que los "estudios descriptivos buscan especificar propiedades y características importantes de cualquier fenómeno que se analice. Describen tendencias de un grupo o población".

3 Modelo desarrollado por el autor a partir del C2M2, orientado a la protección de infraestructuras críticas y a la gestión priorizada de riesgos (U.S. Department of Energy 2021).

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 45 • mayo-agosto 2026 • pp.99-118
ISSN 1390-4299 (en línea) y 1390-3691

Pasco Dalla Porta, Cárdenas-Vuckovic y Hernández-Aburto (2021) establecen que el rastreo de procesos es crecientemente utilizado en la investigación social que busca entender los nexos y mecanismos causales en los fenómenos investigados, es un método muy utilizado en la ciencia política. Es de utilidad para analizar los documentos constitucionales, legales, normativos y doctrinarios que configuran el marco referencial internacional y nacional de la ciberseguridad y la ciberdefensa; permiten establecer tanto fortalezas como debilidades, así como identificar oportunidades de mejora. Yin (2018) complementa esta propuesta, al referirse al estudio de caso y sus características como el tamaño de muestra reducido y múltiples fuentes de información.

Finalmente, se acude a la interpretación, para analizar las métricas de los índices relacionados con la ciberseguridad y ciberdefensa, basado en el método comparativo. Según Tonon (2011), este método permite describir similitudes y disimilitudes en un despliegue horizontal de objetos que pertenecen al mismo género y son homogéneos. En este contexto, dicho enfoque permitirá profundizar el análisis de las métricas contenidas en las Políticas y Estrategias de Seguridad Cibernética de Chile, Colombia y Ecuador; así como de las dimensiones del GCI, los indicadores del NCSI y los niveles de Seguridad Cibernética (SC) alcanzados por varios piases.

Resultados y discusión

Visión de los organismos multilaterales para la ciberseguridad y ciberdefensa

La Organización de Naciones Unidas (ONU) considera que la ciberseguridad es un desafío complejo que abarca múltiples aspectos operativos, técnicos, legales de gobernanza y políticos. Propuso una guía basada en modelos marcos y referencias existentes y reconocidas, centrada en la protección de los aspectos civiles del ciberespacio, que destaca los principios generales y las buenas prácticas que deben considerarse en el proceso de redacción, desarrollo y gestión de una Estrategia Nacional de Ciberseguridad (ENC). Además, proporciona una visión general de los componentes centrales que necesitaría un país para estar preparado cibernéticamente (Council of Europe et al. 2021). Esta guía ha servido para que varios países desarrollen sus estrategias nacionales en torno a la ciberseguridad.

La Unión Europea (UE) propuso que, para promover la ciberresiliencia, los sectores público y privado desarrollen capacidades y cooperen eficazmente, a fin de contrarrestar los riesgos y amenazas cibernéticos que tienen una dimensión transfronteriza. En esta línea, promulgó una propuesta de estrategia de ciberseguridad de la Unión Europea, basada en una fuerte protección y promoción de los derechos de los ciudadanos, para hacer que su entorno en línea sea el más seguro del mundo. Resalta que se requiere un fuerte apoyo y compromiso del sector privado y la sociedad civil, actores clave para mejorar el nivel de seguridad y salvaguardar los derechos de los ciudadanos (High Representative of the Europe Union for Foreign Affairs and Security 2020).

Lo anterior evidencia la tendencia internacional de colaboración alrededor de la ciberseguridad, en gran medida orientada a las organizaciones civiles. Considerando esta tendencia y la participación activa de las Fuerzas Armadas en este ámbito, pero de manera independiente en cada Estado, la Junta Interamericana de Defensa (JID), con lineamientos de la Organización de Estados Americanos (OEA), promovió la comunicación y la colaboración en ciberdefensa entre las fuerzas armadas y de seguridad del hemisferio occidental. La JID generó una *Guía de Ciberdefensa* que proporciona "un conjunto de principios para la planificación, diseño, desarrollo y despliegue de capacidades de ciberdefensa" (Junta Interamericana de Defensa 2020). Adicionalmente, con el apoyo del Gobierno de Canadá, lanzó el Programa de Ciberdefensa, que apoya a los países miembros con actividades y ejercicios enfocados a generar y desarrollar capacidades individuales y colectivas de ciberdefensa (Junta Interamericana de Defensa 2020).

La Junta Interamericana de Defensa (JID) define a la ciberdefensa como la "capacidad organizada y preparada para combatir en el ciberespacio. Comprende actividades defensivas, ofensivas y de inteligencia", y se desarrolla a través de cuerpos doctrinales que regulan las operaciones militares en el ciberespacio. Entre los estándares para el sector incluyen, como norma guía, a la familia ISO/IEC 27000 (Junta Interamericana de Defensa 2020).

Consecuentemente la comunidad internacional, a través de lineamientos y estrategias de los organismos multilaterales, ha generado documentos guía para la política pública que los Estados podrían adaptar en el ámbito de la ciberseguridad. Así mismo, se desarrollaron instrumentos con lineamentos de doctrina operativa para el ámbito de ciberdefensa que buscan estandarizar y facilitar la comunicación y colaboración de la comunidad internacional regional y mundial. Estas acciones se promueven debido a la trasnacionalidad y a las graves implicaciones para la seguridad nacional y mundial de las actividades maliciosas en el ciberespacio. A continuación, se analiza el resultado de las actuaciones en ciberseguridad y ciberdefensa del Ecuador frente a los lineamientos de los multilaterales, medición de índices y situación de otros países.

Los lineamientos de la ONU, la Unión Europea y la JID evidencian enfoques diferentes pero complementarios sobre la ciberseguridad y la ciberdefensa, que fluctúan entre la protección del ámbito civil, la cooperación público-privada y el desarrollo de capacidades militares. No obstante, se presentan desafíos para adoptar estos marcos en países con capacidades institucionales y tecnológicas heterogéneas. En este contexto, su análisis permite identificar brechas, convergencias y limitaciones relevantes para formular políticas nacionales. Estos referentes permiten evaluar el grado de alineación y respuesta de Latinoamérica y Ecuador frente a las tendencias internacionales.

Marco normativo de la ciberseguridad y ciberdefensa en Ecuador

La Constitución de la República del Ecuador reconoce el derecho de las personas al acceso universal a las tecnologías de información y comunicación (art. 16), y el derecho a la protección

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 45 • mayo-agosto 2026 • pp.99-118
ISSN 1390-4299 (en línea) y 1390-3691

de datos personales e inviolabilidad de la correspondencia virtual (art. 66). Para esto, el Estado ecuatoriano tiene el derecho de administrar, regular, controlar y gestionar los sectores estratégicos como las telecomunicaciones y el espectro radioeléctrico (art. 261) (Asamblea Nacional del Ecuador 2008). En línea con los mandatos constitucionales, se promulgaron o reformaron varios cuerpos legales para regular delitos, contravenciones, estándares técnicos y actores del ciberespacio.

El Ministerio de Telecomunicaciones del Ecuador (MINTEL) implementó un Sistema de Gestión de Seguridad de la Información en el Sector Público (MINTEL 2024), en el que define parámetros para proteger la infraestructura crítica y servicios esenciales. Además, mediante la Política de Ciberseguridad (MINTEL 2021) y Estrategia Nacional de Ciberseguridad (MINTEL 2022), abordó los temas de seguridad y soberanía en el ciberespacio, y definió como un pilar a la ciberdefensa. Por otro lado, el Plan Sectorial de Seguridad 2017-2021 estableció la misión del Comando de Ciberdefensa (COCIBER 2024), sobre la cual la Agenda Política de la Defensa del Ecuador 2018 (MIDENA 2018) desarrolló la estrategia para la ciberdefensa. Finalmente, el Ministerio de Defensa Nacional (MIDENA), mediante la Estrategia de Ciberdefensa 2022, orientó a la ciberdefensa hacia la protección efectiva de la infraestructura crítica digital y servicios esenciales de las áreas estratégicas, fortalecer las capacidades y la cooperación internacional, y aportar a la seguridad y defensa del Ecuador. Estos preceptos están en línea con lo manifestado por Sancho (2017, 14) acerca de que "la existencia de riesgos y amenazas obliga a considerar la ciberseguridad como una condición que debe ser provista por el Estado […] desde una perspectiva de política pública".

En cuanto a la estructura organizacional operativa, el Gobierno del Ecuador, a través del MIDENA, creó, en 2014, el COCIBER, como un comando operacional del Comando Conjunto de las Fuerzas Armadas, con la misión de ejecutar operaciones de defensa, exploración y respuesta en el ciberespacio, para proteger la infraestructura crítica digital, servicios esenciales del Estado e infraestructura crítica digital del sector defensa. Concomitante con lo anterior, el MINTEL creó, en 2023, el Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT), para brindar apoyo en la prevención y resolución de incidentes de seguridad informática, a través de la coordinación, capacitación y soporte técnico. El CSIRT Ecuador es parte de la red CSIRT Américas.

De esta información se colige que la política pública de ciberseguridad y ciberdefensa en Ecuador está sustentada desde la Constitución de la República; que existe un Sistema de Gestión de Seguridad de la Información en el Sector Público con políticas y estrategias que buscan la seguridad y soberanía en el ciberespacio, y que, en la concepción ecuatoriana, la ciberdefensa es considerada un pilar para defender la soberanía e integridad territorial en el ciberespacio.

Al contrastar las actuaciones del Ecuador frente a los preceptos intencionales, encontramos que el análisis comparativo de las estrategias nacionales de ciberseguridad en América del Sur, de la Organización de Estados Americanos (OEA), estableció que las estrategias nacionales de ciberseguridad (ENC) de Argentina, Brasil, Chile, Colombia, Ecuador y Paraguay, presentan

áreas comunes. Además, a excepción de Paraguay, las ENC de la región consideran la seguridad nacional un motivador para elaborar sus respectivas estrategias (Organización de Estados Americanos 2022). Se deduce que el Ecuador ha estandarizado estrategias con varios países de la región, y que la ENC ecuatoriana se enfoca en asegurar la información para garantizar los derechos y libertades de los ciudadanos mediante la construcción y el fortalecimiento de capacidades nacionales de ciberseguridad, así como la protección de los activos legales del estado en el ciberespacio, con lo que contribuye al desarrollo económico y humano.

Así mismo, luego de contrastar los contenidos del análisis de la OEA y de la *Guía de Ciberdefensa* de la JID con el respaldo legal, doctrina y estructura organizacional de la ciberdefensa en Ecuador, se puede afirmar que está en plena concordancia con estos instrumentos. Ecuador considera a la ciberdefensa como un pilar de la ciberseguridad y, por tanto, emitió la Estrategia de Ciberdefensa 2022, dentro de la cual el COCIBER está llamado a proteger la Infraestructura Crítica Digital (ICD) y los servicios esenciales, mediante operaciones defensivas, ofensivas y de inteligencia, esto último también en línea con las tendencias internacionales.

Tendencias en materia de ciberseguridad y ciberdefensa en otros países, contrastado con el caso ecuatoriano

En el trabajo "Políticas públicas de ciberdefensa en Chile y Colombia" (Montenegro Moreno et al. 2022), se estableció que el diseño y la formulación de las políticas públicas en ciberdefensa en Colombia y Chile, y a nivel regional, se suscribieron en adhesión a regímenes internacionales de orden mundial. Se reconocen tres elementos centrales que han contribuido a desarrollar esas políticas: el Convenio de Budapest, la Estrategia Interamericana Integral de Seguridad Cibernética de la OEA y la Estrategia de Ciberdefensa para la Unión Europea.

La OEA y el BID han sido los actores más relevantes desde los cuales se formulan lineamientos y parámetros para construir una política hemisférica enfocada hacia la ciberdefensa y la ciberseguridad. Se estableció "una relación entre la OEA como organismo regional y su incidencia en la formulación de las políticas de ciberdefensa de Colombia y Chile" (Montenegro Moreno et al. 2022, 14), y que, a pesar de los esfuerzos de estas organizaciones, "de dotar con modelos o estrategias para afrontar las amenazas de ciberdefensa y ciberseguridad a los Estados" (Vargas, Recalde y Reyes 2017, 35) y de brindar estándares para la formulación de políticas públicas sobre ciberdefensa, para el 2018 solo 10 Estados de América Latina y el Caribe (ALC) contaban con políticas de seguridad acerca de ciberdefensa. (Álvarez 2018).

Mediante el Observatorio de la Ciberseguridad en América Latina y el Caribe, la OEA y el BID, establecieron una propuesta para medir el avance del desarrollo de capacidades de ciberdefensa y ciberseguridad, basado en cinco indicadores, que se miden en cinco niveles: inicial, formativo, establecido, estratégico y dinámico (BID y OEA 2020). La figura 1 muestra la información de Chile, Colombia y Ecuador para el indicador Política y Estrategia de Seguridad Cibernética, medido por el Observatorio. Se comparan datos del 2020 y se

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 45 • mayo-agosto 2026 • pp.99-118
ISSN 1390-4299 (en línea) y 1390-3691

Figura 1. Datos de Política y Estrategia de Seguridad Cibernética de Chile Colombia y Ecuador al 2020

Fuente: Observatorio de la Ciberseguridad en ALC, Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe. Reporte 2020.

observa que, a esa fecha, Colombia presentaba una estrategia nacional de seguridad cibernética con nivel "Estratégico", y está por delante de Chile y Ecuador, que alcanzaron niveles "Establecido" y "Formativo", respectivamente. Los otros aspectos de este indicador: Respuesta a incidentes, Protección de Infraestructura Crítica, Manejo de Crisis y Defensa Cibernética, presentan niveles con la misma tendencia.

Desde 2020 Chile y Ecuador han generado cambios significativos. En la actualidad, los datos evidencian que Chile lleva el liderazgo en varios índices y que Ecuador ha mejorado en otros. En 2023 Chile presentó mejores niveles en el Índice Nacional de Ciberseguridad (NCSI), con una valoración de 59,74, y superó a Colombia y Ecuador, ambos con 53,25 puntos. La misma tendencia es observada en el nivel de Seguridad Cibernética (SC) (MixMode.AI. 2024): Chile alcanzó 68,31 puntos, frente a los 62,66 de Colombia y los 45 de

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 45 • mayo-agosto 2026 • pp.99-118
ISSN 1390-4299 (en línea) y 1390-3691

Tabla 1. Dimensiones del GCI de Chile, Colombia y Ecuador 2024

País	Desarrollo de capacidades*	Medidas de cooperación*	Medidas Legales*	Medidas Organizativas*	Medidas técnicas*
Chile	11,5	16,8	14,7	13,4	13,8
Colombia	15,1	10,2	13,4	10,9	16,2
Ecuador	13,8	17,7	19,2	18,6	17,9

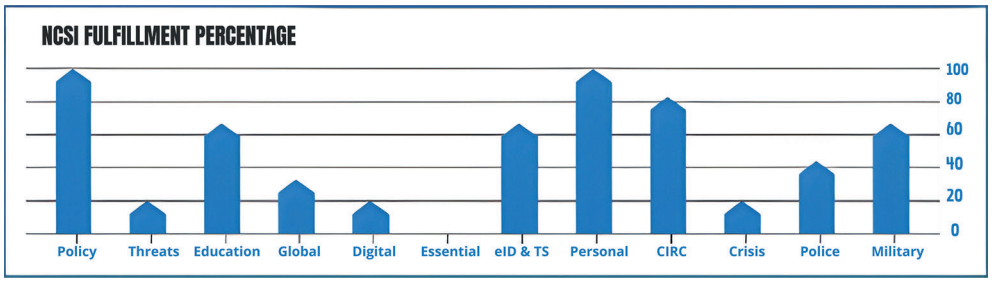
Fuente: Índice Global de Ciberseguridad.
* Valor máximo 20

Ecuador. Por su parte Ecuador, en 2024, registró mejores niveles en cuatro de las cinco dimensiones del Índice Global de Ciberseguridad (GCI) (tabla 1).

El análisis comparativo de Chile, Colombia y Ecuador evidencia que los tres países adoptan los lineamientos internacionales de ciberseguridad y ciberdefensa, aunque con niveles de madurez desiguales. Colombia alcanzó de manera temprana un enfoque estratégico, mientras que Chile consolidó avances que le permiten liderar índices recientes. Ecuador presenta avances relevantes en dimensiones legales, organizativos y de cooperación. Estas diferencias se explican por capacidades institucionales y ritmos de implementación distintos.

Con énfasis en Ecuador se examina con mayor detalle la información del NCSI, GCI, CSIRTAmericas y del Análisis de amenazas cibernéticas en 70 países provisto por MixMode.AI.[4] Según el NCSI (figura 2), en Ecuador el análisis e información sobre amenazas cibernéticas (*Threats*), la protección de servicios digitales (*Digital*), la protección de servicios esenciales (*Essential*) y gestión de crisis cibernéticas (*Crisis*) tienen los más bajos desempeños, por debajo del 20 %. El nivel relacionado con los servicios esenciales (*Essential*) no presenta evolución. Por otro lado el desarrollo de políticas de ciberseguridad (*Policy*), protección de

Figura 2. Indicador General de Ciberseguridad del NCSI para Ecuador



Fuente: National Cyber Security Index.

4 MixMode.AI: plataforma de ciberseguridad que utiliza inteligencia artificial (IA) para detectar y responder a amenazas en tiempo real. Según su página web "puede identificar anomalías y amenazas, incluyendo ataques de día cero, con una precisión de alerta de más del 99 % [...] por lo que es utilizado por organizaciones de los sectores de la banca, entidades públicas y el gobierno". Analizó las amenazas cibernéticas en 70 países tomando en cuenta el NCSI, el GCI y el Índice de Exposición a la Ciberseguridad (CEI), para determinar una puntuación final de seguridad cibernética (2024, tomado de https://bit.ly/413yck5).

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 45 • mayo-agosto 2026 • pp.99-118
ISSN 1390-4299 (en línea) y 1390-3691

Tabla 2. Indicadores del NCSI con menor desarrollo en Ecuador

Análisis e información sobre amenazas cibernéticas	Protección de servicios digitales	Protección de servicios esenciales	Gestión de crisis cibernéticas
Unidad de análisis de amenazas cibernéticas	Responsabilidad de los proveedores de servicios digitales en materia de ciberseguridad	Identificación de operadores de servicios esenciales	Plan de gestión de crisis cibernéticas
informes anuales sobre amenazas cibernéticas	Norma de ciberseguridad para el sector público	Requisitos de ciberseguridad para los operadores de servicios esenciales	Ejercicio de gestión de crisis cibernéticas a nivel nacional
Sitio web sobre seguridad y protección cibernética	Autoridad supervisora competente	Autoridad supervisora competente	Participación en ejercicios internacionales de crisis cibernéticas
		Seguimiento periódico de las medidas de seguridad	Apoyo operativo de voluntarios en crisis cibernéticas

Fuente: elaboración del autor con datos de del NCSI.

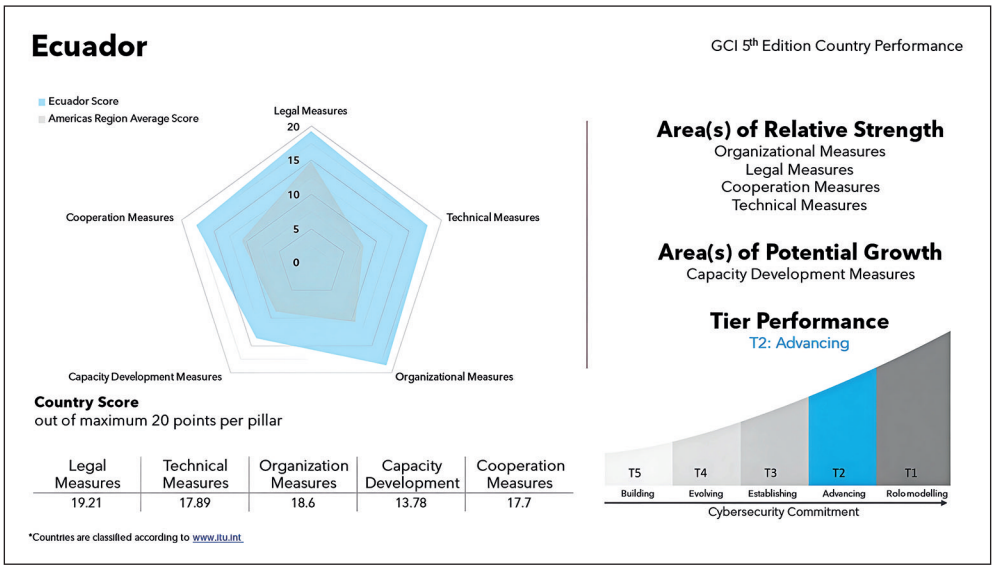
datos personales (*Personal*) y respuesta a incidentes cibernéticos (CIRC) tienen los mejores desempeños. La estructura de los indicadores con los menores desempeños se muestra en la tabla 2; permite identificar qué aspectos se deberían mejorar para elevar el nivel de los indicadores antes citados.

Según el GCI 2024, Ecuador evidencia un desarrollo sostenido en su compromiso con la ciberseguridad a nivel global, pues se ubicó en el segmento "T2 Avanzado". Los pilares sobre los cuales se basa este indicador (medidas legales, medidas técnicas, medidas organizativas, desarrollo de capacidades y cooperación) han experimentado mejoras. La figura 3 evidencia que cuatro de los cinco pilares del GCI están calificados con una "fortaleza relativa" (*Areas of Relative Strenght*), y uno de ellos, el de "desarrollo de capacidades" (*Capacity Development Measures*) está como un área de "potencial crecimiento" (*Areas of Potential Growth*). Esta última se refiere a las campañas de concientización, capacitación, educación e incentivos para el desarrollo de capacidades.

La Red de los Equipos de Respuesta gubernamentales ante Incidentes Cibernéticos (CSIRT), de los Estados miembros de la OEA, (CSIRTAmericas), registra los centros de respuestas de los países miembros. Para el caso del Ecuador, lista al COCIBER (militar), CSIRT-ARE (militar) y EcuCERT (Gobierno-nacional). Como referencia, Argentina registra 7 CSIRT, Colombia 8, Perú 7 y Chile 3. Brasil y Estados Unidos, considerados como modelos a seguir, registran un solo CSIRT de nivel nacional. Uruguay, que en los últimos años ha experimentado avances positivos en ciberseguridad, reporta 2, un nacional y uno militar. Lo anterior permite inferir que, más allá del número de CSIRT, lo realmente determinante es su capacidad técnica-operativa (OEA-OAS 2023).

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 45 • mayo-agosto 2026 • pp.99-118
ISSN 1390-4299 (en línea) y 1390-3691

Figura 3. Datos de Ecuador del Índice Global de Ciberseguridad (GCI) 2024



Fuente: Global Cybersecurity Index 2024.

MixMode.AI determinó que entre los países con el ciberespacio más seguro se encuentran Finlandia, Noruega y Dinamarca, con puntajes de 93, 93 y 92 sobre 100, respectivamente. Estados Unidos obtuvo una puntuación de 89, Brasil 71,37, Chile 68,31 y Colombia 62,66. Ecuador obtuvo un puntaje de 45, y se ubica en la posición 66 de 70 países estudiados (tabla 3). De acuerdo con MixMode.AI, el "Ecuador enfrenta importantes vulnerabilidades a las amenazas cibernéticas". Por otro lado, en la tabla 3 se identifica la realidad del Ecuador frente a otros países; se observa que el índice que menos desarrollado tiene el Ecuador es el GCI (26,3), seguido del Índice de Exposición a la Ciberseguridad (34,8). Los datos nos conducen a revisar con mayor detalle los pilares del GCI para Ecuador. Se evidencia que el pilar con mayor nivel es el relacionado con las medidas legales (19,21) y el de menor nivel es el de Desarrollo de Capacidades (13,78); las Medidas Técnicas y Medidas de Cooperación alcanzaron niveles de 17,89 y 17,7, respectivamente. El máximo valor que puede alcanzar cada parámetro es 20.

Tabla 3. Seguridad Cibernética (SC) de varios países

Clasificación	País	Índice Nacional de Ciberseguridad	Índice de Exposición Ciberseguridad	Índice Global Ciberseguridad	Índice de Resiliencia Cibernética	Puntuación Final Seguridad Cibernética
1	Finlandia	85,71	89,0	95,78	93,64	92,81
9	Estados Unidos	64,94	85,5	100,00	80,31	88,60
42	Brasil	51,95	45,9	96,60	71,62	71,37
49	Chile	59,74	53,1	68,83	83,00	68,31
54	Colombia	53,25	41,0	63,72	83,25	62,66
66	Ecuador	53,25	34,8	26,35	73,89	45,00
70	Bolivia	31,17	21,7	16,14	77,33	38,39

Fuente: elaboración del autor con datos de MixMode.AI (2024).

De acuerdo con la información expuesta, pueden identificarse las oportunidades que tendría el Ecuador para fortalecer la ciberresiliencia y alcanzar mejores estándares internacionales. Derivados de los documentos de la OEA se identifican los siguientes aspectos de mejora: seguridad en la provisión de servicios digitales; proteger el comercio e información personal en línea; desarrollar la industria nacional de ciberdefensa; perfeccionar la identificación y manejo de incidentes, y promover las alianzas público-privadas. Por otro lado, de la información del NCSI se desprenden los siguientes puntos: identificar operadores de servicios esenciales y normar los aspectos relacionados con la ciberseguridad; fortalecer las normas y definir exigencias de ciberseguridad para los proveedores de servicios digitales; mejorar la gestión de crisis cibernéticas y ponerla a prueba con ejercicios nacionales e internacionales. Finalmente, de la información del GCI se extraen: incrementar las campañas de concientización, capacitación y educación; promover incentivos para el desarrollo de capacidades en ciberseguridad, y generar esquemas de certificación de ciberseguridad.

El análisis del NCSI, GCI, CSIRTAmericas y MixMode.IA evidencia que Ecuador presenta avances normativos y, en menor medida, capacidades operativas en ciberseguridad. Los bajos niveles en análisis de amenazas, protección de servicios esenciales y gestión de crisis reflejan debilidades en prevención y respuesta. Aunque los indicadores globales muestran mejoras relativas, el desarrollo de capacidades sigue siendo el principal desafío. La comparación internacional sugiere que el problema no es estructural, sino de efectividad y madurez. En conjunto, los resultados demandan un enfoque orientado a capacidades y ciberresiliencia.

Las acciones establecidas como producto del análisis de este trabajo concuerdan con lo propuesto por Možnik et al. (2023), que presentan un nuevo modelo conceptual de ciberresiliencia, que incluye la ciberseguridad, la seguridad de la información y sistemas de información y la ciberdefensa, con el objetivo de encontrar y utilizar procesos efectivos para una resiliencia cibernética ágil dentro de un sistema que pueda afrontar con éxito eventos impredecibles. Desde el interés académico, un estudio más profundo podría analizar el modelo frente a las realidades específicas del Ecuador.

Conclusiones

La información de los organismos multilaterales y organizaciones con y sin fines de lucro, como OEA/JID, BID, el NCSI, el GCI y la Red CSIRT Américas, permite concluir que la ciberseguridad y ciberdefensa en Ecuador cuenta con los lineamientos constitucionales, legales, normativos, organizativos y doctrinales en línea con las mejores prácticas internacionales. Esta alineación es sobre todo normativa y declarativa, y no necesariamente se traduce en la consolidación en capacidades operativas. El Ecuador ha implementado un Esquema Gubernamental de Seguridad de la Información apoyado en servicios de respuesta a incidentes de seguridad informática (CSIRT) y operaciones de seguridad a través del Comando de Ciberdefensa de sus Fuerzas Armadas, para hacer frente a las crecientes amenazas cibernéticas a la infraestructura crítica y servicios esenciales del país. La efectividad de estos mecanismos está supeditada a superar las brechas relacionadas con la coordinación interinstitucional, la asignación sostenida de recursos y la continuidad de las políticas públicas. Esta concepción es similar a la de países como Argentina, Brasil, Colombia, España, Estados Unidos y Perú, lo que sugiere una convergencia doctrinal regional que no siempre se refleja en niveles equivalentes de madurez técnica y operativa. Los principales retos del Ecuador están en la generación de políticas públicas que permitan fortalecer y alcanzar los niveles técnico-operativos acordes con dichos estándares internacionales.

La literatura citada evidencia que las políticas públicas de ciberdefensa en Chile, Colombia y Ecuador se suscribieron con adhesión a actores internacionales, siendo la OEA y el BID los más relevantes; este patrón confirma una dependencia estructural de marcos exógenos para la formulación estratégica en el ámbito cibernético. En el caso ecuatoriano. la información analizada muestra que la concepción de la ciberdefensa es similar a la de Colombia y Chile, al haberse estructurado en torno a las recomendaciones de la JID; esto refuerza una visión predominantemente militar de ciberespacio, con limitada integración de enfoques civiles y multisectoriales. La ciberdefensa en el Ecuador opera en el quinto dominio, el ciberespacio, y tiene como misión el garantizar la seguridad de los ciudadanos en este. Asimismo, persisten vacíos conceptuales y operativos en la delimitación de responsabilidades entre defensa, seguridad interna y gestión civil del riesgo cibernético.

La información del Observatorio de Ciberseguridad en ALC permite contrastar la situación del indicador Política y estrategia de seguridad cibernética de Chile, Colombia y Ecuador. En 2020 Colombia presentaba una estrategia nacional de seguridad cibernética con nivel “estratégico” y estaba por delante de Chile y Ecuador que mostraban niveles “establecido” y “formativo”, respectivamente. Los datos de 2023 y 2024 muestran que actualmente Chile presenta mejores niveles en el NCSI y en los indicadores de seguridad cibernética; mientras que Ecuador alcanza mejores resultados en todas las dimensiones del Índice Global de Ciberseguridad. Esto evidencia avances cuantitativos relevantes, aunque no necesariamente equivalentes a una consolidación estructural de capacidades sostenibles en el tiempo.

Un análisis integrado del NCSI, GCI, CSIRTAmericas y el panorama de amenazas cibernéticas permiten identificar oportunidades de mejora específicas para el Ecuador. En particular, se evidencia que entre los indicadores del NCSI con menor nivel de desarrollo se destacan la Protección de servicios esenciales, con un nivel de 0 %, y los de Análisis e información de amenazas cibernéticas, Protección de servicios digitales y el Manejo de crisis cibernéticas, con niveles de 20 %. Estas brechas constituyen vulnerabilidades críticas que limitan la resiliencia nacional frente a incidentes cibernéticos de alto impacto. El análisis de las debilidades cibernéticas a partir del GCI muestran que Ecuador presenta una "fortaleza relativa" en cuatro de los cinco pilares, mientras que el pilar de Desarrollo de capacidades se identifica como un área de "potencial crecimiento". Así, se refuerza la necesidad de priorizar inversiones sostenidas en formación especializada, desarrollo tecnológico y ejercicios de preparación operativa.

Bibliografía

Aguilar-Antonio, Juan. 2023. "China y Estados Unidos: antagonismos y liderazgos en el ciberespacio frente a América Latina". *Revista Latinoamericana de Estudios de Seguridad (36)*: 66-84. https://doi.org/10.17141/urvio.36.2023.5845

Álvarez Valenzuela, Daniel. 2018. "Ciberseguridad en América Latina y ciberdefensa en Chile". *Revista Chilena de Derecho y Tecnología* 7(1): 1-2. https://dx.doi. org/10.5354/0719-2584.2018.50416

Asamblea Nacional del Ecuador. 2008. *Constitución de la República del Ecuador*. Quito: Publicada en el *Registro Oficial* N.º 449 20 de octubre de 2008.

BID (Banco Interamericano de Desarrollo) y Organización de Estados Americanos (OEA). 2020. *Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe*. Reporte 2020. https://bit.ly/415T8qL

Carr, Madeline. 2016. "Public-private partnerships in national cyber-security strategies". *International Affairs* 92: 43-62. https://doi.org/10.1111/1468-2346.12504

Centro de Respuesta a Incidentes de Seguridad Informática. 2023. https://bit.ly/4hshGQl

Carmichael, Logan. 2025. "Lessons from small and highly-digitalized Estonia: Decision-making in the aftermath of cybersecurity crises". *Internet Policy Review* 14 (3). https://doi.org/10.14763/2025.3.2028

COCIBER. 2024. "Misión de Comando de Ciberdefensa. 2024", https://cociber.ccffaa.mil.ec/mision/

Council of Europe (CoE), Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organisation (CTO), Geneva Centre for Security Sector Governance (DCAF), Deloitte, Forum of Incident Response and Security Teams (FIRST), Global Cyber Security Capacity Centre (GCSCC), Geneva Centre for Security Policy (GCSP), Global Partners Digital (GPD), International Criminal Police Organization (INTERPOL), International

Telecommunication Union (ITU), Microsoft, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Potomac Institute for Policy Studies (PIPS), RAND Europe, World Bank, United Nations Institute for Disarmament Research (UNIDIR), United Nations Office of Counter-Terrorism (UNOCT), United Nations University (UNU). 2021. *Guide to Developing a National Cybersecurity Strategy 2nd Edition – Strategic engagement in cybersecurity.* Creative Commons Attribution-NonCommercial 3.0 IGO (CC BY-NC 3.0 IGO*)*.

Dewar, Robert S. 2018. *National Cybersecurity and Cyberdefense Policy Snapshots: Collection* 1, 2018. Center for Security Studies (CSS), ETH Zürich.

Duffany, Jeffrey. 2018. *Computer Security*. Computer and Network Security Essentials. Springer, Cham: 3-20.

Dunn Cavelty, Myriam. 2018. *Europe's cyber-power*. European Politics and Society. https://doi.org/10.1080/23745118.2018.1430718

Equipo de seguridad de Microsoft. 2021. Protección de los servidores Exchange on-premises contra ataques recientes. 18 de marzo. https://bit.ly/40PUW5X

Eriksson, Johan y Giampiero Giacomello. 2022. "Cyberspace in space: Fragmentation, vulnerability, and uncertainty". En *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*, editado por Myriam Dunn Cavelty y Andreas Wenger, 95-108. Abingdon: Routledge.

Flor-Unda Omar, Freddy Simbaña, Xavier Larriva-Novo, Ángel Acuña, Rolando Tipán, Patricia Acosta-Vargas. 2023. "A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America". *Informatics 10* (13): 71. https://doi.org/10.3390/informatics10030071

Hernández Sampieri, Roberto, Carlos Fernández y Pilar Baptista Lucio. 2014. *Metodología de la invetsigación. México:* McGraw-Hill Sexta edición.

High Representative of the Europe Union for Foreign Affairs and Security. 2020. The EU's Cybersecurity Strategy for the Digital Decade. https://bit.ly/3Kjuiy6

ISO. 2012. "Portal de ISO 27001 en español", http://www.iso27000.es/

ITU. 2007. "Guía de ciberseguridad para los países en desarrollo", https://bit.ly/3Eu7Mix

ITU. 2017. "Guía para la elaboración de una estrategia nacional de ciberseguridad", http://bit.ly/44HjvEE

Galinec, Darko, y William Steingartner. 2017. "Combining Cybersecurity and Cyber Defence to achieve Cyber Resilience". *IEEE 14th International Scientific Conference on Informatics:* 87-93. https://doi.org/10.1109/INFORMATICS.2017.8327227

Garcés-Montalvo, David. 2024. "La vigilancia líquida como instrumento de la ciberdefensa implementada por los Estados Unidos en la administración de George W. Bush". Tesis de maestría, Facultad Latinoamericana de Ciencias Sociales, FLACSO Ecuador.

Georgiadou, Anna, Ariadni Michalitsi-Psarrou, Fotios Gioulekas, Evangelos Stamatiadis, Athanasios Tzikas, Konstantinos Gounaris, Georgios Doukas, Christos Ntanos, Luis Ribeiro, y Dimitris Askounis. 2021. "Hospitals' Cybersecurity Culture during the COVID-19 Crisis". *Healthcare* 9 (10): 1335. https://doi.org/10.3390/healthcare9101335

Junta Interamericana de Defensa. 2020. *Guía de Ciberdefensa Orientación para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar*. Washington, DC: Junta Interamericana de Defensa.

Kim, Seungmin, Gyunyoung Heo, Enrico Zio, Jinsoo Shin, Jae-gu Song. 2020. "Cyberattack taxonomy for digital environment in nuclear power plants". *Nuclear Engineering and Technology* 52 (5): 995-100. https://doi.org/10.1016/j.jsis.2024.101861

Lippert, Kari J., y Robert Cloutier. 2021. "Cyberspace: A Digital Ecosystem". *Systems* 9 (3): 48-66. https://doi.org/10.3390/systems9030048

López, L. Carlos., y José Carrillo. 2023. "Modelo de madurez de ciberseguridad para infraestructuras críticas caso de estudio: Ecuador". *Pro Sciences: Revista de Producción, Ciencias e Investigación* 7 (48): 39-56. https://doi.org/10.29018/issn.2588-1000vol7iss48. 2023pp39-56

McGuinness, Damien. 2017. **"**Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país". *El País*, 6 de mayo. http://bit.ly/3CAVYur

MIDENA (Ministerio de Defensa Nacional). 2018. "Agenda Política de la Defensa del Ecuador", https://bit.ly/4hMZjp3

MINTEL (Ministerio de Telecomunicaciones y de la Sociedad de la Información). 2024. Esquema gubernamental de seguridad de la Información (EGSI). https://bit.ly/3EolOT1

MINTEL (Ministerio de Telecomunicaciones y de la Sociedad de la Información). 2021. "Política de Ciberseguridad", https://bit.ly/4hJWipw

MINTEL (Ministerio de Telecomunicaciones y de la Sociedad de la Información). 2022. "Estrategia Nacional de Ciberseguridad", https://bit.ly/3EtBdBu

Mishra, Alok, Yehia Alzoubi, Memoona Anwar, y Asif Gill. 2022. "Attributes impacting cybersecurity policy development: An evidence from seven nations". *Computers & Security* 120: 1-23. https://doi.org/10.1016/j.cose.2022.102820

MixMode.AI. 2024. "Niveles de Seguridad Cibernética (SC)", https://bit.ly/413yck5

Montenegro Moreno, Hackzel. Maverick Pantoja Rosero, Angie Rojas Larrotta, y Ricardo Garcia Briceño. 2022. "Políticas públicas de ciberdefensa en Chile y Colombia: Un análisis desde el rastreo de procesos". *Brújula Semilleros De Investigación* 10 (20): 7-16. https://doi.org/10.21830/23460628.118

Možnik, Darko, Damir Delija, Domagoj Tulčić, y Darko Galinec. 2023. "Cybersecurity and Cyber Defense Insights: The Complementary Conceptual model of Cyber resilience". *ENTRENOVA - Enterprise Research Innovation* (9): 1-12. http://dx.doi.org/10.54820/entrenova-2023-0001

National Institute of Standards and Technology. 2025. GLOSSARY: Countermeasures. 19 de febrero http://bit.ly/4gIFe2k

Nobrega, Kristel, Anne Rutkowski y Carol Saunders. 2024. "The whole of cyber defense: Syncing practice and theory". *The Journal of Strategic Information Systems* 33 (4). https://doi.org/10.1016/j.jsis.2024.101861

O'Brien, James. 2023. "Una filtración de la Fiscalía colombiana deja al descubierto la identidad de decenas de agentes de la DEA". *Insight Crime*, 10 de noviembre. https://bit.ly/4hMUJY0

Organización de Estados Americanos (OEA). 2022. *NCS: Lessons Learned and Reflections from the Americas and Other Regions*. Washington, D.C: Organización de Estados Americanos.

Organización de los Estados Americanos (OEA). 2023. *Guía práctica para CSIRTs Un modelo de negocio sustentable*. Red CSIRTAmericas 2.

Pasco Dalla Porta, Mario, Vania Cárdenas-Vuckovic y Angello Hernández-Aburto. 2021. "El rastreo de procesos en el análisis causal cualitativo y su aporte al estudio de las organizaciones". *Revista Pesquisa Qualitativa* 9 (21): 486-510. https://doi.org/10.33361/RPQ.2021.v.9.n.21.473

Perera, Srinath, Xiaohua Jin, Alana Maurushat, y De-Graft Joe Opoku. 2022. "Factors Affecting Reputational Damage to Organizations Due to Cyberattacks". *Informatics* 9 (1): 28. https://doi.org/10.3390/informatics9010028

Raiyn Jamal. 2014. "A survey of cyber attack detection strategies". *International Journal of Security and Its Applications* 8 (1): 247-256. http://dx.doi.org/10.14257/ijsia.2014.8.1.23

Ron, Mario, Walter Fuertes, Theofilos Toulkeridis y Javier Díaz. 2018. "Cybercrime in Ecuador, an Exploration, which allows to define National Cybersecurity Policies". *13th Iberian Conference on Information Systems and Technologies (CISTI)*, 1-7.

Solar, Carlos. 2023. *Cybersecurity Governance in Latin America. States, Threats, and Alliances.* Albany: State University of New York Press.

Sancho Hirare, Carolina. C. 2017. "Ciberseguridad. Presentación del dossier/Cybersecurity. Introduction to Dossier". *URVIO. Revista Latinoamericana de Estudios de Seguridad* (20): 8-15. https://doi.org/10.17141/urvio.20.2017.2859

Tidy, Joe. 2023. "La otra guerra inclemente que libran Ucrania y Rusia". *BBC News*, 15 de abril. https://bit.ly/3Cu6tQg

Tonon, Graciela. 2011. "La utilización del método comparativo en estudios cualitativos en Ciencia Política y Ciencias Sociales". *Kairos: Revista de temas sociales* 15 (27).

Unidad de Comunicación Institucional. 2023. "Hacienda no perdió información de expedientes ni impuestos por ciberataque". 6 de febrero. https://bit.ly/413iOEc

Vargas Borbúa, Robert, Luis Recalde y Rolando P. Reyes. 2017. "Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa". *URVIO Revista Latinoamericana de Estudios de Seguridad*, (20): 31-45. https://doi.org/10.17141/urvio.20.2017.2571

Woods, Daniel, y Sezaneh Seymour. 2023. "Evidence-based cybersecurity policy? A meta-review of security control effectiveness". *Journal of Cyber Policy* 8 (3): 365-383. https://doi.org/10.1080/23738871.2024.2335461

Yin, Robert. 2018. *Case Study Research: Design and Methods*. Thousand Oaks, CA: Sage Publications. 2018.