AMENAZAS HÍBRIDAS Y CIBERDEFENSA EN AMÉRICA LATINA: EL CASO ECUATORIANO COMO ESTUDIO COMPARATIVO

HYBRID THREATS AND CYBER DEFENSE IN LATIN AMERICA: THE ECUADORIAN CASE AS A COMPARATIVE STUDY

Tcrn. de E.M Arias Peña Cristian Fernando, Mgs
Centro de Educación Militar-CEDMIL
Av. Gral. Enríquez S/N, Sangolquí 171103, Quito, Ecuador
Código ORCID: https://orcid.org/0009-0007-1105-9461
Correo del autor: cfariasp@ejercito.mil.ec

Benavides Ortiz Germán Gustavo, MBA
Unidad Educativa Misión Geodésica
Pucará S1-121 y San Francisco de la Pita, San Antonio de Pichincha, Mitad del Mundo, Ecuador
Código ORCID: https://orcid.org/0000-0003-4233-1572
Correo del autor: germanben27@gmail.com

RESUMEN

La presente investigación aborda el fenómeno creciente de las amenazas híbridas que está teniendo lugar en América Latina, y que tiene un carácter comparativo en torno al caso ecuatoriano. Utiliza un diseño exploratorio-documental y siguiendo el protocolo PRISMA, se analizaron 38 fuentes de información seleccionadas entre los años 2018 y 2024. Se hallaron vulnerabilidades criticas dentro del sistema de ciberdefensa, por ejemplo, no existir un marco regulatorio que lo consolide, la falta de capacidades humanas especializadas en esta área, y escasa participación en alianzas internacionales de cooperación. En cambio, otros países de la región como Colombia, Chile o Brasil han avanzado notablemente en el desarrollo de estrategias nacionales de ciberseguridad. La investigación aborda el impacto práctico de estas debilidades en seguridad nacional o la gobernabilidad, particularmente frente a amenazas cibernéticas como lo son, ciberataques electorales, campañas de desinformación y fugas masivas de datos. La investigación también aborda el rol de tecnologías emergentes como inteligencia artificial y blockchain y como pueden ser incorporadas a los sistemas de defensa digital.

Revista electrónica TAMBARA, ISSN 2588-0977
Diciembre 2025-marzo 2026
Edición 28 No. 155, pp. 2498-2509

Manuscrito recibido: octubre 2025
Aceptado: noviembre 2025

Se concluye reforzando la urgencia de elaborar una estrategia nacional robusta e integrada, promoviendo la necesidad de avanzar en la cooperación regional como un eje predominante en la defensa digital Latinoamericana.

Palabras clave: Amenazas híbridas, ciberdefensa, cooperación regional, seguridad digital.

Códigos JEL: F51, F52, O33

ABSTRACT

This research addresses the growing phenomenon of hybrid threats that is taking place in Latin America, and which has a comparative character around the Ecuadorian case. It uses an exploratory-documentary design and following the PRISMA protocol, 38 sources of information selected between 2018 and 2024 were analyzed. Critical vulnerabilities were found within the cyber defense system, for example, the lack of a regulatory framework that consolidates it, the lack of specialized human capabilities in this area, and little participation in international cooperation alliances. On the other hand, other countries in the region such as Colombia, Chile or Brazil have made significant progress in the development of national cybersecurity strategies. The research addresses the practical impact of these weaknesses on national security or governance, particularly in the face of cyber threats such as electoral cyberattacks, disinformation campaigns and massive data leaks. The research also addresses the role of emerging technologies such as artificial intelligence and blockchain and how they can be incorporated into digital defense systems. It concludes by reinforcing the urgency of developing a robust and integrated national strategy, promoting the need to advance regional cooperation as a predominant axis in Latin American digital defense.

Keywords: Hybrid threats, cyber defense, regional cooperation, digital security.

JEL Codes: F51, F52, O33

1 INTRODUCCIÓN

Durante las dos últimas décadas, el contexto de seguridad internacional ha mutado de forma drástica como consecuencia del surgimiento de las amenazas híbridas, que combinan estrategias convencionales, irregulares y cibernéticas para desestabilizar Estados sin recurrir necesariamente a la confrontación (Álvarez-Valenzuela & Vera-Hott, 2022). Estas amenazas, las cuales incluyen operaciones de desinformación, ciberataques, coerción económica y manipulación de instituciones democráticas, suponen un reto especialmente complejo para países con capacidades tecnológicas limitadas y estructuras de defensa tradicionales, como suele ser el caso de muchas de naciones de América Latina.

La ciberdefensa, entendida como la capacidad estatal para proteger su infraestructura crítica, sus sistemas de información y su soberanía digital frente a los ciberataques ha emergido como eje estratégico dentro de las políticas de seguridad y defensa nacional (Fuertes et al., 2018). No obstante, en América Latina, los avances en este ámbito han sido desiguales. Mientras que Brasil o Colombia han estructurado capacidades institucionales y doctrinarias de ciberseguridad, otros como Ecuador se encuentran aún con importantes obstáculos vinculados

con inversiones, coordinación interinstitucional y formación de talento especializado (Flor-Unda et al., 2023).

En este orden, el presente trabajo se propone abordar las amenazas híbridas que enfrenta el país andino en su entorno virtual e intentar compararlas con su capacidad de respuesta ante otras naciones latinoamericanas, prestando atención a los marcos normativos, estructuras institucionales e intercambio en el área de ciberdefensa con socios regionales. Otro de los objetivos del presente estudio es la identificación de las vulnerabilidades que presenta el sistema ecuatoriano y la elaboración de lineamientos que tiendan hacia la mejora de su posicionamiento cibernético en una esfera geopolítica cada vez más compleja. Este enfoque comparativo se considera importante ya que Ecuador ha sido víctima de diversas formas de presiones externas y de sabotajes digitales oscilantes (Toapanta et al., 2019); por esta razón se propone una discusión crítica sobre el papel que juega el Estado a la hora de garantizar la protección cibernética del país, en la que se articulen elementos de seguridad, diplomacia y tecnología. En última instancia, el autor de este trabajo también intenta contribuir con el debate académico y político sobre la necesidad de una estrategia regional de ciberseguridad en Latinoamérica que contemple no solo los riesgos tecnológicos, sino que también tome en consideración las dimensiones asimétricas, la geopolítica y lo social que integran las híbridas amenazas actuales (Farah y Richardson, 2022; Solar, 2023).

El concepto de las amenazas híbridas ha tenido una creciente relevancia y un auge en el ámbito de la seguridad internacional y de la defensa a lo largo de las últimas dos décadas. Esta forma de amenazas se define por la combinación de herramientas convencionales y no convencionales —militares, cibernéticas, informativas, económicas o diplomáticas— empleadas por distintos actores, tanto estatales como no estatales, con el fin de conseguir objetivos de carácter estratégico sin la necesidad de recurrir a una guerra convencional (Álvarez-Valenzuela & Vera-Hott, 2022). La naturaleza ambigua hace que la identificación del posible agresor resulte difícil y permite llevar a cabo acciones hostiles sin una formalización del conflicto, quedando ubicada en la denominada "zona gris" de la guerra.

En el ámbito cibernético, las amenazas híbridas se ven intensificadas mediante el uso de las tecnologías digitales como instrumentos para desestabilizar regímenes, manipular la opinión de la sociedad o paralizar infraestructuras esenciales (Flor-Unda et al., 2023). En este contexto es donde introduce la ciberdefensa, la cual se considera, en sentido amplio, el conjunto de capacidades y de estrategias que se emplean para detectar, prevenir, mitigar o responder a ataques cibernéticos en los que se ve comprometida la seguridad nacional (Fuertes et al., 2018). En este sentido, se diferencia de la ciberseguridad, la cual se encuentra más vinculada a la protección de los sistemas informáticos, mientras que la ciberdefensa pondría en juego una cadena de capacidades que formarían parte de una estrategia del Estado que incluiría en su mezcla a los sectores militar, gubernamental y civil.

Históricamente, los Estados latinoamericanos han sido, (a diferencia de los de otras regiones), más vulnerables a este tipo de amenazas, ya que la baja inversión en tecnología, la debilidad institucional y una cooperación regional escasa han dado lugar a una condición de mayor vulnerabilidad (Solar, 2023). A esto se suma que las potencias extranjeras, entre ellas la República Popular China y la Federación de Rusia, han comenzado a utilizar geopolíticamente la ciberinteligencia con el propósito de incrementar las posibilidades de injerencias híbridas en

países que poseen capacidades tecnológicas aún menores, como Ecuador (Farah & Richardson, 2022). El resultado de esta simbiosis entre capacidades tecnológicas minúsculas y amenazas sofisticadas es un entorno asimétrico digital en el cual los Estados latinoamericanos se encuentran en situación de desventaja.

El marco teórico de esta investigación se fundamenta en los postulados de la teoría crítica de la seguridad y la misma implica un enfoque multidimensional del concepto de seguridad insertando elementos políticos, sociales y tecnológicos en el mismo. Desde esta perspectiva, las amenazas híbridas son entendidas como un fenómeno que no solo afecta a las capacidades militares, sino también a la soberanía de los Estados, a su democracia y a su desarrollo (Toapanta et al., 2019).

El estudio de las amenazas híbridas y la ciberdefensa en América Latina ha ido incrementándose en los años recientes, aunque hasta ahora lo ha hecho de forma fraccionada. En esto, varios autores han señalado que, a pesar de haber incrementado la frecuencia y la sofisticación de las ciberamenazas, muchos países de la región no han dictado normas sólidas ni disponen de políticas públicas efectivas en ciberseguridad nacional (Flor-Unda et al., 2023; Orellana, 2020).

En el caso específico de Ecuador, Fuertes et al. (2018) propusieron un modelo de ciberdefensa adaptativa basado en indicadores globales, derivando de su estudio que las instituciones presentan la existencia de una baja madurez institucional y una desconexión entre las políticas de seguridad y las capacidades tecnológicas. Toapanta y Sañicela (2019), por su parte, llevaron a cabo un análisis del proceso electoral ecuatoriano donde identificaron vulnerabilidades críticas en los sistemas informáticos del Consejo Nacional Electoral.

En el ámbito regional Solar (2023) estudió los marcos de gobernanza cibernética en América Latina donde mostró que Ecuador carece de una estrategia nacional cohesiva y de mecanismos de interoperabilidad con otros países; mientras que, Farah & Richardson (2022) concluyeron que los actores extranjeros están aprovechando las debilidades estructurales de varios Estados sudamericanos con la finalidad de hacer avanzar distintas agendas geoestratégicas mediante ciberoperaciones encubiertas.

Otros trabajos, como el desarrollado por Álvarez-Valenzuela y Vera-Hott (2022), abordan el vacío normativo en el derecho internacional sobre el tema de los ciberconflictos, lo que empeora la situación de los países con un marco normativo obsoleto o inexistente, mientras que Orellana (2020) aporta su visión desde la pequeña y mediana empresa, brindando el resultado de que incluso en el sector privado no existen protocolos de ciberseguridad elementales. Los estudios mencionados coinciden, en todo caso, en la imperiosa necesidad de articular políticas nacionales integrales, de invertir en capacitación y de crear mecanismos regionales de ciberdefensa ante amenazas híbridas

2 METODOLOGÍA

El presente estudio es de enfoque cualitativo con diseño exploratorio-documental, en la medida que persigue el examen de una problemática escasamente estudiada de forma sistemática y reflexiva: las amenazas híbridas en América Latina y la respuesta del Estado ecuatoriano a través de la capacidad de ciberdefensa. La investigación está orientada hacia la construcción de un

conocimiento teórico-conceptual y comparativo, basado en fuentes secundarias, ya que no se provocará una intervención directa en campo.

El diseño exploratorio documental es relevante para el tratamiento de fenómenos emergentes en los que los marcos teóricos son todavía difusos o escasos, como ocurre con la guerra híbrida en entornos digitales en América Latina. Siguiendo a Hernández, Fernández y Baptista (2014), el presente tipo de estudio facilita obtener aproximaciones iniciales a fenómenos complejos, lo que favorece la delimitación de variables y categorías fundamentales que son necesarias para investigaciones posteriores de corte empírico. Se justifica el enfoque cualitativo, dada la naturaleza interpretativa del objeto de estudio, por cuanto se busca comprender, analizar e interpretar los discursos, las estrategias y los marcos normativos referidos a la ciberseguridad y a la defensa en el Ecuador y en otros países de la región.

La investigación es no experimental, por cuanto no se manipulan variables, y es transversal, porque la recopilación y análisis de la información se realiza en un único momento del tiempo (Creswell & Creswell, 2018). Así mismo, es de tipo comparativo, porque se contrastan las políticas y capacidades de Ecuador con las de otros Estados latinoamericanos como Colombia, Chile y Brasil, en función de indicadores de ciberdefensa, amenazas híbridas y cooperación internacional.

La técnica fundamental utilizada es la revisión sistemática de literatura científica, normativa y documentos técnicos, siguiendo los lineamientos del protocolo PRISMA (Preffered Reporting Items for Systematic Reviews and Meta-Analyses), que fue propuesto por Moher et al. (2009). Ese protocolo permite asegurar transparencia, reproducibilidad y rigor metodológico en la selección, evaluación y análisis de fuentes documentales.

Con este propósito, se diseñó la estrategia de búsqueda, incorporando consonancias tales como: cyber defense, hybrid threats, cybersecurity, Latin America, Ecuador, national security, digital sovereignty y otras más. Se realizaron búsquedas en bases de datos científicas. Primordialmente en Scopus, SpringerLink, ScienceDirect, ProQuest, Google Scholar, y se incorporaron repositorios institucionales tales como: FLACSO Andes y el Repositorio de la ESPE.

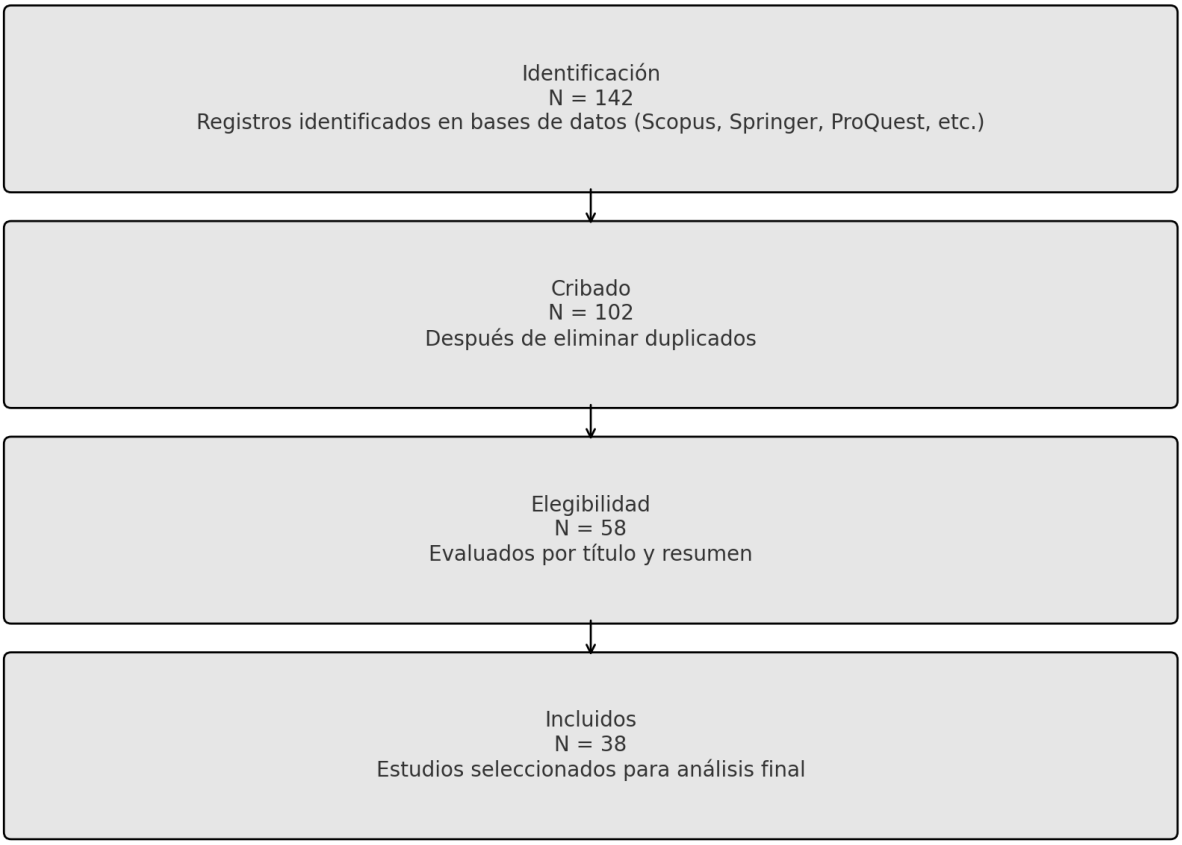
Los criterios de inclusión fueron: (a) publicaciones entre 2018 y 2024, (b) artículos revisados por pares, (c) documentos que mantengan consonancia al contexto latinoamericano y (d) artículos que mantuvieran consonancias con el tema en estudio, ciberdefensa y ciberseguridad. Las fuentes excluidas fueron publicaciones sin respaldo académico, documentos que no eran citables por ser de opinión y/o eran redundantes.

El análisis de los artículos se realizó mediante técnicas de análisis de contenido desde la vertiente temática y categorizada, organizando los resultados obtenidos a partir de las secciones principales: marcos normativos, capacidades institucionales, cooperación regional, vulnerabilidades cibernéticas y respuesta ante las amenazas híbridas. Se utilizó una técnica inductiva, permitiendo que emerjan categorías de los datos revisados (Gibbs, 2007).

3 RESULTADOS

La revisión sistemática mediante el protocolo PRISMA permitió identificar inicialmente 142 documentos, entre artículos científicos, informes técnicos y documentos institucionales. A partir de la aplicación de los criterios de inclusión y exclusión, se obtuvieron 38 fuentes de consenso, como se plantea en la Figura 1, que fueron analizadas tomando como base cinco dimensiones.

Figura 1: Método PRISMA



3.1. Marco normativo nacional e institucionalidad en ciberdefensa

La regulación y la gobernanza de la ciberseguridad en Ecuador son incipientes y fragmentarias. En comparación con los países de la región, como Colombia, que posee una política nacional integral sobre el tema desde el 2011, o Brasil, que se ha planteado el desafío de elaborar una Estrategia Nacional de Ciberseguridad (ENCC), en Ecuador se debe avanzar en la elaboración de un marco normativo único y actualizado (Solar, 2023; Flor-Unda et al., 2023). Si bien ha desarrollado y emitido algunas directrices para ello desde el Consejo de Seguridad del Estado (COSEPE), no ha podido elaborar la legislación pertinente y crear la agencia nacional de ciberdefensa de forma autónoma.

3.2. Capacidades técnicas y humanas

Evidencias obtenidas de informes a nivel regional (Fuertes et al., 2018; Toapanta & Sañicela, 2019) muestran que Ecuador está atrasado, incluso, a la hora de formar talento especializado en

el ámbito de ciberseguridad. En este sentido, el país no cuenta con una buena estrategia de desarrollo de capacidades para ello y la ciberdefensa queda restringida al ámbito militar, con escasa articulación con el ámbito civil o el académico. Como contraste, se pueden observan avances en diplomacia digital y programas universitarios de ciberseguridad en el caso de Chile, y, en Colombia, el funcionamiento de un Centro Cibernético Policial gestionado por la Policía Nacional.

3.3. Amenazas híbridas documentadas en Ecuador

Se pueden explicar al menos tres ejemplos de amenaza híbrida relevantes en el presente contexto:

- Filtración masiva de información personal (2019): afectaron a cerca de 17 millones de personas, incluida información de bases de datos de distintas instituciones de naturaleza pública y privada. De acuerdo con Solar (2023) este caso demuestra la fragilidad del Estado frente a las amenazas cibernéticas internas y externas.

- Ataques a los sistemas electorales (2019-2021): fáciles de rastrear en los procesos electorales, se daban como intrusiones, desinformación digital y suplantación de identidad de ciberactores, como se ha visto en estudios como el de Toapanta et al. (2019).
- Ciberespionaje político y campañas de desinformación: registradas por organizaciones como Access Now y Citizen Lab, relacionadas con conflictos internos y tensiones internacionales con otros Estados (Farah, R., & Richardson, 2022).

Estos ejemplos muestran cómo las tácticas híbridas se presentan de forma clara, en donde se aglutinan estrategias cibernéticas con fines geopolíticos y psicológicos.

3.4. Cooperación internacional y alianzas

A pesar de que participa en foros como el de la Organización de Estados Americanos (OEA) y el Foro de Cooperación América Latina-Asia del Este (FOCALAE), Ecuador tiene limitada participación en mecanismos multilaterales de ciberdefensa. Mientras que Colombia y México han suscrito memorandos de entendimiento con Estados Unidos y la Unión Europea sobre ciberseguridad (Álvarez-Valenzuela & Vera-Hott, 2022).

Igualmente, no se han encontrado acuerdos bilaterales públicos en torno a otros tipos de potencias tecnológicas (EE. UU., Estonia, Israel) donde se impulse la infraestructura crítica resiliente; y, en consecuencia, se limita la capacidad de respuesta ante éstas y se incrementa la vulnerabilidad del país.

3.5. Políticas públicas y estrategias nacionales

Ecuador no tiene una estrategia nacional de ciberdefensa consolidada. De acuerdo con el índice de la ciberseguridad global (UIT, 2021), Ecuador se posiciona en la agrupación de países con bajo nivel de preparación, por debajo de Uruguay, Chile y Brasil. En cambio, Argentina ha iniciado su andadura legislativa para poder afrontar las amenazas digitales desde una narrativa de derechos humanos, desarrollo y defensa.

La Tabla 1 expone el resumen comparativo de las dimensiones identificadas en la revisión bibliográfica: Marco legal, Capacidades humanas, Amenazas híbridas documentadas, Cooperación internacional y Estrategia nacional.

Tabla 1: Síntesis comparativa

Dimensión	Ecuador	Colombia	Chile	Brasil
Marco legal	Fragmentado, sin ley específica	Política Nacional desde 2011	Estrategia digital interministerial	Estrategia Nacional de Ciberseguridad (ENCC)
Capacidades humanas	Limitadas, poco articuladas	Centro Cibernético Policial	Formación universitaria específica	Formación militar y civil avanzada
Amenazas híbridas documentadas	Alta exposición (datos, elecciones, desinformación)	Actividad de APTs y cárteles	Ciberataques a infraestructura crítica	Uso de ciberdefensa en operaciones reales
Cooperación internacional	Limitada	Activa con EE.UU. y UE	Activa en la OEA	Miembro activo del MERCOSUR Digital
Estrategia nacional	No consolidada	Consolidada y evaluada	En ejecución	Implementada y en revisión periódica

4 DISCUSIÓN

Los resultados obtenidos en el presente estudio demuestran el notable grado de asimetría que existe entre las amenazas híbridas que tienen que lidiar los Estados latinoamericanos, y muy especialmente concretamente Ecuador, y sus respectivas capacidades institucionales para abordarlas de una forma sólida. Dicha asimetría, comporta un reto a nivel técnico, pero no es menos cierto que también se traduce en una amenaza estructural a la seguridad nacional, a la gobernanza democrática y a la soberanía digital.

4.1. Implicaciones prácticas para la defensa y la seguridad

Desde un punto práctico, los resultados apuntan a que Ecuador no tiene una estructura ciberdefensiva correctamente articulada, lo cual tiene un impacto directo sobre su capacidad para detectar, responder y recuperarse de ciberataques complejos en el marco de campañas híbridas. Las filtraciones masivas de datos personales, las intrusiones en procesos electorales y las campañas de desinformación son indicios empíricos de la gravedad de la exposición del país en tanto que tal. Este tipo de contexto, en el cual las amenazas híbridas se han manifestado a

través de ciberataques, debe conducir a que los entornos de defensa realicen una integración de las doctrinas de ciberdefensa tanto a nivel estratégico como a nivel operativo. Así las Fuerzas Armadas no deben tener únicamente un enfoque de reacción, sino que al mismo tiempo deben desarrollar capacidades preventivas y realizar un control permanente del ciberespacio. Implica la creación de centros de operaciones cibernéticas (COC) y el trabajo colaborativo con las agencias civiles, las universidades y el sector privado (Flor-Unda et al., 2023; Fuertes et al., 2018).

Así mismo, la falta de normas específicas y de instancias reguladoras independientes limita la acción coordinada ante las amenazas transnacionales; países con estructuras de ordenamiento jurídico y operativo más avanzadas, como Colombia o Chile, tienen mejor eficiencia en cuanto a la preparación y la resiliencia.

4.2. Importancia de las tendencias tecnológicas emergentes

Los resultados también confirmaron que mientras las amenazas se van constituyendo mediante tecnologías avanzadas —como la inteligencia artificial (IA), el big data, los deepfakes o las redes automatizadas de bots— no existen actualmente aplicaciones tecnológicas que se integren en los Estados como Ecuador que den soporte a sus sistemas de defensa y a la vigilancia. Esta disrupción tecnológica profundiza la vulnerabilidad de los Estados y los coloca en situación de desventaja ante actores con capacidades ofensivas avanzadas.

Las tecnologías emergentes no solo implican retos, sino también oportunidades para reforzar las capacidades estratégicas del Estado. La utilización de IA para controlar patrones anómalos, los algoritmos de machine learning para el desarrollo de ciberinteligencia y los sistemas blockchain para la defensa de infraestructuras críticas podrían llegar a cambiar la postura defensiva del país. Sin embargo, su implementación requiere de relativa infraestructura y de políticas públicas en la línea de la innovación y de la formación de talento humano especializado (Solar, 2023).

4.3. Vacíos objetivos en la literatura y en la política pública

Uno de los elementos más significativos del trabajo realizado ha consistido en establecer vacíos objetivos críticos sobre la literatura y la política pública de ciberdefensa en Ecuador: Escasa documentación sobre amenazas híbridas en Ecuador: la mayoría de los estudios indicados son descriptivos y no abordan análisis profundos sobre las amenazas físicas, digitales y psicológicas. Falta de estudios comparados con el resto de las regiones: no existen investigaciones suficientes que contrapongan la situación de Ecuador con los países de la región, lo que dificulta establecer estrategias regionales coordinadas y basadas en evidencias. Falta de indicadores y adecuada evaluación de desempeño: Ecuador carece de indicadores formales para evaluar el grado de ciberdefensa, lo que obstaculiza el aprendizaje institucional. Total, desprecio de los derechos humanos: en la mayoría de las políticas analizadas no se llevan a cabo garantías de privacidad, libertad de expresión o rendiciones de cuentas.

5 CONCLUSIONES

El estudio en curso ha permitido contrastar, de manera comparativa, las condiciones con las que Ecuador enfrenta las ciberamenazas híbridas, en relación a otros países de América Latina. Asimismo, y a partir de la revisión de literatura científica, normativa y documentos técnicos, se identificaron aquellos elementos clave para comprender el estado actual del país en términos de ciberdefensa, gobernanza digital y preparación estratégica. Uno de esos aprendizajes centrales es que Ecuador es un país con un cierto retraso estructural de la construcción y la implementación de políticas de ciberdefensa frente a las ciberamenazas híbridas.

La literatura revisada es concordante en que Ecuador no cuenta con el soporte normativo, las instituciones especializadas, y las capacidades técnicas y humanas para responder efectivamente a ciberataques complejos, flujos masivos de datos, o a campañas desinformativas. Efectivamente, se evidencia que otros países de la región como son Colombia, Brasil y Chile han iniciado un proceso de transición hacia un modelo de ciberseguridad integral, a diferencia de Ecuador que opera con un sistema fragmentado, con falta de articulación entre el sector civil, militar, académico y privado. Ello deja al país, como es natural, en una amplia brecha correspondiente a la vulnerabilidad estratégica, no solo frente a actores externos, también frente a las amenazas internas de las que se tiene constancia, pero que se ven potenciadas por el entorno digital.

A partir del análisis realizado, se sugiere que en futuras investigaciones se debería profundizar en estudios empíricos sobre las amenazas híbridas en Ecuador, integrando enfoques interdisciplinarios que no solo aborden los aspectos técnicos, sino también los políticos, sociales y jurídicos. Además, es crucial fomentar estudios comparativos regionales más sistemáticos que ayuden a identificar las mejores prácticas y a promover marcos de cooperación en defensa cibernética entre países con contextos similares. En términos prácticos, se recomienda establecer un centro nacional de ciberdefensa multidisciplinario, que cuente con la participación de diversas instituciones y que tenga la capacidad de interoperar con actores internacionales.

También es necesario desarrollar protocolos y sistemas de alerta temprana, especialmente para proteger infraestructuras críticas, procesos electorales y sistemas de información gubernamentales. Por último, invertir en educación especializada en ciberseguridad, desde el nivel universitario hasta la formación militar, debe ser una prioridad nacional para disminuir la dependencia tecnológica externa. Los resultados de esta investigación refuerzan la idea de que la ciencia y la tecnología no son solo herramientas complementarias, sino elementos centrales en la defensa nacional del siglo XXI. La innovación tecnológica aplicada a la seguridad permite anticipar amenazas, crear sistemas de defensa resilientes y consolidar la soberanía digital de los Estados.

En este contexto, Ecuador necesita reconocer que fortalecer sus capacidades tecnológicas es esencial para llevar a cabo una defensa nacional efectiva en situaciones híbridas, donde las líneas entre guerra, diplomacia, economía y tecnología se vuelven cada vez más borrosas. Por lo tanto, es crucial que la política pública en defensa y seguridad integre de manera estructural una perspectiva fundamentada en el conocimiento científico, el desarrollo tecnológico y la cooperación internacional, ya que estos son pilares clave para enfrentar los desafíos de un mundo interconectado y cada vez más conflictivo en el ámbito digital.

REFERENCIAS BIBLIOGRÁFICAS

Álvarez-Valenzuela, D., &Vera-Hott, F. (2022). Cyber operations in South America. Baltic Yearbook of International Law, 20(1), 163-190. https://brill.com/view/journals/byio/20/1/article-p163_9.xml

Creswell, J. W., & Creswell, J. D. (2018).Research design: Qualitative, quatitative, and mixed methods approaches (5th ed.). SAGE Publications.

Farah, D., & Richardson, M. (2022). Dangerous alliances: Russia's strategic inroads in latin America. Strategic Perspectives, 10. https://digitalcommons.ndu.edu/inss-strategic-perspectives/10/

Flor-Unda, O., Simbaña, F., Larriva-Novo, X., & Acuña, Á. (2023). A comprehensive analysis of the worst cubersecurity vulnerabilities in Latin America. Informatics, 10(3), 71. https://www.mdpi.com/2227-9709/10/3/71

Fuentes, W., Bustamante, F., Toulkeridis, T., & Peláez, J. (2018). Situational status of global cybersecurity and cyber defense according to global indicators. Adaptation of a model for Ecuador. In Cybersecurity and Cyberdefense (pp. 25-42). Springer. https://www. researchgate.net/publication/345142742

Gibbs, G. (2007). Analyzing quallitative data. SAGE Publications.

Hernández, R., Fernández, C., & Baptista, P. (2014). Metodología de la investigación (6ªed.). McGraw-Hill

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. PLos Medicine, 6(7), e1000097. https://doi.org/10.1371/journal.pmed.1000097

Orellana, F. D. (2020). Cybersecurity incident response capabilities in the Ecuadorian small business sector: A qualitative study. ProQuet Dissertations. https://search.proquest.com/openview/05929b02aa9fe10cbad74c6880aaa513

Solar, C. (2023). Cybersecurity governance in Latin America: States, threats, and alliances. Google Books. https://books.google.com/books?hl=en&id=BOWbEAAAQBAJ

Toapanta, S. M. T., & Sañicela, S. X. R. (2019). Analsis of information security for a voting process for sectional governments in Ecuador. Advances in Science, Technology and Engineering Systems Journal, 4(6), 72-80. https://www.researchgate.net/publication/337447242