

El artículo propone un Modelo Operativo de Defensa Híbrida (MODH) para fortalecer la transformación estratégica de la defensa nacional frente a las amenazas híbridas en América Latina. Mediante una investigación cualitativa basada en revisión de literatura y análisis comparado, identifica brechas doctrinales, tecnológicas e institucionales y plantea un modelo sustentado en doctrina adaptativa, arquitectura cibernética, liderazgo resiliente, interoperabilidad multisectorial y planificación predictiva. Se concluye que la integración de estas dimensiones fortalece la capacidad de respuesta y la resiliencia de los sistemas de defensa regionales.

TRANSFORMACIÓN ESTRATÉGICA DE LA DEFENSA NACIONAL ANTE AMENAZAS HÍBRIDAS: UN MODELO OPERATIVO PARA AMÉRICA LATINA



STRATEGIC TRANSFORMATION OF NATIONAL DEFENSE IN THE FACE OF HYBRID THREATS: AN OPERATIONAL MODEL FOR LATIN AMERICA

This article proposes an Operational Hybrid Defense Model (OHDM) to strengthen the strategic transformation of national defense against hybrid threats in Latin America. Using a qualitative approach based on literature review and comparative analysis, it identifies doctrinal, technological, and institutional gaps and presents a model built on adaptive doctrine, cyber architecture, resilient leadership, multisectoral interoperability, and predictive planning. The study concludes that integrating these dimensions enhances resilience and defense capabilities in the region.



Villena, J. (2026). Transformación estratégica de la defensa nacional ante amenazas híbridas: un modelo operativo para América Latina. *Revista Pensamiento Conjunto*, Año 14, N° 1. pp. 92-100. ISSN° 2707-367X

Fecha de recepción: 31 de mayo de 2026.
Fecha de aceptación: 22 de junio de 2026.
Fecha de publicación: 30 de junio de 2026.

INTRODUCCIÓN

El orden internacional contemporáneo se halla sometido a tensiones estructurales que trascienden los paradigmas convencionales del conflicto armado, por lo tanto, la irrupción de las denominadas amenazas híbridas —entendidas como la combinación sincrónica de medios militares, cibernéticos, económicos, desinformativos y criminales orientados a erosionar la cohesión del Estado— ha reconfigurado de manera profunda el espacio conceptual y operativo de la seguridad nacional (Hoffman, 2007, p. 8). América Latina no es ajena a esta transformación: la región enfrenta un escenario de creciente complejidad en el que los actores estatales y no estatales explotan las vulnerabilidades sistémicas de los Estados para alcanzar objetivos estratégicos por debajo del umbral de la guerra convencional.

La literatura especializada ha avanzado significativamente en la caracterización del fenómeno híbrido; sin embargo, persiste un déficit notable en la producción de modelos operativos que permitan a los sistemas de defensa latinoamericanos responder de manera articulada a esta tipología de amenaza, bajo esta línea de análisis Arias y Benavides (2025), señalan que "las Fuerzas Armadas de la región carecen de marcos doctrinales unificados que integren la dimensión cibernética con la acción convencional" (p. 47), lo que genera inconsistencias operacionales críticas frente a adversarios que actúan en múltiples dominios de forma simultánea.

El presente artículo aborda este vacío mediante la propuesta del Modelo

PALABRAS CLAVE: AMENAZAS HÍBRIDAS; DEFENSA NACIONAL; TRANSFORMACIÓN ESTRATÉGICA; CIBERDEFENSA; PLANIFICACIÓN PREDICTIVA.

KEYWORDS: HYBRID THREATS; NATIONAL DEFENSE; STRATEGIC TRANSFORMATION; CYBER DEFENSE; PREDICTIVE PLANNING.



Magíster
José Luis Anderson
Villena Balladares

Licenciado en Ciencias Militares por la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi". Ingeniero en Telecomunicaciones por la Universidad Nacional Federico Villarreal. Magíster en Ciencias Militares por la Escuela Superior de Guerra del Ejército y Magíster en Gestión Pública por la Universidad Nacional Mayor de San Marcos. Actualmente es doctorando en Administración por la Universidad Continental. Ha cursado Operaciones Cibernéticas por el Centro de Altos Estudios Nacionales (CAEN), Programa Complementario del Arma de Comunicaciones, Programa Básico del Arma de Inteligencia, Programa Básico de Inteligencia y Diplomado en Empleo de Grandes Unidades tipo Batallón de Comunicaciones. Ha realizado el Programa de Inteligencia y Análisis de Operaciones Transnacionales en el Western Hemisphere Institute for Security Cooperation (WHINSEC), Estados Unidos.



Operativo de Defensa Híbrida (MODH), un marco integrador de cinco dimensiones que articula el pensamiento estratégico clásico con las exigencias de la guerra del siglo XXI. La relevancia de la propuesta se sustenta en la convergencia de tres tendencias: (a) el incremento sostenido de las operaciones híbridas en el entorno geopolítico global, particularmente en el Indo-Pacífico y sus repercusiones sobre América Latina (Gualberto, 2024, p. 194); (b) la aceleración de la transformación digital en los sistemas de defensa (Torres et al., 2025, p. 143); y (c) la insuficiencia de los modelos de planificación estratégica vigentes ante escenarios de incertidumbre radical (Bertin, 2024, p. 12).

Metodológicamente, el artículo adopta un diseño cualitativo de carácter teórico-analítico que combina la revisión sistemática de literatura con el análisis comparado de marcos normativos y doctrinales regionales, las fuentes primarias incluyen políticas nacionales de defensa, documentos estratégicos institucionales y estudios de caso empíricos, mientras que el corpus teórico integra obras fundacionales del pensamiento estratégico-militar y producción académica, el artículo se organiza en seis secciones: tras la presente introducción, la sección 2 desarrolla el marco teórico-conceptual; la sección 3 presenta el diagnóstico regional de amenazas; la sección 4 expone el modelo MODH; la sección 5 analiza su aplicabilidad a través de estudios de caso; y la sección 6 articula las conclusiones y recomendaciones.

RESULTADOS

El pensamiento estratégico-militar constituye la base intelectual de las arquitecturas de defensa modernas, iniciando desde la perspectiva clásica de Sun Tzu (1999) donde sostuvo que “el supremo arte de la guerra consiste en someter al enemigo sin combatir” (p. 18), principio vigente frente a amenazas híbridas, donde la disuasión se proyecta en los dominios cognitivo y de influencia. Esta tradición fue ampliada por Paret (1986), quien identificó una tensión persistente entre rigidez doctrinal y adaptabilidad táctica, especialmente relevante ante la complejidad tecnológica contemporánea, asimismo, Mahan (1911) destacó la importancia del control de las líneas de comunicación marítima como factor del poder na-

cional (p. 89), principio que hoy puede trasladarse al ciberespacio mediante el control de infraestructuras digitales críticas, como cables submarinos, nodos de comunicación y sistemas SCADA.

En una línea similar, Douhet (2001) planteó que el dominio aéreo era condición para la victoria (p. 23), función estratégica que actualmente encuentra un equivalente en el ciberespacio como quinto dominio operacional, finalmente, Ramos (2020) señala que el pensamiento estratégico latinoamericano ha tendido históricamente hacia la imitación de doctrinas foráneas sin la debida contextualización regional (p. 363), lo cual ha generado marcos conceptuales inadecuados para las realidades sociopolíticas específicas del subcontinente, esta observación resulta central para la propuesta del MODH, que parte de la necesidad de desarrollar doctrina autóctona fundada en las particularidades geopolíticas, institucionales y culturales de la región.

La conceptualización de las amenazas híbridas permite comprender la convergencia de medios convencionales, tácticas irregulares, criminalidad, terrorismo, coerción económica, desinformación y capacidades cibernéticas en los conflictos contemporáneos, como la definición de guerra Híbrida de Hoffman (2007) “el empleo simultáneo de capacidades militares convencionales, tácticas y formaciones irregulares, actos terroristas y comportamientos criminales en el mismo espacio de batalla” (p. 14), concepto inicialmente asociado al conflicto libanés de 2006 y luego ampliado hacia los dominios informativo, económico y cibernético.

En América Latina, estas amenazas adquieren una especificidad vinculada a la fragilidad institucional y al crimen organizado transnacional; por ello, Leonardo (2025) advierte que “la región enfrenta un escenario en el que el crimen organizado adopta capacidades propias de actores estatales, difuminando la frontera entre seguridad pública y defensa nacional” (p. 3). Esta tendencia se evidencia en el caso ecuatoriano, donde Arias y Benavides (2025) identifican la convergencia entre amenazas cibernéticas y operaciones criminales como factor de una crisis de gobernanza sin precedentes (p. 52). Para graduar su análisis, Muñoz (2024) distingue tres ni-



veles de intensidad: interferencia estratégica, desestabilización activa y confrontación híbrida abierta (pp. 34-38), taxonomía útil para el modelo MODH al permitir diferenciar umbrales de amenaza y articular respuestas entre seguridad pública, defensa nacional, inteligencia estratégica, ciberdefensa y protección de infraestructura crítica.

La transformación digital redefine la defensa al incorporar tecnologías emergentes y nuevas exigencias organizacionales, por tanto, Aguilar (2017) destaca que la ciberresiliencia requiere colaboración público-privada, pues “ningún Estado puede enfrentar de manera solitaria la sofisticación creciente de los actores cibernéticos hostiles” (p. 43), asimismo, Torres et al. (2025) señalan que la inteligencia artificial, los sistemas autónomos, la computación cuántica y la cadena de bloques transforman el conflicto armado (p. 147), no obstante, su adopción exige madurez digital, capacidades dinámicas y cultura de innovación (Weritz et al., 2020, p. 6). En este marco, el blockchain fortalece el comando y control, la trazabilidad logística y la verificación de identidades (Palomo, 2018, pp. 892-895), mientras que la inteligencia artificial incrementa la eficiencia operacional, aunque introduce vulnerabilidades sistémicas que deben gestionarse anticipadamente (Avendaño et al., 2024, p. 6205).

El liderazgo transformacional en el sector defensa es el articulador de visión estratégica a ejecución táctica en entornos inciertos, como sostiene Calderón y Sánchez (2023) que el “liderazgo militar del siglo XXI exige competencias éticas, comunicacionales y adaptativas más allá de la formación técnica tradicional” (p. 18), en la misma línea, Fernández (2024) señala que la gobernabilidad en crisis requiere líderes capaces de generar confianza institucional y gestionar la ambigüedad estratégica (p. 61), mientras que Csombók (2023) afirma que la confianza moral es la base de la autoridad transformacional, pues “sin una base ética sólida, la transformación digital en las organizaciones genera alienación y resistencia en lugar de compromiso” (p. 7), asimismo, Fachrunisa et al. (2020) evidencian que el liderazgo y la flexibilidad estratégica favorecen la transformación digital en organizaciones complejas (p. 77), lo que aplicado al ámbito militar exige líderes sistémicos,

adaptativos y capaces de conducir organizaciones en red.

DIAGNÓSTICO REGIONAL: AMENAZAS HÍBRIDAS EN AMÉRICA LATINA

América Latina atraviesa una bifurcación estratégica marcada por la rivalidad geopolítica entre China y Estados Unidos, cuyos efectos se proyectan sobre la seguridad, la economía y la autonomía decisional de la región (Gualberto, 2024, p. 196), en este escenario, el Perú y los países andinos enfrentan amenazas híbridas asociadas al crimen organizado transnacional, la desinformación, la vulnerabilidad de infraestructuras críticas y la presión de potencias extrarregionales (Eduardo, 2025a, p. 5), Sin embargo, la respuesta regional ha sido fragmentada y asimétrica, debido a diferencias en capacidades cibernéticas, rigidez doctrinal y persistencia de modelos organizacionales centrados en el conflicto convencional (Magnani, 2024, p. 15).

En el caso peruano, la seguridad y defensa nacional han sido históricamente subordinadas a otras prioridades políticas, generando déficits de capacidades frente a amenazas emergentes (Vivanco, 2024, p. 21), a ello se suman vulnerabilidades estructurales recurrentes: fragmentación doctrinal, brechas de ciberdefensa, déficit de inteligencia estratégica, rigidez institucional y descoordinación multisectorial, es así que, Muñoz (2024) advierte que la mayoría de países carece de doctrina integrada para la defensa híbrida, limitándose a adaptar marcos externos, principalmente atlánticos (pp. 41-44); Arias y Benavides (2025) evidencian, en el caso ecuatoriano, la exposición crítica de infraestructuras digitales por ausencia de arquitectura de ciberdefensa operativa (p. 55); Castro (2024) identifica limitaciones ético-legales y técnicas en inteligencia estratégica regional (pp. 9-12); Jaramillo y Ortiz (2024) destacan la persistencia de currículos militares rígidos, centrados en competencias técnico-tácticas antes que en pensamiento crítico y adaptación estratégica (p. 5); y Amado (2024) señala, para el caso peruano, la falta de articulación entre seguridad, defensa y políticas económicas, ambientales y digitales (p. 19).

Finalmente, la seguridad ambiental emerge como



dimensión estratégica de las amenazas híbridas, pues la degradación ambiental, la escasez hídrica y los fenómenos climáticos extremos actúan como multiplicadores de conflictividad, migración y penetración de actores violentos no estatales (Buelvas et al., 2023, p. 67), en consecuencia, las Fuerzas Armadas latinoamericanas, y particularmente las peruanas, están llamadas a desempeñar un rol estratégico ampliado frente a crisis globales, desastres, pandemias y conflictos migratorios, lo que exige una transformación doctrinal, organizacional y tecnológica acorde con un sistema de seguridad multidimensional (Eduardo, 2025b, p. 8).

EL MODELO OPERATIVO DE DEFENSA HÍBRIDA (MODH)

El Modelo Operativo de Defensa Híbrida (MODH) propone una arquitectura sistémica para responder a amenazas híbridas mediante capacidades adaptativas, liderazgo transformacional y articulación nacional-regional. Supera la lógica lineal de amenaza-respuesta al reconocer que los riesgos contemporáneos operan en múltiples dominios y requieren respuestas integradas. Su base metodológica es la planificación basada en capacidades, entendida como el desarrollo de capacidades militares orientadas a escenarios futuros de ame-

naza y no solo a riesgos presentes (Bertin, 2024, p. 15).

El modelo se organiza en cinco dimensiones interdependientes: (a) Doctrina Adaptativa, orientada a construir una doctrina regional flexible frente al conflicto híbrido, cuya transformación exige revisar supuestos estratégicos y no solo actualizar terminología (Sánchez, 2021, p. 12); (b) Arquitectura Cibernética, centrada en proteger infraestructuras críticas, desarrollar comandos cibernéticos, SOC militares y capacidades de disuasión activa, bajo un enfoque técnico, jurídico y público-privado (Rutz, 2021, p. 4; Gallardo et al., 2022, pp. 47-52); (3) Liderazgo Resiliente, que reconoce el papel de la cultura organizacional, la formación adaptativa y el liderazgo distribuido en el desempeño institucional (Peña y Caruajulca, 2024, p. 306; Jaramillo y Ortiz, 2024, p. 7); (d) Interoperabilidad Multisectorial, dirigida a coordinar defensa, seguridad, inteligencia, diplomacia, economía y comunicaciones mediante instancias interministeriales con capacidad ejecutiva real (Amado, 2024, p. 22); y (e) Planificación predictiva, que integra inteligencia estratégica, análisis de escenarios, alerta temprana e inteligencia artificial, entendida como amplificador de la inteligencia humana y no como sustituto del juicio estratégico (Contreras, 2024, pp. 62-67).

TABLA 1. ESTRUCTURA DEL MODELO OPERATIVO DE DEFENSA HÍBRIDA (MODH)

Dimensión	Componentes clave	Objetivo estratégico	Referentes doctrinales
a. Doctrina Adaptativa	Doctrina integrada, POE multidominio, armonización regional	Marco conceptual unificado para amenazas híbridas	Hoffman (2007); Paret (1986)
b. Arquitectura Cibernética	Comando Cibernético, SOC militar, disuasión activa	Dominio y resiliencia en el ciberespacio	Aguilar (2017); Rutz (2021)
c. Liderazgo Resiliente	Formación adaptativa, cultura organizacional, liderazgo distribuido	Capital humano transformador	Fernández (2024); Csombók (2023)
d. Interoperabilidad Multisectorial	Coordinación interministerial, cooperación regional, protocolos conjuntos	Respuesta integrada multi-institucional	Amado Asenjo (2024); Eduardo (2025a)
e. Planificación predictiva	IA, análisis de escenarios, alerta temprana, simulaciones	Capacidad predictiva y respuesta proactiva	Contreras Machado (2024); Bertin Wiehoff (2024)

Nota. Elaboración propia con base en el análisis de la literatura especializada.



APLICABILIDAD DEL MODH: ESTUDIOS DE CASO

La aplicabilidad del Modelo Operativo de Defensa Híbrida (MODH) se evidencia en los casos de Ecuador y Perú, donde las amenazas híbridas han expuesto brechas doctrinales, cibernéticas, institucionales y multisectoriales, así como en Ecuador, la convergencia de ataques cibernéticos, desinformación y violencia del crimen organizado generó una crisis multidimensional que superó las capacidades estatales existentes (Arias y Benavides, 2025, pp. 48-59). Desde el MODH, el caso revela déficits en doctrina adaptativa, arquitectura cibernética e interoperabilidad; no obstante, también muestra que la crisis puede actuar como catalizador de transformación, acelerando capacidades cibernéticas y revisión doctrinal (Arias y Benavides, 2025, p. 61).

En el Perú, la construcción de la Política Nacional Multisectorial de Seguridad y Defensa Nacional al 2030 representa un avance relevante, aunque todavía incompleto, para articular seguridad, defensa, transformación digital y respuesta ante amenazas híbridas (Amado, 2024, pp. 17-23), asimismo, la incorporación de drones en operaciones de seguridad ciudadana evidencia el potencial de las tecnologías emergentes, pero también la necesidad de marcos jurídicos, protocolos operacionales y formación especializada (Febres, 2025, pp. 43-58), en conjunto, ambos casos muestran que la implementación del MODH exige adaptación nacional, cooperación regional, priorización estratégica de recursos y participación de la academia, el sector privado y la sociedad civil, además, la resiliencia económica resulta indispensable para sostener procesos de modernización defensiva en el tiempo, pues “un sistema de defensa eficaz requiere una economía suficientemente resiliente para sostener el esfuerzo de modernización” (Chichulina et al., 2024, p. 4).

DISCUSIÓN

Los resultados confirman que América Latina enfrenta un escenario de amenazas híbridas frente al cual sus sistemas de defensa presentan brechas doctrinales, tecnológicas, institucionales y humanas, esta constatación, valida la hipótesis central del estudio: la transformación estratégica no puede

abordarse desde una sola dimensión, sino mediante respuestas sistémicas e integradas, en este sentido, el MODH aporta un marco adaptado al contexto latinoamericano, al reconocer sus particularidades geopolíticas, institucionales y culturales, evitando la importación acrítica de modelos externos, una limitación recurrente del pensamiento estratégico regional señalada por Ramos Rojas (2020, p. 364), de igual forma, el modelo concibe la transformación estratégica como un proceso no lineal ni secuencial, sino simultáneo en sus dimensiones doctrinal, cibernética, humana, multisectorial y predictiva; los casos de Ecuador y Perú evidencian que priorizar únicamente la tecnología, sin acompañarla de cambios doctrinales, jurídicos y organizacionales, genera respuestas incompletas frente a amenazas híbridas.

En cuanto a la inteligencia artificial, el estudio adopta una posición equilibrada: reconoce su valor para fortalecer la predicción, el análisis de escenarios y la toma de decisiones, pero advierte que no debe reemplazar el juicio estratégico humano; en esa línea, Contreras (2024) sostiene que la IA debe operar como amplificador de la inteligencia humana y no como sustituto del discernimiento estratégico (p. 67), finalmente, la investigación evidencia que la interoperabilidad regional constituye un desafío no solo técnico, sino también político, pues exige confianza institucional, armonización normativa, cooperación sostenida e intercambio seguro de información sensible, por ello, la transformación estratégica de la defensa latinoamericana demanda una agenda académica y política orientada a fortalecer capacidades compartidas, resiliencia institucional y cooperación regional frente a amenazas que trascienden las fronteras nacionales.

CONCLUSIONES

- Este artículo ha propuesto el Modelo Operativo de Defensa Híbrida (MODH) como respuesta a la insuficiencia de los marcos de análisis y actuación existentes ante la creciente prevalencia de las amenazas híbridas en América Latina, las conclusiones principales pueden sintetizarse en cinco proposiciones:
- Las amenazas híbridas constituyen el desafío estratégico definitorio del siglo XXI para las fuer-



zas armadas latinoamericanas, y su naturaleza multidimensional exige respuestas igualmente multidimensionales que integren capacidades militares, cibernéticas, informativas y diplomáticas en marcos operacionales coherentes.

- Los sistemas de defensa de la región presentan brechas estructurales críticas en las cinco dimensiones del MODH —doctrina, ciberseguridad, liderazgo, interoperabilidad y planificación— que no pueden ser subsanadas mediante inversiones sectoriales aisladas, sino que requieren estrategias de transformación integrales y sostenidas.
- La transformación estratégica efectiva no es primariamente un fenómeno tecnológico sino cultural e institucional. La modernización de equipos y sistemas sin la correspondiente transformación de la cultura organizacional, los modelos de liderazgo y los marcos doctrinales produce resultados subóptimos e insostenibles en el tiempo.
- La dimensión regional es inseparable de la dimensión nacional en la respuesta a las amenazas híbridas. Los actores hostiles operan en ecosistemas transfronterizos que las respuestas puramente nacionales no pueden contener. La cooperación regional en inteligencia, ciberseguridad y planificación estratégica es una condición de posibilidad de la defensa nacional efectiva.
- La academia, el sector privado y la sociedad civil son actores imprescindibles —no complementarios— de la transformación estratégica de la defensa. La complejidad de las amenazas contemporáneas supera las capacidades exclusivas de las instituciones militares y demanda ecosistemas de conocimiento y colaboración que las fuerzas armadas latinoamericanas deben construir activamente.

RECOMENDACIONES

Con base en las conclusiones anteriores, el artículo formula las siguientes recomendaciones dirigidas a los decisores de política de defensa en América Latina:

- Actualizar las políticas nacionales de seguridad y defensa incorporando el enfoque de

amenazas híbridas, de modo que integren capacidades militares, cibernéticas, informativas, diplomáticas y de inteligencia bajo un marco operacional común.

- Adoptar el MODH como matriz de transformación integral, fortaleciendo simultáneamente sus cinco dimensiones: doctrina adaptativa, arquitectura cibernética, liderazgo resiliente, interoperabilidad multisectorial y planificación predictiva.
- Reformar la educación y capacitación militar para desarrollar líderes con pensamiento crítico, competencias digitales, visión estratégica, capacidad de adaptación y comprensión de las amenazas híbridas.
- Fortalecer la cooperación regional mediante mecanismos permanentes de inteligencia estratégica, ciberseguridad, alerta temprana, ejercicios conjuntos y protocolos seguros de intercambio de información.
- Institucionalizar plataformas de cooperación entre Fuerzas Armadas, academia, sector privado y sociedad civil, orientadas a investigación aplicada, innovación tecnológica, ciberresiliencia y formación especializada.

REFERENCIAS

- Aguilar, L. J. (2017). Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0). *Cuadernos de Estrategia*, (185), 19–64.
- Amado Asenjo, C. (2024). Preparación de la Política Nacional Multisectorial de Seguridad y Defensa Nacional al 2030 del Perú ante amenazas de transformación digital y guerras híbridas. *Seguridad y Política*, 3(1). <https://doi.org/10.56221/spt.v3i1.47>
- Arias Peña, C. F., & Benavides Ortiz, G. G. (2025). Amenazas híbridas y ciberdefensa en América Latina: el caso de Ecuador. En T. Tambara (Ed.), *Seguridad híbrida y ciberdefensa en América Latina* (pp. 43–68). Tambara-Instituto de Estudios.
- Avendaño Barrera, J., Sánchez Torres, Y., & Velazco Alarcón, L. (2024). La tecnología y su impacto en la gestión de procesos y estrategias de au-



- tomatización. *Ciencia Latina Revista Científica Multidisciplinar*, 8(4), 6198–6221. https://doi.org/10.37811/CL_RCM.V8I4.12822
- Bertin Wiehoff, C. (2024). América Latina y el desafío de la planificación basada en capacidades. *Revista Política y Estrategia*, 143, 9–28. <https://dialnet.unirioja.es/descarga/articulo/10247895.pdf>
- Buelvas, E. P., Cabrera Ortiz, F., & Sandner, J. (Eds.). (2023). *Estrategias de seguridad ambiental en América Latina y el Caribe: construyendo resiliencia*. Opciones Gráficas.
- Calderón Arregui, D., & Sánchez Gordon, W. (2023). El camino hacia el liderazgo militar de excelencia: estrategias para formar líderes efectivos en la Escuela Superior Militar «Eloy Alfaro». *Revista de Ciencias de Seguridad y Defensa*, 8(3), 1–22. <https://doi.org/10.24133/RCSD.VOL08.N03.2023.02>
- Castro González, L. G. (2024). La ética y la actividad de inteligencia para la seguridad nacional. *Revista de Ciencia e Investigación en Defensa*, 5(3), 6–18. <https://doi.org/10.58211/d86qp338>
- Chichulina, K., Klievtsievych, N., Kharchenko, O., Zadorozhna, O., & Sanchenko, G. (2024). Economic policy adjustments amidst military conflict: Strategies for sustaining economic and financial stability. *Salud, Ciencia y Tecnología – Serie de Conferencias*, 3. <https://doi.org/10.56294/sctconf2024.1137>
- Contreras Machado, J. L. (2024). Toma de decisiones estratégicas en la defensa nacional: un abordaje desde la inteligencia artificial. *Revista Científica de la Escuela Superior de Guerra del Ejército*, 3(1), 57–70. <https://doi.org/10.60029/rcesge.v3i2arti5>
- Csombók, J. (2023). Challenges of transformational leadership in the digital age: The role of moral trust in maintaining transformational approaches. <https://doi.org/10.24405/14925>
- Douhet, G. (2001). *El dominio del aire*. Ministerio de Defensa. (Trabajo original publicado en 1921)
- Fachrunnisa, O., Adhiatma, A., Lukman, N., & Majid, M. N. Ab. (2020). Towards SMEs' digital transformation: The role of agile leadership and strategic flexibility. *Journal of Small Business Strategy*, 30(3), 65–85.
- Febres Trigozo, R. Y. (2025). Seguridad ciudadana en el marco de la Política Nacional Multisectorial de Seguridad y Defensa Nacional al 2030: caso empleo de aeronaves pilotadas a distancia en Lima Metropolitana, 2022–2023 [Tesis de posgrado, Centro de Altos Estudios Nacionales]. Repositorio CAEN. <https://hdl.handle.net/20.500.13097/577>
- Fernández, I. Q. (2024). Tendencias sobre liderazgo transformacional para gobernabilidad en Sudamérica. *PODIUM*, (46), 57–82.
- Gallardo Urbini, I. M., Bazán, P., Venosa, P., & del Río, N. (2022). Estrategia de ciberseguridad distribuida, aplicando el concepto de operación de inteligencia [Tesis de doctorado, Universidad Nacional de La Plata]. Repositorio Institucional UNLP. <https://doi.org/10.35537/10915/147421>
- Gualberto do Nascimento, L. (2024). La geoconomía y geopolítica de las rivalidades China-Estados Unidos en las estrategias del Asia-Pacífico vs Indo-Pacífico. *Relaciones Internacionales*, (57), 191–207. <https://doi.org/10.15366/RELACIONESINTERNACIONALES2024.57.010>
- Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies.
- Jaramillo, R. A. G., & Ortiz, Z. X. R. (2024). Educación militar: una mirada desde la seguridad y defensa. *Región Científica*, 3(2), 2024339.
- Leonardo, C. (2025). Amenazas híbridas: la nueva frontera de la seguridad nacional en América Latina. *Revista Política y Estrategia*. <https://revistacontactord.com/amenazas-hibridas-la-nueva-frontera-de-la-seguridad-nacional-en-america-latina/>
- Magnani Ezequiel (2024). Modelos de política de defensa en América Latina. *Revista Política y Estrategia*, (143). https://ri.conicet.gov.ar/bitstream/handle/11336/256226/CONICET_Digital_Nro.af0080a3-be27-4ea4-bc07-91aaed8ba037_B.pdf?sequence=2



- Mahan, A. T. (1911). *Naval strategy*. Little, Brown, and Company.
- Muñoz Meoño, R. E. (2024). Desafíos y soluciones en la defensa nacional: un marco integral para contrarrestar amenazas híbridas. *Revista de Estudios en Seguridad y Estrategia*. ESGE. <https://hdl.handle.net/20.500.14205/11266>
- Palomo Zurdo, R. J. (2018). «Blockchain»: la descentralización del poder y su aplicación en la defensa. *Bie3: Boletín IEEE*, (10), 885–904.
- Paret, P. (Ed.). (1986). *Makers of modern strategy: From Machiavelli to the nuclear age*. Princeton University Press.
- Peña, J., & Caruajulca, P. (2024). The mediating role of organizational culture between transformational leadership and organizational performance in SMEs. *Academia Revista Latinoamericana de Administración*, 37(2), 301–314. <https://doi.org/10.1108/ARLA-10-2023-0172>
- Ramos Rojas, D. N. (2020). Tratado sobre pensamiento estratégico-militar. *Espiral (Guadalajara)*, 27(78–79), 361–367. <https://doi.org/10.32870/ees.v28i78-79.7140>
- Rutz, A. (2021). Aportes a la ciberdefensa y ciberseguridad para la gestión de las infraestructuras críticas de la información en Argentina. *Revista Defensa Nacional*, (3), 1–12.
- Sánchez Aldana, L. E. (2021). Estrategia de transformación y modernización del ejército de Colombia. *Revista de la Academia de Guerra del Ejército Ecuatoriano*, 14(1), 1–15.
- Sun Tzu. (1999). *El arte de la guerra* (J. García Sánchez, Trad.). Siruela. (Obra original publicada ca. siglo V a. C.)
- Torres González, M. D. J., Zapata Cortes, J. A., Aguirre Restrepo, Y., Jiménez Navia, B., & Paipa Sanabria, E. G. (2025). Tecnologías en el sector de defensa: una revisión internacional. *Revista Logos Ciencia & Tecnología*, 17(2), 142–165. <https://doi.org/10.22335/rlct.v17i2.2007>
- Eduardo V., M. (2025a). Perú ante el reordenamiento mundial: amenazas, desafíos y oportunidades. *Revista de Estudios en Seguridad Internacional*. <https://doi.org/10.58211/6pbvyp93>
- Eduardo V., M. (2025b). Crisis globales emergentes y el rol estratégico de las Fuerzas Armadas en América Latina. *Revista Pensamiento Conjunto*, 45. <https://pensamientoconjunto.com.pe/index.php/PC/article/download/154/162/696>
- Vivanco, C. S. (2024). Priorizar la seguridad y defensa nacional: importante acción para gobernar el Perú. *Revista Cuadernos de Trabajo*, (29), 19–30. <https://doi.org/10.58211/4KSNOW69>
- Weritz, P., Braojos, J., & Matute, J. (2020). Exploring the antecedents of digital transformation: Dynamic capabilities and digital culture aspects to achieve digital maturity. En *Proceedings of the 26th Americas Conference on Information Systems (AMCIS 2020)*. AIS.