UNIVERSIDAD NACIONAL PARA LA DEFENSA
"GENERAL JUAN PABLO DUARTE Y DÍEZ"
(UNADE)
"Desarrollando las capacidades militares y civiles
de la defensa nacional"

SEGURIDAD, CIENCIA & DEFENSA

REVISTA CIENTÍFICA

SEGURIDAD NACIONAL Y COMERCIO
EN APOYO AL DESARROLLO SOCIAL Y ECONÓMICO DEL PAÍS
A TRAVÉS DE LAS CAPACIDADES
DE LAS FUERZAS ARMADAS

ISSN:2413-869X | ISSN-CD:2613-8832 | E-ISSN: 2636-2309 | AÑO XI - NO. 11 - 2025

MINISTERIO DE DEFENSA

UNIVERSIDAD NACIONAL PARA LA DEFENSA
"GENERAL JUAN PABLO DUARTE Y DÍEZ"
(UNADE)

SEGURIDAD, CIENCIA & DEFENSA

REVISTA CIENTÍFICA

SEGURIDAD NACIONAL Y COMERCIO
EN APOYO AL DESARROLLO SOCIAL Y ECONÓMICO DEL PAÍS
A TRAVÉS DE LAS CAPACIDADES DE LAS FUERZAS ARMADAS

Santo Domingo, Distrito Nacional,
República Dominicana

año XI, No. 11, 2025

INFORMACIÓN GENERAL

Título	Seguridad, Ciencia & Defensa
País	República Dominicana
Situación	Vigente
Año de inicio	2015
Frecuencia	Anual
Tipo de publicación	Publicación periódica
Soporte	Impreso en papel y digital
Idioma	Español
ISSN	2413-869X E-ISSN: 2636-2309
Sitio web de difusión	https://revista.unade.edu.do/index.php/rscd
Sitio web de ubicación en el catálogo 2.0	https://www.latindex.org/latindex/ficha/22924
Temas	Ciencias militares y sociales
Subtemas	Defensa y seguridad
Clasificación Dewey	350
Organismo responsable	Ministerio de Defensa
Editorial	Universidad Nacional para la Defensa "General Juan Pablo Duarte y Diez" (UNADE)
Naturaleza de la publicación	Revista de investigación científica
Naturaleza de la organización	Institución educativa
Notas	Fuente: Año 1, No. 1 2015
Fecha última evaluación	2021
Revista arbitrada	Si

SEGURIDAD, CIENCIA & DEFENSA

REVISTA CIENTÍFICA

La Revista Científica "**Seguridad, Ciencia & Defensa**" es el órgano de divulgación científica y de publicación anual de la Universidad Nacional para la Defensa "General Juan Pablo Duarte y Diez" (UNADE), como institución de educación superior militar, coordinada por la Vicerrectoría de Investigación e Innovación y publicada por la Subdirección de Publicación de la UNADE.

La Revista Científica "**Seguridad, Ciencia & Defensa**" de la UNADE ha evolucionado para convertirse en un referente indiscutible en el ámbito de la investigación científica aplicada no solo a la seguridad y defensa nacional, sino a todos los campos del saber de las ciencias del conocimiento.

Al ser un órgano de divulgación, difusión y visibilidad de alto impacto, esta publicación indexada y arbitrada evaluada por pares ciegos, se posiciona como una plataforma clave para compartir los hallazgos más recientes en áreas estratégicas como las Ciencias Militares, Navales y Aeronáuticas, así como en temas de Ciencias de la Salud, de la Geopolítica, de los Derechos Humanos y Derecho Internacional Humanitario, del Derecho Castrense y las Ingenierías. Su nuevo alcance radica en fortalecer el conocimiento con rigor científico y académico en diversas áreas de las ciencias, promoviendo la innovación y el desarrollo de soluciones efectivas para los desafíos actuales y futuros, a fin de garantizar el fortalecimiento de las capacidades militares y civiles de la defensa nacional, con apertura a la comunidad científica en general y, en particular, para cualquier profesional interesado en la investigación.

CONTENIDO

Presentación del ministro de Defensa

Teniente general
Carlos Antonio Fernández Onofre, ERD

Con satisfacción y orgullo presentamos el volumen XI de la revista científica **"Seguridad, Ciencia & Defensa"**, publicación emblemática de la Universidad Nacional para la Defensa "General Juan Pablo Duarte y Díez" (UNADE). Este número se enmarca en la línea de investigación "**Apoyo al Desarrollo Social y Económico del País a través de las Capacidades de las Fuerzas Armadas**", y reúne contribuciones que evidencian la responsabilidad académica, profesional, ética, técnica y humana de escritores nacionales e internacionales, comprometidos con el desarrollo nacional, el bienestar y la seguridad nacional.

Las investigaciones contenidas en estas páginas exploran, desde diversas disciplinas y metodologías, cómo las capacidades de las Fuerzas Armadas pueden ser desplegadas de forma responsable, eficiente y orientada al desarrollo sostenible, la cohesión social y la resiliencia ante riesgos y emergencias. En este volumen se abordan temas de gran importancia y trascendencia que abarcan los aspectos institucionales, la defensa y su fundamento legal, tales como: *Apoyo al Desarrollo Social y Económico del Perú a través de las capacidades de las Fuerzas Armadas; Aportes de la COOPINFA a través de la Educación y la Responsabilidad Social al desarrollo económico y social de los Miembros de las Fuerzas Armadas y la Sociedad Dominicana; La Defensa Nacional como imperativo constitucional en República Dominicana tras la reforma del 2010; Nuevas amenazas a la Seguridad Humana en el Siglo XXI: aproximaciones multidimensionales y perspectivas latinoamericanas; Las tecnologías críticas y emergentes: Oportunidades y Desafíos para la Protección de los Derechos Humanos. Enfoque actual en la República Dominicana; Integración de dominios y ejércitos multimisión: de operaciones conjuntas al multidominio y relaciones internacionales: Una visión tecno-realista desde el Sur Global.*

La notabilidad[1] de este volumen trasciende el ámbito académico: cada artículo es una pieza del diálogo entre la investigación científica, las políticas públicas y la práctica operacional, todos con un rigor científico. A través de estudios de caso, análisis empíricos y propuestas estratégicas, los autores, no podrían llegar a esta edición sin el trabajo riguroso y altruista de los evaluadores (pares ciegos), editores, traductores, diagramadores, correctores, diseñadores y del personal administrativo que hace posible la circulación de conocimientos.

La UNADE de forma ininterrumpida, ha mantenido vivo un espacio académico y científico dedicado a analizar y proponer soluciones que fortalecen nuestras capacidades para servir al país. Es preciso reconocer a los escritores, revisores y al equipo editorial por su esfuerzo en producir conocimiento riguroso y pertinente. La colaboración entre las instituciones académicas y las Fuerzas Armadas es fundamental para enfrentar los desafíos contemporáneos: desde la gestión de desastres hasta la transformación tecnológica y el impulso al desarrollo regional. Este volumen XI es un testimonio del avance conjunto y de la vocación de servir a la nación con profesionalismo y responsabilidad.

1 Se refiere a la cualidad de ser notable o destacarse por alguna característica particular. Puede referirse a una persona muy notable por sus buenas cualidades o por sus méritos, o a algo que es relevante y resalta en un contexto específico. En resumen, la notabilidad implica ser reconocido o destacado por su importancia o excelencia.

Estas palabras reflejan la estrecha relación que debe existir entre la academia y las instituciones públicas encargadas de la seguridad y la defensa, una relación basada en la confianza mutua, la evidencia y la búsqueda constante del bien común. La UNADE, a lo largo de su trayectoria, ha consolidado un modelo académico que integra formación, investigación y extensión, orientado a formar profesionales capaces de contribuir efectivamente en escenarios complejos. Nuestra casa de estudios ha avanzado mediante la creación de programas especializados, la conformación de centros de investigación y la promoción de redes interinstitucionales que potencian la transferencia de conocimientos hacia la sociedad, tal y como se evidencia en su lema: "Desarrollando las capacidades militares y civiles para la defensa nacional".

Mirando hacia atrás, hoy celebramos, además, los logros alcanzados por esta herramienta de divulgación académica, especialmente por las diversas indexaciones obtenidas en el marco de alcanzar una mayor visibilidad internacional, lo que se traduce en el impacto positivo hacia comunidades científicas y académicas, así como a la sociedad en general; lo que nos permite valorar el espíritu perseverante de quienes día a día contribuyen a que la investigación producida tenga relevancia y aplicación práctica en beneficio del país.

Al presentar este volumen XI, renovamos nuestro compromiso con la calidad científica, la ética investigativa y la articulación con actores públicos y privados. Invitamos a nuestros lectores a utilizar estos trabajos como insumo para el diseño de políticas, la mejora de prácticas institucionales y la generación de nuevas líneas de investigación. Esperamos que las reflexiones y propuestas aquí consignadas inspiren diálogo, colaboración multisectorial y acciones concretas que impulsen el desarrollo social y económico de la nación.

Finalmente, extendemos nuestro agradecimiento a todas las personas e instituciones que han hecho posible esta edición. Reconocemos que la ciencia aplicada a la seguridad y defensa, así como al desarrollo, es un esfuerzo colectivo y continuo. Por tal razón, celebramos esta entrega como un escalón más en el largo trayecto institucional de la Universidad Nacional para la Defensa "General Juan Pablo Duarte y Díez" (UNADE) como una contribución sólida al futuro del país.

Prólogo del viceministro de Defensa para Asuntos Navales y Costeros y encargado de Asuntos Educativos de las Fuerzas Armadas.

Vicealmirante
Agustín Morillo Rodríguez, ARD

Es un honor presentar el Volumen XI de la Revista Científica Seguridad, Ciencia & Defensa, dedicado a la línea temática: "Apoyo al desarrollo social y económico del país a través de las capacidades de las Fuerzas Armadas". Esta edición refleja el compromiso permanente del Ministerio de Defensa, a través de la Universidad Nacional para la Defensa "General Juan Pablo Duarte y Díez" (UNADE), con la investigación rigurosa, la excelencia académica y la generación de conocimiento aplicado al fortalecimiento de la seguridad, la defensa y el desarrollo nacional. Vivimos en un mundo marcado por la complejidad de las amenazas híbridas, la interdependencia global y la irrupción acelerada de tecnologías disruptivas.

Estos desafíos obligan a los Estados a repensar sus estrategias de seguridad, defensa y desarrollo, integrando la dimensión militar con las ciencias sociales, jurídicas y tecnológicas en un marco de cooperación interinstitucional e interdisciplinaria. Las Fuerzas Armadas de la República Dominicana desempeñan un papel decisivo en el progreso del país al garantizar la seguridad y la estabilidad necesarias para la inversión, el comercio y el turismo. La protección de las fronteras terrestres,

marítimas y aéreas, así como la lucha contra ilícitos como el contrabando y el narcotráfico, consolidan un entorno de confianza que fortalece el crecimiento económico y social.

Los estudios incluidos en este volumen evidencian cómo las Fuerzas Armadas, más allá de su función tradicional, se constituyen en actores estratégicos de bienestar social, sostenibilidad económica y resiliencia comunitaria. Se abordan temáticas que van desde la asistencia humanitaria y el desarrollo comunitario hasta la gestión de recursos estratégicos, proyectos de infraestructura, integración de dominios en la guerra moderna y el impacto de las tecnologías emergentes, como la inteligencia artificial, en la seguridad global.

Con esta publicación, la UNADE reafirma su compromiso con la formación científica, doctrinal y profesional de alto nivel, orientada a fortalecer la resiliencia del Estado dominicano y de la región latinoamericana y de otros continentes frente a los desafíos contemporáneos. Esta edición se constituye en un espacio de análisis y reflexión académica que conecta a la comunidad militar, académica y civil en torno a la búsqueda de soluciones innovadoras y sostenibles. Las contribuciones aquí reunidas enriquecen el acervo intelectual en materia de seguridad y defensa, estableciéndose en un instrumento de referencia para la toma de decisiones estratégicas, el diseño de políticas públicas y el fortalecimiento doctrinal.

Esta revista está concebida no solo para investigadores y profesionales de la defensa, sino también para autoridades nacionales, responsables de la seguridad regional, académicos de distintas disciplinas y miembros de la sociedad civil interesados en comprender estos desafíos. Al poner el conocimiento científico al servicio de múltiples actores, reafirmamos la convicción de que el vínculo entre ciencia, seguridad, defensa y sociedad es indispensable para garantizar un futuro próspero, democrático y seguro. Al mismo tiempo, esta publicación se proyecta como un puente académico entre la República Dominicana y la región latinoamericana y caribeña, al compartir experiencias, marcos conceptuales y estudios de caso que enriquecen el debate hemisférico sobre seguridad y desarrollo.

La cooperación internacional, el intercambio de conocimiento y la articulación de políticas comunes son hoy más necesarios que nunca para enfrentar amenazas transnacionales que trascienden las fronteras. De igual manera, reafirmamos el valor de la innovación científica y tecnológica como motor de transformación institucional.

La investigación en defensa y seguridad, vinculada a avances en ciberseguridad, inteligencia artificial, gestión de riesgos y sostenibilidad, potencia la capacidad de respuesta del Estado y contribuye directamente a la construcción de un futuro más seguro, resiliente y equitativo para todos los dominicanos. Invitamos a cada lector a recorrer estas páginas con espíritu crítico y reflexivo, convencidos de que la seguridad y la defensa no son solo deberes de las Fuerzas Armadas, sino un compromiso compartido de toda la sociedad, indispensable para garantizar la soberanía, la democracia y el bienestar común.

¡Enhorabuena!

«« ● »»

Prefacio del rector de la UNADE

Mayor general
Rafael Vásquez Espínola, ERD, PhD

Vivimos en un mundo marcado por una conmoción continua, donde las dinámicas geopolíticas y socioeconómicas se transforman de manera acelerada, y configuran un ambiente estratégico de creciente diversidad. Estas mutaciones generan incertidumbre ante lo impredecible y producen un escenario en el que las amenazas emergentes se presentan con un alto grado de híbridación. Frente a esta realidad, los Estados tienen la ineludible misión de garantizar su soberanía, su bienestar, su seguridad y su defensa, ampliando a la vez sus funciones tradicionales con un enfoque multidisciplinario que responda a las complejidades locales y globales.

En este proceso, el Ministerio de Defensa de República Dominicana reafirma su misión y fortalece vínculos estratégicos con los círculos del ámbito académico y científico tanto nacionales como internacionales a través de la Universidad Nacional para la Defensa (UNADE) con el objetivo de generar conocimiento, fomentar la sistematización de experiencias y promover la difusión de buenas prácticas, que contribuyen al desarrollo de

una concepción integral de la seguridad y defensa nacional.

La revista científica Seguridad, Ciencia & Defensa es una plataforma de difusión de saberes que conecta la cultura de la defensa con las aspiraciones legítimas de la sociedad dominicana. En esta edición (volumen XI), se propone un eje de investigación centrado en la evolución del paradigma de la seguridad en el siglo XXI, marcado por la transición desde las operaciones en dominios físicos hacia escenarios multidominio y el ciberespacio, donde la defensa nacional se ve confrontada con ciberataques, desinformación y nuevas formas de criminalidad transnacional.

Este número reúne artículos que abordan, con rigor académico y con enfoque interdisciplinario, cuestiones de vital importancia para la seguridad y defensa. Se inicia con el análisis cualitativo en el mando militar tipo misión, que revisa la doctrina militar clásica del Ejército, destacando su tradición y capacidad contrainsurgente. Le sigue una reflexión en Apoyo al desarrollo social y económico del Perú a través de las capacidades de las fuerzas armadas, también se incluye el estudio de las capacidades híbridas en operaciones cívico-militares de la COMIPOL, que ilustran la intersección entre seguridad y desarrollo.

Otros artículos examinan los aportes de COOPINFA a través de la educación y de la responsabilidad social al desarrollo económico de los miembros de las FF. AA y de la sociedad dominicana. También, la Defensa Nacional como imperativo constitucional tras la Reforma de 2010, que se refiere a la obligación establecida en la Constitución para que el Estado garantice la protección de su soberanía e integridad territorial. Este número también amplía la mirada hacia la agenda global, abordando la transición de amenazas convencionales a amenazas híbridas, las nuevas aproximaciones latinoamericanas a la seguridad humana, y los dilemas éticos y estratégicos derivados de la inteligencia artificial como arma de dominación global y de las tecnologías críticas y emergentes en la protección de los derechos humanos.

Entre otros artículos, se incluyen, también, Capital criminal, necroliberalismo y derechos humanos: Ecuador de 2024, y sobre De la Mar a la nube: Guerra naval e integración de dominios en Ucrania. Finalmente, se presentan artículos que examinan la integración del dominio y ejército multimisión: de operaciones conjuntas al multidominio, y los desafíos de la guerra cognitiva, donde la mente humana se configura como el nuevo campo de batalla.

Expresamos nuestro sincero reconocimiento al ministro de Defensa teniente general Carlos Antonio Fernández Onofre, ERD, por su invaluable apoyo; a los investigadores que han confiado en esta revista para la difusión de sus valiosos aportes; a los revisores que han garantizado la calidad y rigor científico de cada contribución; y al comité editorial por su incansable labor académica.

Con este volumen, la UNADE reafirma la vocación de la revista Seguridad, Ciencia & Defensa de ser un espacio para la construcción y validación del conocimiento científico, sobre la base de un pensamiento estratégico que fortalezca la seguridad nacional, la dignidad humana y la estabilidad de nuestras naciones, información útil para la toma de decisiones estratégicas en el ámbito de la seguridad y defensa.

Invitamos a los lectores a recorrer sus páginas con espíritu abierto, reflexivo y crítico.

¡Felicitaciones!

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Editorial

Coronel (r)
Juan Fabrizio Tirry, PhD
ORCID: https://orcid.org/0000-0002-3608-6657

La Universidad Nacional para la Defensa "General Juan Pablo Duarte y Díez" (UNADE) tiene el honor de presentar a la comunidad científica y académica, tanto a nivel nacional como internacional, el undécimo volumen de la Revista Científica "**Seguridad, Ciencia & Defensa**". En esta edición, la línea de investigación central se enfoca en el "**Apoyo al Desarrollo Social y Económico del País a través de las Capacidades de las Fuerzas Armadas**". Este editorial reconoce el papel fundamental que desempeñan nuestras Fuerzas Armadas no solo en la defensa de la soberanía nacional, sino también en la protección de la integridad territorial, la construcción de un entorno seguro, estable que favorezca el progreso y el bienestar de la sociedad en el impulso del progreso social y económico del Estado.

El presente ejemplar continúa nuestro compromiso de ofrecer un espacio para el análisis y la reflexión sobre temas cruciales para la seguridad y defensa nacional, en un mundo cada vez más complejo y globalizado. Este enfoque no solo incrementa la eficiencia y precisión en el campo, sino que también potencia el análisis estratégico y fomenta una cultura de paz basada en valores fundamentales.

En un mundo caracterizado por diversos escenarios transnacionales, las Fuerzas Armadas han evolucionado para adaptarse a nuevos retos y desafíos, participando activamente en la protección de infraestructuras críticas, el apoyo en situaciones de emergencia y desastres naturales, así como en el resguardo del orden interno cuando las circunstancias lo demandan. Su rol no se limita únicamente al ámbito militar, sino que se extiende a la promoción de iniciativas de desarrollo, colaborando con sectores estratégicos del país para fortalecer la seguridad y la economía. En este contexto, este volumen recopila una serie de estudios y análisis que examinan cómo las capacidades de las Fuerzas Armadas pueden ser aprovechadas para contribuir de manera efectiva al crecimiento sostenible y la estabilidad social.

Los artículos que componen este volumen exploran una amplia gama de aspectos relacionados con la línea de investigación, por lo que los escritos reunidos en este ejemplar abarcan un amplio y pertinente espectro temático — desde el análisis cualitativo del Mando tipo Misión y la integración multimodal de dominios físicos y cibernéticos, hasta la guerra naval contemporánea, la guerra cognitiva y la

influencia de las tecnologías críticas en la protección de los derechos humanos—, articulando perspectivas teóricas, estudios de caso regionales (que abarcan diversos países: Perú, Ecuador, Ucrania, República Dominicana) y reflexiones sobre políticas públicas y capacidades institucionales (COMIPOL, COOPINFA, Fuerzas Armadas). Su alcance trasciende la mera descripción operativa al interconectar seguridad, desarrollo social y económico, derechos humanos y transformaciones tecnológicas, así como al exponer cómo amenazas convencionales y híbridas remodelan la agenda internacional y la seguridad humana en el siglo XXI. La pluralidad metodológica —que incluye análisis cualitativos, estratégicos y multidimensionales— y el diálogo entre académicos, militares y actores civiles fortalecen la aplicabilidad de las propuestas para la toma de decisiones y la formulación de políticas.

El rigor científico de cada contribución, garantizado mediante un proceso de evaluación por pares ciegos, cuyos miembros han dedicado su tiempo y experiencia y con su valiosa labor, han garantizado la calidad, pertinencia e impacto de los contenidos presentados; lo que asegura la solidez analítica, la validez empírica y la pertinencia académica que hacen de este volumen una referencia imprescindible para investigadores, planificadores y responsables de la defensa y el desarrollo en la región y más allá.

A través de este volumen, se busca fomentar la reflexión y el debate en torno a la integración de las capacidades militares en estrategias de desarrollo nacional, considerando tanto su impacto en la seguridad como en la generación de oportunidades para el crecimiento económico. La interrelación entre estos ámbitos es esencial en un mundo globalizado donde las amenazas, retos y desafíos requieren respuestas coordinadas y adaptativas, lo que nos motiva a invitar a nuestros lectores a explorar cuidadosamente los artículos de este volumen y a compartir sus reflexiones y comentarios. Su participación es fundamental para enriquecer el diálogo y avanzar en la búsqueda de soluciones innovadoras para los desafíos que enfrenta nuestro país.

En ese mismo orden de ideas, queremos expresar nuestro más sincero agradecimiento a los investigadores que han contribuido con sus estudios, a los miembros del Comité Científico por su dedicación y compromiso, y a todas las personalidades e instituciones que han hecho posible la publicación de esta edición. La divulgación del conocimiento en temas sobre las Ciencias de la Seguridad y Defensa Nacional es un esfuerzo colectivo que fortalece la visión estratégica y promueve soluciones innovadoras para los desafíos contemporáneos. No queremos pasar por alto a nuestros lectores por su continuo apoyo y compromiso con la promoción del conocimiento en el ámbito de la seguridad y defensa nacional, como también a las distintas personalidades que hacen posible que esta actividad de divulgación del conocimiento se visualice a nivel del mundo.

A tenor de lo antes expuesto, esperamos que esta edición sea una valiosa contribución a la comprensión y el debate sobre el impacto que la Seguridad y Defensa Nacional implica en el desarrollo social y económico del país, con el concurso y el apoyo irrestricto de sus Fuerzas Armadas y en ese contexto, podemos referirnos a una de las frases celebres del **Libertador Simón Bolívar**, al describir en el **Manifiesto de Carúpano en 1814** lo siguiente: "*Un ejército de ciudadanos es la mejor salvaguarda de la libertad, pero también puede ser la más firme columna de la estabilidad y el progreso*".

Por último y no menos importante en consonancia con lo antes citado, es oportuno destacar lo señalado por el Sr. presidente Constitucional de la República Dominicana, Luis Rodolfo Abinader Corona, durante el acto de saludo solemne de nueve pro-

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

mociones oficiales militares y policiales, el 7 de febrero del 2024 al referir lo siguiente, cito: "*Unas Fuerzas Armadas y una Policía Nacional fuertes, es un país fuerte. Unas Fuerzas Armadas y una Policía débil, es un país débi*l". Fin de la cita.

Les invitamos a leer el presente ejemplar y a compartir sus reflexiones y comentarios, con el propósito de enriquecer el análisis y promover nuevas investigaciones en este campo fundamental. Esperamos que encuentren este número de interés, motivándoles a suscribirse y a enviar sus colaboraciones.

¡Gracias por acompañarnos en esta ardua tarea!

SECCIÓN INTERNACIONAL

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

El análisis cualitativo en el mando tipo Misión

Qualitative analysis in mission-type command

Recibido: 13/ 04 / 2025 | Revisado: 29 / 08 / 2025 | Aprobado: 09 / 09 / 2025
DOI: https://doi.org/10.59794/rscd.2025.v11i11.142

Maryor (r) Germán Alberto Bermúdez Ordoñez, ENC
Colombia

Correo: ga.bermudez@uniandes.edu.co
Orcid: https://orcid.org/0000-0001-7162-154X
Afiliación: Universidad de Los Andes

El autor es mayor del Ejército de Colombia en situación de retiro y veterano de guerra. Máster en Construcción de Paz de la Universidad de los Andes. Máster en Educación de la Universidad Sergio Arboleda. Especialista en Administración de Recursos para la Defensa Nacional. Egresado como licenciado en Ciencias Militares de la Escuela Militar de Cadetes General José María Córdova. Como oficial del Ejército de Colombia fue oficial de operaciones de la Brigada Móvil de la Fuerza de Despliegue Rápido, comandante de batallones de operaciones terrestres. Profesor en la Escuela Militar de Cadetes y oficial enlace ante el Departamento de Estado a través del Bureau of International Narcotics and Law Enforcement Affairs (INL). A su vez, como maestro universitario en Colombia, se destaca por sus aportes y estudios en temas de educación, conflicto y postconflicto, los cuales ha expuesto en las universidades de los Andes, Sergio Arboleda, Unicervantes, entre otras. De la misma manera, representó a las víctimas del conflicto armado a través de la ONG "Mil Víctimas" ante el Sistema Integral de Verdad, Justicia, Reparación y No Repetición, ante la Jurisdicción Especial para la Paz, con su contribución en el informe titulado "Devastación de un pueblo: métodos y medios de guerra ilícitos empleados por las FARC", visibilizando así a los militares víctimas de los artefactos explosivos improvisados. Es escritor y ha publicado diversos ensayos, artículos y libros, entre los cuales se destacan Perspectivas de la Pedagogía en Contribución de Paz e Iniciación, Muerte y Vida, y adelanta su tercer libro Disidente. En la actualidad, es profesor invitado en el Goetheanum, en Dornach, Suiza, donde imparte clases de pedagogía Waldorf para la contribución de la paz en los procesos de la educación básica, cátedra que imparte a profesores de diversas nacionalidades.

DOI: https://doi.org/10.59794/rscd.2025.v11i11.142

Resumen

El documento revisa la Doctrina Militar clásica del Ejército, destacando su tradición y capacidad contrainsurgente. A partir de allí, presenta las novedades de la Nueva Doctrina destacando las variables sociales en ella involucradas, para referirse finalmente a los retos que supone la transformación de esta Nueva Doctrina en la cultura institucional del Ejército. Se concluye describiendo el perfil y las competencias del comandante militar para la Colombia del postconflicto; militares que comprendan la política profunda y sistemáticamente, y que conviertan al Ejército Nacional en una herramienta estratégica y exitosa para los fines políticos de paz que persiguen las autoridades civiles. Con estos elementos, el presente trabajo establece diferentes conceptos en un lenguaje claro que contribuirá a entender el cambio organizacional, promoviendo marcos conceptuales, estratégicos e incluso operacionales en los que se está evidenciando la transformación del Ejército de Guerra Irregular en un Ejército Multimisión.

Palabras clave: Mando tipo misión, escenarios, orden, control social del territorio, ciencias sociales

Abstract

The document reviews the classic Military Doctrine of the Army, highlighting its tradition and counterinsurgency capacity. From there, it presents the novelties of the New Doctrine, highlighting the social variables involved in it, to finally refer to the challenges posed by the transformation of this New Doctrine into the institutional culture of the Army. It concludes by describing the profile and competencies of the military commander for post-conflict Colombia; military personnel who understand politics deeply and systematically, and who turn the National Army into a successful strategic tool for the political peace goals pursued by the civil authorities. With these elements, this work establishes different concepts in a clear language that will allow understanding the organizational change, promoting conceptual, strategic and even operational frameworks where the transformation of the Irregular Warfare Army into a Multi-Mission Army is becoming evident.

Keywords: Mission command, scenarios, order, social control of the territory, social sciences

DOI: https://doi.org/10.59794/rscd.2025.v11i11.142

Introducción

Un factor clave en el establecimiento de una paz duradera en Colombia será la orientación que el Estado dé a sus Fuerzas Militares. Al término del conflicto armado con las FARC y con el inicio de las negociaciones con el ELN, muchos se han cuestionado acerca de la labor que éstas, y en especial el Ejército Nacional, cumplirán en el postconflicto y sus nuevas realidades. El presente trabajo tiene como propósito revisar la transformación que vive el pensamiento estratégico militar colombiano, a través de la implementación del "MANDO TIPO MISIÓN" (Mejía, 2017, p. 95). Éste, constituye un cambio de paradigma bajo el cual el objetivo de la guerra ya no se limita a la derrota militar del enemigo, sino que se extiende a la creación de las condiciones para un nuevo orden social y político en paz, al tiempo que se incorporan en la cultura del Ejército elementos novedosos en cuanto a la concepción estratégica general del desarrollo de su misión.

Según Schmidt (2014), contrario a la idea más extendida, derrotar o someter a una fuerza enemiga no es el objetivo de ninguna guerra. El objetivo estratégico es recrear un orden estable que pueda ser sostenido sin una significativa participación militar constante del vencedor en el campo de batalla. La victoria militar así entendida, consiste en establecer las condiciones para el orden social y político que llega después de que se silencian las armas. Dicho de otro modo, la guerra constituye una actividad política, y debe ser luchada teniendo en mente su racionalidad y fines últimos, en función de los cuales deben tomarse todas las decisiones (pp.3-4).

En este proceso de toma de decisiones, es necesario destacar que la cultura del Ejército es de profunda tradición tecnocientífica, en la que los elementos cuantitativos tienden a tener un mayor peso específico en el proceso de toma de decisiones militares, y donde los aspectos tácticos acaparan la mayor parte de la atención. Esto funciona bastante bien cuando se trata de combatir la insurgencia y la criminalidad como enemigos del Estado con diferentes niveles de organización; de hecho, es un enfoque que difícilmente será abandonado en tanto sigan necesitándose el desarrollo de operaciones militares.

No obstante, el momento político actual exige enriquecer estas capacidades con una mentalidad cualitativa, en tanto la guerra es un fenómeno social. Por lo tanto, el logro de una paz estable en Colombia demanda comandantes militares que comprendan la política profunda y sistemáticamente, y que conviertan al Ejército Nacional en una herramienta estratégica exitosa para los fines políticos de paz que persiguen las autoridades civiles. La manera de hacerlo es comenzar a pensar en el contexto y establecer el rol que juega la capacidad militar en dicho contexto con las otras variables de la construcción de la paz.

De esta manera, el MANDO TIPO MISIÓN supone la concreción de la nueva Doctrina Militar, que presenta el cambio del concepto de "control militar de área" al de "control social del territorio", el cual pone de manifiesto el pensamiento militar cualitativo, donde los métodos de las ciencias sociales constituyen herramienta promisoria para la institución militar.

DOI: https://doi.org/10.59794/rscd.2025.v11i11.142

Desarrollo

La Doctrina Militar

En primer lugar, hace falta destacar el carácter constitucional de las Fuerzas Militares, y de su papel dentro del ordenamiento más allá del conflicto armado. Es decir, la razón de ser y existir de las Fuerzas Militares, no se limita a librar el conflicto armado con las guerrillas. Por lo tanto, es absurdo suponer su supresión o eliminación so pretexto de que se ha llegado a un escenario en el que todos los grupos insurgentes han sido disueltos de forma definitiva. Las tareas de defender la Constitución, "la integridad territorial y la soberanía nacional" (Constitución Política de Colombia, 1991, artículo 217) no desaparecen por mérito del éxito del actual proceso de paz, ni se olvidan por mérito de que el conflicto interno persista.

En todo caso, aún con una paz estable frente a los grupos insurgentes, seguirán existiendo diferentes amenazas a la población, la economía, la infraestructura y el ambiente (narcotráfico, terrorismo, contrabando, tráfico de personas, minería ilegal, etc.). En otras palabras, en un país con tantas complejidades sociales, aún sin guerrillas, seguirá siendo necesaria la guerra hacia el combate de otras formas de crimen.

En el caso del Ejército, existe una Doctrina Militar, que es el conjunto de principios de acción que, bajo el mando de las autoridades civiles, definen la acción del Ejército a manera de ideas-fuerza y frente a las cuales se obtiene una noción de "victoria". La doctrina es una guía para la acción, mas no un conjunto de reglas fijas. Establece un marco común de referencia para resolver problemas militares, al tiempo que establece fundamentos "tácticas, técnicas y procedimientos" (Mejía Ferrero, 2017, p.90).

Las nuevas realidades que suponen la paz permanente con las guerrillas ciertamente son razón poderosa para adelantar el replanteamiento de dichos principios. El énfasis ya no puede estar en el control territorial exclusivamente militar en un escenario de hostilidades con insurgentes. Sin embargo, hace falta ver que tal énfasis está impregnado profundamente en la cultura institucional del ejército. Un cambio doctrinal supone un cambio de visión de la victoria como el éxito en el combate a las guerrillas hacia algo distinto, que no será muy claro para la gruesa mayoría del personal militar.

En efecto, durante décadas el Ejército de Colombia basó su organización, entrenamiento, y preparación profesional en el método del combate irregular, cuyo principal fin era "ganar un espacio en el terreno, logrando deslegitimación del adversario, la protección de la población civil y sus bienes, la protección de los recursos del Estado, el debilitamiento organizacional y la derrota de los grupos insurgentes que amenazaran la nación. Esas han sido las bases de la Doctrina Militar, y son el alma del pensamiento de los soldados de Colombia hasta la actualidad. Bajo esta concepción, un comandante estaba obligado a tener una visión cuantitativa de ciertas variables (ver figura 1) para el desarrollo del análisis militar de una situación dada, con el único propósito de retomar el control del territorio.

DOI: https://doi.org/10.59794/rscd.2025.v11i11.142

Figura 1
Desarrollo del análisis militar de una situación dada

Nota. Variables a considerar en desarrollo de operaciones militares con visión táctica- cuantitativa [1]

El documento que más claramente desarrolló este enfoque es el Reglamento de Operaciones y Maniobras de Combate Irregular EJC 3-10-1. Bajo el enfoque de esta reglamentación, desde el momento mismo de su planificación, las operaciones eran conducidas de manera bastante primaria, y solamente para garantizar el control de un área determinada y derrotar al adversario en cuanto a su estructura armada y sus fuentes de financiamiento. Los comandantes a todo nivel fueron dotados de una percepción estrictamente operacional de la situación del país, donde lo primordial era garantizar la integridad del territorio nacional y el orden constitucional a través de las armas.

Consideraciones estratégicas relacionadas con el aporte de esa intervención militar a la construcción de paz, a la seguridad alimentaria, o a la articulación institucional han estado totalmente ausentes del lenguaje y el pensamiento militar. Esta doctrina, tan largamente practicada, hizo muy difícil que los comandantes se hicieran sensibles al contacto con la población civil. Con ello, para el militar ha resultado imposible auto percibirse como una fuerza social influyente en la realidad de las personas en cuyo territorio intervenía. Por eso mismo, no resultaba atractivo, ni para la institución ni para quienes la integraban, capacitarse en conceptos o herramientas que tuvieran el desarrollo social de los pobladores como elemento central.

El Ejército y su tradición contrainsurgente

Para comprender la razón por la cual la Doctrina Militar ha consolidado esta cultura de pensamiento, hace falta reconocer que durante décadas el Ejército de Colombia se haya concentrado en actividades de "contrainsurgencia clásica". Ésta, es entendida como el conjunto de teoría y prácticas desarrolladas en los contextos de guerras de liberación na-

DOI: https://doi.org/10.59794/rscd.2025.v11i11.142

cional (1944 – 1982), la cual constituyó un paradigma dominante durante la segunda mitad del S. XX (Kilcullen, 2006, p.111). Hubo un tiempo en el que se decía que la contrainsurgencia[1] era de interés solo para los historiadores. Pero con la gran densidad de conflictos dentro de la categoría de "guerra irregular" y la llamada "guerra contra el terrorismo" post 9/11, los métodos clásicos contrainsurgentes ganaron renovada atención académica.

Si bien es posible diferenciar una insurgencia "moderna" de una "clásica", para el caso colombiano el enfoque clásico es completamente relevante por tratarse de un conflicto bajo el esquema de rebelión contra el statu quo de un Estado en funcionamiento. En él, no resulta viable ni la toma del control del Estado por parte de los rebeldes, ni la separación de una porción del territorio con fines de gobernarlo creando un Estado independiente. En el mundo, habrá muchas expresiones no clásicas de las insurgencias, tales como aquellas que surgen tras la caída de un estado fallido, aquellas "de resistencia" frente a la invasión de una coalición de países, u otras en las que la insurgencia representa el statu quo y la contrainsurgencia el cambio revolucionario. Pero ninguno de ellos es el caso colombiano.

Sin embargo, la insurgencia colombiana actual recoge importantes características no clásicas que surgen de ciertos efectos de la globalización. Es el caso de los esquemas de cooperación insurgente trasnacional[2], así como el impacto de las comunicaciones basadas en Internet sobre variables de las guerrillas tales como financiamiento, promoción y publicidad de su causa rebelde, comunicación clandestina, inteligencia, así como el desarrollo de su agenda internacional. Otra característica no clásica del caso colombiano puede ser el fenómeno paramilitar que hasta cierto punto rompe la relación binaria guerrilla rebelde – Estado, así como la coexistencia de múltiples guerrillas con ideales revolucionarios no completamente compatibles entre sí.

En una perspectiva general, es posible establecer características de una concepción contrainsurgente más actual, que describa mejor la actuación del Ejército colombiano en el S. XXI, a partir del abordaje de dos frentes teóricos: El primero, que la insurgencia no es un concepto históricamente estático, de modo que en la medida que la insurgencia moderna resulte históricamente evolucionada y diferenciada, habrá necesidad de reinterpretar la concepción de contrainsurgencia. El segundo, que las características de una insurgencia determinada dependen de las características del Estado al cual disputa el control del territorio.

Al revisar ambos frentes en un contexto colombiano, según Kalivas (2006), se encuentra, por una parte, a una insurgencia fundamentalmente clásica, claramente jerarquizada y con líderes plenamente visibles, que interactúa con la población de manera predecible bajo el esquema control – colaboración y que basa su accionar en unidades militares capaces de pasar de la defensiva a la ofensiva, contrarrestados por fuerzas de seguridad especializadas para la ofensiva local y regional. Siendo insurgencias originadas medio siglo atrás en el pasado, se ven naturalmente impregnadas por algunos caracteres no clásicos propios de los tiempos modernos, pero con-

1 Conjunto de medidas adoptadas para suprimir la insurgencia.

2 Se han comprobado importantes nexos de las FARC y el ELN con grupos como el IRA y la ETA para efectos de entrenamiento en prácticas insurgentes.

servando su carácter clásico y ajustándose a la teoría de la contrainsurgencia clásica.

Por otro lado, se encuentra a un Estado – Nación de características clásicas en lo que al Estado moderno se refiere; sensiblemente débil en muchos aspectos, pero suficientemente bien constituido para no ser un estado fallido; con muchas dinámicas de ilegalidad simultáneas que lo hacen particularmente complejo, pero finalmente clásico en lo que respecta a la contrainsurgencia. El conflicto colombiano ha sido, fundamentalmente, de guerrilla y Estado clásicos.

Es de destacar que algunos aportes desde los llamados nuevos paradigmas de la contrainsurgencia moderna resultan también sumamente "clásicos" en el sentido que describen múltiples líneas de acción contrainsurgente que, en el caso colombiano, llevan décadas de implementación por parte de las Fuerzas Militares. Dicho de otro modo, en el caso colombiano, estos llamados "nuevos paradigmas" (Kilcullen, 2006, p. 9) no constituyen marcos teóricos verdaderamente novedosos.

Es el caso del control de un ecosistema de conflicto complejo, caracterizado por la necesidad de poner orden en todo un conjunto de intereses creados en torno a la violencia,[3] y no tanto en la de derrotar a un único adversario insurgente. Igualmente, el enfoque de la contrainsurgencia política, en la que cada operación militar se adelanta en una perspectiva estratégica absolutamente política que trasciende lo militar, en la que los resultados de las operaciones pueden tener repercusiones internacionales, inclusive[4]. También lo es la actitud militar contrainsurgente de contención permanente ante la realidad de que difícilmente se llegará a un escenario de victoria militar definitiva sobre las guerrillas. Todos esos elementos pueden encontrarse arraigados en el Ejército colombiano desde la década de los 80 del S. XX.

Del hecho de que la acción de las Fuerzas Militares colombianas sobre las guerrillas se ajuste al marco teórico de la contrainsurgencia clásica, se desprende la situación de que la Doctrina Militar se haya ajustado, precisamente, a las necesidades de dicha dinámica. Con esto claro, a partir de la comprensión de los cambios en el entorno social y político, pueden comprenderse los cambios de Doctrina que actualmente se adelantan, así como sus motivaciones y retos.

Hacia una cultura de pensamiento estratégico

A la hora de examinar de dónde nacen los principios de Doctrina, hace falta discernir entre los elementos estratégicos y los tácticos operacionales. Los primeros tienen que ver con el porqué de las cosas; las motivaciones de las acciones militares y su finalidad última en términos de los efectos que quieren generarse, especialmente en el largo plazo. Los segundos, tienen que ver con cómo se ejecutan las órdenes superiores a partir de un conjunto limitado de recursos (tiempo, personal, suministros, armamentos, municiones, etc.).

Bajo la tradición contrainsurgente del Ejército Nacional, el objetivo estratégico es el control militar de un territorio y el logro de la victoria

3 La acción contrainsurgente colombiana cuenta con una larga tradición de abordar esquemas complejos de criminalidad mucho más allá del combate a la insurgencia por sí solo. No se trata de ninguna novedad. Es el caso del narcotráfico, el secuestro, la extorsión, el reclutamiento forzado, y más recientemente el combate a las bacrim y la minería ilegal.

4 Es el caso de la Operación Jaque, y todas aquellas operaciones que abatieron altos jefes guerrilleros.

DOI: https://doi.org/10.59794/rscd.2025.v11i11.142

sobre un enemigo en combate armado. Esa concepción estratégica se mantuvo prácticamente estática, hasta darse por sentada en todas las operaciones, sin que mediara ningún matiz. Sin embargo, dadas las nuevas realidades políticas y sociales, es urgente remontase a los fundamentos de las Ciencias Militares y formular un planeamiento estratégico refrescante, que considere la racionalidad de la guerra en Colombia, así como sus objetivos y largo plazo.

Muy por el contrario, a la concepción más extendida, la guerra no solo trata de derrotar al enemigo. "En realidad, la guerra trata de crear el orden social y político cuando los sistemas de orden del pasado se han desintegrado, o han sido intencionalmente destruidos por la fuerza militar" (Schmidt, 2014, p. 2). La estrategia militar eficaz exige que el rol de las fuerzas enemigas sea considerado en un contexto de orden social y político más general. Toda planificación operacional válida depende de esta claridad estratégica. En realidad, el derrotar a una fuerza enemiga no es el objetivo estratégico de ninguna guerra.

El verdadero objetivo estratégico es recrear un orden estable que pueda ser sostenido sin una significativa participación militar constante del vencedor en el campo de batalla. El derrotar a los enemigos militarmente tan solo es un prerrequisito de la victoria estratégica, no su conclusión. Es posible que algo que en el campo de batalla es llamado "victoria", rápidamente pueda condenar al fracaso las probabilidades del éxito estratégico.

La "victoria" entendida desde la óptica de la Doctrina Militar de mayor tradición en el Ejército de Colombia, solo establece las condiciones para el orden social y político transformativo que llega después de que los acuerdos de paz con las guerrillas se hayan decantado con éxito. Llegados a este punto, y sin menoscabo del principio militar de abstenerse de intervenir en actividades o debates de partidos o movimientos políticos, un comandante militar competente debe ver en la guerra una labor política[5]. Es preciso identificar como falsa aquella tesis que sostiene que son los militares los encargados de ganar la victoria, mientras que los actores civiles son los encargados del "trabajo político" de preservarla. "La guerra es una labor política:

Las Fuerzas Armadas —especialmente los ejércitos— son herramientas que se usan para hacer el trabajo fundamental de la política" (Schmidt, 2014, p.4). La fuerza bien dirigida determina quién sentará las bases del orden social y político cuando las estructuras de poder son inexistentes o han dejado de funcionar. Ciertamente, el poder de la fuerza militar en manos de comandantes que desconozcan este elemental principio es algo muy peligroso. La guerra, como actividad política, debe ser luchada sin perder de vista su racionalidad y fines últimos, en función de los cuales deben tomarse todas las decisiones.

5 Cabe destacar una importante limitación semántica de la palabra "política" en el idioma español. A diferencia de lo que ocurre en otras lenguas como el inglés, en el español se emplea la misma palabra "política" para hacer referencia al debate propio de los movimientos políticos de carácter electoral (en inglés, politics) y para referirse al conjunto de ideas, principios y métodos para regular y desarrollar la vida social y comunitaria (en inglés, policy). En absoluto respeto y apego al principio de que las fuerzas militares son no deliberantes, deben mantenerse al margen del debate político electoral (politics), más se plantea que los comandantes militares para el postconflicto colombiano deben tener excepcional comprensión de la formulación, ejecución y evaluación de las políticas públicas (public policy) tanto en los niveles local, regional y nacional.

En este proceso de toma de decisiones, es necesario destacar que la cultura del Ejército es de profunda tradición tecnocientífica, en la que los elementos cuantitativos tienden a tener un mayor peso específico en el proceso de toma de decisiones militares, y donde los aspectos tácticos acaparan la mayor parte de la atención: número de efectivos, cantidades y rendimiento de armas, posicionamiento en el terreno, movilidad, suministros, comunicaciones, etc. Esta concepción busca maximizar la probabilidad de éxito en todo enfrentamiento al minimizar los riesgos y administrar la dinámica de las variables involucradas a partir del control y previsibilidad que ofrece la aplicación de la estadística, la logística y la teoría de probabilidades, entre otras herramientas de descripción matemática.

Esto funciona bastante bien cuando se trata de combatir la insurgencia y la criminalidad como enemigos del Estado con diferentes niveles de organización; de hecho, es un enfoque que difícilmente será abandonado en tanto siga siendo necesario el desarrollo de operaciones militares. Sin embargo, la guerra exige una mentalidad cualitativa porque la guerra es un fenómeno social. Los comandantes militares deben comprender la política profunda y sistemáticamente si desean garantizar que la fuerza militar sea una herramienta estratégica exitosa. Necesitan pensar en términos estratégicos sobre los objetivos finales que apoyará la fuerza bajo su control.

La manera de hacerlo es comenzar a ubicarse en el contexto, y estableciendo el rol que juega la fuerza en dicho contexto con las otras variables en el campo de batalla. Ciertamente, toman decisiones más acertadas aquellos comandantes provistos de contexto que aquellos que conocen los hechos. Para tener acceso con claridad a este necesario contexto, surge la necesidad de la aplicación sistemática de las Ciencias Sociales a la estrategia militar. En efecto, el pensamiento estratégico implica la evaluación de las fuerzas políticas, económicas, psicológicas y militares para garantizar que las operaciones militares apoyen las políticas nacionales a cargo de las autoridades civiles democráticamente electas (Mejía, 2017).

Si bien esta metodología es esencial para el pensamiento estratégico eficaz, es contraria a la cultura profesional dominante en el Ejército. La cultura del Ejército prefiere una metodología tecnocientífica, debido a que es percibida como fuente de certeza asistida por la razón. Sin embargo, la guerra no es para nada previsible; mucho menos se caracteriza por ofrecer certezas plenas. Aún para los científicos sociales acostumbrados, resulta frustrante establecer claras teorías de causa-efecto para fenómenos tales como la guerra.

Es imposible hacer predicciones respecto a la guerra con el mismo grado de certidumbre con que las ciencias naturales y las matemáticas pueden predecir, por ejemplo, la trayectoria de un proyectil. No se trata de que los planteamientos cuantitativos deban ser descartados. Se trata de reconocer sus limitaciones inherentes y de enriquecerlos con criterios cualitativos propios de las Ciencias Sociales, a la hora de abordar la tarea de usar la fuerza para crear estados finales sociopolíticos cualitativos. Al respecto, la mayoría de las organizaciones militares avanzan sobre el supuesto de que de que los formuladores de política civiles han atado los cabos sueltos entre la intención estratégica y las capacidades militares. Sin embargo, esto puede estar equivocado.

Los acontecimientos por lo general evolucionan tan rápido que solamente el comandante militar tiene ocasión de reunir oportunamente los elementos de juicio suficientes para abor-

DOI: https://doi.org/10.59794/rscd.2025.v11i11.142

dar "las preguntas fundamentales en la planificación militar, o sea, aquellas que analizan el objetivo estratégico: ¿Cuales cambios militares y políticos lograría, a la larga, una serie de operaciones militares? ¿Cuál es el cambio cualitativo en las condiciones (por ejemplo, el número de efectivos en determinada región) que los planes de guerra deberían lograr? ¿En qué medida apoyarían esas nuevas condiciones al logro de los objetivos estratégicos de la nación?" (Schmidt, 2014, p. 5) Esto permite lograr claridades necesarias cuando las metas nacionales parezcan ambiguas o cuando no resulte claro si vale la pena asumir o no los costos militares en tiempo, sangre y dinero frente a una operación determinada.

Decidiendo estratégicamente, los comandantes militares intentarán comprender los cambios cualitativos en los complejos contextos políticos, económicos, psicológicos y militares, obteniendo así mejores resultados de cara a la misión constitucional de la fuerza armada, y los mejores resultados con los menores costos. "Un planteamiento cualitativo en el pensamiento estratégico implica una descripción de los valores e intereses de los grupos sociales legítimos y una garantía de que estos valores e intereses sean representados en los procesos de toma de decisiones públicas" (Schmidt, 2014, p. 8).

Estas decisiones pueden transformarse en la medida que los valores públicos cambien, de ahí que el comandante militar competente deba estar dotado de un finísimo pulso político para medir la temperatura y caudal de las "aguas políticas" en las que inevitablemente está inmerso, ejerciendo su función y adelantando su carrera. Una vía para adquirir esa delicada aptitud es a través del dominio de las herramientas de las Ciencias Sociales, que por la vía del pensamiento cualitativo permiten decisiones militares consecuentes, racionales, efectivas y constructivas de logro de las metas y objetivos de Estado.

La nueva Doctrina

La Doctrina Militar que sostiene el combate a la insurgencia como su elemento central, resulta claramente insuficiente y desactualizada para un escenario de postconflicto en el que la insurgencia de otrora se ha integrado a la vida civil. Además, aquella concepción no ofrece herramientas para una interoperabilidad alineada a los fines del Estado Social de Derecho, y es incapaz de dar respuestas al complejo contexto social que enfrentan hoy las comunidades que habitan los territorios donde el Ejército lleva a cabo sus operaciones militares. A la luz de esto, vale la pena revisar los principales cambios que se han venido introduciendo en la Doctrina Militar por parte del alto mando del Ejército.

Una de sus principales características es su perfil internacional, alineándose de manera muy clara a los preceptos de la OTAN. El superar las condiciones excepcionales que suponía el combate a las guerrillas históricas, le permite al Ejército ponerse en mejor sintonía con su importancia geoestratégica y geopolítica en la región, así como con los retos militares propios de una nación latinoamericana frente al resto del mundo.

En cuanto a la acción dentro del país, se plantean cambios de doctrina en los siguientes aspectos (Plan Estratégico Militar, 2015):

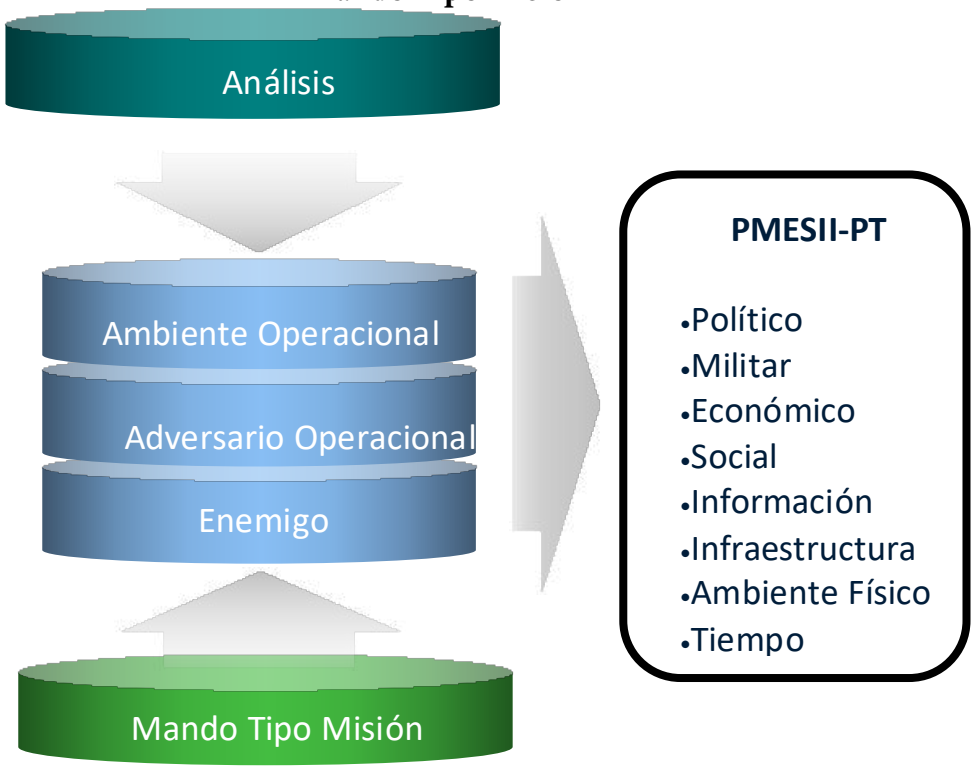
- Visión de la naturaleza de las Operaciones.
- Fundamentos de realización de las Operaciones.
- Métodos mediante los cuales se ejerce el comando de las misiones.

DOI: https://doi.org/10.59794/rscd.2025.v11i11.142

Con esta nueva Doctrina se busca fomentar la iniciativa y el pensamiento creativo al enfocarse en cómo pensar, y no en qué pensar. Esta transformación inicia con un replanteamiento del Currículo Profesional Militar, de modo que un comandante militar esté en capacidad de sintetizar datos que le permitan comprender, visualizar, describir y dirigir el área de operaciones, con mucha mayor amplitud de criterio para ejercer su labor como fuerza socialmente influyente en el territorio.

De todas estas consideraciones de replanteamiento doctrinal, surge el concepto del Mando Tipo Misión, el cual concreta la manera de aplicar la nueva Doctrina en desarrollo de las operaciones militares. Se define como "el ejercicio de autoridad y orientación del comandante mediante el uso de órdenes tipo misión para permitir la iniciativa disciplinada dentro de la intención del comandante a fin de habilitar a los líderes ágiles y adaptables en la conducción de las operaciones terrestres unificadas" (Mejía Ferrero, 2017, p.92). El Mando Tipo Misión considera que la compresión de una situación militar debe tener en cuenta los siguientes elementos (figura 2).

Figura 2
Mando Tipo Misión



Nota: Mando Tipo Misión. Variables a considerar en desarrollo de una operación militar, permitiendo la iniciativa disciplinada [1, 2].

Al efectuar el análisis de la situación desde esta perspectiva, hay un mejor conocimiento de la situación nacional y del contexto en el que se desarrollan las operaciones militares, haciendo posible alinear el desarrollo de cierta misión con el conjunto de la política gubernamental y la legislación vigente. A partir de esta visualización se da origen a las operaciones terrestres unificadas, con el fin de permitir a los comandantes "considerar combinar

DOI: https://doi.org/10.59794/rscd.2025.v11i11.142

tareas que se centren en la población (operaciones de estabilización o de apoyo civil) así como las tareas que se enfocan en las fuerzas del enemigo".

La unión de los anteriores elementos permitirá un proceso de toma de decisiones más adecuado, pudiendo identificar aquellos que resulten desordenados o difíciles, y permitiendo darle una capa de sentido profundo a las variables tácticas clásicas como misión, el enemigo, terreno, tiempo, tropas y apoyo disponibles, tiempo disponible, y consideraciones civiles, dando un amplio margen para la resolución no solo a los problemas netamente operativos.

Además, permite caracterizar el problema a partir de las siguientes actividades (Department of the US Army, Civil Affairs Operations [DUACAO], 2014)

1. Comparar la situación con el efecto deseado.
2. Definir el ámbito o los límites del problema.
3. Identificar a quien afecta el problema. (¿Qué es afectado? ¿Cuándo ocurrió el problema? ¿Dónde está el problema?)
4. Identificar la causa del problema. (¿Por qué ocurrió el problema?)
5. Determinar qué obstáculos se presentan para solucionarlo.
6. Determinar la causa de los obstáculos existentes.

El anterior ejercicio nos arrojará todo un contexto en donde se pone de manifiesto no solo el esfuerzo militar, sino también el esfuerzo social donde intervienen el análisis de la geografía, la topografía del área de operaciones, su situación política, económica, social y cultural. El comandante determinará sus capacidades (medios para un fin), la estructura (integración de las unidades) y el tiempo para la ejecución de la operación, visualizando que no simplemente se trata de los problemas tácticos habituales como calcular armas, hombres, logística, apoyos de combate (aviación, cañones, tanques, tecnología de inteligencia, etc.) sino que podrá concebir no solo el control militar del área en sentido clásico, sino modular la intervención militar con más y mejor contacto con la población civil, de acuerdo con los índices de las necesidades básicas insatisfechas, las demandas de infraestructura, las iniciativas productivas y de desarrollo económico, así como los requerimientos de apoyo social, entre otros indicadores.

Así, el área de operaciones no solo se convierte en una plantilla de inteligencia, sino que se puede establecer una *Plantilla de Información para el Desarrollo Comunitario*, donde se da origen a un teatro de operaciones no solamente militar, sino de profundo alcance social. De esta manera, dentro de la reconfiguración de la línea de acción del Ejército, se identifican tres conceptos clave:[6]

1. **Innovación social**: Entendida como la acción militar como motor del cambio social y el progreso económico de la región donde las operaciones se realicen. El comandante militar, bajo la nueva doctrina (Ver figura 2), es capaz de ponerse en sintonía con su contexto, de ser sensible a la realidad de su entorno, y a partir de

6 Esto, constituye una lectura personal de la Doctrina Damasco, de reciente definición por parte del comando del Ejército.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

su autonomía,[7] es capaz de identificar caminos de transformación social más allá del uso del poder militar para suprimir agentes criminales y amenazas a la seguridad. Esto, exige desarrollar mayor capacidad de interacción e influencia sobre las diferentes comunidades, bajo criterios de absoluto respeto por su cultura, tradiciones, cosmovisión, identidad y particular visión del progreso y del desarrollo en cada caso.

2. **Acción unificada**: Por un lado, se profundiza en la acción armónica conjunta del Ejército con las demás Fuerzas Militares. Sin embargo, para ser un agente exitoso de transformación social (innovador social exitoso) requiere ampliar su capacidad de articular las acciones militares con la misión de todas las agencias del gobierno, lo mismo que con las organizaciones no gubernamentales y el sector privado. Junto con la Innovación Social, la Acción Unificada busca poner al alcance de la población y las comunidades el desarrollo de sus territorios a partir de proyectos productivos rentables, que mejoren la calidad de vida, generen confianza y realmente materialicen el Estado Social de Derecho a partir de la presencia del Ejército. De esta manera, el Ejército busca lograr su objetivo estratégico de recrear un orden estable que puede ser sostenido en el futuro sin una significativa participación militar en el territorio como campo de batalla.

3. **Seguridad integral**: Pese a las nuevas realidades de la paz con las FARC, la realidad de muchas regiones colombianas está lejos de ser la más propicia o la más receptiva a los planteamientos de cooperación y desarrollo que propone la Innovación Social y la Acción Unificada. A menos que la población no disfrute de una "paz como tranquilidad" (Cárdenas, 2016) no será posible ni la influencia social ni el desarrollo territorial propuesto. El logro de esa tranquilidad tiene como condición esencial e imprescindible, la seguridad. Aún sin las guerrillas, la realidad de muchas regiones colombianas permanecerá sumamente compleja por cuenta de la persistencia de múltiples fenómenos de criminalidad que traerán consigo el surgimiento de la "amenaza híbrida", que es la diversa y dinámica combinación de fuerzas regulares, fuerzas irregulares, fuerzas terroristas, elementos criminales o la combinación todos estos elementos unificados para alcanzar efectos de beneficio mutuo al margen de la ley.

Este tercer componente de **Seguridad Integral** es una de las variables críticas en el logro de la paz estable y duradera en el postconflicto (desde el punto de vista del conflicto con las guerrillas; pues a menos que se garantice la seguridad frente a estas amenazas híbridas, todos los esfuerzos de paz quedarán frustrados por la vía de quitar a la subversión simplemente para abrirle el espacio a otros actores criminales. Esto, de paso sería un retroceso en materia de Innovación Social y la Acción Unificada, haciendo que se regrese a la concepción militar de la vieja doctrina, sin mencionar la perpetuación del ambiente de conflicto y el clima de violencia a pesar de los esfuerzos de paz.

Por eso el ambiente operacional es complejo e inestable, lo cual hace necesario y conveniente que persistan elementos de la

7 Una autonomía disciplinada, y de acuerdo con los lineamientos e intenciones de su comandante.

DOI: https://doi.org/10.59794/rscd.2025.v11i11.142

anterior doctrina, si bien enriquecida con la visión social del Mando Tipo Misión, pero dando respuesta a realidades que requieren la toma del mando y el control del territorio que esté manos de agentes criminales de cualquier índole (figura 3). En ese sentido, el conflicto persiste y tanto persistan amenazas que empleen la violencia como medio para perseguir sus metas políticas, ideológicas o económicas.

Figura 3
Toma del mando y el control del territorio

Nota: Operaciones Terrestres Unificadas. Mando Tipo Misión en desarrollo del componente de Seguridad Integral – Pese a la paz con las FARC (o con todas las guerrillas) persiste la necesidad de la toma de mando y control del territorio que esté manos de agentes criminales de cualquier índole.

Esta nueva visión obliga al dominio de un arte del diseño militar muy comparable al arte de los formuladores civiles de política pública: planificación - preparación - ejecución - evaluación para un adecuado mando. Así, el comandante dará importancia a los aspectos civiles del ambiente operacional, junto con los parámetros establecidos en el análisis de la situación ya antes mencionado. Esto se traduce en el desarrollo de una "consciencia situacional" por parte de un comandante competente. A partir de esta consciencia, la naturaleza ofensiva militar se orienta hacia las necesidades de la población civil, permitiendo unas operaciones que, si bien estarán dotadas de todas las características y atributos

operacionales clásicos, permitirán crear nuevas oportunidades párale desarrollo social y territorial (DUACAO, 2014, p.84).

Retos de la Institucionalidad Militar frente a la Nueva Doctrina

Pasar de un paradigma de control del territorio, a veces temporal, y exclusivamente por vía de las armas, a uno de construcción de sociedad y territorio desde la presencia militar, supone un reto muy fuerte para la cultura del Ejército. Si bien el surgimiento de la nueva Doctrina Militar se reconoce como una realidad objetiva, y como una respuesta natural a las nuevas realidades de la paz con la subversión, es necesario reconocer que existe una muy poca claridad, cuando no una total incertidumbre, frente a qué estrategias y acciones han de adelantarse para convertir esta Nueva Doctrina en hechos ciertos que transformen la cultura del Ejército.

A partir de lo anteriormente explicado, se identifica una fortaleza militar en las operaciones de contrainsurgencia, así como una notable debilidad en las consideraciones estratégicas dentro del proceso de toma de decisiones militares, especialmente en el más alto nivel. La necesidad es establecer un claro nexo entre la estrategia y la táctica operacional, de modo que las acciones tácticas no sean "rueda suelta", divorciadas de los grandes lineamientos, sino que todas las veces se capitalicen en un éxito estratégico y en un aporte claro al logro de los objetivos del Estado.

El reto tiene que ver con la cultura de formación militar. Frente a ello, el cambio curricular de la instrucción militar es un claro acierto, pero que bien pude quedarse corto si no se tiene claro cuál es el perfil del comandante militar de Colombia en los escenarios que se aproximan, a saber: en los escenarios de postconflicto: ESTABILIZACIÓN (2014-2018) – TRANSICIÓN (2018-2022) –CONSOLIDACIÓN (2022-2030).

Se trata de un comandante militar profundamente conocedor de la realidad social del país y sus regiones, diestro en el manejo de las herramientas tecnocientíficas que hacen las operaciones militares más eficientes y costo-efectivas; pero también es un militar conocedor de las herramientas de las Ciencias Sociales, que le permiten usar el pensamiento estratégico en ambientes institucionales y operacionales en distintos niveles. A partir de ese conocimiento, adquiere un educado tacto político, que le capacita para ubicarse en el contexto social, económico, geográfico y militar propio del territorio en el que deba intervenir.

Es un profesional capaz de construir conocimiento sobre un problema desconocido y que aprovecha esta comprensión para crear un planteamiento general respecto a la resolución de problemas, no solo militares, sino sociales. En ese sentido, es un formulador de política pública, capaz de diseñar soluciones en permanente contacto con la población civil, quien constantemente cuestiona sus suposiciones y comprueba los límites de sus conocimientos.

La línea de acción del Ejército, bajo su nueva configuración demandará algunas competencias específicas, a saber:

1. En Innovación social: Exige conocimiento de la identidad cultural, tradiciones e idiosincrasia de aquellas comunidades que serán impactadas por la acción militar en un territorio determinado, así como un compromiso ético irrenunciable de respe-

DOI: https://doi.org/10.59794/rscd.2025.v11i11.142

to hacia todos estos elementos. También, exige sensibilidad social para diagnosticar las potencialidades de cada territorio en términos de recursos naturales, y actividades económicas sostenibles que permitan desarrollar el territorio, en respeto a la visión de desarrollo de cada comunidad en cada territorio. Y fundamentalmente exige capacidad de relacionamiento con la población para poder acercarse a su realidad y a partir de ello sintonizar las acciones militares tanto armadas (operaciones militares) como no armadas (construcción de infraestructura, desarrollo de proyectos productivos, asistencia social, etc.).

2. En Acción unificada: Exige capacidad de interacción y relacionamiento con las diferentes instituciones del Estado. En este aspecto, puede ser deseable un cierto grado de especialidad sectorial según diferentes necesidades de desarrollo de cada territorio: una cosa es asistir la conectividad a Internet; otra, aumentar la cobertura de saneamiento básico, y otra diferente, la asistencia técnica agropecuaria. En este sentido, la ventaja comparativa del Ejército es tener la capacidad de llegar a territorios alejados a los que la oferta institucional del Estado difícilmente llegaría por sí sola. Si bien no se espera que sea el Ejército la institución experta en todos los sectores, sí puede ser el mejor agente articulador de los esfuerzos del Estado, especialmente en los territorios donde la presencia estatal no armada ha sido históricamente poca o nula. De esta manera, la presencia militar puede traducirse en agente de reducción de las brechas sociales y de desarrollo de los territorios donde opera.

3. En Seguridad integral: Es la capacidad mejor desarrollada en el Ejército Nacional, frente a la cual solo cabría agregar aquellas competencias que mejoren la presencia y el perfil del Ejército en el plano internacional a través de, por ejemplo, la adopción de estándares OTAN y los métodos de articulación con otras fuerzas militares continentales y hemisféricas en el plano geopolítico y geoestratégico.

La única manera de lograr un perfil y competencias así es a través de una agresiva estrategia educativa que asigne oficiales en los programas doctorales de las universidades de primer nivel en Ciencias Sociales, formulación de Proyectos, e Innovación Social. Los estudios de Maestría pueden ayudar también, pero la Nueva Doctrina Militar demanda de sus oficiales, en el fondo, la capacidad de generar nuevo conocimiento, así como de dominar herramientas y metodologías de investigación en Ciencias Sociales aplicadas.

En cuanto al desempeño conjunto del Ejército, se identifica Plantillas de Información para el Desarrollo Comunitario, una importante oportunidad para el desarrollo socioeconómico del país. A través de la centralización de la información de inteligencia, no solo respecto al control militar de áreas y problemas de seguridad, sino de necesidades básicas insatisfechas, de demandas de infraestructura, de iniciativas productivas y de desarrollo económico de las diferentes regiones, es posible establecer estrategias de alcance nacional sobre líneas comunes, a partir de las cuales se puedan localizar recursos económicos, logísticos y humanos para impulsar la productividad colombiana, el empleo formal, el aseguramiento del ingreso mínimo, y el desarrollo socioeconómico en general. Esto, con la ventaja particular de poder incluir a las regiones más apartadas y a las comunidades más desfavorecidas.

Si el cambio cultural dentro del Ejército obedecerá un proceso educativo más o menos agresivo, la obtención de la aceptación organizacional bien tendrá mucho de ejercicio de la autoridad miliar en el sentido más puro. En ese sentido, los oficiales a cargo del comando deben ser los motores del cambio a través del ejemplo, de modo que toda la estructura, hasta en los nieles más básicos, asimile el enfoque social y sintonice su actuar operativo con los grandes objetivos estratégicos. Para los comandantes del nivel superior, el reto es trascender la preparación en Ciencias Militares hacia la asimilación de las Ciencias Sociales aplicadas como herramienta que les permita comprender aquellos mecanismos a través de los cuales se logra la creación de un orden social y político a través de la guerra.

Conclusiones

El cambio en la Doctrina Militar, plasmado en la estructura de Mando Tipo Misión, plantea todo un nuevo perfil y características para las actividades militares del postconflicto colombiano. En primer lugar, el surgimiento de amenazas híbridas hace necesario que se conserven los elementos de la Doctrina tradicional, enriqueciéndolos con la nueva, habida cuenta que, pese a los éxitos de los esfuerzos de paz con las guerrillas, la realidad social colombiana sigue siendo muy compleja y altamente demandante de acciones militares de control del territorio. Los elementos de esta nueva Doctrina recaban en la importancia del sentido estratégico de las acciones militares, al tiempo que plantea la transformación de un Ejército de Guerra Irregular en un Ejército Multimisión, capaz de ser agente de transformación social y progreso para las regiones y territorios que sean objeto de las actividades militares.

Estos principios se decantan en el Comando Tipo Misión, el cual reúne, a manera de texto de instrucción militar, la manera de conducir las operaciones militares de acuerdo con la nueva Doctrina. En este esquema de comando novedoso se destacan como los principales conceptos clave la Innovación Social, la Acción Unificada y la Seguridad Integral. La relevancia y complejidad de los primeros dos componentes supone un choque con la cultura actual del Ejército, cuya tradición no se caracteriza ni por el pensamiento estratégico ni por su enfoque en el desarrollo territorial o social. Este choque con la cultura imperante al interior del Ejército demanda una agresiva estrategia educativa orientada hacia los oficiales a cargo de adelantar el Comando Tipo Misión, intensiva en el uso de las herramientas de la generación de nuevo conocimiento en Ciencias Sociales.

De allí, puede identificarse el perfil del comandante militar para el postconflicto colombiano: aquel que sin perder de vista la tradición contrainsurgente del Ejército, sea altamente capaz de combatir amenazas a la seguridad y el territorio, pero que adicionalmente sea también un líder social y un agente de progreso para la región donde adelanta su actividad militar. Este liderazgo debe estar apuntalado por una concepción estratégica de la guerra como fuerza de creación del orden social y político, y por una comprensión de que su misión, en última instancia, es el sostenimiento de ese orden sin su constante intervención militar. Éste, ha de ser un orden próspero en el que desde la seguridad se logre la tranquilidad que permita el desarrollo de la población civil en su pleno potencial económico, cultural y social.

DOI: https://doi.org/10.59794/rscd.2025.v11i11.142

Referencias

Cárdenas, J. (2016). Paz con la naturaleza: La paz como tranquilidad. *La Silla Vacía*.

Comando General Fuerzas Armadas de Colombia. (2015). *Plan Estratégico Militar 2030*. https://www.fac.mil.co/sites/default/files/linktransparencia/Planeacion/Planes/plan_estrategico_militar_2030.pdf

Constitución Política de Colombia [Const]. Art. 217. 7 de julio de 1991 (Colombia).

Department of the US Army [DUACA0], (2024). *Civil Affairs Operations FM 3-57*. U. S Army, Editor.

Kalyvas, N. (2006). *The logic of violence in civil war*. Cambridge University Press.

Kilcullen, D. (2006). Counter-Insurgency Redux. *Journal of Strategic Studies*.

Mejía Ferrero, A. (2017). *Apoyo de la defensa a la autoridad civil MFE 3-28*. Ejército Nacional.

Mejía Ferrero, A. (2017). *Estabilidad MFE 3-07*. Ejército Nacional.

Mejía Ferrero, A. (2017). *Doctrina Damasco*. Ejército Nacional.

Resolución 0317 de 2010 [Comando del Ejército Nacional]. *Por la cual se aprueba el reglamento de operaciones y maniobras de combate irregular*. 08 de marzo de 2010.

Schmidt, M. (2014). La guerra como una labor política: Cómo usar las Ciencias Sociales para lograr el éxito estratégico. *Military Review*.

Apoyo al desarrollo social y económico del Perú a través de las capacidades de las Fuerzas Armadas

Support to the Social and Economic Development of Peru through the capabilities of the Armed Forces

Recibido: 14/ 05 / 2025 | Revisado: 18 / 07 / 2025 | Aprobado: 30 / 09 / 2025
DOI: https://doi.org/10.59794/rscd.2025.v11i11.143

Coronel (r) Carlos Hurtado Noriega, EP
Perú

Correo: hurtadocarlos1967@gmail.com.
investigacion@ucs.edu.pe

Orcid: https://orcid.org/0000-0002-0873-8419

Afiliación: Universidad Católica Sedes Sapientiae

El autor es un coronel EP en situación de retiro. Es Doctor en Ciencias Ambientales en la UNMSM. Posee una Maestría en Sociología en la Pontificia Universidad Católica del Perú, una Maestría en Desarrollo y Defensa Nacional en el CAEN y actualmente realiza estudios de Maestría en Gestión Pública en el CAEN. Tiene un Diplomado en Gobierno de personas en la Universidad de Piura, un Diplomado en Seguridad y Salud en el Trabajo, un Diplomado en Gestión de Riesgo de Desastres. Ha estudiado en la Academia Diplomática del Perú, Escuela Superior de Guerra del Ejército y Centro de Altos Estudios Nacionales. Ejerce la docencia universitaria a nivel de pre y post grado en diferentes Universidades de Perú desde el año 2018. A lo largo de su carrera militar se ha desempeñado entre otros puestos como, Observador Militar en una Misión de Paz de la ONU en Liberia – África en el 2007, jefe de Unidad del Grupo de Artillería de Campaña N° 8 en Las Lomas – Piura en el 2010, asesor del presidente de la Junta Interamericana de Defensa en Washington DC – EE. UU. en los años 2013 y 2015 y capacitador Indeci de Gobiernos Locales de Lambayeque en el 2023.

DOI: https://doi.org/10.59794/rscd.2025.v11i11.143

Dr. Hugo Bernabé Moreno
Perú

Correo: hj.bernabem@alum.up.edu.pe

Orcid: https://orcid.org/0000-0002-8952-9044

Afiliación: Universidad del Pacífico

El coautor es doctor en Gestión y Desarrollo, con maestrías en Administración y Ciencias Militares, y se ha especializado en Planeamiento Estratégico y Toma de Decisiones. Su formación como licenciado en Ciencias Militares con especialización en Ingeniería le confiere una perspectiva integral en la gestión de recursos y la seguridad. Su experiencia docente abarca pre y posgrado en reconocidas instituciones académicas. Profesional con una trayectoria consolidada en la docencia universitaria y en responsabilidad social, seguridad y defensa, derechos humanos y gestión pública. Su enfoque pedagógico y académico se orienta hacia la generación de conocimiento estratégico y el impacto social, formando profesionales con principios éticos y una visión de desarrollo sostenible. Académico adscrito a redes académicas internacionales como REDDOLAC, REDULAC RRD y URSULA, donde contribuye activamente al desarrollo de estudios en seguridad y gestión de riesgos. Actualmente, coordina la edición de la Revista Seguridad y Poder Terrestre, una publicación del Centro de Estudios Estratégicos del Ejército del Perú que difunde investigaciones sobre seguridad, defensa y la profesión militar, fortaleciendo el debate académico en estos ámbitos.

Resumen

La participación de las Fuerzas Armadas del Perú en el desarrollo social y económico es clave para el desarrollo del país y contribuye con una serie de actividades, gracias a sus capacidades operativas, al personal especializado y a su despliegue estratégico a través de todo el territorio nacional, sobre todo en lugares remotos y de difícil acceso, donde muchas veces el Estado no llega. El objetivo de esta investigación es describir la participación de las FF. AA. en el desarrollo social y económico del país. La metodología empleada se fundamenta en una revisión bibliográfica exhaustiva que integra un enfoque cualitativo basado en el análisis documental y hermenéutico; se examinan fuentes académicas, normativas legales, informes gubernamentales y estudios recientes que abordan el desempeño estratégico de las Fuerzas Armadas; a través de esta metodología, se interpreta el marco constitucional y políticas estratégicas nacionales para analizar las actividades realizadas por las Fuerzas Armadas., proporcionando una visión integral de su rol en la sociedad. Como conclusión las FF. AA. contribuyen significativamente al desarrollo social y económico del país a través de su capacidad de respuesta ante desastres, la creación de un ambiente seguro para la inversión, la educación y la modernización del personal militar, y su papel en la construcción de una sociedad más cohesiva. Estas interacciones fortalecen no solo la seguridad, sino también la estructura económica y social del Perú, preparando al país para enfrentar desafíos presentes y futuros.

Palabras clave: Capacidades operativas, desarrollo social y económico, desarrollo sostenible, Fuerzas Armadas del Perú, nuevos roles estratégicos

Abstract

The participation of the Armed Forces (AF) of Peru in social and economic development is key to the development of the country, contributing with a series of activities thanks to its operational capabilities, specialized personnel and its strategic deployment throughout the national territory, especially to remote and difficult to access places where the State often does not reach. The objective of this research is to describe the participation of the armed forces in the social and economic development of the country. The methodology used is based on an exhaustive bibliographic review, integrating a qualitative approach based on documentary and hermeneutic analysis; academic sources, legal regulations, government reports and recent studies that address the strategic performance of the Armed Forces are examined; through this methodology, the constitutional framework and national strategic policies are interpreted to analyze the activities carried out by the Armed Forces, providing a comprehensive vision of their role in society. In conclusion, the armed forces contribute significantly to the country's social and economic development through their capacity to respond to disasters, the creation of a safe environment for investment, education and modernization of military personnel, and their role in building a more cohesive society. These interactions strengthen not only security, but also Peru's economic and social structure, preparing the country to face present and future challenges.

Keywords: Operational capabilities, social and economic development, sustainable development, the Peruvian Armed Forces, new strategic roles

Introducción

A raíz del fin de la guerra fría, el nuevo reordenamiento mundial y la delimitación de las líneas fronterizas, muchos países en el mundo han restructurado sus políticas de seguridad ante nuevos escenarios, asignando nuevas misiones a sus FF. AA. El Perú no ha sido la excepción y el Estado ha considerado nuevos roles estratégicos alineados con su carta magna y políticas estratégicas nacionales.

De manera general las FF. AA. del Perú participan en diferentes actividades de apoyo al desarrollo socioeconómico del país en beneficio de la población y su bienestar general. Así el Ejército en la construcción y mantenimiento de carreteras, caminos y puentes con sus batallones de Ingeniería y realizando acciones cívicas. La Marina de Guerra con sus Plataformas Itinerantes de Acción Social (PIAS) a través de los ríos amazónicos y Lago Titicaca, llevando desarrollo y apoyo social a las comunidades más necesitadas. La Fuerza Aérea del Perú realizando acciones cívicas en comunidades de bajos recursos económicos, trasladando poblaciones aisladas o evacuando heridos y accidentados, siempre en coordinación con otras entidades del Estado (Fuerza Aérea del Perú, 2022).

Asimismo, las FF. AA. apoyan con ayuda humanitaria ante desastres naturales y antrópicos de acuerdo con Ley del Sistema Nacional de Gestión de Riesgos de Desastres (SINAGERD), pero también colaboran con el combate a actividades criminales, protección de los recursos naturales y cuidado del ambiente, contribuyendo a un ambiente de paz y tranquilidad que permita el desarrollo social y económico del país (Ley N° 29664, 2021).

Finalmente, las FF. AA. tienen el desafío de continuar apoyando con diversas responsabilidades en el desarrollo socioeconómico, protección de los recursos naturales y del ambiente del país, sin descuidar sus principales responsabilidades en la seguridad y defensa.

Desarrollo

Las normativas delineadas en la Constitución Política del Perú, el Acuerdo Nacional y los distintos planes estratégicos y políticas nacionales y sectoriales, constituyen el marco fundamental que orienta el desarrollo nacional (El Peruano, 2021; Constitución Política del Perú, 1993), garantizando la articulación de esfuerzos y la consolidación de una visión compartida para el progreso sostenible.

Figura 1
Normativas y Políticas: Hacia un Perú sostenible

Nota: Acuerdo Nacional (2002)

Esta participación de las FF. AA. se ve reforzada por políticas estratégicas nacionales, como las delineadas en el Libro Blanco de Defensa Nacional y el Acuerdo Nacional, que integran los objetivos de seguridad con las metas de desarrollo; en ese sentido, el Estado peruano asignó nuevos roles estratégicos a las FF. AA. entre las cuales tenemos: Apoyo al desarrollo nacional y Apoyo al sistema nacional de gestión de riesgos de desastres (Resolución Ministerial 1411, 2016). Durante su evolución, han ampliado significativamente su impacto en la sociedad, consolidándose como un referente en la estabilidad y el progreso del país; además, su participación garantiza la seguridad y la estabilidad, también ayuda a crear condiciones favorables para el desarrollo económico y el bienestar común (Tello Medina et al., 2020).

Las FF. AA. del Perú desempeñan un papel significativo en el desarrollo social y económico del país a través de diversas iniciativas y actividades que van más allá de sus misiones tradicionales. Estas instituciones contribuyen a la seguridad, a la estabilidad económica y a la mejora de la calidad de vida de la población en varias dimensiones. Las FF. AA. conformadas por el Ejército, Marina de Guerra y Fuerza Aérea, poseen un conjunto de capacidades operativas que contribuyen con el desarrollo socioeconómico de país, teniendo entre otras misiones la de brindar asistencia a la ciudadanía en general cuando lo requiera; teniendo como finalidad adicional la de fortalecer los lazos entre FF. AA. y ciudadanía.

El apoyo al sistema nacional de gestión de riesgos de desastres está normado dentro de la ley del Sistema Nacional de Gestión del Riesgo de Desastres, dentro de los procesos de preparación y respuesta; para ello, las FF. AA. participan brindando un importante apoyo a la población frente a emergencias como las

DOI: https://doi.org/10.59794/rscd.2025.v11i11.143

lluvias intensas, inundaciones, huaycos, friaje, terremotos, aluviones, sequías, entre otros peligros identificados; toda vez que su organización castrense y la ubicación de las unidades militares en todas las regiones del país, facilita intervenir de manera inmediata como entidad de primera respuesta en casos de emergencias por desastres de origen natural o antrópicos en cualquier región del país (Sierra-Zamora y Rueda-Serbousek, 2024); esto no solo mejora la resiliencia de las comunidades, sino que también promueve la confianza en las instituciones del Estado, lo cual es crucial para un desarrollo sostenible (Jara et al., 2021).

El apoyo al desarrollo nacional se da mediante el Comando de Apoyo al Desarrollo Nacional del Ejército (COADNE) que planifican dicho apoyo según las prioridades establecidas, para ello cuentan con los Batallones de Ingeniería que realizan la construcción y mantenimiento de carreteras, puentes, túneles, vados, etc. que son esenciales para la conexión y desarrollo de las comunidades. Asimismo, el COADNE dispone de los Batallones de Asuntos Civiles en condiciones de realizar actividades de desarrollo e inclusión social, gestión de riesgos de desastres y desarrollo e integración fronteriza (Suárez-Alemán y Domínguez, 2024; Castillo-García, 2021). Estos Batallones de Ingeniería son empleados de manera efectiva y rápida; sin embargo, existe la problemática que dichas unidades no cuentan con los equipos suficientes que optimizan la eficiencia de la unidad frente a la ocurrencia de desastres (Alvarado, 2021).

Las capacidades militares desempeñan un papel crucial al proporcionar seguridad y estabilidad, factores indispensables para fomentar la inversión y el crecimiento económico (Diez Mayrena, 2021). En este sentido, la integración de políticas de defensa con estrategias de desarrollo sostenible fortalece el concepto de bienestar general, asegurando que la protección y el progreso sean parte de un mismo proceso integral. Por ello, la planificación estratégica debe contemplar el impacto a largo plazo de las inversiones en seguridad sobre la calidad de vida de la población, estableciendo un equilibrio entre protección, desarrollo y sostenibilidad (CEPLAN, 2024).

En muchas instancias, especialmente en desastres severos o en ubicaciones muy remotas, las FF. AA. cumplen una dualidad funcional: actúan como "primeros respondedores" debido a su capacidad de despliegue rápido, y como "último recurso" cuando las capacidades civiles están sobrepasadas o son inexistentes. Su estructura organizada, activos logísticos (transporte aéreo, marítimo y terrestre), sistemas de comunicación y personal disciplinado les permiten movilizarse y operar eficazmente en entornos caóticos post-desastre, donde las agencias civiles pueden enfrentar dificultades iniciales; esta doble responsabilidad subraya la naturaleza indispensable de las FF. AA. en el sistema nacional de respuesta a emergencias del Perú.

Las FF. AA. participan en el combate contra las actividades ilícitas, protección de recursos naturales y del medio ambiente; al respecto, la protección ambiental señala un reconocimiento de que estos temas están intrínsecamente ligados a la seguridad nacional, la estabilidad económica y el desarrollo nacional a largo plazo; no obstante, esta estrategia requiere una planificación cuidadosa para asegurar que las tareas de desarrollo no comprometan la preparación y el entrenamiento para las misiones militares primordiales (Acuerdo Nacional, 2002). Por ello, las FF. AA. desempeñan un papel crucial en los pilares del desarrollo sostenible -económico, social y am-

biental- al colaborar estrechamente con los diferentes sectores del Estado ya sea en el traslado y resguardo de los ciudadanos (ESAN, 2022), así como en la cooperar en la intervención multisectorial de las políticas nacionales.

En el caso del Ejército, realiza trabajos de construcción y mantenimiento de carreras con sus Unidades de Ingeniería; asimismo, por su despliegue estratégico por todo el territorio nacional le permite participar en acciones cívicas por su presencia en áreas remotas, con personal y logística de primera mano. En la Figura 2 se muestra la distribución de 10 Batallones de Ingeniería del Ejército del Perú que vienen participando en la gestión del riesgo de desastres a nivel nacional, son unidades especializadas y equipadas para cumplir una misión fundamental para la protección de la población y contribuir al desarrollo del país. Es decir, dichos Batallones de Ingeniería están ubicados en todo el país y trabajan para garantizar la seguridad, el bienestar y el progreso de las personas.

Figura 2
Batallones de Ingeniería del Ejército en apoyo al desarrollo nacional

Nota: COADNE (2021)

Es por ello, que ante la mayor incidencia de desastres naturales y para dar cumplimiento al rol asignado, el Ejército crea la 1ª Brigada Multipropósito en el 2018, una unidad especializada encargada de la evacuación, búsqueda, rescate, traslado y atención de heridos en caso de desastre y emergencia, teniendo como referente a la Unidad Militar de Emergencias de España.

La 1ª Brigada Multipropósito es la gran unidad que inicialmente se creó con 1500 hombres entre oficiales, supervisores, técnicos y

DOI: https://doi.org/10.59794/rscd.2025.v11i11.143

sub oficiales que fue incrementándose progresivamente, dispone de cuatro compañías de intervención rápida para desastres, un batallón de sanidad, una compañía contra conflictividad social y un equipo de fumigación y salud pública; además, esta Gran Unidad cuenta con un vehículo Visat (de Comunicaciones), maquinaria pesada de ingeniería, un vehículo lanzapuente MTU, vehículos cisterna, dos vehículos Lanzacohete Otorongo, camiones MAN, etc. Además, cuenta con el apoyo de helicópteros con sistema contraincendios Bambi Bucket de la Aviación del Ejército (Ministerio de Defensa, 2018).

Figura 3
El Batallón de Asuntos Civiles del Ejército del Perú, en trabajos de limpieza y descolmatación del río Grande de Arahuay, en la provincia de Canta, departamento de Lima

Nota: COADNE (2021)

La Marina de Guerra, a través de su Dirección de Hidrografía y Navegación custodia el patrimonio natural, participando en la protección ambiental, la lucha contra actividades ilícitas que depredan recursos y la conservación de la biodiversidad. Por otro lado, el Servicio Industrial de la Marina (SIMA), aporta conocimiento científico y capacidad industrial; como principal Astillero del Perú, efectúa el mantenimiento, modernización y construcción de barcos de la Marina de Guerra, y realiza proyectos relacionados con la industria naval y metalmecánica para el sector estatal y privado, nacional y extranjero; dentro de los estándares de calidad acordes con la normativa de la ISO 9001, con la finalidad de contribuir a la defensa y el desarrollo socio-económico y tecnológico del país (LBDN, 2006).

El SIMA, debido a su consolidada trayectoria, capacidades técnicas desarrolladas y su alineación con las demandas emergentes del mercado global, se posiciona como un referente estratégico en el ecosistema marítimo-industrial de la región (SIMA PERÚ, 2024). El SIMA opera a través de tres centros industriales: Callao, Chimbote e Iquitos, que en conjunto conforman una infraestructura nacional única. Estos centros están equipados con gradas de hasta 50,000 tonelaje (DWT), lo que le permite manejar grandes envergaduras y desarrollar simultáneamente varios

proyectos. Además, cuenta con una capacidad metalmecánica instalada de 15,000 toneladas al año, respaldada por expertos en armamento naval y sistemas electrónicos, incluyendo a la empresa Northrop Grumman-Sperry Marine, que respalda su perfil tecnológico (Northrop Grumman-Sperry Marine, 2024).

Su alineación con la política nacional de defensa es uno de los pilares estructurales de su propuesta de valor (MINDEF, 2023). Este enfoque enfatiza la estabilidad institucional y la capacidad de planificación estratégica a largo plazo, lo que facilita la creación de alianzas público-privadas y consorcios internacionales. En este sentido, SIMA ha fortalecido su proceso de internacionalización mediante alianzas estratégicas como la establecida con HD Hyundai Heavy Industries, que permite la integración de tecnología puntual, impulsa la transición energética naval (buques propulsados por GNL, petróleo o hidrógeno) y cierra brechas tecnológicas que, de otro modo, supondrían un riesgo de obsolescencia competitiva (HD Hyundai Heavy Industries, 2023).

La Fuerza Aérea del Perú provee servicios esenciales de cartografía y apoyo a la investigación. Asimismo, a través del Servicio de Mantenimiento (SEMAN) son especialistas en el servicio de mantenimiento aeronáutico a nivel internacional y tiene Convenios de cooperación con instituciones militares y civiles de otros países; además del mantenimiento de aeronaves, también ofrece servicios especializados en pruebas no destructivas, fabricación de componentes estructurales, reparaciones, alteraciones, reparaciones de materiales compuestos avanzados, etc. (LBDN, 2006).

El SEMAN, en base a su consolidada trayectoria institucional de más de cincuenta años y el respaldo de una infraestructura moderna estratégicamente ubicada en la ciudad de Lima (capital de Perú), que incluye hangares especializados, oficinas, laboratorios, instalaciones de prueba y una Unidad Funcional Aeronáutica en el Aeropuerto Internacional Jorge Chávez, brinda servicios integrales de mantenimiento, reparación y revisión (MRO) con estándares internacionales. Su posición se ha visto fortalecida por una cartera de certificaciones de alto nivel de la FAA (Estados Unidos), EASA (Unión Europea), AS9100, ANAC Brasil y ANAC Argentina, que le otorgan la autoridad para intervenir en aeronaves de gran tamaño como los Boeing 737, 767, 777, C-130 y el futuro Airbus A320. Además, actúa como centro regional para operadores civiles y militares (SEMAN PERÚ, 2024).

A su vez, el SEMAN es considerado como el segundo MRO en Sudamérica con esta capacidad, el hito técnico realizó el mantenimiento de Check C de un Boeing 777, fortaleciendo su dominio operativo y técnico en inspecciones de trenes de aterrizaje, materiales compuestos y ensayos no destructivos. A través de su alianza estratégica con Derco/Lockheed Martin les otorga acceso preferencial a tecnologías y recursos clave, lo que les permite participar en programas de modernización de aeronaves militares en el país y la región, como el F-5, el C-130 y el KT-1P (Lockheed Martín, 2024).

Además, el SEMAN ha fortalecido su visibilidad internacional participando en congresos como CANSEC (Canadá) y SITDEF (Perú), y ha ampliado su cartera de servicios para incluir nuevos servicios de mantenimiento de UAV, en línea con la tendencia global de adopción de sistemas no tripulados. Su estrategia de expansión incluye la construcción del hangar H-3002 para alojar aeronaves con fuselaje ancho, la obtención de certificaciones específicas para la familia Airbus A320 y A321,

DOI: https://doi.org/10.59794/rscd.2025.v11i11.143

y la investigación de nuevos nichos como el apoyo a aerolíneas de bajo coste, ambulancias aéreas y operadores logísticos humanitarios (SEMAN PERÚ, 2024).

Desarrollo social

Las FF. AA. también participan en expediciones de investigación científica en la Antártida, promoviendo la investigación científica y la protección del medio ambiente dentro del marco de los tratados internacionales antárticos; además contribuyen con logística y seguridad, facilitando la labor de científicos que estudian aspectos como la biodiversidad y el cambio climático (Calderón et al., 2022).

Periódicamente, el Comando Conjunto de las Fuerzas Armadas (CCFFAA) planifican y ejecutan acciones cívicas con el apoyo de los tres institutos armados: Ejército, Marina de Guerra y Fuerza Aérea, a las poblaciones más necesitadas del país, llevando atención médica, dental, servicios de peluquería, asesoría legal, show infantil, demostraciones militares, banda de músicos, entre otros (CCFFAA, 2024). Además, a través de acciones cívicas, las FF. AA. fortalecen el vínculo con la sociedad mediante actividades temporales que, con sus propios recursos, personal y material, no solo refuerzan la imagen institucional, sino que también fomentan el sentido de identidad nacional; todo ello sin desviar su misión principal (roles estratégicos constitucionales según Figura 6), consolidando que la seguridad y el desarrollo vayan juntos en beneficio de los ciudadanos.

Durante la pandemia del Covid 19, las FF. AA. apoyaron a la Policía Nacional del Perú en sus tareas de vigilancia por calles y locales del país, controlando peatones y conductores para que cumplan las disposiciones del gobierno sobre las medidas de aislamiento e inmovilización social, recalcándoles la importancia de permanecer en sus domicilios, el control del toque de queda de 20:00 a 05:00 horas del día siguiente, así como apoyando los centros de vacunación en todo el país (Pizarro, 2021). Asimismo, la Fuerza Aérea apoyó con sus aeronaves para la evacuación de pacientes críticos con Covid 19 desde las distintas ciudades del país hasta Lima (Becerra-Canales, 2023; Sigueñas, 2021; Salas, 2020).

El Ejército, a través de un convenio de cooperación interinstitucional con el Ministerio de Desarrollo e Inclusión Social (MIDIS), implementa las Plataformas Itinerantes de Acción Social (PIAS) terrestres, facilitando el despliegue de caravanas que acercan atención médica, servicios de identidad, gestión de riesgos de desastres, acceso a justicia y otros recursos fundamentales a poblaciones alejadas (Ejército del Perú, 2025; MIDIS, 2024).

La Marina de Guerra, en coordinación con el MIDIS mediante el Programa Nacional País y con el apoyo de otros sectores del Estado peruano, desarrolla una labor social en las comunidades y poblaciones vulnerables de la selva peruana mediante sus PIAS. Estas embarcaciones recorren los ríos amazónicos y el Lago Titicaca, llevando servicios básicos y programas de desarrollo a comunidades remotas, llevando personal de la Dirección de Salud y Educación de la región, Banco de la Nación, Seguro Integral de Salud, Registro Nacional de Identificación y Estado Civil; además de los Ministerios de Salud, de la Mujer y Poblaciones Vulnerables, entre otros, así como representantes del gobierno regional y gobiernos locales; todo en beneficio de estos grupos vulnerables (Marina de Guerra del Perú, 2025; Pinto et al., 2022).

Figura 4
Las PIAS de la Marina de Guerra del Perú en coordinación con el MIDIS realizando actividades de apoyo social en los pueblos amazónicos

Nota: MIDIS (2024)

Asimismo, la Marina de Guerra realiza contribuciones científicas e industriales altamente especializadas gracias a su Dirección de Hidrografía y Navegación que administra e investiga las actividades de Oceanografía, Hidrografía, Meteorología, Cartografía y Señalización Náutica, esta información generada es vital para la seguridad marítima, la gestión de recursos marinos (pesquerías, potencial energético offshore) y la protección del medio ambiente acuático. Adicionalmente, el SIMA promueve y desarrolla la industria naval del Estado, apoyando la construcción y reparación naval, lo que permite retener y desarrollar capacidades industriales críticas dentro del país (LBDN, 2006).

Por otro lado, la Fuerza Aérea del Perú juega un papel igualmente vital, en especial dada la geografía del país, realizando puentes aéreos en apoyo a poblaciones de bajos recursos mediante vuelos de acción cívica para el transporte aéreo de personal, alimentos, hospitales de campaña, medicinas, maquinarias, materiales de construcción y combustible; asimismo, evacuando a las poblaciones afectadas por los desastres, así como llevando material, alimentos y medicinas (LBDN, 2006). Además, realiza evacuaciones aeromédicas en coordinación con el Ministerio de Salud (MINSA) y MIDIS, desde zonas alejadas y fronterizas de país hasta hospitales de primer nivel de las grandes ciudades, trasladando heridos y accidentados de gravedad, recibiendo tratamiento y estabilización al paciente mientras dura el vuelo (Llanos-Zavalaga et al., 2021).

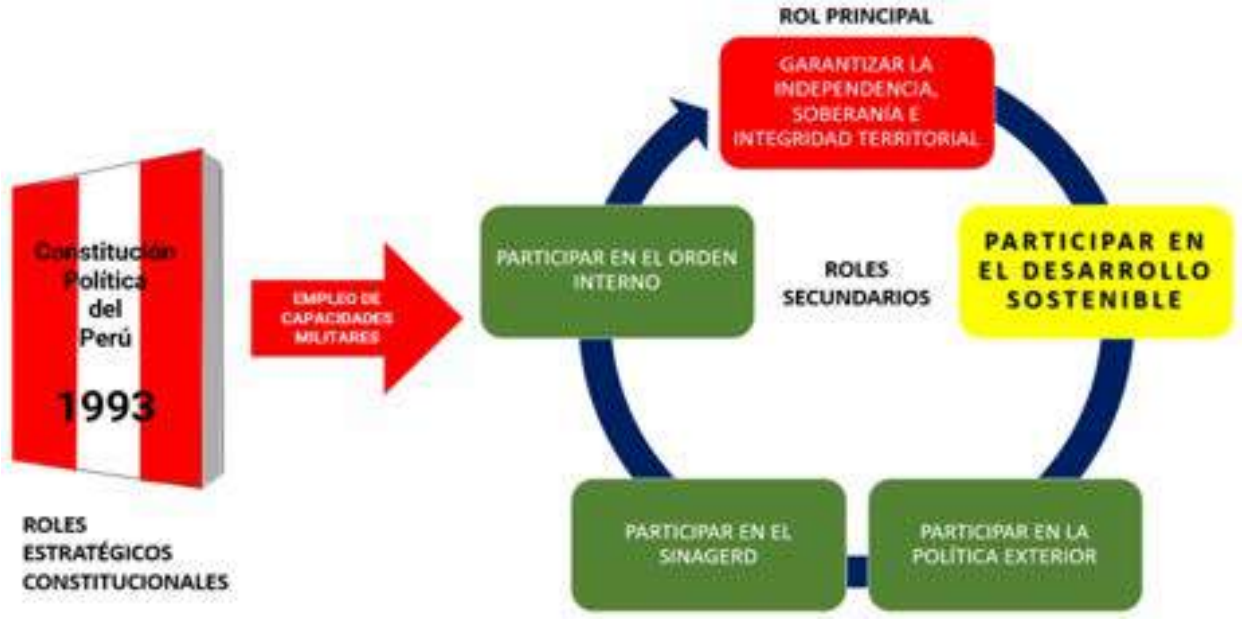
DOI: https://doi.org/10.59794/rscd.2025.v11i11.143

Figura 5
Personal de la Fuerza Aérea y Ministerio de Salud evacuando a un herido en Cajamarca

Nota: Fuerza Aérea del Perú (2022)

Además, la Fuerza Aérea del Perú también realiza aportes fundamentales, aunque a veces menos visibles, a la planificación de la infraestructura. Sus "labores de fotografía aérea para catastros urbanos y rurales, estudios de suelos, proyectos de vialidad, turismo, arqueología e investigación científica" proveen información cartográfica y de reconocimiento esencial. Estos datos son la base para una planificación territorial ordenada, la gestión eficiente de recursos, el desarrollo de proyectos de infraestructura bien concebidos y la promoción de sectores como el turismo (LBDN, 2006).

Figura 6
Roles estratégicos para el desarrollo social



Nota: CCFFAA (2024)

Otro aspecto en el que las FF. AA. impactan el desarrollo social es a través de la educación y la capacitación del personal militar y civil. La modernización y la profesionalización de las FF. AA. incluyen programas de formación que no solo benefician al personal militar, sino que también generan un impacto positivo en las comunidades. Al respecto, se han implementado plataformas virtuales, como por ejemplo el Aula Virtual del Ejército para garantizar formación continua, lo que apoya en la educación de los miembros del Ejército y también puede beneficiar a la sociedad civil en diversas capacidades técnicas (Gallegos, 2023).

Por otro lado, el compromiso de las FF. AA. con el desarrollo social también se ve reflejado en su involucramiento en actividades que fomentan la cohesión social y la estabilidad política. El histórico rol de las FF. AA. en la política peruana ha evolucionado hacia una participación más constructiva, abogando por la gobernabilidad y el respeto a los derechos humanos, lo que repercute en un mayor desarrollo social (Jara et al., 2021). Este alineamiento con la construcción de una sociedad más inclusiva y equitativa es crucial para un desarrollo más integral.

Desarrollo económico

Desde un punto de vista económico, las FF. AA. también contribuyen a crear un ambiente seguro necesario para la inversión y el crecimiento económico, reduce los riesgos para las empresas, aumenta la confianza de los inversores, protege las industrias legítimas (como el turismo, comercio y agricultura) ya que, sin un entorno seguro, la inversión extranjera y nacional tiende a disminuir, lo que afecta directamente el desarrollo económico del país. La percepción de seguridad fortalecida por la presencia de las FF. AA. permite movilizar recursos hacia sectores vitales como la minería y la infraestructura, impulsando así el crecimiento económico (Simón et al., 2023). Además, el desarrollo de la infraestructura financiera permite una mejor asignación de recursos y fomenta la movilización de ahorros, lo cual es crítico para el crecimiento económico a largo plazo (Villafrádez et al., 2022).

El desarrollo de capacidades industriales nacionales es otra área de contribución. La participación del SIMA de la Marina de Guerra y, análogamente, los esfuerzos de la Fuerza Aérea del Perú con el SEMAN en la industria aeronáutica (LBDN, 2006), buscan desarrollar y mantener capacidades industriales estratégicas dentro del país. Estas iniciativas no solo pueden reducir la dependencia de proveedores extranjeros para ciertos bienes y servicios de defensa, sino también generar empleo cualificado, retener conocimiento tecnológico y estimular actividades económicas auxiliares.

El desarrollo de las zonas de frontera, a menudo económicamente marginadas, pero estratégicamente importantes, también recibe atención. Las FF. AA. buscan "Fomentar la integración y el desarrollo de pueblos fronterizos", y el Ejército participa en programas de "asentamiento rural fronterizo" a través de los Comandos de Asentamiento Rural (COAR). Estos esfuerzos pueden desbloquear el potencial económico local, mejorar los medios de vida de las comunidades fronterizas y fortalecer la soberanía nacional en estas áreas sensibles (LBDN, 2006).

Una iniciativa gubernamental destacada es la promoción de "Proyectos en Activos", que busca utilizar terrenos de las FF. AA. para atraer inversiones privadas. Se ha identificado una cartera de "50 Proyectos en Activos en terrenos de las FF. AA. donde pueden desarrollarse inversiones potenciales por más de 2,000

millones de soles". Estos proyectos abarcan diversas áreas, incluyendo "proyectos inmobiliarios, energéticos (como parques eólicos) y otros" (Andina, 2019). Esta estrategia representa un enfoque novedoso mediante el cual los activos militares, principalmente terrenos, se convierten en un motor para la generación de actividad económica y desarrollo.

Otro aspecto, es la modernización del Hospital Militar como un ejemplo de cómo estos proyectos pueden beneficiar directamente a la familia militar y mejorar los servicios. Este modelo de colaboración público-privada, impulsado por entidades como ProInversión, es visto como una estrategia clave para dinamizar la economía peruana (Andina, 2019).

Además, la capacitación ofrecida al personal durante el servicio militar voluntario, como la que brinda la Marina (LBDN, 2006), puede dotar a los jóvenes de habilidades técnicas, disciplina y experiencia laboral que son transferibles al mercado de trabajo civil. Esto representa una contribución al desarrollo del capital humano del país, mejorando la empleabilidad de los licenciados del servicio militar.

Conclusiones

Las FF. AA. del Perú contribuyen significativamente al desarrollo social y económico del país a través de su capacidad de respuesta ante desastres, la creación de un ambiente seguro para la inversión, la educación y la modernización del personal militar, y de su papel en la construcción de una sociedad más cohesiva. Estas interacciones fortalecen no solo la seguridad, sino también la estructura económica y social del Perú, preparando al país para enfrentar desafíos presentes y futuros.

Las FF. AA. del Perú disponen de capacidades militares para cumplir con la finalidad primordial que es la de garantizar la independencia, soberanía e integridad territorial, simultáneamente, promueven el desarrollo sostenido (social y económico). Su labor trasciende la seguridad nacional al integrar a las regiones mediante la implementación de políticas de diseño orientadas al bienestar general, tales como la seguridad alimentaria, la administración de los recursos naturales y la gobernanza sostenible. Acciones militares que coordina con diferentes sectores, posibilitando el desarrollo del país.

Referencias

Acuerdo Nacional. (2002). *Informe final de las FF. AA.* https://www.studocu.com/pe/document/universidad-nacional-agraria-la-molina/sociedad-y-cultura-peruana/acuerdo-nacional-informe/36241307

Alvarado, C. (2021). *Capacidad de respuesta del Batallón de Asuntos Civiles N° 2 frente a la ocurrencia de desastres en la carretera central, Chosica 2019* [Tesis de maestría, Escuela Superior de Guerra del Ejército – Escuela de Postgrado]. https://hdl.handle.net/20.500.14141/198

Andina. (2019, 27 de marzo). *Gobierno lanza oportunidades de inversión en terrenos de FF. AA. por S/ 2,000 millones.* https://andina.pe/agencia/noticia-gobierno-lanza-oportunidades-inversion-terrenos-ff-aa-s-2000-millones-1023801.aspx

Becerra-Canales, B. (2023). Evaluación de la atención primaria durante la pandemia por COVID-19 en una región del Perú. *Enfermería Global*, 22(1), 283–308. https://doi.org/10.6018/eglobal.521201

Calderón, C. E. Á., Rivera-Páez, S., & Ramírez-Pedraza, Y. E. (2022). La Antártida desde la dimensión de la seguridad multidimensional y su impacto en Colombia. En *La importancia de la Antártida para Colombia: Medio ambiente, seguridad internacional y contribución militar* (pp. 41–83). https://doi.org/10.25062/9786287602205.07

Castillo-García, R. F. (2021). Evolución de la planificación urbana en el Perú 1946–2021: De la planificación urbana normativa a la planificación del desarrollo urbano sostenible. *Paideia XXI*, 11(1), 79–112. https://doi.org/10.31381/paideia.v11i1.3783

CCFFAA. (2024). *Comando Conjunto de las Fuerzas Armadas* [Página web]. Gobierno del Perú. https://www.gob.pe/ccffaa

CEPLAN. (2024, 1 de enero). *Aportes para la articulación entre el planeamiento estratégico y la asignación presupuestal* [Documento de trabajo]. Centro Nacional de Planeamiento Estratégico. https://www.gob.pe/institucion/ceplan/informes-publicaciones/4989817-aportes-para-la-articulacion-entre-el-planeamiento-estrategico-y-la-asignacion-presupuestal

COADNE. (2021). *Red social oficial del Comando de Apoyo al Desarrollo Nacional del Ejército.* Ministerio de Defensa. https://www.facebook.com/coadne/?locale=es_LA

Constitución Política del Perú [Const]. (1993) https://www.gob.pe/institucion/presidencia/informes-publicaciones/196158-constitucion-politica-del-peru

Diez Mayrena, J. (2021, 1 de noviembre). La capacidad militar de las FFAA y los derechos fundamentales de las personas en el contexto de la emergencia. *Defensa CAEN*, 2(1), 11. https://doi.org/10.58211/recide.v2i1.50

Ejército del Perú. (2025, 30 de abril). *Ejército del Perú*. Plataforma del Estado. https://www.gob.pe/institucion/ejercito/institucional

El Peruano. (2021, 20 de agosto). Jefe del Estado lidera sesión del Foro del Acuerdo Nacional [En vivo]. *El Peruano.* Recuperado el 24 de abril de 2025, de https://elperuano.pe/noticia/127249-jefe-del-estado-lidera-sesion-del-foro-del-acuerdo-nacional-en-vivo

ESAN. (2022, 6 de septiembre). ¿Por qué es importante el desarrollo sostenible para las empresas? *Conexión ESAN*. https://www.esan.edu.pe/conexion-esan/por-que-es-importante-el-desarrollo-sostenible-para-las-empresas

Fuerza Aérea del Perú. (2022). *Capacidades operativas y misiones de rescate en el Perú* [Publicación interna]. Ministerio de Defensa.

Gallegos, G. (2023). Plataformas virtuales en la enseñanza militar: Una visión tecnológica. *RCESGE.* https://doi.org/10.60029/rcesge.v2i1art2

HD Hyundai Heavy Industries. (2023). *Naval technology transfer agreements and global collaborations.* https://www.hhi.co.kr

Jara, M., Villamil, X., & Montaño, A. (2021). *Un estudio comparado de las reformas del sector seguridad y las relaciones civiles-militares en Perú, Chile, El Salvador y Guatemal*a (pp. 147-174). https://doi.org/10.21830/9789585350601.06

Ley N° 29664 (2021). *Ley del Sistema Nacional de Gestión de Riesgos de Desastres* (SINAGERD) https://www.gob.pe/institucion/indeci/infor-

mes-publicaciones/2370524-ley-n-29664-ley-del-sistema-nacional-de-gestion-del-riesgo-de-desastres-sinagerd

LBDN (2006). *Libro Blanco de Defensa Nacional del Perú*. Comando Conjunto y Fuerzas Armadas del Perú. https://bvs.minsa.gob.pe/local/MINSA/1320_GOB530.pdf

Llanos-Zavalaga, F., Siles, D. A., Valcárcel, B., & Huertas, O. H. (2021). Historia de la atención primaria de salud en Perú: Entendiendo su camino y perspectivas actuales. *Revista Médica Herediana,* 31(4), 266-273. https://doi.org/10.20453/rmh.v31i4.3861

Lockheed Martin. (2024). *Strategic partnerships in Latin America: SEMAN–Derco initiatives*. https://www.lockheedmartin.com

Marina de Guerra del Perú. (2025, 30 de abril). *Marina de Guerra del Perú*. https://www.gob.pe/institucion/marina/institucional

MIDIS. (2024). *Archivo digital del Ministerio de Desarrollo e Inclusión Social*. Presidencia del Consejo de Ministros. https://www.facebook.com/MidisPeru/?locale=es_LA

Ministerio de Defensa del Perú. (2018, 20 de marzo). El ejército presentó la Primera Brigada Multipropósito para desastres *[Comunicado de prensa*]. https://www.gob.pe/institucion/mindef/noticias/12294-ejercito-presento-primera-brigada-multiproposito-para-desastres

Ministerio de Defensa del Perú. (2023). *Política nacional de defensa 2023–2030.* https://www.gob.pe/mindef

Northrop Grumman-Sperry Marine. (2025). *Naval systems and integrated electronics*. https://www.sperrymarine.com

Pinto, G., Estrada, G. C. T., Mitma, J. I., & Mancesidor, J. M. G. (2022). Participación ciudadana y gestión pública en Lima, Perú. *Revista Venezolana de Gerencia*, 27(100), 1474-1488. https://doi.org/10.52080/rvg-luz.27.100.12

Pizarro, V. (2021). Participación de las FF. AA. del Perú en la emergencia sanitaria nacional por la Covid-19. *Revista de Ciencia e Investigación en Defensa*, 2(1), 6-19. https://doi.org/10.58211/recide.v2i1.49

Resolución Ministerial 1411-2016-DE-CCFFAA. (2016). *Nuevos roles estratégicos de las FF. AA*. Comando Conjunto de las Fuerzas Armadas del Perú.

Salas, S. (2020). Creación de un escuadrón aéreo especializado para evacuaciones aeromédicas en el Grupo Aéreo N° 8. *Revista Científica Ad Majorem Patriae Gloriam*, 3(3). http://revista.esfap.edu.pe/index.php/admajorem/article/view/19

SEMAN PERÚ. (2024). *Informe técnico y proyección operativa* 2024–2025. https://www.seman.com.pe

Sierra-Zamora, P., & Rueda-Serbousek, A. (2024). Logística humanitaria. En P. A. Sierra Zamora & J. C. Aristizábal Murillo (Eds.), *El Ejército Nacional de Colombia y la gestión de la logística humanitaria* (pp. 13-32). https://doi.org/10.21830/9786289620320.01

Sigueñas, O. (2021). Transformación del poderío aéreo peruano ante la pandemia de COVID-19: Ayuda humanitaria en el marco del Plan Tayta. *Revista Fuerza Aérea-EUA*, 3(1). https://www.airuniversity.af.edu/Portals/10/JOTA/Journals/Volume%203%20Issue%201/05-Siguenas_s.pdf

SIMA PERÚ. (2024). *Perfil corporativo y capacidades industriales*. https://www.sima.com.pe

Simon, W., Gómez, E., Baylón, A., & Ruiz, S. (2023). El impacto de la minería en el desarrollo económico y social de la región sur del Perú del 2007 al 2020. *Revista del Instituto de Investigación de la Facultad de Minas Metalurgia y Ciencias Geográficas,* 26(51), e25261. https://doi.org/10.15381/iigeo.v26i51.25261

Suárez-Alemán, A., & Domínguez, E. C. (2024). *Evidencia regional en el uso del mecanismo de iniciativas privadas para el desarrollo de infraestructura y mejores prácticas internacionales: Una revisión de la experiencia de Brasil, Chile, Colombia y Perú, y recomendaciones de política.* https://doi.org/10.18235/0012894

Tello Medina, D., Lozano Gracia, N., & Eraso Puig, B. (2020, 28 de octubre). ¿Cómo pueden los países apoyar el crecimiento y mejorar los niveles de vida en todas las regiones? *Banco Mundial.* https://blogs.worldbank.org/es/latinamerica/como-pueden-los-paises-apoyar-el-crecimiento-y-mejorar-los-niveles-de-vida-en-todas

Villafrádez, R., Suárez, J., & Méndez, É. (2022). ¿Qué tan competitivos son los países de la Alianza del Pacífico en infraestructura financiera, 2010-2019? *Hitos de Ciencias Económico Administrativas,* 28(82), 366-387. https://doi.org/10.19136/hitos.a28n82.5418

La actual agenda de seguridad internacional: De las amenazas convencionales a las amenazas híbridas en el contexto global

The Current International Security Agenda: From Conventional to Hybrid Threats in the Global Context

Recibido: 01/ 05 / 2025 | Revisado: 01 / 07 / 2025 | Aprobado: 11 / 09 / 2025
DOI: https://doi.org/10.59794/rscd.2025.v11i11.147

Licda. Soraya Zuinaga de Mazzei
Venezuela

Correo: szmazzei@gmail.com

Orcid: https://orcid.org/0000-0002-1342-9063

Afiliación: Instituto de Altos Estudios de Seguridad de la Nación

La autora es Licenciada en Estudios Internacionales, Universidad Central de Venezuela (UCV). Magister Scientiarum en Seguridad y Defensa Nacional (IAESEN); Curso de Gerencia Internacional de los Recursos para la Defensa. Instituto de Gerencia de Recursos para la Defensa. Escuela de Postgrado Naval, Monterrey, California, Estados Unidos de Norteamérica-IAEDEN; Curso de Ampliación "Prospectiva". Universidad Central de Venezuela. Facultad de Ciencias Económicas Sociales, Comisión de Estudios de Postgrado; Seminario "Sobre el equilibrio de los de los Poderes del Estado y el Respeto a las Garantías Democráticas con relación a la Lucha contra los Delitos de Terrorismo". Centro de Formación de la Cooperación Española en Cartagena de Indias (Colombia). Auspiciado por la Fiscalía del Gobierno Español. La Embajada del Reino de España en Colombia y La Agencia Española de Cooperación Internacional; Curso de Capacitación Docente en Educación Superior. Universidad José María Vargas; Diplomado Internacional en Estudios del Terrorismo, Universidad Pedagógica Experimental Libertador (UPEL), Asociación de Naciones Unidas en Venezuela (ANUV), Cátedra UNESCO, World Federation of United Nations y Catedra Libre "Dag Hammarskjold" Caracas, Venezuela; Seminario de Especialización en Derecho Internacional Humanitario. Tema Migratorio. Comité Internacional de la Cruz Roja en Venezuela Coordinadora Académica de la Maestría en Seguridad y Defensa Nacional, Jefe de la División de Investigación y Profesora Asociada en situación de jubilación del Instituto de Altos Estudios de Seguridad de la Nación "Gran Mariscal de Ayacucho Antonio José de Sucre" (IAESEN) Caracas, Venezuela. Investigadora por Venezuela en el Centro de Seguridad, Defensa y Asuntos Internacionales (CESDAI). Bogotá, Colombia 2011-2013. Coautora del Libro La Encrucijada de la Política Exterior y el Terrorismo (2012). Autora de artículos en revistas científicas "La nueva agenda de las relaciones internacionales en la posguerra fría", "El terrorismo una aproximación teórica en cuanto a su definición", "El enfoque de la geopolítica en el contexto de las relaciones internacionales del siglo XXI". Analista y asesora en temas de seguridad, estrategia, geopolítica y prospectiva. Académica Independiente.

Resumen

Este artículo analiza la actual agenda de seguridad internacional, enfocándose en la naturaleza de las amenazas híbridas, que trascienden la violencia militar convencional para incluir ciberataques, guerra psicológica, difusión masiva de noticias falsas y desinformación, facilitadas por las tecnologías de la información y la comunicación a nivel global. La investigación se basa en un enfoque cualitativo documental, mediante la revisión de textos, libros, prensa y revistas especializadas. Se concluye que, en un entorno de seguridad cada vez más complejo e incierto, es imprescindible desarrollar estrategias de respuesta coordinadas e inmediatas, abordando estas amenazas desde una perspectiva multidisciplinaria y no solo desde el ámbito policial o militar con el fin de proteger la estabilidad de las democracias y sus instituciones.

Palabras clave: Agenda, seguridad internacional, amenazas convencionales, amenazas híbridas y contexto global

Abstract

This article analyzes the current international security agenda, focusing on the nature of hybrid threats, which transcend conventional military violence to include cyberattacks, psychological warfare, mass dissemination of fake news and disinformation, facilitated by information and communication technologies at the global level. The research is based on a qualitative documentary approach, through the review of texts, books, press and specialized journals. It is concluded that, in an increasingly complex and uncertain security environment, it is essential to develop coordinated and immediate response strategies, addressing these threats from a multidisciplinary perspective and not only from the police or military field in order to protect the stability of democracies and their institutions.

Keywords: Agenda, international security, conventional threats, hybrid threats and global context

DOI: https://doi.org/10.59794/rscd.2025.v11i11.147

Introducción

Así como el concepto de Seguridad ha variado en el tiempo en cuanto a su enfoque, de igual modo las amenazas que surgen y la manera de afrontarlas han cambiado a través de la historia, es por ello que la arquitectura conformada de la Seguridad Internacional varía durante los períodos de la llamada Guerra Fría, luego de finalizada la Segunda Guerra Mundial en 1945; todo ello marcó una diferencia en cuanto a características y formas de acción, en comparación con la conceptualización de la Seguridad Internacional de la llamada Post Guerra Fría. Luego de la caída del muro de Berlín en 1989 y la disolución de la Unión Soviética, se genera una nueva concepción de seguridad.

Se establece un nuevo concepto, que tiene como antecedente los atentados terroristas de septiembre del 2001 en los Estados Unidos. Cabe destacar, que el escenario internacional de cada periodo antes mencionado, tuvo rasgos distintos y por ende el concepto de Seguridad fue interpretado bajo diferentes situaciones, visiones, percepciones y puntos de vista de por diferentes expertos, organismos internacionales y gobiernos, de acuerdo al escenario internacional del momento.

Durante el orden mundial bipolar que abarcó 1947 al 1991 donde dos actores principales personificaron un enfrentamiento junto a sus países satélites, las tesis de seguridad estaban enmarcadas, por un lado, por la Doctrina de Seguridad Nacional de los Estados Unidos y, por la otra, por la Doctrina Militar de Seguridad de la Unión de Repúblicas Socialistas Soviéticas (URSS), en ambas la amenaza principal fue la nuclear-militar representada por una inmensa rivalidad por el dominio de la superioridad atómica y el desarrollo de la carrera armamentística.

De este modo, las amenazas que implicaban el uso de la fuerza militar, así como la proliferación de misiles nucleares de corto, mediano y largo alcance eran lo más representativo de la Guerra Fría, donde la estrategia de guerra basada en la disuasión, configuró esa etapa; es por ello, luego del fin de la URSS y la independencia de todas sus repúblicas en 1991, todos estos conflictos latentes inmersos en ambos bloques de poder hicieron erupción luego de estar contenidos por cuarenta y cuatro (44) años convirtiéndose en una nueva fuente conflicto predominante que se proyectó en los años subsiguientes y que algunos de ellos se mantienen en actual desarrollo.

En consecuencia, luego del final de la Guerra Fría, el desmantelamiento gradual de ojivas retiradas por parte de Rusia y los Estados Unidos ha superado normalmente el ritmo de despliegue de nuevas ojivas, lo que ha dado lugar a una disminución global del inventario nuclear año tras año. Sin embargo, esta tendencia probablemente se revertirá en los próximos años, ya que el ritmo de desmantelamiento se está desacelerando, mientras que el despliegue de nuevas armas nucleares se está acelerando (Instituto Internacional para la Paz de Estocolmo [SIPRI] 2025).

Sin embargo, luego del fin de la confrontación ideológica-militar entre los Estados Unidos y la ex Unión Soviética en 1991, la diferenciación de las amenazas surgidas en la post Guerra Fría, alejaron a los Estados de las antiguas agendas militaristas para dar paso a nuevas realidades socioeconómicas, a las vulnerabilidades vinculadas con el medio ambiente y, en el caso de algunos países, de

su localización geográfica, con las asimetrías económicas, que generaban una infinidad de problemas fronterizos, con la fragilidad institucional de algunos gobiernos y con el surgimiento de actores no estatales ilegales, cada vez más contestatarios a la autoridad de los Estados (Rodríguez, 2007).

Todos estos cambios presentes en el Sistema Internacional desde 1991, indiscutiblemente abarcaron el tema de la Seguridad Internacional, con el impacto de la globalización como un fenómeno de repercusión automática, instantánea y de alcance mundial, que se dio en el ámbito de las actividades sociales, económicas y financieras y que se originó principalmente por la acción combinada de las tecnologías de la información y de las comunicaciones, surgiendo así la denominada sociedad de la información, de este modo se dio paso al surgimiento de una nueva visión de las amenazas y de la necesidad de una nueva arquitectura de la seguridad internacional.

En septiembre del 2001 después de los atentados terroristas en los Estados Unidos una de las características de las nuevas amenazas a la seguridad fue su naturaleza transnacional ya que poseían la capacidad de traspasar a un Estado, afectando a cualquier sociedad sin importar su origen, procedencia o distancia; lo que sucedería en cualquier lugar del mundo, podría afectar la seguridad en el conjunto de la Sociedad Internacional, convirtiéndose un evento de carácter particular en algo de tendencia global.

Esto tuvo como consecuencia, la Declaración sobre Seguridad en las Américas, aprobada el 28 de octubre de 2003 en el marco de la Conferencia Especial sobre Seguridad de la Organización de Estados Americanos (OEA) celebrada en Ciudad de México. En ella se reafirmó que la nueva concepción de la Seguridad en el hemisferio era de alcance multidimensional, incluyendo las amenazas tradicionales y las nuevas amenazas, incorporando las prioridades de cada Estado, como un valor compartido y enfoque común (Benegas, 2017).

En este sentido, de allí en adelante la nueva visión de la seguridad cambia, por ende, también el enfoque de las amenazas, ya que no solo se habla de amenazas convencionales o tradicionales, sino de amenazas emergentes, preocupaciones y desafíos de naturaleza diversa que impactan de manera negativa a la seguridad, incluyendo así al terrorismo internacional, el resurgimiento de nacionalismos, los fundamentalismos religiosos e ideológicos, las economías ilícitas trasnacionales (tráfico de armas, de drogas ilícitas, de seres humanos, de órganos, etc.), los problemas ambientales mundiales, los migraciones y refugiados, la escasez de recursos, la corrupción, la extrema pobreza, ataques a la seguridad cibernética, entre otros; de allí surge una nueva forma de categorizar a las amenazas, su abordaje y resolución, que no dependerán en adelante, de la perspectiva militar-policial, sino de una combinación de factores para su resolución.

En este nuevo escenario, se observa la apertura de conflictos de gran envergadura, la aparición de amenazas de tipo multidimensional, de actores de carácter difuso, signado por la variable de la incertidumbre y el dinamismo de los acontecimientos constituyó el espectro, la metodología y estrategia de la nueva visión de defensa que comienza a evolucionar para la contención dichas amenazas, es fundamental resaltar que el enfoque de seguridad multidimensional reconoce que las amenazas actuales no se limitan a lo militar o policial, sino que incluyen aspectos políticos, económicos, sociales, de salud y ambientales. Este

paradigma, consolidado en la Declaración de Seguridad de las Américas (OEA, 2003), plantea la necesidad de metodologías y estrategias adaptativas para enfrentar un entorno caracterizado por la incertidumbre y el dinamismo, manteniendo vigente la visión de seguridad multidimensional en la región (Ehrenfeld, 2023).

Desde el 2010 a la actualidad, las amenazas comienzan a presentarse de manera combinada y coordinadas, en este caso híbridas, a veces de manera imperceptible y hasta silente enmascaradas en acciones de tipo económica, política, tecnológica, informativa y hasta jurídicas, el ciberespacio se ha convertido en el escenario perfecto para el desarrollo de esta tipología de amenazas cuyo objetivo de los denominados ataques híbridos es casi siempre el mismo: influir en los diferentes mecanismos de toma de decisiones de la víctima (Estado u organización), ya sean decisiones a nivel local, estatal, nacional o institucional, para favorecer o alcanzar los objetivos estratégicos del atacante al tiempo que socava la credibilidad, la estabilidad o la moral de la víctima (Galán, 2018).

Este fenómeno de amenazas híbridas hace que el engaño, la manipulación y la desinformación se conviertan en un arma poderosa que coloca en riesgo el ejercicio de la democracia en cualquier país y es por ello que hacer frente a ellas o prevenirlas constituye una complejidad un gran reto desde el punto de vista de la defensa. Bajo este contexto, esta investigación coloca en perspectiva la actual agenda de seguridad internacional, que va desde la evolución de las amenazas convencionales o tradicionales a las amenazas de tipología híbridas presentes en el complejo escenario global y así analizar las características y alcance de dichas amenazas, como los mecanismos de defensa para hacerles frente por el riesgo a la seguridad actual de cualquier nación.

De este modo, el presente artículo se divide en tres (03) partes: en la primera se expone la evolución del concepto de seguridad y de las amenazas en las diferentes transiciones sufridas en el Sistema Internacional; en la segunda se examina la definición, características y tipologías de las amenazas híbridas, así como los mecanismos para enfrentarlas y en la tercera se presentan las conclusiones.

Desarrollo

La evolución del concepto de Seguridad y de las amenazas en la dinámica de los cambios del Sistema Internacional.

Desde la perspectiva de diferentes teorías que explican el comportamiento de los actores que hacen parte del Sistema Internacional, la conceptualización de la seguridad, así como su interpretación, ha sido marcada por distintos enfoques y paradigmas que explican en cierta forma el dinamismo de esos cambios, la primera de ellas y que destaca casi a mitad del s. XX fue la comprendida entre 1947 a 1989 como la denominada Guerra Fría.

En este importante periodo, prevaleció el enfoque de la teoría realista fundamentada por un lado por Hans Morgenthau, quien trató de contextualizar la relaciones conflictivas surgidas por el enfrentamiento Este-Oeste en el ámbito internacional bajo los términos de

la guerra y la paz y basada en las relaciones de poder, es por ello que consideraba que el elemento principal que permite al realismo político, encontrar un rumbo en el panorama de la política internacional es el concepto de interés definido en términos de poder, en este caso, el realismo plantea que los actores del sistema internacional constituído por los Estados, estarán en una lucha constante y permanente por el poder (Morgenthau, 1986).

Bajo esta premisa la teoría realista concibe al poder dentro del sistema internacional como una lucha por conseguirlo, permitiendo vislumbrar a los diferentes Estados del entorno mundial que tienen como objetivo inmediato su consecución de la búsqueda y lucha por el poder, es por ello que el conflicto entre los mismos se desarrollará de manera permanente y continua, en un mundo anárquico, sin presencia de un gobierno central que controle acciones y donde cada Estado es responsable de su soberanía y su propia supervivencia, donde le queda confiar, sólo en sí mismo, para protegerse de los demás.

Es por ello que la ontología realista, considera que las partes que conforman la realidad poseen una lógica de funcionamiento fundada en una serie de principios (poder, conflicto y dominación) provenientes de una naturaleza inherentemente antagónica y conflictiva que actúa haciendo caso omiso de la moral (Valencia & Morales, 2018).

En este escenario del realismo, la seguridad estatal se erige como el imperativo central para la supervivencia en un sistema internacional anárquico, donde la ausencia de una autoridad supranacional legitima se sustenta en la búsqueda constante del poder relativo. La incertidumbre estructural fomenta un clima de desconfianza sistémica entre actores, en el cual las alianzas se configuran como instrumentos tácticos y efímeros, subordinados a intereses coyunturales del momento. De este modo, el sistema internacional se caracteriza por un equilibrio de poder, que obliga a los Estados a desarrollar capacidades políticas, militares, diplomáticas y económicas robustas para mitigar amenazas externas e internas, preservar su facultad estratégica y evitar la subordinación frente a actores rivales.

Como lo explica Leal (2003) la Guerra Fría surgió de la bipolaridad política e ideológica en que resultó dividido el mundo al finalizar la Segunda Guerra Mundial y de la competencia de los dos bloques mundiales por el control estratégico de áreas geográficas importantes, por ello, la rápida invasión militar y sometimiento político de los países de la Europa Oriental por parte de la Unión Soviética en la fase final de esa guerra, aceleró la reacción de los Estados Unidos contra el comunismo acrecentando la conflictividad ideológica y la lucha firme por la obtención del poder en el escenario mundial.

En este caso, cada potencia desarrollo por su lado sus Doctrinas de Seguridad, que regirían al mundo en la Guerra Fría, Estados Unidos, en su doctrina de seguridad nacional, estuvo determinado desde su origen e influencia, por la estrategia de contención, que pretendía lograr una modificación de la conducta soviética por medio de una combinación de disuasiones y recompensas, es por ello que George Kennan, quien elaboró el concepto de contención luego de la Segunda Guerra Mundial, lo resumió así: "contención prolongada, paciente pero firme y vigilante de las tendencias expansivas rusas" (Deibel & Gaddis, 1992).

En cuanto a la Doctrina Militar de Seguridad Soviética fue un conjunto de ideas establecidas para un bloque de repúblicas que conformaban la URSS, válidas para un período de-

terminado y limitado, que se refirieron para el momento en la esencia, objetivos y naturaleza de una posible guerra futura, así como a la preparación continua para el adiestramiento y preparación de las Fuerzas Armadas Soviéticas en el campo de la guerra, mediante los medios establecidas por el Gobierno y el Partido Comunista Soviético como eje en su política de defensa.

De allí que la confrontación permanente de más de 40 años presente en el Sistema Internacional mediante el desarrollo armamentístico, la carrera nuclear con la realización de ensayos nucleares de ambas potencias y sus países satélites, representó una disputa por el poder, donde las amenazas a la seguridad eran de carácter ideológico y militar, premisas básicas en la articulación de una agenda de seguridad nacional, presente para cada bloque de poder.

De este modo, la Guerra Fría estuvo marcada por una confrontación estratégica prolongada entre dos bloques de poder que desplegaron una carrera armamentística y nuclear intensa, incluyendo múltiples ensayos nucleares. Esta rivalidad se fundamentó en amenazas de carácter ideológico y militar, que configuraron las agendas de seguridad nacional de ambos bloques, y que requirieron el desarrollo de estrategias de disuasión complejas para evitar un conflicto abierto (Cioffi-Revilla, 2024).

Es por ello que el poder nacional de los Estados era direccionado al desarrollo y capacidad del estamento militar. Por su parte, otra teoría válida, presente en este contexto, fue la neorrealista, siendo uno de sus máximos exponentes, Waltz Kenneth (1988), quien consideró el concepto de la autoayuda, mediante la cual la lucha por el poder en el Sistema Internacional, representaba un dilema de seguridad que viene dado en que, si un Estado realiza una determinada acción, el otro Estado o los demás Estados deberán tomar medidas para responder a dicha acción, es decir, entre mayores capacidades tenga un Estado para garantizar su seguridad mayor será la amenaza que representa para los demás Estados, promoviendo así, que estos últimos puedan adquirir capacidades similares que garanticen su seguridad y así poder responder a determinada acción (Cujabante, 2009).

En este sentido, la conflictividad típica de la Guerra Fría representó el desarrollo de amenazas de índole territorial, nuclear, militar e ideológica, donde la agenda de seguridad de los Estados giraba en torno a estos temas, basados en la interpretación de los enfoques teóricos realistas y neorrealistas, en los cuales, las amenazas giraban en torno a un enemigo externo.

Luego del fin de la Guerra Fría, se reconfigura el escenario mundial y con ello surgen nuevos paradigmas y visiones teóricas con el fin de entender la nueva realidad de la seguridad internacional y de las amenazas que, ante el mundo se hacían presentes, es innegable que con la aparición del fenómeno de la globalización se muestra una sociedad altamente interconectada, la revolución en el campo de las comunicaciones y la información posibilitó un acercamiento de las distancias y una aceleración del tiempo.

Indiscutiblemente, esta nueva dinámica presente en el ámbito internacional, denominada la era de la post Guerra Fría, con fecha de aparición en 1989, hizo que las agendas de seguridad de los países a nivel local, regional y mundial se reevaluaran y como muy bien lo proyectó el académico y profesor universitario Barry Buzan, como consecuencia de esa rapidez de avance, los conflictos futuros no tendrán mucho que ver con los presentes, por

lo que la estrategia militar se va a ver envuelta en una permanente revisión (Franco, 1998).

Esta sabia reflexión de Buzan parecía como una premonición ante los inciertos escenarios que se producirían luego de la caída del muro de Berlín y la implosión de la Unión Soviética en donde nuevos actores harían su irrupción, así como la manifestación de situaciones inesperadas de gran complejidad que permitirían el florecimiento de nuevas amenazas nunca ante previstas ni analizadas y que para solucionarlas no podrían implementarse solo medidas de carácter militar como en la época de la Guerra Fría.

Es así que para los nuevos análisis de la realidad internacional surgen teorías como la interdependencia compleja expuesta en los años 70 por Robert Keohane y Joseph Nye, la cual cobro vigencia en esta etapa de transición ya que colocan en perspectiva la existencia de una diversidad de actores en el escenario global, pasando de esta forma el papel protagónico del Estado a un segundo plano, donde la existencia de canales múltiples conectan a distintas sociedades en relaciones de tipo interestatal, transgubernamental y trasnacional y donde la fuerza militar no es empleada por los gobiernos para resolver los desacuerdos en materia económica con otros gobiernos que mantengan alianzas en bloque regionales, pero sí muy relevante para las relaciones políticas y militares de esa alianza con un bloque rival (Keohane & Nye, 1998).

En ese nuevo orden post Guerra Fría, surgen una multiplicidad de temas que van de lo social a lo ambiental: la globalización cambió con inusitada velocidad, las relaciones y estructuras del sistema internacional, con profundas implicaciones en el enfoque de la seguridad nacional de los Estados y por ende de la seguridad internacional, el dinamismo y la incertidumbre abrió paso a nuevas amenazas que un gran número de académicos y expertos han analizado a nivel global, no obstante estas tipologías de amenazas es muy probable que hayan estado presentes en lo interno de los Estados solo que en la época de la Guerra Fría predominó el tema militar e ideológico sobre todos lo demás.

Es por ello que la aceleración de la globalización ha transformado profundamente las relaciones internacionales y las estructuras del sistema global, generando un entorno caracterizado por riesgos transnacionales complejos y dinámicos, desde crisis climáticas y pandemias hasta ciberconflictos y migraciones masivas. Esta realidad obliga a los Estados a replantear sus enfoques de seguridad nacional, integrando dimensiones sociales, ambientales y tecnológicas, más allá de la tradicional perspectiva militar que predominó durante la Guerra Fría (Foro Económico Mundial, 2024).

Autores como Alvin Tofler, Zbigniew Brzezinski, Francis Fukuyama, Samuel Cohen entre otros tantos que analizaron y dieron sus perspectivas de como estaría configurado y reordenado el mundo luego del fin de la Guerra Fría, consideraron caso Fukuyama en su ensayo titulado ¿El Fin de la Historia?, que las ideas liberales habían triunfado de manera concluyente y que las guerras y revoluciones se daban por terminado (Fukuyama, 1992), algo muy alejado de la realidad en la post Guerra Fría.

En esta etapa los riesgos, desafíos y nuevas amenazas o amenazas emergentes a la seguridad toman otro significado y se convierten en el tema de la agenda principal de los países: el narcotráfico, el narcoterrorismo, la lucha por recursos escasos, catástrofes naturales y pandemias, el terrorismo internacional, la

migración descontrolada, el crimen organizado transnacional, la pobreza y la exclusión social, los nacionalismos, el cambio climático entre otros, lo importante de destacar de esa etapa en adelante, es su carácter global en un mundo en constante transformación, con la aparición de países emergentes caso Rusia, China, India, Turquía, Brasil, así como países del bloque de la Unión Europea (UE).

De esta forma, las nuevas amenazas o amenazas emergentes, muchas de ellas de origen local, que se producirían en el interior de un Estado, se constituirían en muchos casos, de ahora en adelante, en fuente de desestabilización general del sistema internacional y por tanto deberían ser gestionadas, tratadas y solucionadas de acuerdo a sus dimensiones de manera regional y hasta global. Un ejemplo de ello es el crimen organizado transnacional, que, por sus dimensiones, debe ser tratado de manera integral, entendiendo que viene determinado desde lo económico, jurídico, sociológico, político y policial, mediante un enfoque multidisciplinario y de acciones coordinadas en materia de seguridad e inteligencia, para así, hacer frente a este tipo de amenazas.

De este modo, la cooperación política y diplomática se pone de manifiesto en foros de carácter multilateral y organismos internacionales, así como bloques de integración para el logro de una solución consensuada frente a esta tipología de amenazas, en esta etapa los foros políticos se convierten en el centro de atención para el tratamiento de estas temáticas dejando en un segundo plano la estrategia militar, no obstante, estos mecanismos de posible resolución, no cumplen a veces con las expectativas para lo que fueron creadas, debido a la naturaleza y complejidad de la amenaza, que en algunos casos, tiene la capacidad de traspasar las fronteras estatales, de modo que todo aquello que sucede en alguna parte especifica del planeta puede afectar de una u otra forma a la seguridad del conjunto.

A continuación, se presenta en la tabla 1 los elementos conceptuales que integran la nueva arquitectura de seguridad luego del fin de la Guerra Fría.

Tabla 1
Elementos Conceptuales de la Arquitectura de la Seguridad post Guerra Fría

Elementos conceptuales	Descripción
Instituciones internacionales	Organismos como la ONU, Consejo de Seguridad, OEA, y otras organizaciones multilaterales que establecen normas y coordinan acciones para la paz y seguridad global.
Cooperación regional y subregional	Redes de colaboración entre países de una misma región para abordar amenazas comunes y fortalecer la estabilidad local. Surgimiento de nuevos esquemas y foros de integración regional.
Normativa en materia de seguridad	Conjuntos de reglas, tratados y acuerdos que regulan el uso de la fuerza, el control de armamentos, la no proliferación y la respuesta a amenazas transnacionales.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Elementos conceptuales	Descripción
Amenazas multidimensionales	Reconocimiento que la seguridad no solo es militar, sino que incluye amenazas terroristas, biológicas, cibernéticas, ambientales y sociales que requieren respuestas integradas. Surgimiento de una nueva tipología de amenazas.
Interdependencia compleja	La seguridad de un Estado o región está vinculada a factores políticos, económicos, sociales y tecnológicos globales, lo que ocurre en un lugar o zona geográfica puede impactar en otro, lo que exige enfoques coordinados y multilaterales.
Responsabilidad y control	Se enfatiza la responsabilidad del Estado en proteger a sus ciudadanos (seguridad humana) y el control cívico sobre las fuerzas armadas para evitar abusos y garantizar legitimidad.
Capacidad de respuesta	Mecanismos para anticipar, prevenir y responder a situaciones de emergencia y conflictos, incluyendo fuerzas de respuesta rápida, cooperación en el área de inteligencia y contrainteligencia policial y militar, manejo y gestión de crisis.

Nota: Elaboración propia en base al análisis del artículo de Cujabante, X. (2009).

Es por ello, que la nueva arquitectura de la seguridad internacional, luego de esta etapa post Guerra Fría, en la primera y segunda década del nuevo milenio, comienza a referirse a los conflictos y amenazas desde un punto de vista asimétrico. La tipología de amenazas en esta etapa refleja un cambio significativo respecto al periodo anterior, pasando de amenazas principalmente interestatales y militares a una diversidad de riesgos transnacionales y no tradicionales.

De acuerdo a Mejía (2017) estos nuevos riesgos o amenazas asimétricas de carácter no convencional tratan de explotar la vulnerabilidad de un país al tiempo de reducir su seguridad y tienen un denominador común que están dirigidos en algunos casos por actores no estatales de naturaleza difusa que pueden contar con el apoyo de Estados fallidos para atentar contra las instituciones de un país, sus infraestructuras, sus comunicaciones y sobre todo su población.

Indistintamente de cualquiera que sea la tipología de la amenaza, el fin de la misma es impactar de manera negativa la seguridad de cualquier Estado y actualmente algunas de ellas tienen aspectos poco visibles, en muchos casos, el ciberespacio ha contribuido a esto, sumado a la incertidumbre, el dinamismo, la conectividad y la complejidad del escenario internacional, esta situación llama a replantearse las agendas de seguridad de los Estados, tanto a nivel local como regional para enfrentarse a lo desconocido.

Es por ello que en esta nueva fase las amenazas a las organizaciones y gobiernos serán diferentes según Setec (2025), las organizaciones enfrentan amenazas que son cada vez más sofisticadas y duraderas. La expansión de la digitalización, la integración de entornos híbridos y el manejo intensivo de datos sensibles han ampliado considerablemente las posibles vías de ataque. Por ello, resulta fundamental que las organizaciones desarrollen habilidades para prever, identificar y reaccionar con rapidez ante estos incidentes, con el

fin de preservar la continuidad y estabilidad de sus operaciones en esta nueva etapa.

En la etapa de la post Guerra Fría, se produce una transformación de las amenazas a la seguridad, la complejidad de los conflictos es diferente, han cambiado de naturaleza y desde el inicio del nuevo milenio, deben ser tratados mediante un enfoque no solo particular, con enfoque multidimensional, sino en muchos casos. en forma conjunta o colectiva para su prevención, detección y respuesta, ya que cada día se habla del uso de la simetría y asimetría por parte de actores no estatales y hasta estatales, convirtiéndolos en una nueva tipología de amenazas con un poder más letal que las mismas amenazas de carácter militar de tipo convencional.

En la actualidad, con la invasión de Rusia a Ucrania en febrero de 2022 y el desarrollo del conflicto bélico entre ambas naciones, la confrontación de la Organización del Tratado del Atlántico Norte (OTAN), la Unión Europea (UE) contra Rusia, y el enfrentamiento continuo entre los Estados Unidos y China, estos actores se han acusado mutuamente de amenazas de carácter híbrido para el logro de sus objetivos ya sea en el campo de desarrollo militar, en la área comercial, diplomático o tecnológico, en todo caso habría que destacar cuales serían los argumentos que expone cada actor para indicar que están envueltos en una guerra híbrida.

En este escenario de enfrentamiento entre Moscú y Kiev, la guerra híbrida se presenta en conflictos actuales, combinando tácticas convencionales y no convencionales, utilizando medios militares, económicos, tecnológicos y diplomáticos simultáneamente. En el caso de la invasión rusa a Ucrania, se observa el uso de ciberataques, dependencia energética, y operaciones de influencia, en un escenario donde actores estatales y no estatales se acusan mutuamente de emplear amenazas híbridas para alcanzar objetivos estratégicos (Arré Duarte, 2025).

Las Amenazas Híbridas presentes en el Contexto Global

Es importante destacar que en los últimos años se ha dado un giro en el enfoque de la arquitectura de la Seguridad Internacional, desde organismos internacionales como la Organización de Naciones Unidas (ONU), Organización de Estados Americanos (OEA), hasta lo interno de los Estados en sus agendas de seguridad y defensa ya que se han visto en la necesidad de enfocarla de manera integral y reforzarlas desde los términos cívico-militar, de manera estratégica, mediante la colaboración interagencial, en inteligencia y contra inteligencia, desde el plano nacional e internacional, debido a la complejidad de las nuevas amenazas y del carácter híbrido de alguna de ellas.

De este modo, para la caracterización de lo híbrido, ante esto último, surgen una serie de interrogantes: ¿Qué es lo que se denomina actualmente una amenaza híbrida?, ¿Cuáles son sus características?, ¿Qué actores dentro del Sistema Internacional la aplican? y ¿Cuáles deberían ser las estrategias a implementar para neutralizar dichas amenazas?

Respondiendo a cada interrogante, tenemos primero que definir que es hibrido, el término latino hybrÍda llegó al castellano como híbrido, un adjetivo que puede usarse en diversos contextos. En el sentido más amplio, se califica como híbrido a aquello que presenta características o elementos de diferente naturaleza. Ahora bien que es una amenaza híbrida, en este caso lo "híbrido", ya sea en forma de guerra o de amenazas, es una idea originaria

del ámbito académico que fue popularizada por Frank G. Hoffman a mediados de la pasada década en su libro, Conflict in the 21th Century: The Raise of Hybrid Wars, el autor destaca la tendencia en los nuevos conflictos a la aparición de lo que denomina amenazas híbridas, esto es, adversarios capaces de emplear simultáneamente una amplia gama de formas de hacer la guerra.

Esta convergencia de diferentes modos estratégicos, de capacidades convencionales con tácticas irregulares, se puede complementar con el uso indiscriminado de la violencia y tener lugar en un escenario donde la distinción entre combatientes y no combatientes no está clara (Peco, 2017).

Hay otras consideraciones en cuanto a que el modelo híbrido hace referencia a una forma ambigua de confrontación, en que actores estatales o no estatales tienen la capacidad de combinar acciones militares convencionales y no convencionales con acciones no militares fundamentadas en una estrategia de desestabilización del adversario a través del uso de diferentes acciones disponibles que pueden ir desde lo diplomático, militar, económico, social y de información, por ello esta estrategia permite explotar las debilidades y vulnerabilidades de las sociedades occidentales en todos sus aspectos con el objetivo de influir en el direccionamiento político y en la opinión pública en general (Gutiérrez de León, 2020).

Otros autores señalan a las amenazas híbridas como un fenómeno resultante de la convergencia e interconexión de diferentes elementos que, en conjunto, constituyen una amenaza más compleja y multidimensional (Galán, 2018). De este modo, las amenazas híbridas se identifican con la conducta de aquellos actores que, en inferioridad de condiciones, no renuncian a ninguno de los medios disponibles con la finalidad de alcanzar los objetivos planteados ya sea mediante estrategias asimétricas que pueden ir desde la manipulación de la información, guerra psicológica, el engaño hasta el uso de armamento convencional.

Lo anterior tiene relación y refuerza las premisas planteadas por unos coroneles estrategas de la fuerza aérea China, quienes plantearon una nueva teoría en cuanto a la confrontación entre los Estados Unidos y China, que, de acuerdo a su percepción, va más allá del simple teatro de operaciones militares y afirman que el nuevo campo de batalla de la guerra va más allá de los límites y puede estar en todos los espacios naturales, basado este en el nuevo horizonte de finales del siglo XX, representado por el espacio tecnológico en rápido crecimiento. Bajo estas consideraciones, estos estrategas chinos vislumbraron un mundo en el que las amenazas sobrepasarían el ámbito estrictamente militar, en una era marcada por la globalización y los medios para enfrentarlas podrían estar presentes en cualquier espacio ya sea financiero, jurídico y tecnológico entre otros (Liang & Xiangsui, 1999).

Ahora bien, teniendo este antecedente que explica una visión para hacer frente la aparición de este tipo de amenazas en donde la República Popular China ha sido acusada de desplegar este tipo de actividades por parte de los Estados Unidos y otros países europeos, de igual modo, el gobierno de la República Popular China ha conferido acusaciones de presuntas amenazas híbridas, realizadas por el gobierno norteamericano, sin embargo, es importante destacar que uno de los pensadores y estratega chino Sun Tzu quien escribió

en China el primer tratado sobre el arte de la guerra y que inspiró a muchas figuras expertas en el tema, consideró como principio importante, que todo arte de la guerra debe estar basado en el engaño como premisa principal y quebrar la resistencia del enemigo sin luchar (Tzu, 2008).

Lo citado por el estratega militar Sun Tzu en cuanto a quebrar la resistencia del enemigo sin luchar o pelear, da para entender el uso de estrategias y medios distintos a los utilizados en una confrontación armada con el fin de confundir y desorientar, al contrario, estos métodos podrían considerarse como híbridos ya que es lograr la rendición del oponente sin la necesidad de una lucha armada. No obstante, hay otros expertos que conceptualizan las amenazas híbridas y la definición realizada por Frank Hoffman indica que son aquellas en que cualquier adversario, que de forma simultánea y adaptativa emplea una combinación fusionada de armas convencionales, tácticas irregulares, terrorismo, comportamiento delictivo (delincuencia organizada y cyber delincuencia) e información y desinformación en el espacio de batalla para obtener sus objetivos políticos (Álvarez, 2017).

Como bien lo expresa el autor anterior, dichos procesos de información, desinformación y propaganda contra el enemigo pueden ser ejercidas por distintas vías, por actores no estatales, por un país o coalición de países que ejecutan la amenaza híbrida, por ejemplo, planteando una guerra híbrida contra ese enemigo; lo que coinciden muchos autores que estudian la complejidad de esta amenaza, son ciertas características como la desinformación y manipulación de la realidad como una estrategia viable para impactar a un determinado auditorio, ya que se explotan los puntos débiles del objetivo, en este caso de una sociedad específica, y puede ser mediante el bombardeo de noticias falsas (fake news) a veces con el fin de crear confusión o polarizar sobre un tema o acción determinada a la población en general y donde las redes sociales y medios digitales pueden jugar un papel protagónico para tales fines.

La guerra híbrida utiliza tácticas de manipulación informativa y operaciones encubiertas en entornos digitales para desestabilizar sociedades, explotando las vulnerabilidades sociales y políticas mediante la difusión de desinformación y noticias falsas, dificultando su detección y respuesta (Maschmeyer, 2023).

En todo caso se habla de estas amenazas híbridas, como acciones que pueden usar métodos militares tradicionales o convencionales, combinados con ciberataques, operaciones de manipulación de la información, o elementos de presión económica, diplomática o política, con la finalidad de desestabilizar cualquier sistema de gobierno y a la vez lograr la polarización entre otras cosas de la opinión pública en general. Las amenazas híbridas persiguen un objetivo claro, conseguir ventaja y éxito, sin recurrir a un enfrentamiento bélico, de allí, que hay autores que también lo denominan ataques híbridos, ya que diluyen los límites entre guerra y paz.

De este modo, se utilizan una serie de tácticas y acciones para explotar las oportunidades que brinda un mundo interconectado y globalizado, y así debilitar al adversario sin desgastarse en el terreno convencional (Colom Piella, 2018). Seguidamente se presenta la tabla 2 explicativo de las diferencias entre amenazas convencionales e híbridas.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Tabla 2

Diferencias entre las amenazas convencionales y las amenazas híbridas

Aspecto que considerar	Amenazas Convencionales	Amenazas Hibridas
Definición	Conflictos militares tradicionales con uso abierto de fuerzas armadas, armas convencionales y enfrentamientos directos.	Ataques complejos y coordinados que combinan métodos digitales (ciberataques, desinformación) y físicos (sabotaje, espionaje), operando en la «zona gris» donde es difícil identificar al agresor y se debate en la frágil línea entre la guerra y la paz.
Métodos y tácticas	Uso directo de fuerzas militares, maniobras tácticas y estratégicas con armamento convencional y guerra abierta.	Uso simultáneo de ciberataques, guerra de desinformación, sabotaje físico, espionaje, operaciones encubiertas, guerra política y económica, propaganda y utilización de medios y plataformas digitales.
Objetivo principal	Derrotar militarmente al adversario, controlar territorio y lograr objetivos militares claros y declarados	Desestabilizar sociedades, influir en la opinión pública, explotar vulnerabilidades sistémicas y dificultar la toma de decisiones políticas, erosión de las instituciones democráticas.
Naturaleza del conflicto	Se refiere a enfrentamientos armados que siguen patrones, reglas y tácticas tradicionales entre fuerzas militares claramente definidas, con enfrentamientos abiertos y reconocimiento explícito del estado de guerra.	Ambigua, con “negación plausible” que es la capacidad de negar algo de forma que otros consideren esa negación como posible o creíble, aunque en realidad se haya estado involucrada o tenga conocimiento del hecho, difícil atribución y operación bajo el umbral de la guerra declarada
Ámbito de acción de la amenaza	Principalmente militar, con operaciones y uso de armamento bélico en tierra, mar y aire, con objetivos militares claros, en escenarios físicos claramente delimitados, contra centros de poder económico y político, infraestructuras críticas e instalaciones militares	Multidominio: digital, político, económico, social, militar y mediático.

Aspecto que considerar	Amenazas Convencionales	Amenazas Hibridas
Actores ejecutantes de la acción	Son principalmente las fuerzas militares oficiales de un Estado, es decir, los ejércitos regulares y las fuerzas de seguridad establecidas por un gobierno, con una estructura jerárquica formal y una cadena de mando claramente definida.	Son diversos y combinan tanto elementos estatales como no estatales que operan de manera coordinada para explotar vulnerabilidades específicas del adversario.
Impacto en la sociedad	Impacto directo y visible en el campo de batalla y en las zonas de conflicto.	Busca generar caos controlado, desestabilización política, social y económica, erosionando la confianza en instituciones y el orden democrático.

Nota: Elaboración propia en base al análisis de los artículos de Maschmeyer, L. (2023) y Colom Piella, G. (2018, junio).

Lo anterior explica a lo que se refiere la amenaza convencional y la híbrida, su diferencia radica principalmente en su naturaleza, ámbito de acción, objetivos, actores involucrados y cómo impacta finalmente en un auditorio muy importante como lo es la sociedad. En cuanto a los casos de actores que aplican la amenaza híbrida como estrategia o táctica principal para el logro de sus objetivos se encuentran actores estatales y no estatales, entre los actores estatales se podrían señalar casos particulares como el del gobierno ruso que ha sido señalado por varios países entre ellos los Estados Unidos y Europa de aplicar estrategias híbridas por ejemplo en el caso específico de Ucrania y la adhesión de Crimea por parte de la Federación Rusa en 2014 y como logró ganar el referéndum que se realizó para declarar la independencia de esta, de acuerdo a Martin (2022) con la ocupación de Crimea y la crisis de Ucrania en 2014 y 2015, luego que Viktor Yanukovych abandonara el poder en ese país, poniendo en evidencia que una nueva forma de guerra se había materializado.

Basado en este tipo de acciones en la cual ha sido señalada en reiteradas oportunidades la Federación Rusa durante los sucesos en Ucrania en el 2014, quedaron identificadas por un gran número de expertos en temas de análisis en seguridad y defensa con el nombre de guerra híbrida, debido a la combinación del empleo de estrategias militares no convencionales, con operaciones hostiles de inteligencia, información, desinformación a la población como a las tropas militares ucranianas, comunicación o amenazas y presiones políticas que entraban en el terreno de una guerra psicológica de amplio alcance.

Dentro de este orden de ideas, China también ha sido señalada por sus adversarios sobre todo los Estados Unidos como un país que utiliza acciones consideradas de tipo híbridas en cuanto a su penetración tecnológica y su agresiva avanzada comercial en todo el mundo, un elemento emblemático de ello es el caso entre Huawei, empresa tecnológica multinacional china y el primer gobierno presidido por Donald Trump en los Estados Unidos, que desató una crisis que culminó con la detención de su directora ejecutiva Meng Wanzhou en Canadá el 1 de diciembre de 2018, siguiendo una orden internacional

emitida por Estados Unidos bajo la acusación de haber violado las sanciones contra Irán, permitiéndole el acceso al sistema financiero basado en el dólar, mediante dos firmas pantalla; igualmente se acusó a esa compañía telefónica, de efectuar una trama de conspiración para cometer fraude y robo de secretos tecnológicos de empresas estadounidenses.

Además, altos funcionarios estadounidenses sostuvieron que la empresa representaba una amenaza para la seguridad nacional, ya que su tecnología podría ser una puerta para el espionaje a gran escala (Deutsche Welle, 2021). Por su parte la empresa y el gobierno chino acusaron al gobierno de los Estados Unidos representado por Donald Trump de presiones, debido al dominio de Huawei sobre la tecnología 5G a un bajo costo, algo que, según funcionarios chinos, no manejan las empresas norteamericanas, el gobierno de Beijing acusó a los Estados Unidos de cometer imposiciones y amenazas de carácter híbrido en este caso particular.

Dentro de este orden de ideas, es importante destacar que las acciones realizadas por actores no estatales del terrorismo internacional, caso Estado Islámico, Al Qaeda y otros grupos terroristas de nuevo surgimiento siguen estas mismas tácticas, consideradas de tipología híbrida, ya que han utilizado para sus acciones elementos de guerra convencional mezcladas con tácticas y adoctrinamiento mediante audios, videos y a su vez en su momento mantuvieron una campaña de información y desinformación a través de redes sociales. Es por ello, que los actores que se mueven en el umbral hibrido, desdibujan las fronteras habituales de la política internacional y operan en las interfaces entre lo externo y lo interno, lo legal y lo ilegal, la paz y la guerra (Obdola, 2022).

En vista de todos estos antecedentes y argumentos, se dio respuesta en su momento a las inquietudes planteadas en la Agenda Europea de Seguridad de la Comisión en la EU en 2015, con el fin de contrarrestar las amenazas híbridas. En este sentido, en noviembre de 2017 se creó el Centro Europeo de Excelencia Contra las Amenazas Híbridas (CoE Híbrido) inaugurado en la capital de Finlandia, Helsinki con la finalidad de reforzar cooperación entre la UE y la OTAN, en la elaboración y coordinación de metodologías para prevenir, combatir y mitigar el creciente desafío de las amenazas híbridas y de este modo organizar entrenamientos para incrementar la capacidad de reaccionar de los Estados ante dichas amenazas.

El Centro cuenta con alrededor de cuarenta (40) analistas pertenecientes a los 36 países participantes en estrecha colaboración de la UE y la OTAN, su actual directora es la finlandesa Teija Tiilikainen, dicho Centro define en su página web las amenazas híbridas como "una acción llevada a cabo por actores estatales o no estatales, cuyo objetivo es socavar o dañar un objetivo mediante la combinación de medios militares y no militares abiertos y encubiertos" (Hybrid CoE, 2025).

No obstante, según Gardner (2023) explica que este fenómeno híbrido consiste en un formato de amenaza muy ambiguo, contra el que las naciones les resulta muy difícil a veces identificarlos, luchar y protegerse de ellos, según su criterio, existen numerosas formas de que un Estado perjudique a otro sin recurrir a la acción militar directa y en algunos casos, la utilización de medios convencionales y acciones híbridas en conjunto para el logro de los objetivos que se deseen alcanzar. Por tal razón, en el manual elaborado por el CoE Híbrido en el que se describen las amenazas marítimas híbridas y que contiene 10

escenarios imaginarios pero muy probables, se incluyen, desde el empleo clandestino de armas submarinas hasta la proclamación de una zona de control alrededor de una isla, así como el bloqueo de estrechos.

Esto nos indica que los países en conjunto, están tomando medidas para hacer frente y monitorear este tipo de amenazas de difícil apreciación o percepción, ubicándose, en el umbral de lo legal, basadas en muchos casos, en actuaciones encubiertas y clandestinas. Sin duda las amenazas híbridas aplican en el umbral del actual conflicto bélico entre Rusia y Ucrania, producto de la invasión rusa al este de territorio ucraniano mediante la denominada operación especial de febrero de 2022, todo ello combinó el empleo de estrategias y tácticas militares no convencionales, con operaciones hostiles de desinformación, inteligencia, contrainteligencia, presiones políticas, en el marco de una guerra psicológica, junto a medios convencionales presentes en una contienda militar a gran escala.

En este caso, para comprender la realidad de la permanente crisis entre Ucrania y Rusia, enmarcada en un contexto histórico a lo largo de los últimos años, se debe analizar primero desde el concepto de "guerra híbrida". De acuerdo a esta valoración, Rusia interviene en Ucrania mediante dos tipos de fuerzas: por un lado, a través de los grupos armados no convencionales (el servicio de espionaje) y, por el otro, a través de las fuerzas militares (Valle, 2022).

Por su parte, como expone Macedo (2022), desde al punto de vista de la diplomacia rusa representada por el canciller Serguéi Lavrov quien dejó entrever, posterior a la serie de sanciones impuesta por Occidente a la administración del Kremlin, luego del inicio de la ofensiva contra Ucrania, expresó categóricamente que su país se le ha declarado una guerra híbrida donde muchos políticos europeos tienen el objetivo de quebrar y asfixiar la economía rusa y a la nación en forma general. Lo anterior explica como las grandes potencias que se debaten en un escenario internacional anárquico, en el cual cada uno de ellos quiere hacer prevalecer sus reglas y no el respeto al Derecho Internacional dentro de ese complejo juego de supremacía mundial, están familiarizados con el uso del término de guerra o amenaza híbrida.

Conclusiones

Indiscutiblemente el mundo se presenta en la actualidad, en un constante cambio, a cada segundo, esas transformaciones han producido un nuevo entorno para el desarrollo de conflictos, de características sui generis con una amplia complejidad, donde el concepto de seguridad debe ser continuamente revisado y replanteado desde la perspectiva local, regional y global, en este caso la experiencia del periodo de la Guerra Fría generó un sistema que contuvo los problemas, en lugar de resolverlos, que reprimió una serie de amenazas bajo el halo de lo militar e ideológico, lo cual marcó un antes y un después en la manera de comprender y analizar la tipología de los conflictos y de sus amenazas derivadas que aun en este tiempo presente tienen consecuencias.

Sansó y Pascal (2017) sustentan que ante los nuevos retos y desafíos que en el ámbito de la seguridad y defensa se deben reclamar en el contexto de nuevas respuestas; pretender combatir la nuevas amenazas de carácter híbrido, con esquemas de seguridad del siglo XX, resulta totalmente inoperante, la discu-

sión y toma de decisiones debería girar en torno a qué estrategias deben establecerse para hacer frente a fenómenos complejos como los aquí analizados, enfocados desde una perspectiva multidisciplinaria y no solo desde lo policial o militar, ya que el objetivo de estas novedosas amenazas híbridas es fragmentar, confundir las sociedades y ponerlas al frente de sus propias dudas y contradicciones con la finalidad de erosionar las democracias, sistemas e instituciones, con el agravante de no ser fácilmente perceptibles, actuando en la clandestinidad o el anonimato, apoyado en algunos casos en la era digital.

Es importante hacer mención, que los Estados rivales utilizan cada vez más tácticas híbridas para explotar las vulnerabilidades e influir en los procesos democráticos, dichas tácticas incluyen el uso coordinado y sincronizado de instrumentos de poder violentos y no violentos para ejecutar actividades entre dominios, a menudo eludiendo la detección y la atribución, que se llevan a cabo por debajo del umbral del conflicto militar armado convencional (Bertolini et al., 2023).

Igualmente, el tema de la cooperación internacional en materia de seguridad, defensa, inteligencia y contrainteligencia debería asumir un papel relevante frente a este tipo de amenazas, los Colegios de Defensa a nivel internacional con el importante capital humano y trabajos de investigación que poseen, podrían ser los llamados a la construcción una estrategia macro en seguridad que abarque varias aristas, junto a decisiones que no sean solo de carácter político, para convertirse en un complejo de ciberseguridad para empresas, organizaciones y gobiernos, en una sociedad que hoy en día se hace más global, móvil y digital agregando la aparición de la Inteligencia Artificial (IA) como telón de fondo, donde, igualmente, se necesita proteger la información para evitar ataques, como robo o manipulación de información y datos con fines no deseados, pero esto debe ir más allá y tomar como ejemplo, el trabajo del Centro Europeo de Excelencia Contra las Amenazas Híbridas (CoE Híbrido) podría replicarse en varias partes del mundo, con la finalidad de elaborar análisis y seguimiento a este tipo de amenazas, que cada vez son más imperceptible y más peligrosas en el ataque a las democracias y al estado de derecho.

El fenómeno de la globalización y la creciente interdependencia geopolítica han configurado una tendencia hacia una seguridad multidimensional e interfactorial, caracterizada en muchos casos por la multilateralidad. Estos factores contribuyen a la creación de un entorno de seguridad cada vez más complejo, donde los escenarios son difíciles de prever. En este contexto, el ámbito de operaciones de un conflicto bélico trasciende el territorio de un Estado específico, extendiéndose hacia espacios como el ciberespacio y las redes de comunicación, tal como se observa en los nuevos conflictos o amenazas híbridas.

Referencias

Álvarez, J. (2017). *La guerra híbrida: ¿Un nuevo concepto*? http://forodeanalisis.org/la-guerra-híbrida-un-nuevo-concepto/

Arré Duarte, G. (2025). Guerra híbrida y amenazas: Hechos y tendencias. *Escenarios Actuales*, *30*(1), 35–52. *Centro de Estudios*

e Investigaciones Militares. https://www.cesim.cl/wp-content/uploads/2025/06/ESCENARIOS-ACTUALES-N1-2025.pdf

Benegas, A. (2017). ¿Existen estrategias para combatir las amenazas multidimensionales en la región? *Revista Política y Estrategia, 129*, 89–120. https://www.politicayestrategia.cl/index.php/rpye/article/view/72/112

Bertolini, M., Minicozzi, R., & Sweijs, T. (2023). *Ten guidelines for dealing with hybrid threats: A policy response framewor*k. The Hague Centre for Strategic Studies. https://hcss.nl/wp-content/uploads/2023/04/Guidelines-for-the-Deterrence-of-Hybrid-Threats-HCSS-2023.pdf

Cioffi-Revilla, C. (2024). *Deterrence among three to twelve nuclear powers: Fundamental instability and mitigation strategy.* https://nsiteam.com/social/wp-content/uploads/2024/05/2024-05-09-Cioffi-SMA-SDF-Multi-Actor-Deterrence-final4.pdf

Colom Piella, G. (2018, junio). Guerras híbridas: Cuando el contexto lo es todo. *Ejército de Tierra Español, 927*, 38–44.

Cujabante, X. (2009). La seguridad internacional: Evolución de un concepto. *Revista de Relaciones Internacionales, Estrategia y Seguridad, 4*(2), 93–106. http://www.redalyc.org/articulo.oa?id=92712972007 https://www.oas.org/36ag/espanol/doc_referencia/DeclaracionMexico_Seguridad.pdf

Deibel, T., & Gaddis, J. (1992). *La contención: Concepto y política.* Grupo Editor Latinoamericano.

Ehrenfeld, E. (2023). Revisitar el enfoque de seguridad multidimensional postpandemia a veinte años de su declaración: Estudio comparativo de Argentina, Chile y Colombia. *Revista de Relaciones Internacionales, Estrategia y Seguridad, 18*(2), 73–89. https://www.redalyc.org/journal/927/92778943006/html/

EE. UU. declara Huawei una amenaza para su seguridad. (2021, 13 de marzo). *Deutsche Welle.* https://www.dw.com/es/eeuu-declara-a-huawei-una-amenaza-para-su-seguridad/a-56860457

Foro Económico Mundial. (2024, 7 de junio). 9 cambios que afectan la seguridad nacional y la cooperación económica. https://www.weforum.org

Franco, J. (1998). *Barry Buzan: Introducción a los estudios estratégicos, tecnología militar y relaciones internacionales.* https://dialnet.unirioja.es/descarga/articulo/4553585.pdf

Fukuyama, F. (1992). *El fin de la historia y el último hombre.* Editorial Planeta.

Galán, C. (2018). Amenazas híbridas: Nuevas herramientas para viejas aspiraciones. *Real Instituto Elcano.* http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido ?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/dt20-2018-galan-amenazas-híbridas-nuevas-herramientas-para-viejas-aspiraciones

Gardner, F. (2023, 14 de febrero). Qué es el centro de amenazas modernas de Finlandia que estudia los ataques híbridos que enfrenta Occidente. *BBC Mundo.* https://www.bbc.com/mundo/noticias-internacional-64592466

Gutiérrez de León, B. (2020). Amenaza híbrida, la guerra imprevisible. En Curso Internacional de Defensa (Ed.), *El concepto de lo híbrido: De las estrategias híbridas a la zona gris* (pp. 29–34). Ministerio de la Defensa.

Instituto Internacional de Investigación para la Paz de Estocolmo (SIPRI). (2025). *Aumentan los riesgos nucleares ante una nueva carrera armamentista.* https://www.sipri.org/sites/default/files/WNF%202025%20PR%20ESP.pdf

Keohane, R., & Nye, J. (1998). *Poder e interdependencia.* Grupo Editor Latinoamericano.

Leal, F. (2003). La doctrina de seguridad nacional: Materialización de la Guerra Fría en América del Sur. *Revista de Estudios Sociales, 74*–87.

Liang, Q., & Xiangsui, W. (1999). *Guerra irrestricta.* PLA Literature and Arts Publishing House.

Macedo, G. (2022, 26 de marzo). Guerra híbrida: ¿Qué es y qué relación tiene con el conflicto Ucrania–Rusia? *El Periódico.* https://www.elperiodico.com/es/internacional/20220326/guerra-híbrida-que-es-rusia-ucrania-13435046

Maschmeyer, L. (2023). Assessing hybrid war: Separating fact from fiction. *Center for Security Studies, ETH Zürich.* https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse332-EN.pdf

Martin, L. (2022, 24 de enero). La guerra híbrida, un reto para Occidente. *Atalayar.* https://www.atalayar.com/articulo/politica/guerra-híbrida-reto-occidente/20220124163129154781.html

Mejía, S. (2017, 26 de noviembre). Las amenazas asimétricas convencionales. *Diario La Prensa / Opinión.* https://www.prensa.com/opinion/amenazas-asimetricas-internacionales_0_4903009716.html

Morgenthau, H. (1986). *Política entre naciones: La lucha por el poder y por la paz.* Grupo Editor Latinoamericano.

Obdola, J. (2022, 6 de mayo). Terrorismo híbrido. *Jornadas de Geopolítica y Seguridad, Universidad Isabel I.* https://www.ui1.es/sala-de-prensa/johan-obdola-sera-necesario-cambiar-el-escenario-de-la-geopolitica-mundial-y-las

Organización de Estados Americanos (OEA). (2003). *Declaración sobre Seguridad en las Américas.* https://www.oas.org/36ag/espanol/doc_referencia/DeclaracionMexico_Seguridad.pdf

Peco, M. (2017). La persistencia de lo híbrido como expresión de vulnerabilidad: Un análisis retrospectivo e implicaciones para la seguridad internacional. *Revista UNISCI / UNISCI Journal, 44.* http://dx.doi.org/10.5209/RUNI.55777

Rodríguez, G. (2007). Antiguas y nuevas amenazas a la seguridad de América Latina. *Revista Bien Común, 1*(152), 15–18.

Sansó, D., & Pascual, R. (2017). *Democracias bajo presión: Estado, fuerzas armadas y crimen organizado en América Latina: ¿Éxito o fracaso de la estrategia de contención militar?* Dykinson.

Satec. (2025, 8 de abril). Ciberseguridad en 2025: Amenazas y soluciones más relevantes para empresas. https://www.satec.es/es/blog/ciberseguridad-en-2025-amenazas-y-soluciones-clave/

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). (2025). *Hybrid threats.* https://www.hybridcoe.fi/hybrid-threats/

Tzu, S. (2008). *El arte de la guerra.* Editorial Porrúa.

Valle, J. (2022). El conflicto en Ucrania: Guerra híbrida e intervención militar convencional. *Revista Seguridad y Poder Terrestre, 1,* 61–76. https://revistas.ceeep.mil.pe/index.php/seguridad-y-poder-terrestre/article/view/7/12

Valencia, A., & Morales, D. (2018). El poder nacional-internacional de los Estados: Una propuesta transestructural. *Revista de Estudios sobre Espacio y Poder,* 137–169. http://dx.doi.org/10.5209/GEOP.57778

Waltz, K. (1988). *Teoría de la política internacional.* Grupo Editor Latinoamericano.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Nuevas amenazas a la seguridad humana en el siglo XXI: Aproximaciones multidimensionales y perspectivas latinoamericanas

New Threats to Human Security in the 21st Century: Multidimensional Approaches and Latin American Perspectives

Recibido: 01/ 05 / 2025 | Revisado: 10 / 09 / 2025 | Aprobado: 16 / 09 / 2025
DOI: https://doi.org/10.59794/rscd.2025.v11i11.148

Dr. Alexis José Colmenares-Zapata
Ecuador

Correo: alexis.colmenares@iaen.edu.ec

ORCID: http://orcid.org/0000-0001-8857-9923

Afiliación: Instituto de Altos Estudios Nacionales

El autor es Doctor en Estudios Internacionales por FLACSO-Ecuador y Magíster en Relaciones Internacionales y Diplomacia por el Instituto de Altos Estudios Nacionales – IAEN. Además, cuenta con especializaciones de posgrado en Derecho y Política Internacional (Universidad Central de Venezuela) y en Prospectiva Estratégica (Universidad de Ciencias Empresariales y Sociales, Argentina). Actualmente se desempeña como docente- investigador en la Escuela de Relaciones Internacionales del IAEN, donde coordina programas de la maestría en Relaciones Internacionales y Diplomacia en sus dos menciones: Política Exterior y Movilidad Humana. Sus líneas de investigación se centran en los estudios de futuro, la prospectiva estratégica, la seguridad humana y la gobernanza global, con especial interés en el análisis de escenarios y el impacto de los riesgos globales sobre las estructuras del Estado y las relaciones internacionales. Con más de dos décadas de experiencia profesional, Colmenares ha ejercido funciones como planificador, diplomático de carrera, negociador, asesor y docente universitario. En el ámbito académico, ha sido profesor visitante en FLACSO-Ecuador y en la Universidad San Francisco de Quito, impartiendo cursos sobre teoría de las relaciones internacionales, seguridad humana, resolución de conflictos y estudios de paz, entre otros temas. Su trayectoria investigativa se refleja en múltiples publicaciones arbitradas. Su tesis doctoral, titulada "Difusión del enfoque de seguridad humana: Costa Rica y Ecuador (2001–2016)", fue publicada como libro en 2021 bajo el título La seguridad humana en Costa Rica y Ecuador: los debates y la difusión. Asimismo, ha difundido sus hallazgos en revistas especializadas de la región, incluyendo artículos sobre la adopción del enfoque de seguridad humana en Ecuador y Costa Rica, contribuyendo al debate académico internacional en torno a la seguridad humana.

DOI: https://doi.org/10.59794/rscd.2025.v11i11.148

Resumen

El presente artículo analiza las nuevas amenazas a la seguridad humana en el siglo XXI desde un enfoque multidimensional, con énfasis en el caso de Ecuador y su contexto latinoamericano. A partir de un estudio cualitativo de tipo documental, se identifican cinco amenazas prioritarias que inciden de manera sinérgica en las dimensiones económica, social, política y ambiental del bienestar: crimen organizado transnacional, crisis climática, migraciones forzadas, riesgos cibernéticos y pandemias. El objetivo general es analizar estas amenazas desde la perspectiva de la seguridad humana, y como objetivos específicos se plantea: (1) examinar la evolución conceptual de la seguridad humana y su pertinencia regional; (2) identificar las principales amenazas contemporáneas que enfrenta Ecuador; (3) analizar sus impactos multidimensionales; y (4) evaluar las respuestas institucionales y de cooperación internacional. El caso de Guayaquil se presenta como ilustración empírica de una crisis compleja. El análisis revela cómo estas amenazas desbordan los marcos tradicionales de seguridad centrados en el Estado y demandan respuestas integrales orientadas a la protección de las personas. En este contexto, se discuten las tensiones entre el paradigma securitizado y el enfoque de seguridad humana, proponiendo a este último como una alternativa más eficaz, inclusiva y sostenible para el diseño de políticas públicas.

Palabras clave: Seguridad humana, amenazas contemporáneas, enfoque multidimensional, Ecuador, cooperación internacional

Abstract

This article analyzes the new threats to human security in the 21st century from a multidimensional perspective, with a focus on Ecuador and its Latin American context. Based on a qualitative documentary study, five priority threats are identified that synergistically impact the economic, social, political, and environmental dimensions of well-being: transnational organized crime, climate crisis, forced migration, cyber risks, and pandemics. The general objective is to analyze these threats from a human security perspective, with the following specific objectives: (1) examine the conceptual evolution of human security and its regional relevance; (2) identify the main contemporary threats faced by Ecuador; (3) analyze their multidimensional impacts; and (4) assess institutional and international cooperation responses. The case of Guayaquil is presented as an empirical illustration of a complex crisis. The analysis reveals how these threats transcend traditional state-centered security frameworks and demand comprehensive responses focused on the protection of individuals. In this context, the article discusses the tensions between the securitized paradigm and the human security approach, proposing the latter as a more effective, inclusive, and sustainable alternative for public policy design.

Keywords: Human security, contemporary threats, multidimensional approach, Ecuador, international cooperation

Introducción

El siglo XXI ha transformado las nociones tradicionales de seguridad. El paradigma centrado en la defensa estatal frente a amenazas militares ha cedido progresivamente ante enfoques centrados en las personas, sus derechos y condiciones de vida. Esta transformación no obedece únicamente a un ajuste terminológico, sino a la necesidad urgente de respuestas más integrales ante amenazas complejas. La seguridad humana, formulada por el Programa de las Naciones Unidas para el Desarrollo (en adelante PNUD) (1994), propone una mirada multidimensional anclada en la prevención, la dignidad y la agencia de los individuos y comunidades, que enfatiza la protección integral de las personas ante amenazas múltiples y simultáneas.

En América Latina, y especialmente en Ecuador, estas amenazas se entrecruzan con violencia estructural, exclusión social y debilitamiento institucional, configurando entornos de inseguridad persistente (Sanahuja & Mila-Maldonado, 2024). Con una tasa de homicidios de 38,8 por cada 100.000 habitantes en 2024, Ecuador se ha convertido en el país más violento de la región (El País, 2025; InSight Crime, 2025), lo que evidencia el agotamiento del enfoque securitario clásico.

Este estudio propone analizar estas amenazas desde una perspectiva multidimensional, evaluando su impacto en las dimensiones económica, social, política y ambiental, así como las respuestas institucionales desplegadas. Desde esta perspectiva, el objetivo general de este estudio es analizar las nuevas amenazas a la seguridad humana en Ecuador desde un enfoque multidimensional. Se plantean cuatro objetivos específicos: (1) examinar la evolución conceptual de la seguridad humana y su aplicabilidad en América Latina; (2) identificar las principales amenazas contemporáneas que enfrenta el país; (3) analizar los impactos de estas amenazas en las dimensiones económica, social, política y ambiental; y (4) evaluar las respuestas institucionales y los mecanismos de cooperación internacional orientados a enfrentar estos desafíos.

Metodológicamente, se trata de una investigación cualitativa sustentada en una revisión documental sistemática de fuentes secundarias publicadas entre 2015 y 2025. El artículo se estructura en seis secciones: marco teórico, metodología, análisis de amenazas, discusión sobre políticas públicas, y conclusiones con recomendaciones estratégicas.

Desarrollo

Fundamentos conceptuales y relevancia actual de la seguridad humana

Comprender las nuevas amenazas a la seguridad humana en América Latina exige revisar críticamente los pilares conceptuales, la evolución histórica del enfoque y su resignificación en contextos específicos. La noción de seguridad humana surge como respuesta a las limitaciones del paradigma clásico centrado en el Estado y la defensa militar, enfo-

cado exclusivamente en amenazas externas y conflictos armados, insuficiente para abordar los riesgos contemporáneos. Lejos de tratarse de una categoría estática, la seguridad humana ha ido ampliando sus contornos teóricos a partir de realidades marcadas por la interdependencia global, las asimetrías estructurales y los efectos concretos de la inseguridad sobre las personas y comunidades.

El Informe sobre Desarrollo Humano del PNUD (1994) constituye el punto de partida más reconocido del concepto. Este informe propone situar a las personas —y no a los Estados— en el centro del análisis y la protección, desplazando la atención desde amenazas externas y armadas hacia riesgos cotidianos como la pobreza, la exclusión o la represión política. El enfoque se articula en torno a siete dimensiones interrelacionadas: seguridad económica, alimentaria, sanitaria, ambiental, personal, comunitaria y política.

Esta arquitectura multidimensional propuesta por el PNUD mostró que la inseguridad no es una excepción, sino una condición estructural derivada de múltiples vulnerabilidades sistémicas (Tadjbakhsh & Chenoy, 2007). En 2012, la Asamblea General de las Naciones Unidas (mediante la Resolución 66/290) consolidó esta perspectiva, definiendo la seguridad humana como un enfoque centrado en las personas, adaptado a los contextos y orientado a la prevención, que integra paz, desarrollo y derechos humanos (Asamblea General de Naciones Unidas, 2012).

Autores clave en el campo de los estudios de seguridad han contribuido a ampliar los fundamentos del enfoque de seguridad humana. Johan Galtung, al introducir el concepto de violencia estructural, sentó las bases para comprender que las amenazas a la seguridad no se reducen a actos de violencia directa, sino que también se manifiestan en estructuras sociales que generan pobreza, exclusión y desigualdad sistemática. En esta línea, el enfoque de seguridad humana retoma dicha perspectiva al considerar que la inseguridad puede derivarse de factores económicos, sociales o políticos naturalizados en el orden institucional (Galtung, 1969).

Por su parte, Barry Buzan y la Escuela de Copenhague aportaron el concepto de securitización, al señalar que las amenazas no son objetivas per se, sino construidas socialmente a través de discursos políticos que legitiman medidas extraordinarias (Buzan, 1991). Esta visión crítica resulta esencial para comprender cómo, en América Latina, ciertos problemas como la migración o la criminalidad han sido securitizados, desplazando respuestas centradas en los derechos humanos por otras basadas en la coerción. Ambos enfoques permiten trascender una visión reduccionista de la seguridad y nutren la perspectiva multidimensional que plantea la seguridad humana.

Los informes recientes del PNUD (2022, 2024) alertan sobre una "paradoja del progreso": pese al desarrollo económico en muchos países, la percepción de inseguridad y la vulnerabilidad emocional se han intensificado. Este fenómeno evidencia la necesidad de replantear el contrato social desde una perspectiva centrada en la protección integral de las personas.

Visiones y debates: enfoque amplio vs. restringido

El debate sobre la seguridad humana ha girado en torno a dos visiones predominantes. La visión amplia (*freedom from want*) promueve un concepto holístico que incorpora dimensiones socioeconómicas, ambientales y culturales del bienestar humano, adoptada

por Japón y respaldada por el PNUD. Desde esta perspectiva, las amenazas incluyen no solo la violencia física, sino también la pobreza, las enfermedades, el deterioro ambiental y otras formas de vulnerabilidad (Alkire, 2004). En contraste, la visión restringida (*freedom from fear*), promovida por Canadá, se enfoca en la protección frente a amenazas directas como los conflictos armados, el genocidio o el terrorismo (Bajpai, 2000).

Los críticos de la visión amplia argumentan que su extensión conceptual dificulta su operativización y medición, pero enfoques integradores como el de la Comisión de Seguridad Humana (2003) han buscado articular protección y empoderamiento. Esta formulación sostiene que los Estados deben garantizar condiciones que permitan a las personas desarrollar sus capacidades en contextos de paz y libertad, y que la comunidad internacional tiene la responsabilidad de actuar cuando los Estados no cumplen esa función (ICISS, 2001).

Perspectiva latinoamericana y aportes recientes

En América Latina, el enfoque de seguridad humana ha sido adaptado a contextos de inseguridad cotidiana, marcados no por guerras interestatales, sino por conflictos internos vinculados al crimen organizado, la violencia urbana, la exclusión estructural y la degradación ambiental. Esta adaptación ha dado lugar al enfoque de "seguridad ciudadana", centrado en el control del delito y la protección de las personas, pero con frecuencia limitado para abordar las causas estructurales de la violencia (Sorj, 2005). Así, dimensiones como la seguridad ambiental, sanitaria o económica han quedado rezagadas frente al enfoque punitivo.

Según el Real Instituto Elcano (Malamud & Núñez, 2024), aunque América Latina alberga solo el 8% de la población mundial, concentra cerca del 30% de los homicidios globales, la mayoría relacionados con el crimen organizado. Además, el 76% de los ciudadanos teme ser víctima de un delito, incluso en países con tasas de homicidio relativamente bajas (Latinobarómetro, 2024). Estas cifras reflejan una percepción generalizada de desprotección, que exige políticas territorializadas, culturalmente sensibles y construidas desde las realidades locales. La seguridad humana, en este contexto, requiere reconocer la intersección entre violencia directa, desigualdad estructural y debilidad institucional.

A diferencia de modelos universales o tecnocráticos, las políticas de seguridad deben ser territorializadas y culturalmente adaptadas, incorporando la voz de actores locales y de poblaciones históricamente excluidas. A nivel regional, la Declaración sobre Seguridad en las Américas (OEA, 2003) marcó un hito al incorporar un enfoque multidimensional, reconociendo amenazas no solo militares, sino también sociales, ambientales y económicas, como los desastres naturales, la corrupción, el narcotráfico y la migración forzada. Esta visión ha sido retomada en políticas que integran seguridad y desarrollo.

Desde el ámbito académico y técnico, se han realizado aportes fundamentales para analizar las particularidades de la región. Hurrell (1998) propuso entender América Latina como un espacio donde coexisten zonas de estabilidad con focos persistentes de alta conflictividad, desafiando la idea de una región homogéneamente pacífica y evidenciando los riesgos asociados a la exclusión y la debilidad institucional.

Más recientemente, investigaciones como las del Observatorio Ecuatoriano de Crimen Organizado (en adelante OECO) (2023) ad-

vierten que Ecuador enfrenta amenazas simultáneas de origen interno y externo, en un entorno marcado por la fragmentación estatal y la expansión de economías ilícitas. Las disputas entre organizaciones criminales por el control de rutas y territorios han intensificado la violencia armada, generando impactos directos en la gobernabilidad y el tejido social. El informe subraya que el crimen organizado tiene efectos negativos en las dimensiones política, económica y social, profundizando la inseguridad.

En la misma línea, un estudio conjunto realizado por el Centro de Estudios de Defensa Hemisférica William J. Perry, la Universidad de las Fuerzas Armadas – ESPE y la Universidad Andina Simón Bolívar, estos dos últimos centros académicos ecuatorianos, documenta cómo el debilitamiento institucional interno en Ecuador se ve agravado por redes transnacionales de narcotráfico y capitales ilícitos (Rodríguez et al., 2024). Estos hallazgos refuerzan la idea de que la inseguridad en América Latina no puede comprenderse como un fenómeno aislado, sino como una manifestación de dinámicas interdependientes que articulan factores estructurales, geopolíticos y territoriales.

Una contribución clave desde América Latina ha sido la visibilización de experiencias de seguridad construida "desde abajo", donde comunidades locales, redes de mujeres, pueblos indígenas y organizaciones sociales despliegan prácticas de protección, resiliencia y cuidado colectivo ante el abandono estatal. Este protagonismo territorial y comunitario desafía las visiones verticales del concepto de seguridad (Gómez, 2012), y promueve la democratización de sus prácticas y discursos (PNUD Costa Rica & IIDH, 2011).

Metodología

La presente investigación adopta un enfoque cualitativo, de tipo interpretativo-crítico, sustentado en un diseño documental. Su objetivo es analizar de forma sistemática y comprensiva las nuevas amenazas a la seguridad humana en el contexto latinoamericano, con especial atención al caso ecuatoriano. La elección metodológica responde al carácter multidimensional del objeto de estudio y a la necesidad de interpretar no solo los hechos empíricos, sino también los discursos y prácticas que los producen y legitiman.

La estrategia de análisis se estructuró en torno a tres ejes: (i) caracterización de las amenazas contemporáneas a la seguridad humana; (ii) identificación de las dimensiones afectadas a partir del marco del PNUD (1994); y (iii) análisis crítico de las respuestas institucionales. A través de estos ejes se buscó articular un enfoque multiescalar que permitiera situar lo nacional en diálogo con lo regional y global.

La selección de fuentes siguió criterios de pertinencia temática, actualidad (2015–2025) y diversidad institucional, priorizando literatura académica arbitrada, informes técnicos de organismos multilaterales (PNUD, CEPAL, ONU Mujeres, ACNUR), documentos gubernamentales y reportes especializados sobre seguridad humana. Se excluyeron materiales sin validación académica o institucional, así como aquellos con evidentes sesgos partidarios o falta de rigor conceptual.

El corpus documental fue sometido a un análisis categorial-temático, mediante un proceso de lectura hermenéutica orientado a identificar patrones de afectación, recurrencias narrativas y articulaciones entre amenazas y dimensiones de seguridad. Se aplicó una estrategia de triangulación interna, comparando evidencias y perspectivas de distintas

fuentes sobre cada amenaza, lo que permitió una interpretación más robusta de los fenómenos abordados.

Esta metodología permitió analizar las amenazas no solo como eventos objetivos, sino también como construcciones sociales e institucionales que impactan diferencialmente según el grupo poblacional, el territorio y la respuesta estatal. En consonancia con los postulados del enfoque de seguridad humana, se privilegió una lectura contextualizada, centrada en las personas, y atenta a las intersecciones entre vulnerabilidad, poder y desigualdad estructural.

Principales amenazas contemporáneas a la seguridad humana

El entorno de seguridad en Ecuador ha experimentado una transformación profunda y acelerada. Las amenazas actuales no pueden explicarse únicamente desde factores delictivos o coyunturales; responden a dinámicas estructurales y transnacionales que interactúan de forma simultánea. Esta sección examina cinco amenazas prioritarias: crimen organizado transnacional, crisis climática, riesgos cibernéticos, migraciones forzadas y pandemias. Cada una de ellas afecta de forma diferenciada las dimensiones de la seguridad humana, generando efectos acumulativos.

Crimen organizado transnacional

Ecuador registró en 2024 la mayor tasa de homicidios de América Latina (38,8 por cada 100.000 habitantes) (InSight Crime, 2025). Esta violencia responde a su rol en las vías del narcotráfico global, con Guayaquil como nodo logístico (Ayuso, 2024). Grupos como Los Choneros, Los Lobos y Los Tiguerones controlan territorios, extorsionan comunidades y operan desde un sistema penitenciario colapsado, con más de 400 muertes en cárceles entre 2021 y 2024 (Ayuso, 2024; USCRI, 2025).

Crisis climática y vulnerabilidad ambiental

El cambio climático representa una amenaza estructural y transversal a la seguridad humana en Ecuador. Las inundaciones, sequías, deslizamientos y alteraciones de los ciclos de precipitación impactan directamente en la agricultura, el acceso al agua y la salud pública (Banco Mundial, 2021). La sequía de 2024, con apagones de hasta 14 horas diarias, reveló la dependencia crítica del país de la generación hidroeléctrica, afectando la producción, los servicios y la vida cotidiana en zonas urbanas y rurales. A esto se suma la deforestación, que afecta a más de 90.000 hectáreas anuales y amplifica la degradación de cuencas y la pérdida de biodiversidad (Serrano, 2022).

La deforestación y la minería ilegal no solo agravan el cambio climático, sino que aumentan la vulnerabilidad local a desastres naturales y pérdida de biodiversidad, afectando especialmente a comunidades indígenas. Además, la presencia del crimen organizado en actividades extractivas representa una amenaza tanto ecológica como cultural.

Además, la variabilidad climática y la degradación ambiental repercuten en la seguridad alimentaria, especialmente en zonas rurales e indígenas donde la agricultura de subsistencia es la principal fuente de sustento. Según datos de la Clasificación Integrada de la Seguridad Alimentaria en Fases (CIF) para el período septiembre 2024 - marzo 2025, la inseguridad alimentaria aguda afecta a provincias como Esmeraldas (25%) y Pastaza (23%), con un

impacto importante en zonas rurales debido a la pérdida de empleo y aumento de precios de alimentos.

Provincias como Guayas, Manabí, Los Ríos y Pichincha presentan grandes poblaciones afectadas, reflejando la precariedad económica y dificultades de acceso a alimentos en el país (CIF, 2024). Estos datos evidencian que el deterioro ambiental no solo es ecológico, sino también una amenaza directa a la nutrición y al desarrollo humano.

Riesgos cibernéticos y digitalización insegura

A medida que el país avanza en su digitalización, aumenta también su exposición a vulnerabilidades cibernéticas que pueden comprometer tanto infraestructuras críticas como información sensible de ciudadanos e instituciones. En 2019 ocurrió una masiva filtración de datos personales (Borner, 2019). En 2025, la Asamblea Nacional sufrió ciberataques que evidencian la fragilidad institucional y los riesgos para la seguridad nacional (Ecuavisa, 2025; El Universo, 2025). Estos eventos reflejan una tendencia preocupante: el incremento de ataques dirigidos contra instituciones gubernamentales, que pueden comprometer la seguridad nacional y la confianza ciudadana en las instituciones democráticas.

Migraciones forzadas

Ecuador ha pasado a ser uno de los principales países de acogida de población migrante en América Latina, recibiendo a más de 474.000 personas venezolanas (ACNUR, 2024). Esta situación ha generado tensiones en los servicios básicos, la infraestructura y el empleo, especialmente en ciudades como Quito, Guayaquil y Tulcán. Si bien la migración ha sido históricamente una estrategia de resiliencia, la llegada masiva y sostenida de población desplazada en contextos de precariedad estatal ha generado nuevas formas de exclusión, xenofobia y explotación laboral, afectando la seguridad humana tanto de migrantes como de comunidades receptoras. Además, la migración irregular está siendo cooptada por redes criminales.

Según Cruz et al. (2024), esto es un fenómeno complejo relacionado con aspectos económicos, sociales y de derechos humanos. Por esta razón, el autor enfatiza la importancia de adoptar un enfoque integral que combine medidas estrictas contra las redes de traficantes con políticas públicas que ofrezcan rutas seguras y legales para la migración. Esta situación evidencia cómo distintas amenazas a la seguridad humana pueden converger y potenciarse mutuamente.

Pandemias y crisis sanitarias

La pandemia de COVID-19 demostró la vulnerabilidad de Ecuador frente a emergencias sanitarias. Guayaquil fue epicentro de una de las crisis más dramáticas en la región, con un colapso del sistema sanitario y funerario. El impacto no fue únicamente epidemiológico, sino económico, social y político (Banco Central del Ecuador [BCE], 2021). La economía se contrajo un 7,8% en 2020; la pobreza y el empleo inadecuado se dispararon; y la confianza en las autoridades se erosionó. Además, el uso de tecnologías de vigilancia generó preocupaciones sobre la protección de derechos fundamentales (Asociación para el Progreso de las Comunicaciones, 2020).

El riesgo de futuras pandemias—agravado por la deforestación, la urbanización descontrolada y el cambio climático—refuerza la necesidad de consolidar capacidades preventivas,

sanitarias y comunitarias para proteger la seguridad humana. Las amenazas aquí descritas no operan de forma aislada, sino que inciden de manera transversal en múltiples dimensiones del bienestar humano. A continuación, se presenta un cuadro sintético (ver tabla 1) que relaciona las principales amenazas identificadas con las dimensiones de la seguridad humana planteadas por el PNUD (1994), lo cual permite observar la naturaleza integral y simultánea de sus efectos.

Tabla 1.
Dimensiones de la Seguridad Humana y amenazas relevantes en el contexto ecuatoriano[1]

Dimensión de Seguridad Humana	Amenazas identificadas en Ecuador
Económica	Pobreza, desempleo, trabajo precario
Alimentaria	Desnutrición infantil, inseguridad alimentaria rural
De salud	Enfermedades endémicas, déficit de infraestructura sanitaria
Ambiental	Deforestación, contaminación hídrica, desastres naturales
Personal	Crimen organizado, violencia interpersonal
Comunitaria	Conflictos interculturales, migración forzada
Política	Corrupción institucional, desconfianza institucional

Nota. Elaboración propia.

Las amenazas que enfrenta Ecuador no son aisladas, sino que forman parte de un patrón regional de inseguridad multidimensional. Por ejemplo, países como México y Colombia también enfrentan altos niveles de violencia asociada al crimen organizado transnacional, con dinámicas similares de disputa territorial y cooptación institucional (Malamud & Núñez, 2024). En el caso de Honduras y El Salvador, la convergencia entre violencia, pobreza y migración forzada ha sido ampliamente documentada como un círculo vicioso que compromete la seguridad humana (PNUD, 2013).

Asimismo, el Perú experimenta efectos críticos del cambio climático sobre la agricultura familiar, especialmente en regiones altoandinas, generando impactos similares a los observados en la Sierra ecuatoriana. Estas comparaciones refuerzan la idea de que las amenazas a la seguridad humana en América Latina no responden solo a variables nacionales, sino a factores estructurales comunes como la desigualdad, la fragilidad institucional y la vulnerabilidad ambiental.

En síntesis, queda evidenciado que estas amenazas se interconectan y afectan simultáneamente la seguridad humana. Superarlas requiere enfoques integrales, multidimen-

1 Aunque algunas de las amenazas incluidas en el cuadro no han sido desarrolladas en detalle en las secciones previas, su incorporación se justifica por el reconocimiento que han recibido por parte de organismos multilaterales y estudios especializados, dada su relevancia para la seguridad humana en el contexto ecuatoriano.

sionales y centrados en la dignidad humana. Esta comprensión es clave para avanzar hacia respuestas más eficaces e integrales, aspecto que se abordará en la siguiente sección sobre las dimensiones afectadas: económica, social, política y ambiental.

Dimensiones afectadas: económica, social, política, ambiental

Las amenazas contemporáneas a la seguridad humana en Ecuador afectan múltiples dimensiones del bienestar individual y colectivo, generando impactos sistémicos e interdependientes que se retroalimentan en ciclos de vulnerabilidad acumulativa. Las esferas económica, social, política y ambiental no pueden abordarse de manera aislada, pues su interacción amplifica las brechas estructurales, especialmente entre poblaciones históricamente excluidas. A continuación, se examinan sus principales efectos.

Dimensión económica

La dimensión económica se ve particularmente afectada por una convergencia de factores: el auge del crimen organizado, las crisis macroeconómicas recurrentes, el cambio climático y las consecuencias de pandemias recientes. Esto ha evidenciado y profundizado la fragilidad del modelo económico ecuatoriano. Según Carrillo et al. (2023), las economías criminales en Ecuador generan cerca de 10.000 millones de dólares anuales lo que representa un peso equivalente al 8-15% del PIB, en línea con estimaciones globales del Foro Económico Mundial (Primicias, 2024). Esta presencia delictiva desestructura el tejido productivo mediante prácticas como la extorsión (conocida como "vacunas"), que en 2022 registró más de 5.800 denuncias con un aumento interanual del 293% (Ecuavisa, 2023).

A estas distorsiones se suman los efectos acumulados de sucesivas crisis económicas. La crisis financiera de 1999, por ejemplo, redujo el ingreso per cápita en un 10% y disparó la pobreza, perjudicando especialmente a sectores urbanos y rurales (Larrea, 2004). Décadas después, como se mencionó anteriormente, la pandemia de COVID-19 volvió a golpear con fuerza: en 2020, la pobreza multidimensional se incrementó por el aumento del desempleo y el trabajo precario, afectando sobre todo a mujeres, jóvenes y habitantes rurales (Quilli-Granda & García-Vélez, 2023). Además, el PIB cayó un 7,8%, profundizando problemas estructurales como la informalidad, la baja calidad del empleo y la disminución del consumo (BCE, 2022).

Si bien en 2021 se registró un repunte económico del 4,2%, esta recuperación ha sido desigual y frágil. Factores como la alta informalidad laboral, la escasa inversión pública y la dependencia de sectores extractivos han limitado una reactivación sostenida (Ochoa et al., 2024). Finalmente, el cambio climático ha agravado esta vulnerabilidad. En 2024, una intensa sequía provocó apagones que generaron pérdidas diarias de hasta 72 millones de dólares estadounidenses (USD), afectando hogares, industrias y servicios públicos (Diario Expreso, 2024). El impacto en el sector agrícola, que emplea al 30% de la población económicamente activa y representa el 8% del PIB, también ha sido severo (Aguirre, 2023).

Dimensión social

Los impactos de las amenazas contemporáneas sobre la dimensión social de la seguridad humana son profundos y transformadores. La

violencia criminal ha alterado las dinámicas comunitarias, generando temor, desconfianza interpersonal, retraimiento del espacio público y debilitamiento de la cohesión social. Según Latinobarómetro (2024), el 51% de los ecuatorianos reportó haber sido víctima de un delito o tener un familiar cercano afectado. Además, un 75% dice sentirse inseguro de forma permanente.

Por otra parte, uno de los efectos más preocupantes es el reclutamiento de adolescentes y jóvenes por parte de organizaciones criminales, especialmente en barrios periféricos, donde la violencia se convierte en un sustituto de oportunidades legítimas. En contextos marcados por la exclusión socioeconómica, la presencia estatal débil y la falta de oportunidades, estas estructuras ilegales ofrecen ingresos inmediatos, protección y un sentido de pertenencia. Este fenómeno ha alcanzado incluso las instituciones educativas. En sectores de Guayaquil y Esmeraldas se han documentado casos de extorsión a escuelas y redes de reclutamiento forzado dentro de centros educativos (Human Rights Watch, 2024).

Las migraciones forzadas, tanto internas como externas, también están transformando el tejido social. El arribo masivo de personas venezolanas ha generado presión sobre servicios públicos y tensiones comunitarias (ACNUR, 2024), mientras que la emigración ecuatoriana ha fragmentado núcleos familiares. El cambio climático agrava estas desigualdades: comunidades rurales, indígenas y periurbanas enfrentan mayores impactos y menor capacidad adaptativa. El acceso desigual a políticas de mitigación genera brechas territoriales e intergeneracionales (Banco Mundial, 2024).

Desde una perspectiva de género, las amenazas a la seguridad humana descritas previamente se manifiestan de manera particularmente severa sobre las mujeres, niñas y diversidades sexo-genéricas. La violencia criminal se traduce en un aumento de femicidios, trata de personas con fines de explotación sexual y violencia sexual como mecanismo de control territorial en zonas disputadas por grupos armados.

En contextos migratorios, las mujeres en movilidad enfrentan riesgos agravados de abuso, extorsión y explotación. Por su parte, las crisis sanitarias y ambientales profundizan las desigualdades de cuidado, ya que las mujeres asumen de manera desproporcionada la responsabilidad del sostenimiento familiar y comunitario (ONU Mujeres et al., 2023). En suma, la interacción entre género, pobreza y exclusión territorial convierte a ciertos cuerpos en blanco preferente de múltiples formas de inseguridad, lo que exige respuestas institucionales sensibles al género y culturalmente pertinentes.

Dimensión política

Las amenazas a la seguridad humana también generan efectos corrosivos sobre el sistema político y el ejercicio democrático. El crimen organizado desafía directamente el monopolio estatal de la violencia legítima, infiltrando fuerzas del orden, el sistema judicial y el penitenciario (Latinobarómetro, 2024). Esta penetración ha generado una profunda desconfianza en el Estado. Solo el 17% de los ecuatorianos confía en la policía y el 12% en la justicia. Esta percepción de ineficacia incentiva prácticas como la justicia por mano propia y la formación de grupos de autodefensa (Human Rights Watch, 2024).

La crisis de seguridad también ha impactado en el proceso electoral y la representación política. El asesinato del candidato presidencial

Fernando Villavicencio en 2023 evidenció cómo el crimen puede condicionar procesos democráticos, limitando la participación política y el debate. Además, los ciberataques recientes a la Asamblea Nacional revelan una nueva dimensión de fragilidad institucional, donde incluso la infraestructura digital se convierte en blanco de amenazas.

Dimensión ambiental

La dimensión ambiental de la seguridad humana en Ecuador se encuentra amenazada por el cambio climático, la expansión de actividades ilegales y el deterioro ecológico acumulado. Aunque Ecuador contribuye con menos del 0,2% de las emisiones globales, sufre impactos desproporcionados, como el retroceso glaciar, sequías prolongadas, inundaciones y pérdida de biodiversidad (Banco Mundial, 2021).

El retroceso de los glaciares andinos, la variabilidad en los patrones de lluvia y la creciente frecuencia de inundaciones y sequías están afectando directamente el abastecimiento de agua, la agricultura y la salud pública. La sequía de 2024 dejó sin servicio eléctrico a grandes zonas del país y comprometió hospitales, escuelas y transporte, evidenciando la fragilidad del sistema energético.

Un aspecto crítico es la relación entre crimen organizado y degradación ambiental. La minería ilegal—cada vez más asociada a redes criminales—genera contaminación con mercurio en la Amazonía, afecta fuentes hídricas y desplaza comunidades indígenas (Pastrana et al., 2023). La deforestación incrementa la vulnerabilidad a deslizamientos y erosión. El deterioro ecológico también amenaza la seguridad cultural. Para muchos pueblos indígenas, el territorio no es solo un medio de vida, sino un espacio espiritual y comunitario. La destrucción de estos ecosistemas representa también una amenaza a la identidad, la cosmovisión y la subsistencia cultural (Cando & Villalva, 2024).

Con esta visión general de los impactos económicos, sociales, políticos y ambientales, en la próxima sección se examinará el estudio de caso de Guayaquil, que ilustra la convergencia de estas dimensiones en un territorio específico.

Caso de estudio: Guayaquil – epicentro de una crisis multidimensional de seguridad

Para comprender de forma situada los efectos sinérgicos de las amenazas contemporáneas a la seguridad humana en Ecuador, se presenta el estudio de caso de la ciudad de Guayaquil, el cual refleja la interacción de múltiples factores que desbordan las capacidades estatales y demandan enfoques integrales.

Guayaquil, principal puerto y centro económico de Ecuador, ejemplifica cómo diversas amenazas a la seguridad humana pueden converger y potenciarse mutuamente en un territorio específico. Esta ciudad de aproximadamente 2,7 millones de habitantes (INEC, 2017) ha experimentado una transformación dramática en su panorama de seguridad, pasando de ser un modelo de regeneración urbana en los primeros años del siglo XXI a convertirse en uno de los epicentros de violencia criminal en América Latina.

El puerto de Guayaquil se ha consolidado como nodo central del narcotráfico internacional, conectando la producción andina de cocaína con mercados globales. Esta posición estratégica ha desencadenado una violenta disputa territorial entre organizaciones criminales como Los Choneros y Los Lobos, que

mantienen vínculos con carteles mexicanos y albaneses (Human Rights Watch, 2024). Entre 2017 y 2024, la ciudad de Guayaquil experimentó un aumento exponencial en su tasa de homicidios, alcanzando un nivel sin precedentes de 89,11 homicidios por cada 100.000 habitantes. Esta cifra, correspondiente a la Zona 8 —que comprende Guayaquil, Durán y Samborondón—, la posiciona como la jurisdicción con la mayor tasa de homicidios del país (OECO, 2023).

El Estado, en lugar de actuar como garante de protección, ha cedido presencia y control territorial. Como documenta el OECO (2023), en múltiples sectores periféricos de Guayaquil las bandas criminales cumplen funciones que van desde la provisión de seguridad hasta la regulación del comercio local y el "cobro de impuestos". Esta situación refleja una preocupante sustitución del Estado por actores ilegales que ejercen control sobre la vida cotidiana de la población, en un contexto de debilidad institucional, corrupción policial y desconfianza generalizada.

Durante la pandemia de COVID-19, Guayaquil se convirtió en símbolo de la devastación sanitaria, evidenciando el colapso del sistema sanitario y funerario (Borja, 2020). Esta crisis reveló vulnerabilidades estructurales en servicios básicos y sistemas de protección social, exacerbadas por la alta densidad de población, la desigualdad social y las condiciones precarias de vivienda en asentamientos informales (Nascimento & Procopiuck, 2023).

Adicionalmente, Guayaquil enfrenta una creciente vulnerabilidad frente al cambio climático. Su ubicación en el estuario del río Guayas la expone a inundaciones recurrentes, cuya frecuencia e intensidad han aumentado en las últimas décadas (Care Environnement, 2018). El incremento proyectado del nivel del mar amenaza áreas de desarrollo informal ubicadas en zonas bajas, mientras que la expansión urbana no planificada reduce áreas de manglar que históricamente han funcionado como barreras naturales contra inundaciones y marejadas.

En suma, Guayaquil encarna la convergencia simultánea de múltiples amenazas a la seguridad humana: violencia criminal, crisis sanitaria, deterioro ambiental y exclusión estructural. Este caso ilustra la urgencia de respuestas integrales, que vayan más allá de la represión, incorporando estrategias de desarrollo urbano justo, fortalecimiento institucional y protección de derechos humanos, que trasciendan aproximaciones sectoriales o fragmentadas.

Actores y mecanismos de difusión: rol de organismos internacionales, gobiernos, sociedad

Frente a la complejidad e interdependencia de las amenazas contemporáneas a la seguridad humana, la acción coordinada de múltiples actores resulta indispensable. Este entramado incluye organismos internacionales, gobiernos nacionales y locales, sociedad civil y sector privado, cuyos roles y capacidades son diversos, complementarios y, en ocasiones, contradictorios.

Organismos internacionales

Organismos como el PNUD, la Oficina de las Naciones Unidas contra la Droga y el Delito (en adelante UNODC) y la OEA han sido actores clave en la promoción del enfoque multidimensional de la seguridad (Naciones Unidas en Ecuador, 2024; PNUD Ecuador, 2024; PNUD, s. f.). El PNUD ha impulsado

en Ecuador proyectos de prevención de violencia con énfasis comunitario, particularmente en municipios priorizados.

La UNODC ha brindado asistencia técnica en temas de crimen organizado y justicia penal, mientras que la OEA ha promovido la adopción de marcos regionales como la Declaración sobre Seguridad en las Américas (OEA, 2003). Instituciones financieras internacionales como el Banco Interamericano de Desarrollo (en adelante BID) y el Banco Mundial han empezado a incorporar la seguridad como componente transversal de sus programas de desarrollo, reconociendo la interrelación entre pobreza, exclusión y violencia.

Gobiernos nacionales y locales

La respuesta estatal en Ecuador ha oscilado entre políticas preventivas y una creciente tendencia a la securitización militarizada. En 2024, el presidente Daniel Noboa declaró "conflicto armado interno", otorgando facultades extraordinarias a las Fuerzas Armadas para combatir al crimen organizado, ahora calificado como "terrorismo". Si bien esta estrategia generó capturas masivas y decomisos, también ha despertado alertas sobre su sostenibilidad y respeto a derechos humanos (Human Rights Watch, 2024). A nivel local, gobiernos municipales han implementado iniciativas de recuperación de espacios públicos, videovigilancia y programas de prevención. Sin embargo, estas experiencias se ven limitadas por restricciones presupuestarias, débil coordinación interinstitucional y la magnitud del problema, que supera su capacidad de respuesta.

Sociedad civil

Organizaciones comunitarias, organizaciones no gubernamentales (ONG) de derechos humanos, redes de mujeres, colectivos juveniles e instituciones académicas han desarrollado múltiples iniciativas en contextos de alta vulnerabilidad. Organizaciones como la Fundación Esquel (2020) y el Comité Permanente por la Defensa de los Derechos Humanos (2025) han implementado metodologías de prevención de violencia basadas en mediación comunitaria, educación para la paz y atención a poblaciones vulnerables específicas. Asimismo, destacan experiencias de prevención de violencia, mediación comunitaria y protección de territorios indígenas frente a actividades extractivas ilegales.

La Confederación de Nacionalidades Indígenas del Ecuador (en adelante CONAIE), por ejemplo, ha denunciado sistemáticamente la relación entre minería ilegal y crimen organizado en zonas amazónicas (CONAIE, FEINE y FENOCIN, 2023). Además, la academia—incluyendo centros como el Instituto de Altos Estudios Nacionales y la Facultad Latinoamericana de Ciencias Sociales (FLACSO-Ecuador)—ha generado investigaciones clave para comprender las amenazas y evaluar críticamente las políticas públicas, aunque su incidencia es aún limitada.

Sector privado

El sector privado en Ecuador, particularmente en Guayaquil y las zonas costeras, ha intensificado significativamente su inversión en seguridad privada como respuesta al incremento de la violencia y la criminalidad. En el contexto de un Estado cuya capacidad para garantizar seguridad pública se ha visto desbordada, muchas empresas han asumido el costo de proteger sus activos, empleados y operaciones. Esta tendencia plantea interrogantes sobre la equidad en el acceso a la seguridad, así como sobre la regulación efectiva de estas empresas. En sectores estratégicos

como el agroexportador o el minero, se han desarrollado alianzas público-privadas para proteger cadenas logísticas. Sin embargo, el riesgo de "captura corporativa" de funciones públicas de seguridad sigue siendo una preocupación relevante.

A la luz de estas respuestas institucionales y sociales, en la siguiente sección se analizará el debate entre el enfoque tradicional de seguridad y el enfoque de seguridad humana, así como sus implicaciones para la formulación de políticas públicas sostenibles.

Tensiones conceptuales y operativas entre la seguridad tradicional y la seguridad humana

El caso ecuatoriano evidencia una tensión estructural entre los enfoques tradicionales de seguridad —centrados en el control territorial, la militarización y la defensa nacional— y el enfoque multidimensional de seguridad humana, que propone intervenciones integrales orientadas a la protección de las personas, sus derechos y condiciones de vida.

La declaración del "conflicto armado interno" en 2024 por parte del gobierno ecuatoriano, en respuesta al auge del crimen organizado, ejemplifica esta tensión paradigmática. Esta medida representó un punto de inflexión en la política de seguridad nacional, al permitir la actuación directa de las Fuerzas Armadas en tareas de control interno. Si bien generó una respuesta inmediata en términos de operativos, capturas y visibilidad mediática, también provocó preocupaciones legítimas sobre la normalización del uso de la fuerza militar, el debilitamiento del Estado de derecho y el riesgo de violaciones a los derechos humanos (Human Rights Watch, 2024).

Este tipo de medidas reflejan una lógica reactiva que privilegia la inmediatez y el control físico del territorio sobre las causas estructurales de la inseguridad, como la desigualdad, el desempleo juvenil, la corrupción institucional o el abandono estatal en zonas periféricas. La experiencia latinoamericana, en particular los casos de México, Brasil y El Salvador, muestra que las respuestas militarizadas pueden exacerbar la violencia o generar espirales de securitización "que institucionaliza el predominio de lo militar sobre lo político" (Verdes, 2019, p. 7), sin resolver los factores de fondo.

No obstante, sería un error reducir el debate a una falsa dicotomía entre enfoques "duros" y "blandos". La gravedad de la crisis actual requiere intervenciones de corto plazo que garanticen seguridad inmediata, pero también estrategias de mediano y largo plazo orientadas a transformar las condiciones estructurales que alimentan la violencia.

En ese sentido, la seguridad humana ofrece una perspectiva más adecuada para contextos como el ecuatoriano, al integrar los principios de prevención, protección, empoderamiento y participación ciudadana. Este enfoque no niega la necesidad de respuestas coercitivas ante amenazas inminentes, pero insiste en que estas deben ser parte de una estrategia más amplia basada en derechos, justicia social y resiliencia comunitaria.

El análisis del caso de Guayaquil, por ejemplo, muestra cómo las respuestas policiales son insuficientes si no se acompañan de políticas urbanas redistributivas, inversión social y planificación territorial sensible al riesgo.

Finalmente, la discusión también debe abordar la dimensión institucional y presupuestaria. Según datos del Banco Mundial, en 2023 Ecuador destinó aproximadamente el 2,3% de su Producto Interno Bruto (PIB) al gasto en defensa, lo que equivale a un incremento del 0,05% respecto al año anterior (Banco Mundial, 2025). Este gasto incluyó inversiones en equipamiento policial y militar, refle-

jando el énfasis del país en fortalecer su seguridad interna y capacidades de defensa. En contraste, los programas de prevención, justicia juvenil, rehabilitación penitenciaria o participación ciudadana reciben recursos significativamente menores. Esta brecha refleja una jerarquía de prioridades que limita la eficacia y sostenibilidad de las políticas de seguridad.

Conclusiones

El análisis desarrollado a lo largo de este estudio muestra que Ecuador enfrenta una convergencia de amenazas contemporáneas que trascienden las concepciones tradicionales de seguridad y demandan respuestas multidimensionales, adaptativas y centradas en las personas. El crimen organizado transnacional, el cambio climático, las migraciones forzadas, los riesgos cibernéticos y las pandemias configuran un entorno complejo, donde las distintas dimensiones del bienestar humano se ven simultáneamente afectadas y erosionadas.

Uno de los hallazgos centrales es el carácter sinérgico de estas amenazas, que no operan de forma aislada, sino que se refuerzan mutuamente, exacerbando las condiciones de vulnerabilidad. La violencia organizada se vincula con la pobreza, el desempleo y la exclusión; la degradación ambiental afecta de forma desproporcionada a comunidades empobrecidas; y las crisis sanitarias revelan desigualdades históricas en el acceso a servicios básicos. Esta interdependencia exige superar enfoques sectoriales o fragmentados, y adoptar marcos integrales como el de la seguridad humana.

El estudio también evidencia una distribución desigual de los impactos territoriales y sociales de las amenazas. Zonas fronterizas, áreas urbanas marginales y regiones amazónicas concentran altos niveles de riesgo, mientras que grupos históricamente excluidos (mujeres, pueblos indígenas, jóvenes y migrantes) enfrentan amenazas diferenciadas sin acceso equitativo a mecanismos de protección.

Desde una perspectiva teórica y práctica, el caso ecuatoriano confirma la relevancia del enfoque de seguridad humana como alternativa crítica al paradigma militarizado y estatocéntrico. Al incorporar los principios de protección, prevención, empoderamiento y justicia social, ofrece herramientas para diseñar políticas públicas más eficaces, inclusivas y sostenibles. No obstante, su implementación requiere reformas institucionales, inversión sostenida, voluntad política y participación ciudadana. También demanda una transformación en la forma en que se entiende la seguridad: no como control social, sino como garantía de condiciones dignas para el desarrollo humano.

Referencias

ACNUR. (2024). *Ecuador: Informe operacional: 2023 en resumen.* ACNUR – Agencia de Naciones Unidas para los Refugiados. https://reliefweb.int/report/ecuador/acnur-ecuador-informe-operacional-2023-en-resumen

Aguirre, N. (2023, abril 25). La agricultura aporta más al PIB que la minería metálica [Quito Sin Minería]. *Quito Sin Minería*. https://n9.cl/2e05q

Alkire, S. (2004). A vital core that must be treated with the same gravitas as traditional security threats. *Security Dialogue*, 35(3), 359-360. https://doi.org/10.1177/096701060403500317

Asamblea General de Naciones Unidas. (2012). *Resolución aprobada por la Asamblea General el 10 de septiembre de 2012 (A/RES/66/290; Sexagésimo sexto período de sesiones)*. Naciones Unidas. https://documents.un.org/doc/undoc/gen/n11/476/25/pdf/n1147625.pdf

Asociación para el Progreso de las Comunicaciones. (2020, marzo 18). Ecuador: Las tecnologías de vigilancia en contexto de pandemia no deben poner en riesgo los derechos humanos. *Asociación para el Progreso de las Comunicaciones*. https://n9.cl/50j46

Ayuso, A. (2024). La crisis de Ecuador, mucho más que seguridad (788; CIDOB Opinión). CIDOB – *Barcelona Centre for International Affairs*. https://www.cidob.org/publicaciones/la-crisis-de-ecuador-mucho-mas-que-seguridad

Bajpai, K. (2000). *Human security: Concept and measurement* [Kroc Institute Occasional Paper No. 19:OP:1]. University of Notre Dame.

Banco Central del Ecuador (BCE). (2021, abril 1). *La pandemia incidió en el crecimiento 2020: La economía ecuatoriana decreció 7,8%*. Banco Central del Ecuador. https://n9.cl/lx2g2w

Banco Central del Ecuador (BCE). (2022). *Informe de la evolución de la economía ecuatoriana en 2021 y perspectivas 2022*. Banco Central del Ecuador. https://n9.cl/dbwcx

Banco Mundial. (2021). *Climate risk profile: Ecuador*. The World Bank Group. https://n9.cl/xryao

Banco Mundial. (2024). *Ecuador—Country climate and development report* (Informe No. 193430). Banco Mundial. https://n9.cl/c9eef

Banco Mundial. (2025). *Gasto militar (% del PIB)—Ecuador. World Bank Open Data*. https://data.worldbank.org

Borja, M. S. (2020, abril 6). Ecuador: Enfermar de COVID-19 o no comer, la disyuntiva de la gente pobre. *The Washington Post*. https://n9.cl/g8xg6

Borner, P. (2019, septiembre 20). Una masiva filtración de datos expone los datos personales de todo un país. *The Data Privacy Group*. https://n9.cl/4t6xat

Buzan, B. (1991). New patterns of global security in the twenty-first century. *International Affairs*, 67(3), 431-451. https://doi.org/10.2307/2621945

Cando, L., & Villalva, D. (2024). Perspectivas indígenas y locales sobre los derechos de la naturaleza en el ordenamiento jurídico ecuatoriano. LATAM. *Revista Latinoamericana de Ciencias Sociales y Humanidades*, 5(5), 1738-1752.

Care Environment. (2018). *Vulnerabilidad y adaptación al cambio climático en Guayaquil*. CAF – Banco de Desarrollo de América Latina.

Carrillo, P., Romo, M. P., Carrillo, M., & Andrade, S. (2023). *Economías criminales*. Konrad Adenauer Stiftung.

CIF (Cadena de Inseguridad Alimentaria). (2024, noviembre 8). Ecuador: Instantánea de la inseguridad alimentaria aguda de la CIF (junio 2024 – marzo 2025). *CIF*. https://n9.cl/pfzqu

Comisión de Seguridad Humana. (2003). *Human security now*. Comisión de Seguridad Humana.

Comité Permanente por la Defensa de los Derechos Humanos. (2025). *Desplazamiento*

forzado interno de familias de la comunidad de Socio Vivienda en Guayaquil: Reporte preliminar. https://nube.interfabu.com/s/xMbSk3MNkozQm7Q

CONAIE, FEINE, & FENOCIN. (2023). *Asamblea Nacional en Defensa de los Territorios, la Naturaleza, el Agua y la Vida contra el despojo minero a gran escala en el Ecuador*. https://n9.cl/g6dok

Cruz, I., Murillo, D., & Pita, A. (2024). El tráfico ilícito de migrantes y su afectación en el Ecuador. *Ciencia Latina: Revista Multidisciplinar*, 8(6), 3270-3287. https://doi.org/10.37811/cl_rcm.v8i6.15089

Diario Expreso. (2024, septiembre 27). Horarios de cortes de luz en Ecuador. *Diario Expreso*. https://n9.cl/jm3jg9

Ecuavisa. (2023). Las víctimas de «vacunas» extorsivas en Ecuador desisten de seguir con las denuncias. *Ecuavisa*. https://n9.cl/piznd

Ecuavisa. (2025, febrero 17). La Asamblea denuncia dos ciberataques a su sistema informático. *Ecuavisa*. https://n9.cl/jmjk1

El País. (2025, marzo 2). Ecuador se sitúa como el país más violento de América Latina: Un asesinato cada hora. *El País América*. https://n9.cl/f6wxk

El Universo. (2025, febrero 17). Asamblea alerta de dos ciberataques para "vulnerar información confidencial". *El Universo*. https://n9.cl/jlknod

Fundación Esquel. (2020). *Estudio cualitativo y cuantitativo sobre violencia política contra las mujeres en Ecuador en redes sociales.* ONU Mujeres. https://n9.cl/n7sdu

Galtung, J. (1969). Violence, peace, and peace research. *Journal of Peace Research*, 6(3), 167-191.

Gómez, O. (2012). What is a human security project? The experience of the UN Trust Fund for Human Security. *Global Change, Peace & Security*, 24(3), 385-403. https://doi.org/10.1080/14781158.2012.718430

Human Rights Watch. (2024). Ecuador: Eventos de 2024. En *Informe mundial 2025*. Human Rights Watch. https://www.hrw.org/es/world-report/2025/country-chapters/ecuador

Hurrell, A. (1998). Security in Latin America. *International Affairs*, *74*(3), 529-546. https://doi.org/10.1111/1468-2346.00032

ICISS (International Commission on Intervention and State Sovereignty). (2001). *The responsibility to protect*. International Development Research Centre.

INEC (Instituto Nacional de Estadística y Censos). (2017). *Guayaquil en cifras*. Instituto Nacional de Estadística y Censos. https://www.ecuadorencifras.gob.ec/guayaquil-en-cifras

InSight Crime. (2025, febrero 26). Balance de InSight Crime de los homicidios en 2024. *InSight Crime*. http://insightcrime.org/es/noticias/balance-insight-crime-homicidios-2024

Larrea, C. (2004). *Dolarización, crisis y pobreza en el Ecuador*. Friedrich Ebert Stiftung.

Latinobarómetro. (2024). *Informe 2024: La democracia resiliente*. Corporación Latinobarómetro. https://www.inep.org/images/2024/TXT/Latinobarometro-Informe_2024.pdf

Malamud, C., & Núñez, R. (2024). *América Latina, crimen organizado e inseguridad ciudadana* (No. ARI 154/2024). Real Instituto Elcano.

Naciones Unidas en Ecuador. (2024). Ecuador fortalece la cooperación con la ONU para combatir al crimen organizado transnacional. *Naciones Unidas en Ecuador*. https://n9.cl/2vucj

Nascimento, P., & Procopiuck, M. (2023). COVID-19 in Latin America: Informal settlements and the politics of urbicide. *GeoJournal*, 88(3), 2609-2622. https://doi.org/10.1007/s10708-022-10765-7

Ochoa, R., Rodríguez, J. L., & Díaz, J. (2024). Evolución del PIB y factores de crecimiento en Ecuador (2018-2021). *X-Pedientes Económicos,* 8(19), 172-194.

OEA (Asamblea General de la Organización de Estados Americanos). (2003). *Declaración sobre seguridad en las Américas* (No. CES/dec 1/03 rev.1). OEA.

OECO (Observatorio Ecuatoriano de Crimen Organizado). (2023). Boletín anual de homicidios intencionales en Ecuador: Análisis de las estadísticas finales del año 2023. *Pan American Development Foundation (PADF).* https://n9.cl/wv0kt

ONU Mujeres, PNUD, & UNFPA. (2023). *Programa regional de la Iniciativa Spotlight para América Latina*. ONU Mujeres. https://n9.cl/aqbar

Pastrana, E., Cabrera, F., & Sand, J. (Eds.). (2023). *Estrategias de seguridad ambiental en América Latina y el Caribe: Construyendo resiliencia.* Konrad Adenauer Stiftung. https://n9.cl/dud85

PNUD. (1994). *Human development report 1994.* Oxford University Press.

PNUD Costa Rica, & IIDH. (2011). *Taller Seguridad Humana en América Latina: Memoria, San José, Costa Rica 17 y 18 de mayo de 2011*. PNUD – IIDH. https://www.iidh.ed.cr/IIDH/media/1563/taller-memoria-2011.pdf

PNUD. (2013). *Informe regional de desarrollo humano 2013-2014: Seguridad ciudadana con rostro humano: Diagnóstico y propuestas para América Latina*. UNDP. https://www.undp.org/es/latin-america/publicaciones/informe-regional-de-desarrollo-humano-2013-2014

PNUD Ecuador. (2024). *Impactos del proyecto «Capacidades para la paz, la seguridad y la reducción de las violencias en el Ecuador—Construimos Paz»*. UNDP. https://n9.cl/66ho4

PNUD. (s. f.). *Capacidades para la paz, la seguridad y la reducción de las violencias en Ecuador*. PNUD. https://n9.cl/lxrpj

PNUD. (2022). *Informe especial 2022: Las nuevas amenazas para la seguridad humana en el Antropoceno exigen una mayor solidaridad: Panorama general.* https://hdr.undp.org/system/files/documents/srhs2022overviewes.pdf

PNUD. (2024). Human development report 2023/2024: *Breaking the gridlock, reimagining cooperation in a polarized world*. https://hdr.undp.org/content/human-development-report-2023-24

Primicias. (2024, febrero 18). Así funcionan e impactan las economías criminales en el Ecuador. *Revista Gestión Digital – Primicias.* https://revistagestion.primicias.ec/analisis-economia-y-finanzas/asi-funcionan-e-impactan-las-economias-criminales-en-el-ecuador

Quilli-Granda, K., & García-Vélez, D. (2023). Efectos del COVID-19 en la pobreza multidimensional del Ecuador durante el período

2019-2020. *Estudios de la Gestión: Revista Internacional de Administración*, 15, 173-192. https://doi.org/10.32719/25506641.2024.15.8

Rodríguez, C., Realuyo, C., & Patiño, M. (2024). El impacto de las economías ilícitas en el contexto del crimen organizado en Ecuador. *TAMBARA, 25*(136), 2140-2159.

Sanahuja, J. A., & Mila-Maldonado, A. (2024). *La inseguridad ciudadana y los riesgos para la democracia en América Latina*. Fundación Carolina. https://n9.cl/6yoiw

Serrano, P. (2022). Cómo Ecuador protege los bosques en la Amazonía. *UNDP*. https://www.undp.org/es/latin-america/blog/como-ecuador-protege-los-bosques-en-la-amazonia

Sorj, B. (2005). Seguridad, seguridad humana y América Latina. *Sur: Revista Internacional de Derechos Humanos*, 3(2), 40-59.

Tadjbakhsh, S., & Chenoy, A. (2007). *Human security: Concepts and implications*. Routledge. https://www.taylorfrancis.com/books/mono/10.4324/9780203965955/human-security-shahrbanou-tadjbakhsh-anuradha-chenoy

USCRI (U.S. Committee for Refugees and Immigrants). (2025). *2025 country conditions: Ecuador*. https://refugees.org/wp-content/uploads/2025/04/2025-Country-Conditions-Ecuador.pdf

Verdes, F. (2019). La (re)militarización de la política latinoamericana: Origen y consecuencias para las democracias de la región. *Documentos de Trabajo – Fundación Carolina, 2.ª época* (14), 1-14. https://dialnet.unirioja.es/servlet/articulo?codigo=7097498

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

La inteligencia artificial como arma de dominación global: ¿Quién controla la seguridad humana en el siglo XXI?

Artificial intelligence as a weapon of global domination: Who controls human security in the 21st century?

Recibido: 29/ 05 / 2025 | Revisado: 23 / 07 / 2025 | Aprobado: 17 / 09 / 2025
DOI: https://doi.org/10.59794/rscd.2025.v11i11.151

Brigadier general (r) Fabricio Cabrera Ortiz, ENC
Colombia

Correo: facaor@gmail.com

ORCID:https://orcid.org/0000-0002-7065-7943

Afiliación: Universidad Nacional de Colombia

Brigadier general de la Reserva del Ejército Nacional de Colombia, del arma de Caballería. Doctor en Seguridad Internacional del Instituto Universitario General Gutiérrez Mellado de la Universidad Nacional de España. Cuenta con doble maestría en Estudios Políticos y en Seguridad y Defensa Nacionales, Profesional en Ciencias Militares. Especialista en Relaciones Internacionales, Administración de Recursos Militares y Gerencia del Talento Humano. Profesor universitario en la Pontificia Universidad Javeriana e investigador del Instituto de Estudios Urbanos de la Universidad Nacional de Colombia. Durante seis años, dirigió el Curso de Altos Estudios Militares y el Curso Integral de Defensa Nacional en la Escuela Superior de Guerra. Es editor de múltiples libros y publicaciones especializadas en estrategia, seguridad y defensa nacional. Actualmente, se desempeña como consultor internacional en seguridad, aportando su visión estratégica y experiencia a instituciones públicas y privadas dentro y fuera del país.

Resumen

Este ensayo examina cómo la inteligencia artificial (IA) se ha convertido en una herramienta de dominación global que afecta profundamente la seguridad humana. A través de un enfoque multidimensional –que abarca aspectos económicos, personales, comunitarios, ambientales, políticos, alimentarios y sanitarios– se analiza cómo la IA reproduce desigualdades históricas y refuerza nuevas formas de poder. El artículo identifica cuatro vectores de amenaza: el sesgo geopolítico, la supremacía tecnológica del Norte Global, el uso de IA en conflictos híbridos, y la privatización de la seguridad a través de algoritmos. Se expone cómo América Latina enfrenta una doble condición de vulnerabilidad: dependencia digital y debilidad institucional. Además, se advierte sobre la erosión de derechos fundamentales ante el uso de sistemas automatizados opacos. Finalmente, se plantea la necesidad de una soberanía tecnológica regional basada en marcos éticos, capacidades propias y regulación democrática.

Palabras clave: Inteligencia artificial, seguridad humana, control algorítmico, soberanía digital, conflictos híbridos

Abstract

This essay examines how artificial intelligence (AI) has become a tool of global domination that profoundly affects human security. Through a multidimensional approach, one which encompasses economic, personal, community, political, food and health aspects, it analyses how AI reproduces historical inequalities and reinforces new forms of power. The article identifies four threat vectors: geopolitical bias, the technological supremacy of the Global North, the use of AI in hybrid conflicts, and the privatization of security through algorithms. It highlights how Latin America faces a double condition of vulnerability: digital dependence and institutional weakness. In addition, it warns about the erosion of fundamental rights in the use of opaque automated systems. Finally, it argues for the urgent need to build regional technological sovereignty grounded in ethical frameworks, local capacities, and democratic regulation.

Keywords: Artificial intelligence, human security, algorithmic control, digital sovereignty, hybrid conflicts

Introducción

Durante las últimas décadas, la inteligencia artificial (IA) ha sido presentada por gobiernos, empresas tecnológicas y organismos multilaterales como el catalizador de una nueva era de desarrollo humano. La promesa de automatizar procesos, optimizar decisiones y resolver problemas complejos ha sido abrazada con entusiasmo en sectores tan diversos como la salud, la educación, el transporte, la justicia y la seguridad. Bajo esta narrativa tecnoptimista, la IA aparece como una herramienta universalmente beneficiosa, una suerte de "inteligencia aumentada" puesta al servicio del progreso social.

Sin embargo, este discurso oculta dimensiones mucho más problemáticas. Numerosas investigaciones (Zuboff, 2019; Eubanks, 2018) han advertido que la expansión acelerada de sistemas algorítmicos se está realizando sin controles democráticos, sin transparencia en su funcionamiento y sin marcos éticos adecuados. Lejos de democratizar el conocimiento, la IA está reforzando estructuras de poder preexistentes, exacerbando desigualdades, socavando derechos fundamentales y propiciando nuevas formas de control social.

La centralización de datos, la opacidad de los algoritmos y la concentración del poder tecnológico en manos de un puñado de corporaciones y Estados han abierto la puerta a una distopía algorítmica: un modelo de gobernanza no deliberativa, en el que las decisiones sobre seguridad, movilidad, salud o ciudadanía no son tomadas por personas, sino por modelos matemáticos entrenados con sesgos históricos y diseñados con lógicas económicas utilitarias. Como señala Harari (2018), el control sobre los flujos de datos se ha convertido en la nueva fuente de poder global, desplazando a la soberanía territorial tradicional.

Esta evolución tecnológica plantea interrogantes de gran calado para la seguridad humana. ¿Quién controla los algoritmos que deciden qué es una amenaza? ¿Qué impacto tiene el uso de IA en contextos militarizados, autoritarios o desiguales? ¿Puede una tecnología no regulada comprometer los principios básicos de la dignidad humana, la libertad y la autodeterminación colectiva?

Este artículo se propone analizar la IA no como una herramienta neutral, sino como una tecnología política. Aborda su potencial de convertirse en un instrumento de dominación global que socava la seguridad humana en sus múltiples dimensiones: desde la económica hasta la política, desde la comunitaria hasta la personal. Lo hace desde un enfoque multidimensional e interdisciplinario, combinando estudios críticos de tecnología, geopolítica de los datos, derecho internacional de los derechos humanos y teoría de la seguridad. La tesis central es disruptiva: si la IA no se democratiza, regulariza y socializa, podría consolidar un nuevo régimen de poder silencioso, tecnocrático y global, que trascienda incluso las capacidades de vigilancia de los Estados autoritarios del siglo XX.

Desarrollo

Marco conceptual: seguridad humana e inteligencia artificial

El concepto de seguridad humana surge en la década de los noventa como respuesta a los límites del paradigma tradicional de seguridad centrado en el Estado y la amenaza militar externa. Propuesto formalmente en el Informe sobre Desarrollo Humano del Programa de las Naciones Unidas para el Desarrollo (PNUD, 1994), este enfoque desplaza el centro de gravedad hacia el individuo y reconoce que la inseguridad puede derivarse tanto de la violencia directa como de carencias estructurales, exclusión social o situación de vulnerabilidad tecnológica. La seguridad humana comprende siete dimensiones interdependientes: económica, alimentaria, sanitaria, ambiental, personal, comunitaria y política.

Desde esta perspectiva, la seguridad ya no se limita a la ausencia de guerra, sino que implica la posibilidad de vivir sin miedo ni miseria, con acceso a los bienes fundamentales y con plena garantía de derechos. Esta reconceptualización exige, por tanto, un enfoque holístico e interdisciplinario para abordar las amenazas contemporáneas que afectan la vida cotidiana de las personas.

En este marco, la inteligencia artificial representa una amenaza emergente que no encaja fácilmente en las categorías convencionales de análisis. Su carácter difuso, su capacidad de operar de manera transnacional y su implementación muchas veces silenciosa la convierten en un desafío inédito. La IA puede afectar simultáneamente múltiples dimensiones de la seguridad humana: puede propiciar desempleo estructural (seguridad económica), facilitar la desinformación masiva (seguridad política), amplificar patrones de discriminación algorítmica (seguridad personal y comunitaria) y erosionar la soberanía informativa (seguridad política).

De igual modo, la naturaleza predictiva y automatizada de muchos sistemas de IA desafía los principios de agencia humana y deliberación democrática. Las decisiones que antes requerían responsabilidad pública –como conceder un crédito, vigilar a un sospechoso, asignar un recurso o autorizar un tratamiento médico– ahora pueden ser delegadas a sistemas entrenados con datos históricos, plagados de sesgos estructurales (Noble, 2018 ; Eubanks, 2018) .

Por otro lado, desde una perspectiva geopolítica, la concentración de capacidades en unos pocos actores globales configura una nueva forma de poder estructural, en el cual la soberanía tecnológica se vuelve esencial para preservar la autonomía política y el bienestar social. Así como el control del petróleo definió la geopolítica del siglo XX, el control de los datos y la capacidad de procesamiento algorítmico definen la del siglo XXI (Morozov, 2012).

Este artículo parte entonces de un marco conceptual que articula tres nociones clave: (1) Seguridad humana, como paradigma que centra la atención en los derechos, libertades y necesidades vitales de las personas. (2) IA como tecnología política, cuyo desarrollo, diseño y aplicación están atravesados por relaciones de poder. (3) Soberanía digital, entendida como la capacidad de los Estados y pueblos para ejercer control legítimo sobre sus infraestructuras tecnológicas, sus datos y

las decisiones automatizadas que afectan a su población.

Desde esta perspectiva, el análisis que sigue identifica cómo la IA, en su uso actual, compromete estos tres pilares y configura nuevas formas de inseguridad estructural. No se trata simplemente de una disfunción tecnológica, sino de una arquitectura de dominación en construcción, donde los algoritmos reemplazan a las armas como instrumentos de control, exclusión o sumisión.

Inteligencia artificial y sesgo geopolítico: una herramienta de poder global

La inteligencia artificial, a menudo presentada como un avance universal y objetivo, es en realidad una tecnología profundamente geopolítica. Su desarrollo, implementación y gobernanza no solo están determinados por capacidades técnicas, sino por relaciones asimétricas de poder, intereses estratégicos y modelos ideológicos de sociedad. Desde sus inicios, la IA ha sido monopolizada por un grupo reducido de actores globales –principalmente empresas estadounidenses y chinas–, cuyas agendas comerciales y geoestratégicas terminan imponiendo estándares tecnológicos y normas de facto sobre el resto del mundo (Kwet, 2019).

Esta concentración de poder tecnológico produce lo que se podría llamar un sesgo geopolítico estructural. A diferencia del sesgo algorítmico clásico –aquél que refleja prejuicios en los datos o en la programación–, el sesgo geopolítico se refiere al control de las infraestructuras, los marcos normativos y las arquitecturas de decisión globales. En otras palabras, no solo los algoritmos pueden discriminar, sino también las condiciones globales de su producción y circulación.

Hoy, más del 90 % de la infraestructura de cómputo en la nube, las plataformas de aprendizaje automático y los centros de datos están en manos de empresas del Norte Global (Google, Amazon, Microsoft, Baidu, Tencent, Alibaba). Esto implica que los datos de miles de millones de personas del Sur Global son procesados, almacenados y monetizados fuera de sus países, sin garantías de soberanía informativa, sin acceso al conocimiento derivado de esos datos, y sin mecanismos de reparación en caso de abusos.

Así mismo, muchas de las arquitecturas algorítmicas están diseñadas con lógicas que responden a contextos culturales, jurídicos o económicos propios del Norte, pero son exportadas e impuestas como soluciones universales. Por ejemplo, los sistemas de reconocimiento facial desarrollados en China –basados en vigilancia masiva y control estatal– han sido implementados en países de África, Asia Central y América Latina con escaso escrutinio y sin garantías democráticas. Del mismo modo, empresas de Silicon Valley como Palantir Technologies proveen sistemas de inteligencia predictiva a agencias de seguridad en Latinoamérica, importando algoritmos entrenados en contextos de racismo estructural y vigilancia masiva (Feldstein, 2025).

Este sesgo geopolítico se manifiesta también en el desarrollo de normas internacionales. Las principales iniciativas sobre gobernanza de la IA –como el AI Act en Europa, las pautas de la OCDE o los marcos de la UNESCO– están diseñadas en espacios donde los países del Sur Global tienen escasa voz o capacidad de incidencia. A menudo se asume que los principios éticos son "neutrales", cuando en realidad reflejan prioridades de actores dominantes.

La IA, en ese sentido, está configurando un nuevo orden internacional basado en la asimetría cognitiva y decisional. Quienes controlan los datos y los algoritmos vigilan también las formas de ver, clasificar, predecir e intervenir el mundo. Esto tiene consecuencias profundas para la autodeterminación de los pueblos, para la justicia global y para la seguridad humana. América Latina, en particular, corre el riesgo de ser reducida a una región extractiva de datos –como lo fue de recursos naturales– y a un laboratorio de experimentación algorítmica. Sin capacidad local de auditoría, sin soberanía normativa, sin independencia tecnológica, los países de la región enfrentan una situación de colonización digital silenciosa.

Por lo anterior, es necesario reconceptualizar la IA como un instrumento geopolítico de poder blando, pero también de control duro, que opera mediante infraestructuras invisibles y decisiones automatizadas. El sesgo geopolítico no es un accidente, sino una característica estructural de un sistema tecnológico global que reproduce la desigualdad bajo una nueva forma: el dominio algorítmico.

Supremacía tecnológica y dependencia digital del Sur Global

La noción de supremacía tecnológica se refiere al dominio sostenido que ejercen ciertos actores –ya sean Estados, conglomerados empresariales o alianzas transnacionales– sobre los recursos estratégicos, las infraestructuras, los sistemas de innovación y las capacidades normativas en el ámbito de la tecnología. En el caso de la inteligencia artificial (IA), este dominio se manifiesta en términos de liderazgo técnico o comercial, y también en la capacidad de establecer estándares, definir problemas, priorizar agendas de investigación y condicionar la adopción global de soluciones automatizadas (Mazzucato, 2019).

Esta supremacía tiene un correlato directo, la dependencia digital estructural del Sur Global. A diferencia de las brechas tecnológicas convencionales, que pueden ser abordadas con políticas de conectividad o alfabetización digital, la dependencia digital implica una subordinación funcional a sistemas, plataformas y arquitecturas que escapan al control local. En palabras de Couldry y Mejías (2019), asistimos a una nueva forma de colonialismo, donde los datos –el recurso estratégico del siglo XXI– son extraídos de forma masiva sin control soberano, utilizados por plataformas globales para fines comerciales, de seguridad o control social, muchas veces en detrimento del interés público local.

América Latina representa un caso paradigmático de esa dependencia. La región importa casi la totalidad de sus sistemas operativos, servidores, plataformas digitales, software (programa anti-plagio) de IA y servicios de computación en la nube. Las grandes corporaciones tecnológicas que operan en el continente no están sujetas a regulaciones estrictas ni pagan impuestos proporcionales a su volumen de negocio. La región no cuenta con capacidades autónomas de desarrollo de hardware (equipo informático o componentes físicos) ni con centros de supercómputo de escala global, lo que la condena a ser consumidora de tecnologías "listas para usar" desarrolladas bajo lógicas ajenas a sus contextos sociales y culturales.

Esta situación propicia múltiples riesgos:

1. Soberanía informativa limitada: los gobiernos y las instituciones públicas no tienen control efectivo sobre los datos que se producen dentro de sus territorios, lo

que compromete la planificación, la toma de decisiones y la seguridad nacional.

2. Vulnerabilidad estratégica: la dependencia de infraestructuras críticas alojadas en el extranjero deja expuestos a los Estados frente a bloqueos, espionaje, manipulación de sistemas o restricciones geopolíticas.

3. Imposición de arquitecturas opacas: los sistemas automatizados adoptados sin auditoría local, por ejemplo, para salud pública, educación, justicia penal o subsidios sociales, pueden contener sesgos, errores o lógicas que refuercen la exclusión en lugar de resolverla (Eubanks, 2018).

4. Desigualdad cognitiva: la falta de capacidades locales para interpretar, adaptar o construir modelos de IA propios genera una brecha epistémica profunda, en la que los países del Sur quedan relegados al consumo pasivo de tecnologías que no comprenden ni controlan.

Frente a este panorama, algunos autores advierten que estamos transitando hacia una geopolítica de la inteligencia artificial análoga a la de los recursos energéticos del siglo XX. Así como el control del petróleo permitió a ciertos Estados condicionar el desarrollo de otros, hoy el control de los datos, los algoritmos y las plataformas configura nuevas relaciones de dependencia y dominación (Morozov, 2012).

En ese sentido, la lucha por la soberanía tecnológica no es un lujo ni una aspiración idealista: es una necesidad urgente para garantizar la autonomía estratégica, la seguridad humana y la justicia social en el siglo XXI. La región necesita invertir en capacidades locales de desarrollo de IA, promover redes regionales de cooperación científica y establecer políticas públicas que prioricen el interés general sobre los intereses de mercado. Sin estas acciones, el Sur Global seguirá atrapado en una arquitectura tecnológica diseñada por otros, para otros, y muchas veces en su contra.

IA EN CONFLICTOS HÍBRIDOS: ARMAS SILENCIOSAS EN GUERRAS NO DECLARADAS

En la era digital, las guerras no siempre se libran con balas. La noción de conflicto híbrido ha emergido como una categoría clave para comprender las formas contemporáneas de confrontación entre Estados, actores no estatales y coaliciones transnacionales. Estos conflictos combinan medios militares tradicionales con operaciones cibernéticas, campañas de desinformación, sabotaje digital, presión económica y manipulación algorítmica de la opinión pública. En este nuevo campo de batalla, la inteligencia artificial se ha convertido en un arma silenciosa, ubicua y cada vez más autónoma.

Uno de los elementos más preocupantes sobre el uso de IA en conflictos híbridos es su capacidad para realizar acciones ofensivas sin supervisión humana directa. En 2021, un informe del Panel de Expertos del Consejo de Seguridad de la ONU (Organización de Naciones Unidas) reveló que un dron autónomo de combate habría atacado a un objetivo humano en Libia sin intervención humana, marcando un hito inquietante en la automatización letal (United Nations, 2021). Aunque el caso aún produce debate, lo cierto es que el desarrollo de sistemas de armas autónomas letales (LAWS, por sus siglas en inglés) plantea desafíos jurídicos y éticos de gran magnitud.

Por otra parte, la IA ha sido integrada de forma creciente en operaciones de ciberinteligencia y guerra informacional. Algoritmos de aprendizaje automático son utilizados para diseñar campañas de desinformación hipersegmentadas, manipular narrativas públicas mediante bots (robots de cuentas automatizadas) y trolls (robots de usuarios reales), generar deepfakes (falsificaciones profundas o ultrafalsos) indistinguibles de la realidad y detectar patrones de conducta en opositores políticos o líderes sociales. Estas tácticas al igual que se emplean entre potencias globales, también han sido adaptadas por grupos armados, empresas de seguridad privada e incluso gobiernos autoritarios en contextos locales.

El caso de Cambridge Analytica (Carole y Graham-Harrison, 2018), donde millones de perfiles de Facebook fueron utilizados para influir electoralmente mediante IA, es apenas la punta del iceberg. En América Latina, existen reportes crecientes sobre el uso de algoritmos para vigilancia masiva de opositores, monitoreo predictivo de protestas sociales, y diseminación de noticias falsas durante procesos electorales. Lo preocupante es que muchas veces estas herramientas se adquieren bajo contratos confidenciales, sin supervisión parlamentaria ni debate ciudadano.

Desde la perspectiva de la seguridad humana, la implicación de la IA en conflictos híbridos introduce amenazas profundas a la libertad de expresión, al derecho a la protesta, al acceso a la información veraz y a la privacidad. Además, su uso puede derivar en acciones encubiertas que socaven la soberanía de los Estados, afecten la estabilidad política o exacerben conflictos sociales preexistentes.

En este nuevo escenario bélico, los adversarios ya no necesitan invadir territorios ni derramar sangre para obtener ventajas estratégicas. Pueden desestabilizar democracias, paralizar servicios públicos, deslegitimar liderazgos o sembrar el caos informativo desde la distancia, con bajo costo y alta eficacia. La IA convierte la información en una munición de precisión y convierte la invisibilidad en ventaja táctica.

Frente a este panorama, la región de América Latina y el Caribe se encuentra en una situación crítica. La falta de capacidades técnicas para detectar, mitigar o responder a estas amenazas, sumada a la escasa integración regional en materia de ciberdefensa, deja a los países expuestos a una nueva generación de guerras invisibles. Es urgente incorporar la dimensión algorítmica y cognitiva en las doctrinas de defensa nacional y diseñar políticas públicas que regulen el uso de IA en contextos de seguridad interna, defensa y orden público. La IA en conflictos híbridos no es una amenaza futura: ya está aquí. Y su espacio de operaciones no son solo los campos de batalla, sino las redes, las emociones, las narrativas y los sistemas automatizados que organizan nuestra vida cotidiana.

Privatización de la seguridad: algoritmos que deciden quién es una amenaza

La seguridad, tradicionalmente concebida como una función esencial del Estado, ha experimentado en las últimas décadas un proceso de externalización y privatización progresiva. Este fenómeno ha sido impulsado por el auge de las empresas de seguridad privada, el outsourcing de funciones militares y de inteligencia, y más recientemente, por la incorporación de tecnologías emergentes gestionadas por corporaciones tecnológicas globales. En este contexto, la inteligencia artificial no solo ha transformado la manera cómo se concibe la seguridad, sino también quién la controla y cómo se ejerce.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Uno de los elementos más disruptivos es la proliferación de sistemas de vigilancia predictiva, también conocidos como "predictive policing". Estos sistemas se basan en algoritmos entrenados con grandes volúmenes de datos históricos –muchas veces cargados de sesgos raciales, geográficos o socioeconómicos– para anticipar comportamientos considerados riesgosos. Como han demostrado diversos estudios (Brantingham, Valasik y Mohler, 2018), esta lógica tiende a replicar patrones de discriminación estructural, ubicando a ciertas comunidades bajo sospecha permanente y reproduciendo lo que se ha denominado "racismo algorítmico".

A esta problemática se suma el hecho de que muchos de estos sistemas son desarrollados, operados o licenciados por empresas privadas, cuyas prioridades responden a intereses comerciales, no necesariamente a principios democráticos, derechos humanos o transparencia institucional. Empresas como Palantir Technologies, ShotSpotter o Clearview AI han vendido sus productos a agencias policiales, migratorias y militares en América Latina, sin que exista una normativa clara que regule su uso, audite sus impactos o garantice rendición de cuentas (AI Now Institute, 2021).

La privatización de la seguridad a través de la IA también implica un deslizamiento funcional: algoritmos que antes servían para recomendaciones comerciales o segmentación de clientes son ahora utilizados para establecer perfiles de riesgo, gestionar fronteras, determinar prioridades de patrullaje o decidir si una persona merece vigilancia adicional. Esta lógica de "seguridad como servicio" no solo transforma las capacidades estatales, sino que plantea dilemas éticos sobre la delegación de decisiones que afectan derechos fundamentales a entidades opacas, automatizadas y sin responsabilidad legal.

El riesgo más profundo es que se consolide una arquitectura de vigilancia algorítmica en la que los Estados actúan como simples consumidores de tecnología, mientras que las grandes plataformas definen unilateralmente cuáles conductas son sospechosas, cuáles territorios deben ser vigilados y cuáles poblaciones son peligrosas. Este modelo erosiona el principio republicano de que la seguridad debe estar sometida al imperio de la ley, al control democrático y al respeto por los derechos humanos.

En América Latina, esta tendencia es particularmente peligrosa debido a tres factores: (1) la debilidad institucional para regular el uso de tecnologías emergentes, (2) la alta desigualdad social que amplifica los impactos discriminatorios de los algoritmos, y (3) la fragmentación del sistema judicial que impide establecer mecanismos eficaces de reparación ante violaciones.

Por su parte, la privatización algorítmica de la seguridad puede facilitar nuevas formas de autoritarismo tecnológico. Gobiernos que enfrentan descontento social o crisis de legitimidad pueden utilizar estas herramientas para vigilar opositores, anticipar protestas o reprimir movimientos sociales bajo el pretexto de mantener el orden. La frontera entre seguridad y represión preventivas se diluye peligrosamente cuando las decisiones son tomadas por modelos matemáticos entrenados con datos sesgados.

Frente a este escenario, se requiere una doctrina pública de seguridad digital y algorítmica que recupere el control estatal, garantice los principios de legalidad y proporcionalidad, y prohíba la adopción de tecnologías que no sean auditables, explicables y respetuosas de los derechos humanos. La seguridad no puede estar gobernada por cajas negras. Ni por mercados. Debe estar regida por la ética, la ley y la deliberación democrática.

Implicaciones para América Latina y el Caribe

América Latina y el Caribe se encuentran en un punto de inflexión frente al avance acelerado de la inteligencia artificial y su penetración en los distintos ámbitos de la vida pública y privada. A diferencia de otras regiones que han logrado posicionarse como productoras de tecnología, la región latinoamericana continúa siendo, en gran medida, una importadora neta de sistemas, plataformas y soluciones algorítmicas diseñadas en contextos culturales, políticos y económicos distintos. Esta situación conlleva riesgos no solo tecnológicos, sino también políticos, jurídicos, sociales y estratégicos.

El principal problema no es la adopción de la tecnología en sí, sino la ausencia de un marco soberano, ético y estratégico para guiar su incorporación. Como advierten Couldry y Mejías (2019), el Sur Global enfrenta una nueva forma de colonialismo: el colonialismo de datos, mediante el cual las infraestructuras digitales y los sistemas de inteligencia artificial se imponen sin control soberano, extrayendo valor informacional para intereses externos. América Latina se enfrenta así a una doble condición de vulnerabilidad estructural: por un lado, la carencia de capacidades locales de diseño, auditoría y desarrollo de IA; por otro, la exposición creciente a sistemas de control automatizado que pueden ser utilizados para fines autoritarios, extractivos o discriminatorios.

Entre las principales implicaciones que se derivan para la región se destacan las siguientes:

a. Riesgo de colonización digital

La región puede convertirse en un nuevo laboratorio de experimentación para tecnologías de vigilancia, control social y gestión algorítmica importadas del Norte Global. Esto ya se ha observado en la instalación de sistemas de reconocimiento facial en espacios públicos sin debate ciudadano ni estudios de impacto en derechos fundamentales, como ha ocurrido en ciudades de Argentina, Brasil y México. La imposición silenciosa de estas tecnologías puede replicar lógicas coloniales bajo una nueva fachada: la dependencia algorítmica.

b. Erosión de la soberanía informativa

El almacenamiento y procesamiento de datos personales, financieros, biométricos y conductuales de millones de ciudadanos en infraestructuras alojadas fuera de la región impide el ejercicio efectivo de soberanía. Esto compromete la capacidad de los Estados para proteger a sus poblaciones, tomar decisiones basadas en evidencia local y garantizar el cumplimiento de normas nacionales de privacidad y seguridad.

c. Fragmentación institucional y desarticulación regional

La falta de políticas públicas integrales sobre IA, sumada a la escasa cooperación entre países latinoamericanos, dificulta el desarrollo de respuestas comunes. Mientras potencias como China, Estados Unidos y Unión Europea definen estrategias nacionales y bloques normativos sobre IA, en América Latina predominan las iniciativas aisladas, los vacíos legales y la dependencia de estándares externos.

d. Amplificación de las desigualdades internas

La IA no actúa en el vacío: se alimenta de los datos disponibles y reproduce los sesgos existentes en la sociedad. En regiones marcadas

por profundas desigualdades socioeconómicas, raciales y de género, el uso acrítico de sistemas algorítmicos puede reforzar exclusiones históricas y consolidar nuevas formas de discriminación automática. Esto es especialmente grave en el ámbito de los servicios públicos, la justicia penal, la asistencia social y la seguridad ciudadana.

e. Condición de vulnerabilidad frente a amenazas híbridas

Como se argumentó anteriormente, la IA es ya un componente central de los conflictos híbridos y de las estrategias de guerra informacional. América Latina, con sistemas de ciberdefensa incipientes y escasa capacidad de detección, se encuentra particularmente expuesta a operaciones de desinformación, manipulación electoral, sabotaje digital y espionaje algorítmico. La ausencia de protocolos conjuntos de respuesta amplifica esta amenaza.

Frente a este escenario, es urgente que América Latina y el Caribe desarrollen una agenda regional de soberanía digital e inteligencia artificial, articulada sobre tres ejes estratégicos:

a. Normativo: elaboración de marcos jurídicos comunes que regulen el uso de la IA en función del interés público, los derechos humanos y la transparencia algorítmica. Esto incluye establecer principios de explicabilidad, auditoría externa, proporcionalidad y no discriminación.

b. Institucional: fortalecimiento de capacidades estatales para supervisar, auditar y eventualmente producir tecnologías propias, mediante agencias nacionales y redes de cooperación regional.

c. Epistémico: promoción de una visión latinoamericana de la IA que reconozca las especificidades culturales, sociales y económicas de la región, y que impulse un pensamiento tecnológico descolonizador, autónomo y orientado al bienestar colectivo.

Solo así será posible enfrentar el nuevo orden algorítmico global con dignidad, justicia y autodeterminación. La región no puede resignarse a ser un consumidor pasivo de tecnologías ajenas. Debe convertirse en actor, en creador y en garante de una IA ética, soberana y profundamente humana.

Conclusiones

¿Seguridad humana o algoritmos de control?

La inteligencia artificial se ha convertido en un elemento constitutivo del poder global contemporáneo. Ya no es simplemente una herramienta técnica, sino una arquitectura invisible que organiza flujos de información toma decisiones automatizadas y moldea conductas individuales y colectivas. Esta transformación no es neutra: está cargada de relaciones de poder, conflictos de interés, lógicas de mercado y estrategias de dominación. En este contexto, la pregunta que da título a esta conclusión se vuelve urgente: ¿Nos dirigimos hacia un horizonte de seguridad humana potenciada por la tecnología, o hacia un modelo de control algorítmico que erosiona nuestras libertades fundamentales?

A lo largo de este artículo se ha argumentado que, en su configuración actual, la IA no solo no garantiza la seguridad humana, sino que amenaza sus fundamentos. La concentración del poder tecnológico en manos de un puñado de actores, la opacidad de los sistemas de decisión automatizados, la externalización de

funciones soberanas a empresas privadas y el uso creciente de IA en conflictos híbridos y en contextos de vigilancia social, configuran un escenario de inseguridad estructural global.

Desde una perspectiva crítica, la IA no puede ser tratada como una herramienta meramente técnica, ni como un destino inevitable. Es, ante todo, un campo de disputa: una construcción política y social que puede ser orientada hacia fines emancipadores o hacia formas cada vez más sofisticadas de control, exclusión y subordinación. La alternativa entre seguridad humana o algoritmos de control no es una disyuntiva tecnológica, sino profundamente ética y geopolítica.

América Latina y el Caribe, como parte del Sur Global, enfrentan el desafío histórico de no repetir la lógica de dependencia que caracterizó su relación con los recursos naturales, el capital financiero o las tecnologías industriales del siglo XX. La región tiene la oportunidad –y la obligación– de construir una soberanía digital basada en principios democráticos, derechos humanos, justicia social y cooperación regional. Esto implica no solo regular y limitar los riesgos de la IA, sino también imaginar y producir formas alternativas de inteligencia tecnológica centradas en el cuidado de la vida, el bien común y la dignidad humana.

Para ello, se requieren políticas públicas integrales, instituciones fuertes, marcos jurídicos sólidos, capacidad científica local, pensamiento crítico y voluntad política. La IA no es en sí misma ni buena ni mala: su significado dependerá del proyecto civilizatorio al que se adscriba. Lo que está en juego no es solo la eficiencia de los servicios públicos o la competitividad económica, sino el tipo de sociedad que queremos construir.

En última instancia, el poder de los algoritmos debe estar subordinado al de los pueblos. La seguridad humana, entendida desde su enfoque multidimensional –económica, alimentaria, sanitaria, ambiental, personal, comunitaria y política– no puede ser delegada a sistemas automatizados ni reducida a parámetros de eficiencia técnica. Estos algoritmos, si no son diseñados, regulados y supervisados bajo principios éticos y democráticos, corren el riesgo de erosionar las bases mismas de la dignidad humana. Por ello, es indispensable recuperar el sentido político, ético y humanista de la tecnología. Solo así será posible orientar la inteligencia artificial hacia un modelo civilizatorio que garantice libertad, justicia social y autodeterminación de los pueblos en el siglo XXI.

Referencias

AI Now Institute. (2021, 4 de diciembre). *Enfrentando las cajas negras: un informe paralelo del Grupo de Trabajo del Sistema de Decisiones Automatizadas de la Ciudad de Nueva York*. AI Now Institute. https://ainowinstitute.org/publications/confronting-black-boxes-a-shadow-report-of-the-new-york-city-automated

Brantingham, P. J., Valasik, M., y Mohler, G. O. (2018). ¿Conduce la vigilancia predictiva a arrestos sesgados? Resultados de un ensayo controlado aleatorio. *Statistics and Public Policy,* 1-6. https://www.tandfonline.com/doi/pdf/10.1080/2330443X.2018.1438940

Carole, C., y Graham-Harrison, E. (2018, 17 de mayo). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Couldry, N., y Mejias, U. A. (2019). Data colonialism: Rethinking Big Data's relation to the contemporary subject. *Television & New Media,* 20(4), 336–349. https://journals.sagepub.com/toc/tvna/20/4

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor.* St. Martin's Press.

Feldstein, S. (2025, 8 de mayo). *The global expansion of AI surveillance*. Carnegie Endowment for International Peace. https://carnegie-production-assets.s3.amazonaws.com/static/files/files_WP-Feldstein-AISurveillance_final1.pdf

Harari, Y. N. (2018). *Homo Deus*. Debate.

Kwet, M. (2019). Colonialismo digital: el imperio estadounidense y el nuev o imperialismo en el sur global. *Race & Class*, 60(4), 3-26.

Mazzucato, M. (2019). *El valor de las cosas: quién produce y quién gana en la economía*. Taurus.

Morozov, E. (2012). *The net delusion*. PublicAffairs.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. NYU Press.

Programa de las Naciones Unidas para el Desarrollo (PNUD). (1994). *Informe sobre desarrollo humano 1994.* Fondo de Cultura Económica de México.

United Nations. (2021, 8 de marzo). *Security Council: Letter dated 8 March 2021 from the Panel of Experts on Libya established pursuant to resolution 1973 (2011) addressed to the President of the Security Council*. https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E-4FF96FF9%7D/S_2021_229.pdf

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

Capital criminal, necroliberalismo y derechos humanos: Ecuador 2024

Criminal Capital, Necroliberalism and Human Rights: Ecuador of 2024

Recibido: 07/ 05 / 2025 | Revisado: 17 / 07 / 2025 | Aprobado: 16 / 09 / 2025
DOI: https://doi.org/10.59794/rscd.2025.v11i11.153

Dr. Bárbara Natalia Sierra Freire
Ecuador

Correo: bsierraf@puce.edu.ec

ORCID: https://orcid.org/0000-0002-8540-5343

Afiliación: Pontificia Universidad Católica del Ecuador

La autora es Profesora. Dr. Phil. Sociología. Universidad Libre de Berlín. Alemania. Licenciada en Sociología y Ciencias Política. Universidad Central del Ecuador. Coordinadora del Centro de Estudios Latinoamericanos en Ciencias Sociales y Humanidades PUCE 2023 hasta la fecha. Profesora. Escuela de Sociología PUCE. Profesora Maestría en Derechos Humanos. UASB. Profesora Maestría de Salud Pública PUCE. Profesora IAEN. Profesora Maestría Estudios Interdisciplinarios Universidad del Cauca Colombia. Profesora Especialización Medicina Familiar PUCE. Profesora Maestría de Desarrollo Local y Comunitario PUCE y Profesora del programa de Gobernabilidad para el Distrito Metropolitano de Quito, Ecuador entre otros. Autora de innumerables artículos y libros.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Resumen

Este artículo analiza el fenómeno del narcotráfico, la respuesta desde el Estado y sus efectos en la aceptación y aplicación social de los Derechos Humanos en la sociedad. Para tal propósito, acoge la perspectiva de la teoría crítica a partir de la articulación dialéctica de los conceptos capital criminal, necropolítica, y lucha social. En relación con este entramado teórico-conceptual, por medio de un análisis crítico de documentos oficiales, noticias confirmadas y opinión ciudadana en redes sociales, en el contexto ecuatoriano de la crisis de violencia ocurrida en enero de 2024, se establece la relación que existe entre la expansión de la violencia del narcotráfico, la implementación de un Estado represivo y aplicabilidad de los Derechos Humanos. Como resultado se plantea la implementación de una gubernamentalidad necroliberal funcional al avance del capital criminal, cuyo efecto inmediato es el retroceso de los derechos humanos tanto a nivel de la política estatal en la aplicación de la justicia como de la consciencia social.

Palabras clave: Derechos humanos, narcotráfico, capital criminal, necroliberalismo

Abstract

This article analyzes the phenomenon of drug trafficking, the response from the State and its effects on the acceptability and social application of Human Rights in society. To this end, he welcomes the perspective of critical theory based on the dialectical articulation of the concepts of criminal capital, necropolitics, and social struggle. In relation to this theoretical-conceptual framework, through a critical analysis of official documents, confirmed news and citizen opinion on social networks, in the Ecuadorian context of the violence crisis that occurred in January 2024, the relationship between the expansion of drug trafficking violence, the implementation of a repressive State and the applicability of Human Rights is established. As a result, the implementation of a necroliberal governmentality functional to the advance of criminal capital is proposed, whose immediate effect is the regression of human rights both at the level of state policy in the application of justice and of social consciousness.

Keywords: Human rights, drug trafficking, criminal capital, necroliberalism

Introducción

El narcotráfico es uno de los principales problemas que enfrenta América Latina, se extiende por todos los países y corrompe las instituciones político, jurídicas y sociales de las naciones latinoamericanas.

> El narcotráfico y el crimen organizado tienen enormes implicaciones para la seguridad y la democracia. Por un lado, minan la legitimidad del Estado, porque no es posible que estos fenómenos persistan en el tiempo sin la complicidad de sectores estatales involucrados en dinámicas de corrupción. Con ello, los altos niveles de impunidad son propios de sociedades en las que el narcotráfico y el crimen organizado se han instalado. Por otra parte, afectan desproporcionadamente a los sectores más vulnerables, principalmente jóvenes de bajos recursos, que engrosan las cifras de homicidios y personas privadas de la libertad. (Mantilla, 2023, p. 25)

El primer efecto visible de este fenómeno es la ampliación de la violencia criminal, producto de las operaciones de los grupos de delincuencia organizada (GDO) articulados al narcotráfico. La guerra entre GDO tiene como escenarios: las zonas rurales de producción, los centros penitenciarios de operaciones criminales y los barrios periféricos de reclutamiento. Cuando el nivel de conflicto avanza, la violencia se manifiesta en instituciones estatales de control como Policía, Fuerzas Armadas, Fiscalía y Tribunales de Justicia; en este momento se produce amenazas y asesinatos a policías, militares, fiscales, jueces y abogados. En un nivel más alto, la presencia del narcotráfico contamina la política electoral, amenaza y asesina a altos funcionarios públicos. Finalmente, la violencia del narcotráfico se manifiesta en toda la sociedad con ataques directos a la ciudadanía.

El proceso descrito tiene su verificación en la historia de Colombia desde los años 80, México desde los años 90 y del resto de países de la región desde principios de este siglo. Más allá de la violencia criminal y la corrupción, el crecimiento del narcotráfico y del capital que mueve en la región, hacen de esta actividad económica: "la industria más productiva en los nuevos tiempos" (Cadena, 2011, p. 46). En este contexto:

> ...el Ecuador resulta estratégico al encontrarse entre los dos principales productores de cocaína del mundo y su divisa es internacionalmente apetecida. Por tanto, las organizaciones dedicadas al tráfico de drogas ilícitas utilizan el territorio ecuatoriano como un punto de tránsito, acopio y envío a mercados internacionales". (Rivera-Rhon & Bravo-Grifalba, 2020, p. 17)

Esto explica por qué Ecuador se ha convertido en un territorio de alto interés para la economía del narcotráfico y las operaciones de los grandes GDO transnacional en articulación con los nacionales y locales.

El 19 de enero de 2024, un GDO nacional se asalta el canal de TV Televisión, retiene a sus empleados y trasmiten en vivo a todo el país y al mundo, generando pánico en la sociedad (Europa Press, 2024). Como respuesta, el Gobierno declara la existencia de un conflicto armado no internacional (CANI) y caracteriza a 22 GDO como terroristas; a partir de

esta declaración se crea el espacio político, jurídico y social para la aplicación de una serie de políticas gubernamentales, marcadamente autoritarias, destinadas a combatir al terrorismo que tienden a restringe derechos a la población.

En este contexto, este estudio trata la relación que existe entre el avance y consolidación del narcotráfico, la implementación de una política gubernamental altamente represiva y los efectos en la exigibilidad, aplicación y garantía de los DD. HH., tanto en la consciencia social cuanto, en el ejercicio de la justicia durante el primer gobierno del presidente Daniel Noboa en el año 2024. En especial apunta a definir la forma de operación de la economía del narcotráfico como un tipo de capital criminal imbricado con el movimiento general del capitalismo; el aparecimiento de una nueva gubernamentalidad vinculada al capital criminal que se caracteriza como necroliberalismo; y, el impacto que esta realidad económica y política tiene en la conciencia social sobre los derechos humanos y en su aplicabilidad por parte del Estado y la justicia.

El caso analizado cuenta con todos los elementos necesarios para establecer la relación entre los tres aspectos de interés. El Ecuador se ha convertido en un centro económico del narcotráfico en América Latina, hay una forma gubernamental que se ha desarrollado frente a esta economía y por, último, se ha generado una respuesta jurídica y un debate social en torno a esta realidad en relación a la validez y vigencia de los derechos humanos. El artículo se desarrolla en tres secciones: una primera que expone los conceptos principales que dan cuenta de los tres aspectos que integran la relación objeto de estudio. Una segunda que presenta el caso de estudio en el que se indagada la relación de interés y la metodología utilizada en la investigación. Finalmente, la tercera argumenta la relación existente entre capital criminal, necroliberalismo y derechos humanos.

Desarrollo

Aproximaciones teórico-conceptuales

Con el fin de exponer las estructuras de poder que subyacen en la triple relación (capital criminal, gubernamentalidad necroliberal y derechos humanos) dentro de un análisis que integra la economía, la política y la justicia en el marco del desarrollo y la transformación del modo de producción capitalista, es la teoría crítica el principal enfoque teórico. Para la economía política marxista, el capital es una relación social de producción que por medio de la explotación del trabajo vivo genera una ganancia que se incrementa y acumula constantemente. Esta relación social puede ser de carácter formal y legal o informal e ilegal, cuando sus actividades son exclusivamente ilegales lo convierten en capital criminal.

Integran las operaciones de la economía criminal: el capital productivo en el proceso directo de producción de las mercancías, el capital comercial en la distribución y comercialización de estas, y el capital financiero en el lavado de dinero para reinsertarlo en la economía formal. “En el sistema mundial capitalista, la economía criminal es uno de sus engranajes, no es un ámbito separado, marginal o anómalo, es consustancial a la lógica

de valorización del capital, que no tiene reparos éticos, legales o civilizatorios" (Márquez, 2020, p. 12). La economía del narcotráfico es una de las ramas más importantes del capital criminal (Gómez, 2018, p. 302), cuyas prácticas de corrupción y violencia consolidan el poder de clase del narco-capitalismo que involucra: industrias, financieras, representantes políticos del Estado y GDO, en articulaciones nacionales e internacionales.

El narcotráfico atraviesa los núcleos duros del funcionamiento del sistema capitalista mundial, a partir de una estructura económica y política expansiva que traspasa fronteras nacionales y fortalece su participación en la dinámica de acumulación global. Este gran dinamismo le permite hacer "...partícipe su capital criminal de otros capitales considerados lícitos lo que implica una híbridación entre lo legal y lo ilegal" (Vázquez, 2018, p. 106). Así también, el narcotráfico se vertebra con otras economías ilegales como el tráfico de personas, el tráfico de armas, secuestro, extorsiones, minería ilegal, etc., generando un grupo empresarial con una matriz y sus filiales. De esta forma, además de la ganancia absoluta, y relativa, el capital criminal consigue una ganancia extraordinaria que lo está convirtiendo en un motor de la economía internacional.

Desde la misma línea de argumentación, en el campo de lo político, este artículo toma como conceptos de su análisis: la soberanía, la necropolítica y el necropoder trabajados por Achilles Mbembe. A partir de estos conceptos se articula el concepto de gubernamentalidad necroliberal. "La soberanía reside ampliamente en el poder y la capacidad de decidir quién puede vivir y quién debe morir. Hacer morir o dejar vivir constituyen, por lo tanto, los límites de la soberanía, sus principales atributos" (Mbembe, 2011, p. 19-20). La soberanía, entonces, es la capacidad del Estado -o de un grupo de poder dentro del Estado, en alianza con él o fuera de él- "...para definir quién tiene importancia y quién no la tiene, quién está desprovisto de valor y puede ser fácilmente sustituible y quién no" (Mbembe, p. 46).

La necropolítica: "...da cuenta de la forma en que la política hace hoy del asesinato de su enemigo su objetivo primero y absoluto, con el pretexto de la guerra, de la resistencia o de la lucha contra el terror" (Mbembe, 2011, p. 20). El necropoder, que la acompaña, es aquel capaz de producir y administrar la muerte, a la cual la usa como herramienta política para mantener la dominación. No solo se trata de matar físicamente, sino de someter a poblaciones a condiciones de existencia precarias (hambre, falta de derechos, desplazamiento forzado), donde la muerte es una amenaza constante.

> Por "gubernamentalidad" entiendo el conjunto constituido por las instituciones, los procedimientos, análisis y reflexiones, los cálculos y las tácticas que permiten ejercer esa forma bien específica, aunque muy compleja, de poder que tiene por blanco principal la población, por forma mayor de saber la economía política y por instrumento técnico esencial los dispositivos de seguridad. (Foucault, 1977-1978, p. 136)

La gubernamentalidad liberal hace referencia a un tipo específico de ejercicio de la soberanía política, el poder basado en el régimen de vedad económica que acompaña el desarrollo del capitalismo en sus distintas formas históricas. Del neoliberalismo, que transformó el trabajo en capital humano y convirtió a los trabajadores en emprendedores capaces de administrar su propia explotación, el siglo

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

XXI transita al necroliberalismo que transforma al trabajador en residuo humano, peso muerto del capital, capaz de gestionar su propio sacrificio, su propia muerte. Esta gubernamentalidad se caracteriza por el desprecio total a la vida en función del mantenimiento del orden económico y político vigente, expresa la soberanía como poder y capacidad de decidir quién vive y quién muere. En conclusión, la soberanía de la gubernamentalidad necroliberal se basa en el derecho de matar.

> Para la teoría crítica y contextualizada, los derechos humanos son productos culturales: "...dinámicas y luchas históricas resultado de resistencias contra la violencia que las diferentes manifestaciones del poder del capital han ejercido contra los individuos y los colectivos" (Herrera, 2005, p.219). Procesos en permanente construcción y reconstrucción impulsados en la lucha por la dignidad humana en un contexto histórico concreto de emergencia, desarrollo y transformación de las relaciones sociales capitalistas. Los derechos y los entornos de relaciones se transforman permanentemente en dependencia de los cambios sociales, políticos, jurídicos y económicos que configuran los tramas en que tiene lugar la lucha por la dignidad humana. Los derechos humanos son procesos históricos que: "constituyen la afirmación de la lucha del ser humano por ver cumplimentados sus deseos y necesidades en los contextos vitales en que está situado" (Herrera, 2008, p.14).

La lógica del necropoder busca expulsar, dejar morir o asesinar a una parte de la población que considera excedente, lo cual pone en duda la premisa de que todo ser humano tiene derechos por el solo hecho de existir. La idea esencialista de los derechos humanos no alcanza para captar la radicalidad de la lucha por su garantía, antes y después de su reconocimiento jurídico. El estudio que se presenta, por lo tanto, está inserto en los conflictos y las prácticas sociales que surgen en las luchas por la dignidad en contextos que exigen asumir compromisos y responsabilidad por el derecho a vivir y por el derecho a tener derechos. El compromiso se sitúa en la lucha social en su nivel de defensa práctica y discursiva por el derecho a la vida, esta última disputa el fortalecimiento de: "...la llamada imaginación utópica y de la producción de sentidos emancipatorios" (Herrera, 2008, p.133).

Metodología y caso de estudio

"Percibir la constelación en que se halla la cosa es lo mismo que descifrarla como la constelación que lleva en sí en cuanto producto del devenir" (Adorno, 1984, p. 166). Si el concepto es la respuesta por el ser de la cosa y la cosa es su contexto, el concepto dice de ese entramado complejo de relaciones e interrelaciones que en su devenir constituyen la realidad de la cosa y del propio concepto. Así, la construcción de la relación entre capital criminal, gubernamentalidad necroliberal y derechos humanos conlleva una articulación conceptual que explica el entramado de relaciones e interrelaciones económicas políticas, jurídicas e ideológicas que configuran la violencia del narcotráfico como problema de la totalidad social y no como un hecho aislado.

En el marco del enfoque metodológico de la constelación, el estudio de caso permite comprender esta compleja relación -objeto de esta investigación- en un escenario particular, en su contexto teórico-conceptual e histórico-social donde se destaca el mundo de particula-

ridades y matices del complejo entramado de relaciones económicas, políticas e ideológicas que en su emergencia, desarrollo y transformación lo hicieron posible.

La constelación implica una forma de comprensión y dotación de sentido de los conceptos capital criminal, gubernamentalidad necroliberal y derechos humanos que reivindica la impureza de sus contenidos o sus estrechas relaciones con las expectativas e intereses de los grupos sociales interesados en sus conexiones. "Sólo las constelaciones representan, desde fuera, lo que el concepto ha amputado en el interior, el plus que quiere ser por más que no lo pueda" (Adorno, 1984, p. 166).

La investigación opta por una metodología relacional que tome en cuenta: Por un lado, la determinación del tipo de relaciones por la totalidad social por cuanto las relaciones entre los conceptos propuestos son en sí mismas sus contextos, no su pura identidad conceptual. Por otro, la complejidad del capital criminal, la gubernamentalidad necroliberal y los derechos humanos situados en sus contextos sociales. La relación que buscamos no aparece más que a través de la singularidad del caso de estudio, solo así los conceptos recuperan el conocimiento concreto.

El caso seleccionado es la política de seguridad del gobierno del Ecuador durante el año 2024 frente a la crisis de violencia criminal. En él se indaga la relación que existe entre capital criminal, gubernamentalidad necroliberal y el efecto que esta tiene en la exigibilidad y vigencia de los derechos humanos. La recolección de información se basa en una técnica etnográfica que tiene dos estrategias: 1. Indagar en documentos de archivo digital noticias, documentos oficiales y opinión ciudadana. 2. Observación cotidiana de la violencia del narcotráfico, de la respuesta gubernamental y el ejercicio de la justicia en relación con la exigibilidad y aplicabilidad de los derechos humanos.

Posteriormente, la información recogida es sometida a la interpretación y análisis crítico, con el propósito de encontrar el significado de ese conjunto de relaciones económica, políticas, jurídicas e ideológica, y a partir de allí sus conexiones. Cada relación será codificada a partir de las siguientes preguntas: ¿Qué tipo de relación es? ¿quiénes participan en ella? ¿Cuál es el devenir de esa relación?

Interpretación y análisis crítico de los resultados

> Las masacres carcelarias en las prisiones fueron una de las primeras expresiones de la crisis de seguridad que Ecuador vive desde inicios de 2021. El 23 de febrero de este año, 79 personas fueron asesinadas en cuatro cárceles del país durante un motín múltiple. El origen de esa masacre fue la disputa entre bandas narcodelictivas. En ese momento, empezó una guerra por tomar el mando del mundo criminal... (Primicias, 2022)

Detrás de lo visible de la "violencia subjetiva e irracional" se encuentra la "violencia objetiva" (Žižek, 2009, p. 22), inherente al capitalismo y su enloquecida, imparable y autoestimulante circulación y acumulación de capital, exacerbada en su fase criminal. Los grandes GDO ejecutores de esta violencia están articulados al negocio del narcotráfico, que hoy es una economía en ascenso en el capitalismo global y nuclear en el Ecuador. Al país ingresan, aproximadamente, 3500 millones de dólares anuales, 800 se destinan a la reproducción del nuevo ciclo económico y 2700 se lavan a través del sistema financiero y productivo nacional,

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

cuyo porcentaje está entre el 2% y 5% del PIB anual. Si el Ecuador proyecta un crecimiento legal menor al 2% y el lavado de dinero es de uno a dos puntos porcentuales más, se infiere que el narcotráfico es un puntal fundamental en la economía nacional (CELAG, 2023).

La violencia desatada por los GDO vinculados al narcotráfico es inseparable de las operaciones del capital criminal, que para reproducirse rompe límites jurídicos, políticos, éticos o culturales. La producción de valor de la mercancía ilícita se encuentra en un ejército de seres humanos empobrecidos que son convertidos en mano de obra forzada, a veces esclava, carente de derechos y lanzada a la muerte en medio de la guerra de los cárteles por rutas de circulación y mercados.

Este capital muestra un desprecio total por la vida de los trabajadores, cuya oferta crece por los niveles progresivos de desempleo estructural de la economía formal y legal. La historia del capitalismo nos enseña que en su expansión ha tolerado ilegalidades de todo tipo, ha eludido los controles estatales y ha cometido muchos crímenes para acrecentar sus ganancias. La violencia subjetiva del narcotráfico es parte de la historia de la violencia objetiva del capitalismo, es la forma propia de operar del capital criminal que constituye un elemento orgánico y cuantitativamente significativo de la economía del mundo (Illades, 2024).

El Plan Colombia internacionaliza el ciclo económico del narcotráfico que da lugar a una división internacional y territorial del delito. Hay unas organizaciones que cultivan, otras que producen, otras que trasladan, otras que introducen en los mercados, otras que venden y otras que lavan (Carrión, 2024). En ese contexto, el Ecuador se convierte en un sitio estratégico para el narcotráfico: 1. Se encuentra entre los dos países productores (Colombia y Perú) y tiene salida a dos cuencas de distribución (la del Pacífico y del Amazonas). 2. Es un país dolarizado que lo convierte en un lugar donde se vuelve fácil lavar dinero. 3. Su institucionalidad estatal débil beneficia los negocios ilícitos. Todo esto lo convierte en una plataforma internacional del delito en la que operan empresas criminales transnacionales articuladas a la red global del capital criminal, que con sus sistemas de nodos y redes conecta territorios lejanos y distintos sectores de la economía mundial.

La crisis del precio de los commodities en 2014 y de la pandemia en 2020 agudizaron los niveles de pobreza y lanzaron al empleo informal y al desempleo a más del 60% de la población económicamente activa; la descomposición acelerada de la institucionalidad a partir del 2017, sobre todo, la de los aparatos de control y seguridad del Estado; el aumento exponencial de cocaína en Colombia de 1200 toneladas en 2018, a 1738 toneladas en 2022 para ser movida por Ecuador a un costo de 800.000 dólares, la mitad de lo que cuesta por Colombia; llevó al país a ser uno de los principales puntos de embarque para el tráfico global de cocaína (InsightCrime, 2023).

Todo esto explica por qué el Ecuador: "...se ha convertido en un país que ocupa un puesto privilegiado en la cadena de valor del narcotráfico, al incrementar exponencialmente su participación en la producción, el refinamiento, el almacenamiento y el transporte de drogas ilícitas" (Rivera-Rhon & Bravo-Grifalba, 2020, p. 10).

En el Ecuador existe alrededor de 50000 trabajadores directos de los GDO, dato que indica que el capital criminal ofrece empleo a grandes sectores de la población.

Los hechos y datos expuestos revelan que el narcotráfico en el Ecuador es parte de la red

global del capital criminal y no una economía marginal y local. Este negocio multimillonario integra de manera eficiente los planos local, regional, nacional y mundial de la producción y consumo de mercancías (Illades, 2024). Desde los miles de niños y jóvenes de la costa ecuatoriana -trabajadores asalariados de los GDO nacionales- hasta los consumidores de Estados Unidos, Europa y Brasil, el proceso está totalmente articulado y regulado por medio de la coacción y la violencia.

Se trata de uno de los capitales más exitosos de la globalización, cuyo flujo de ganancia corre por las redes financieras internacionales y a nivel nacional se filtra a todos los sectores económicos: construcción, bancos, cooperativas, equipos de futbol, exportaciones, etc. En otras palabras, la economía nacional depende de la economía del narcotráfico. Finalmente, el análisis expuesto hace suponer que, en el siglo XXI, el capital criminal del narcotráfico se transforma en uno de los capitales dominantes de la economía ecuatoriana.

Como respuesta al ascenso de la violencia criminal del narcotráfico, el presidente Noboa firma el Decreto 111, que en su artículo 1. "Reconoce la existencia de un conflicto armado interno" (Decreto Presidencial, 2024), dispone la movilización e intervención de las Fuerzas Armadas y la Policía Nacional para garantizar la soberanía e integridad territorial contra el crimen organizado transnacional y los actores no estatales beligerantes. Se identifica 22 grupos criminales como organizaciones terroristas de amenaza interna. El decreto "...presenta un retorno a la noción de enemigo de la sociedad, frente al cual 'debe aplicarse una solución rápida que conjure dicho riesgo antes de que ocurra la catástrofe'" (González Mongui, & Carvajal Martínez, 2023, p. 206). De esta manera, la guerra contra el narcoterrorismo afirma jurídicamente, con consenso social, la implementación de una política gubernamental que limita derechos humanos fundamentales.

En los tres primeros meses, desde la declaratoria del CANI, se ejecutaron más de 272 mil operaciones militares, solo 260 contra grupos terroristas; más de 18 mil detenidos, solo 300 de ellos por presunto terrorismo; alrededor de 14 personas abatidas (Primicias, 2024). La intervención de las FF. AA. se da principalmente en las cárceles, en las ciudades y en los barrios más empobrecidos y violentos del país donde operan los GDO. No solo se militariza la seguridad, sino y principalmente la sociedad. "Las escenas se repiten: fusiles apuntan a los rostros de adolescentes, jóvenes y hombres adultos —decenas son afrodescendientes—, detenidos por policías y militares en varias zonas conflictivas en Ecuador como Esmeraldas, Manabí, Guayas" (Noroña, 2024).

Las masacres carcelarias, permitidas por el Servicio Nacional de Atención Integral a Personas Adultas Privadas de la Libertad y a Adolescentes Infractores (SNAI); los asesinatos diarios en las calles protagonizados por los GDO; las desapariciones forzadas y las ejecuciones extrajudiciales perpetradas por los militares a partir del Decreto 111, son signos de la implementación de una política gubernamental que: "...hace del asesinato de su enemigo su objetivo primero y absoluto con el pretexto de la guerra, de la resistencia o de la lucha contra el terror" (Mbembe, 2011, p. 20).

Una necropolítica ejecutada por el Gobierno legal y por los gobiernos ilegales que operan en los territorios dominados por el narcotráfico. El enemigo de esta guerra no es la narcoempresa nacional, ni las grandes estructuras del crimen organizado, que no han sido

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

afectadas, sino: "...estructuras pandilleras que operan en los territorios más violentos del país, donde jóvenes ejecutaban delitos como sicariato o extorsión" (Noroña, 2024), organizaciones delincuenciales pequeñas o simplemente jóvenes empobrecidos y racializados signados como terroristas. "Después de todo, la guerra también es un medio de establecer la soberanía, tanto como un modo de ejercer el derecho a dar la muerte" (Mbembe, 2011, p. 20).

El Estado, con sus aparatos armados, y los GDO implementan un tipo de gubernamentalidad basada en el derecho de matar, en un contexto de avance del capital criminal, de declaración de guerra y de estado de excepción. Las Fuerzas Armadas y la Policía nacional están autorizadas a utilizar armas letales contra los grupos terroristas con la promesa de impunidad. Explica Edward Pérez: "...la experiencia en América Latina nos muestra que el problema es que bajo estos estados de excepción se tienden a esconder atrocidades que luego se mantienen durante décadas en la impunidad y la oscuridad". (Pérez, 2024). De hecho, la presencia del narcotráfico en las Fuerzas Armadas, la Policía y el sistema nacional de justicia abre una zona gris donde es difícil identificar los límites entre el Estado y los GDO (El Comercio, 2024).

"La fiscalía general del Estado investiga el presunto cometimiento del delito por parte de jueces, secretarios, policías, abogados en libre ejercicio y otros funcionarios públicos, en el otorgamiento –ilegítimo– de acciones constitucionales a personas privadas de la libertad" (Fiscalía, 2024). Hay muchas más denuncias de la presencia de intereses del narcotráfico en la estructura estatal que involucra a políticos, altos funcionarios del Estado como lo indica el caso "León de Troya" (Fiscalía, 2023). Al igual que en otros países de la región: "El mecanismo que ha empleado el narcotráfico para incidir en las entidades públicas está vinculado a las debilidades de cada una de las instituciones públicas". (Sierra & Bermúdez, 2021, p. 287).

El nivel de penetración del narcotráfico en la estructura del Estado ecuatoriano hace pensar en la formación de un narcoestado. Las operaciones económicas delictivas del capital criminal influyen con poder, dinero y amenazas las decisiones de estado o, definitivamente, están dirigidas de manera encubierta por funcionarios estatales que son parte de las estructuras criminales. Si esta tesis es cierta, es el narcoestado el que tiene el poder de administrar la muerte a través de una articulación de hecho, aunque no de derecho, del poder militar y policial con lo GDO que actúan como estructuras militares del narcotráfico. Es el narcoestado el que tiene: "...la capacidad de definir quién tiene importancia y quién no la tiene, quién está desprovisto de valor y quién puede ser fácilmente sustituible y quién no" (Mbembe, 2011, 45-46).

A la gubernamentalidad que tiene por blanco principal decidir quién debe morir, en base al saber de la economía política del narcotráfico, y por instrumentos técnico esencial los dispositivos de violencia criminal, la llamo necroliberal. El poder de matar que tiene el narcoestado es lo que le permite, a sus jefes, afirmase como hombres de gobierno capaces de imponer a la población un modo de proceder necrótico. De la gubernamentalidad liberal que consume y administra la libertad del intercambio se pasó a la gubernamentalidad neoliberal que consume y administra la competencia desigual, para hoy transitar a la gubernamentalidad necroliberal que consume y administra la muerte. De la fobia liberal al Estado se pasa al Estado bajo vigilancia permanente del mercado y, de allí, a la filia

DOI: https://doi.org/10.59794/rscd.2025.v11i11.153

narcoestatal a la muerte. El necroliberalismo es una ideología de gobierno que combina el autoritarismo con la tolerancia a la humillación, la tortura y la muerte.

En el contexto de formación del narcoestado ecuatoriano, el Decreto 111 da paso a la implementación jurídica de la gubernamentalidad necroliberal que pone a operar un conjunto de procedimientos y dispositivos de extrema violencia estatal en sintonía con la violencia de los GDO. Se declara la guerra a los jóvenes más empobrecidos, se encuentren o no integrados a las bandas criminales.

Muestra de esta violencia gubernamental son: "La muerte de Javier, el joven que iba a vender un perro y acabó acribillado en un retén militar de Ecuador" (El País, 2024). La detención arbitraria de Raúl, un joven afroecuatoriano de 18 años que "NO tenía antecedentes penales, NO cometió un delito" (Justicia en Cárceles, 2024). El caso de Jonathan que: "Lo secuestraron a las 10 am, estaba en su casa, le dieron una golpiza criminal. Se lo llevaron ya reventado a puñetes y lo siguieron torturando hasta matarlo" (Granja, 2024). Y el caso más conocido, la desaparición forzada con desenlace de asesinato e incineración de los 4 jóvenes de Guayaquil a manos de militares. La gubernamentalidad necroliberal, ejecutado tanto por los aparatos de seguridad del Estado cuanto, por los GDO, somete la vida al poder de la muerte.

El necroliberalismo se configura mediante el primado autoritario y genocida del mercado sobre la democracia y los derechos humanos, sostenido bajo una amenaza de extinción permanente (Viejo, 2022). Para esto se establece una serie de dispositivos disciplinares que destruyen la dignidad de los seres humanos mediante la violencia ideológica que propagandiza el desprecio a la vida de la población empobrecida y racializada, donde se encuentra la inmensa masa de trabajadores del capital criminal convertidos en población sacrificable. Personas sometidas a la violencia del narcoestado que les persigue, criminaliza, humilla, apresa, tortura y mata en las cárceles, los barrios populares y las calles. Las características culturales y sociales de la población objetivo son convertidas en signos de criminalidad y violencia. Así se regula y distribuye la muerte, haciendo posibles las funciones mortíferas del narcoestado.

El necroliberalismo suspende en los hechos la universalidad de los derechos humanos. Hay humanos que importan y otros no, unos que tienen permiso para vivir y otros que no. La población residual, peso muerto del capital, violentamente incorporada a la producción del capital criminal es una población destinada al exterminio. En el ciclo productivo del capital criminal, los medios de producción son ilegales, la mano de obra es delincuencial, la mercancía lleva en sí misma el signo de la muerte (drogas, órganos, tráfico de personas, armas, etc.) y el consumo es delito.

Este proceso funciona violando en cada momento los derechos humanos de las personas involucradas en él mismo, fundamentalmente el derecho a la vida, por lo tanto, su garantía se vuelve absolutamente disfuncional a la acumulación de capital criminal. Los negocios criminales requieren establecer en la población general un tipo de subjetividad adversa a la lucha por la dignidad. Para esto, por ejemplo, se propagandiza por videos las humillaciones y torturas que los militares cometen en contra de jóvenes y niños empobrecidos acusados de terroristas. Propaganda que deja claro que la violación de derechos humanos perpetrada por los militares contra la población criminalizada debe ser aceptada, como se puede ver en la siguiente denuncia:

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Señores y señoras jueces de la @CorteConstEcu, aquí unas imágenes de niños que están siendo tratados como terroristas, (sin sentencia que así lo determine), quienes reciben tratos crueles, inhumanos y degradantes por parte de los miembros de las Fuerzas Armadas. Esto para cuando analicen, valoren y califiquen el Decreto 111, que ojalá sea pronto, porque resulta que son los niños y los jóvenes empobrecidos y racializados del país, quienes están poniendo el cuerpo a la violencia y al conflicto armado interno, sean o no parte de las bandas delincuenciales. (Martínez, 2024).

El necroliberalismo niega "...la dignidad humana como factor esencial intrínseco y del respeto al otro por el hecho de ser mi igual, sin hacer juicios de valor que lo califiquen como seudo-humano" (Galán, 2016, p. 33). La vida del otro y la propia pierde valor o se lo mantiene en niveles mínimos, fenómeno que se manifiesta en la expansión de la práctica criminal del sicariato. En Ecuador este negocio ha quitado la vida a muchos jóvenes integrantes de las bandas y ha alcanzado a alcaldes, jueces, fiscales e incluso a un candidato presidencial. El asesinato a tiros del candidato a la presidencia Fernando Villavicencio ha sacudido Ecuador en plena campaña electoral, es la manifestación de la devaluación de la vida (El País, 2023). Cualquier vida incómoda e innecesaria es una vida sacrificable.

Los sicarios empiezan su actividad delictiva en la pubertad y por lo general mueren asesinados muy jóvenes. Ellos son el signo de desprecio a la vida que promueve el capital criminal, son los que ejecuta el poder de matar por lo cual adquieren valor en el mercado del crimen. El narcoestado y su gubernamentalidad necroliberal interviene sobre la sociedad misma para mercantilizarla e integrarla a los mecanismos de la muerte: adicciones, secuestros, minería ilegal, migración forzada, sicariato, extorsiones, etc.

El enfrentamiento del terrorismo ha puesto en la balanza un supuesto enfrentamiento entre la seguridad humana que como derecho fundamental tienen las comunidades y la libertad frente a la supuesta necesidad de restringir los derechos humanos. El terrorismo es pretexto para que se legisle en contravía de los derechos humanos. (González Mongui, & Carvajal Martínez, 2023, p. 206).

Para restringir derechos humanos se pone en marcha una propaganda ideológica agresiva que los deslegitima en el seno de la sociedad, con el objetivo de hacer que la población acepte la muerte de los otros, narcoterroristas, y renuncien a muchos derechos en nombre de la seguridad y el combate al narcotráfico, el mismo que se centra en las poblaciones empobrecida, racializada y encarceladas. En el contexto del incremento de la violencia, los grandes medios de comunicación, formadores de opinión y troles en redes sociales se dedican a atacar a las organizaciones de derechos humanos, acusándolas de ser defensores de delincuentes. Por ejemplo, sostienen que: "La Corte Interamericana de Derechos Humanos considera que los delincuentes que matan roban y están presos en una cárcel tienen los mismos derechos que las personas que no lo hacen y están libres" (Calderón, 2024).

Esta campaña en contra de los derechos humanos se agudizó en torno a la Consulta popular del 21 de abril del 2024, cuyos resultados mostraron un apoyo mayoritario de la población a todas las medidas de seguridad que abrió paso a la formación de un estado de militarización permanente en el Ecuador. Es común leer opiniones en redes sociales como esta: "...gracias a Dios más del 80% de los ecuatorianos apoyamos a las fuerzas armadas,

si tienen que poner orden de la forma que sea que lo hagan! No tengan miedo" (Cruz, 2024) Un número importante de opiniones en redes apoyan que se torture o asesine a los delincuentes, incluidos niños y adolescentes que fueron detenidos en el marco de la declaratoria del CANI. La intervención ideológica es una técnica gubernamental que busca consenso en la sociedad para que esta acepte sacrificar y ser sacrificada.

¡¡Urgente!! ¡¡Solo el pueblo salva al pueblo!! En Imbabura un delincuente fue quemado vivo por moradores del sector, fue capturado mientras estaba robando en los interiores de una hacienda en San Rafael. Esta vez no hubo perdón. ¿Qué opinan de este tipo de justicia? (Calderón, 2024)

Conclusiones

El capitalismo del siglo XX se ha extendido de la mano de la gubernamentalidad liberal keynesianas y neoliberal según la necesidad de los ciclos de Gonzales su reproducción. Para el siglo XXI, en el ciclo de reproducción criminal de capital, la gubernamentalidad neoliberal muta hacia la gubernamental necroliberal. Se trata de una práctica de gobierno que garantiza la acumulación de capital, de origen ilícito, a través del saber de la economía política de la muerte y de tecnologías y técnicas de dominación basadas en la violencia, el terror, el sufrimiento, el dolor y desangramiento de los cuerpos.

La gubernamentalidad necroliberal es totalmente contraria a la aplicación y aún más a la ampliación de los derechos humanos, no solo aquellos ligados al acceso a beneficios sociales, que ya fueron golpeados por el neoliberalismo, sino al fundamental derecho a la vida. La libertad del mercado que deviene en libertad de matar se constituye en el principio organizador y regulador del narcoestado. La gubernamentalidad necroliberal restringe derechos humanos en base configurar una subjetividad que se criminaliza y administra su propia muerte.

La expansión del capital criminal requiere de un tipo específico de gubernamentalidad que garantice su reproducción. Una forma de gobierno que administre la violencia y la muerte que conlleva este tipo de economía. Los derechos humanos devienen en una traba para la reproducción de la económica criminal, razón por la cual son deslegitimados en la conciencia social y restringidos como ejercicio de justicia por la gubernamentalidad necroliberal.

Referencias

Adorno, T. (1984). *La dialéctica negativa.* Taurus.

Cadena, J. L. (2011). Geopolítica del narcotráfico. México y Colombia: la equivocación en el empleo de las fuerzas militares. *Revista Mexicana de Ciencias Políticas y Sociales,* 52(210), 45-58. https://doi.org/10.22201/fcpys.2448492xe.2010.210.25973

Calderón, Á. (2024, 17 de marzo). Derechos de delincuentes. *El Universo.* https://www.eluniverso.com/opinion/cartas-al-director/derechos-de-delincuentes-nota/

Carrión, F. (2024, 3 de abril). Estallido armado en Ecuador, situación y perspectivas [Video]. *Facebook.* https://www.facebook.

com/watch/?mibextid=rS40aB7S9Ucbxw-6v&v=698836168985882

CELAG. (2023, 8 de enero). Cuánto dinero se lava en el sistema financiero ecuatoriano: una aproximación desde las cifras macroeconómicas. *CELAG*. https://www.celag.org/cuanto-dinero-se-lava-en-el-sistema-financiero-ecuatoriano-una-aproximacion-desde-las-cifras-macroeconomicas/

Cruz, S. [@GyeVivebien]. (2024, 5 de febrero). [Tweet]. *Twitter*. https://twitter.com/GyeVivebien/status/1754641178035712153

Decreto Presidencial, 2024 No. 111. (2024). Dispone la movilización e intervención de las FF. AA. y la Policía Nacional para garantizar la soberanía e integridad territorial. *Presidencia de la República*. Ecuador. 9 de enero 2024.

El Comercio. (2024, 27 de febrero). Fiscalía recurrió a la Asistencia Penal Internacional por caso 'narcos generales'. *El Comercio*. https://www.elcomercio.com/actualidad/seguridad/fiscalia-recurrio-asistencia-penal-internacional-caso-narco-generales.html

El País. (2023, 10 de agosto). Asesinado el candidato presidencial Fernando Villavicencio en Ecuador. *El País*. https://elpais.com/internacional/2023-08-10/asesinado-el-candidato-presidencial-fernando-villavicencio-en-ecuador.html

El País. (2024, 3 de marzo). La muerte de Javier, el joven que iba a vender un perro y acabó acribillado en un retén militar de Ecuador. *El País*. https://elpais.com/america/2024-03-03/la-muerte-de-javier-el-joven-que-iba-a-vender-un-perro-y-acabo-acribillado-en-un-reten-militar-de-ecuador.html

Europa Press. (2024, 14 de marzo). Encapuchados armados toman las instalaciones del canal ecuatoriano TC Televisión. *Europa Press*. https://www.europapress.es/internacional/noticia-encapuchados-armados-toman-instalaciones-canal-ecuatoriano-tc-television-20240109210754.html

Fiscalía General del Estado. (2023, 20 de marzo). FGE decide acumular la causa denominada "León de Troya" en la investigación del "Caso Encuentro". *Fiscalía General del Estado*. https://www.fiscalia.gob.ec/fge-decide-acumular-la-causa-denominada-leon-de-troya-en-la-investigacion-del-caso-encuentro/

Fiscalía General del Estado. (2024, 20 de abril). Caso Plaga 2024 por el cual se investiga delito de delincuencia organizada. *Fiscalía General del Estado*. https://www.fiscalia.gob.ec/caso-plaga/

Foucault, M. (2007). *El nacimiento de la biopolítica: curso en el Collège de France (1978-1979)*. Fondo de Cultura Económica.

Galán G. (2016, enero-junio) Los derechos humanos fundamentados mediante la legitimación y la moral jurídica. *Novum Jus,* 1, 31–48. https://doi.org/10.14718/NovumJus.2016.10.1.2

Gómez, L. (2018). Algunos elementos para entender la economía del narcotráfico. *Revista Internacional de Historia Política e Cultura Jurídica*, 10(2), 301-322. https://www.redalyc.org/journal/3373/337355947009/html/

González Monguí, P. E., & Carvajal Martínez, J. E. (2023). La construcción social del enemigo en el imaginario penal. *Novum Jus,* 17(3), 189-213. https://doi.org/10.14718/NovumJus.2023.17.3.7

Granja, P. [@PedritoExtranja]. (2024, 2 de febrero). [Tweet]. *Twitter*. https://twitter.com/PedritoExtranja/status/1753421107934216628

Herrera, J. (2005). *Los derechos humanos como productos culturales: crítica del humanismo abstracto*. Catarata.

Herrera, J. (2008). *La reinvención de los derechos humanos*. Atrapasueños.

Illades, C. (2024, 11 de febrero). El capitalismo criminal. *Revista Común*. https://revistacomun.com/blog/el-capitalismo-criminal/

Insightcrimen. (2023) Balance de InSight Crime de incautaciones de cocaína de 2023. https://insightcrime.org/es/noticias/balance-insight-crime-incautaciones-cocaina-2023/

Justicia en Cárceles [@JusticiCarcelEc]. (2024, 29 de marzo). [Tweet]. *Twitter*. https://twitter.com/JusticiCarcelEc/status/1773814397728641202

Mantilla, J. (2023, 13 de enero). Narcotráfico y crimen organizado. *Ecuador Decide*. https://ecuador-decide.org/wp-content/uploads/2023/08/Narcotrafico-y-crimen-organizado.pdf

Márquez, H. (2020). El capital es el crimen organizado: violencia, mercancía ilícita y dinero negro. En S. Esquive (Ed.), *Textos y contextos psicosociales: violencia, pobreza, género* (pp. 4-27). CONCYTEQ.

Martínez, S. [@sybelmartinez]. (2024, 26 de enero). [Tweet]. *Twitter*. https://twitter.com/sybelmartinez/status/1750953446948180427

Mbembe, A. (2012). Necropolítica. Una revisión crítica. En H, Chávez (curadora), *Estética y violencia: Necropolítica, militarización y vidas lloradas* (pp. 130-139). Museo Público y Universitario de Arte Contemporáneo; Universidad Nacional Autónoma de México.

Noroña, K. (2024, 17 de marzo). Luis Córdova: Con el 'conflicto armado interno' no solo se militarizó la seguridad, sino la sociedad. *France* 24. https://www.france24.com/es/am%C3%A9rica-latina/20240118-luis-c%C3%B3rdova-con-el-conflicto-armado-interno-no-solo-se-militariz%C3%B3-la-seguridad-sino-la-sociedad

Pérez, M. (2024, marzo 15). Expertos alertan: Estados de excepción en América Latina esconden atrocidades e impunidad. *La Tercera*. https://es.wikipedia.org/wiki/Artículo_%28gramática%29

Primicias. (2022, 15 de febrero). Once masacres carcelarias y 413 presos asesinados en 21 meses. *Primicias*. https://www.primicias.ec/noticias/en-exclusiva/carceles-nueve-masacres-victimas-ecuador/

Primicias. (2024, 2 de abril). Estos son los resultados del estado de excepción que concluyó tras 90 días. *Primicias*. https://www.primicias.ec/noticias/seguridad/estado-excepcion-militares-conflicto-armado-interno/

Rivera-Rhon, R., & Bravo-Grijalva, C. (2020). Crimen organizado y cadenas de valor: el ascenso estratégico del Ecuador en la economía del narcotráfico. *URVIO Revista Latinoamericana de Estudios de Seguridad,* 28, 8-29. https://doi.org/10.17141/urvio.28.2020.4410

Sierra, P., & Bermúdez, M. (2021). La incidencia del narcotráfico en las altas esferas del gobierno peruano. *Novum Jus,* 15(2), 259–293. https://doi.org/10.14718/NovumJus.2021.15.2.10

Vázquez, J. (2018). Economía del narco: prohibicionismo, violencias sistémicas y capital criminal. *Calidoscopio*, 21(38), 105-130. https://revistas.uaa.mx/index.php/caleidoscopio/article/view/917/885

Viejo, R. (2022, 1 de abril). Necroliberalismo. *Rebelión*. https://rebelion.org/necroliberalismo/

Žižek, S. (2009). *Sobre la violencia: seis reflexiones marginales*. Paidós.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Análisis estratégico para la integración del dominio cibernético con los dominios físicos para misiones múltiples de seguridad y defensa

Strategic Analysis for Cyber Domain Integration with Physical Domains for Multiple Security and Defense Missions

Recibido: 03/ 04 / 2025 | Revisado: 21 / 08 / 2025 | Aprobado: 25 / 09 / 2025
DOI: https://doi.org/10.59794/rscd.2025.v11i11.149

General de brigada (r) Boris Saavedra, FAV
Venezuela

Correo: saavedrab@ndu.edu

ORCID: https://orcid.org/0009-0000-1334-2833

Afiliación: National Defense University

El autor es un oficial general en situación de retiro de la Fuerza Aérea Venezolana. Prestó servicio en todas las funciones operativas de dicha fuerza. Ha dedicado más de treinta años de su vida profesional a las actividades académicas, tanto en Venezuela como en los Estados Unidos, en calidad de instructor de vuelo, profesor académico, director de la Escuela Básica de las Fuerzas Armadas y comandante de la Defensa Aérea de Venezuela. Se graduó en la Academia de la Fuerza Aérea de Venezuela, donde obtuvo la licenciatura en Ciencias y Artes Militares, con especialización en Aeronáutica. Realizó todos los cursos y especializaciones previstos en el área operativa como piloto de combate. Es egresado del Curso de Estudios Militares Superiores en l'École Supérieure de Guerre Interarmées de Francia (1983-1986) y del Curso Superior de Defensa Nacional en el Instituto de Altos Estudios de la Defensa Nacional de Venezuela (1988-1989). Además del doctorado obtenido en el Instituto Universitario Gutiérrez Mellado de la Universidad Nacional de Educación a Distancia en España (2014), cuenta con una maestría en Política Internacional y Práctica por la Universidad George Washington en Estados Unidos (2003). En el ámbito de su especialización en Paz y Seguridad Internacional, ha sido coautor de varios libros y artículos en revistas especializadas en España, Inglaterra, Colombia, Chile, Estados Unidos y Venezuela, sobre relaciones civiles-militares en América Latina, seguridad pública y privada, crimen transnacional, terrorismo, planificación estratégica, ciberseguridad y capacidades militares. Actualmente se desempeña como profesor de Asuntos de Seguridad Nacional en el Centro de Estudios de Defensa Hemisférica William J. Perry, ubicado en la Universidad Nacional de Defensa de Washington, DC. Es director del programa de Ciberseguridad y Asuntos de Tecnología Digital Emergente. Antes de asumir este cargo, el Dr. Saavedra fue jefe de Estudios Académicos en el Colegio Interamericano de Defensa en Washington, DC (1996-1998). En Venezuela, su último cargo fue el de director de la Secretaría en el Ministerio de Defensa Nacional (1994-1995).

Lic. Chase Logan Boone
Estados Unidos

Correo: chase.l.boone.civ@ndu.edu

ORCID: https://orcid.org/0009-0002-4356-3260

Afiliación: National Defense University

El autor es máster universitario en Estudios de Seguridad, con especialización en terrorismo y violencia subnacional, por la Edmund A. Walsh School of Foreign Service de la Universidad de Georgetown. Es licenciado en Relaciones Internacionales y Estudios Globales por la Universidad de Texas en Austin. Ha dedicado más de una década a la investigación sobre América Latina y el Caribe, especializándose en la historia, la política y la seguridad y defensa en el continente americano. Posee un profundo conocimiento de las estructuras operativas, los procesos de toma de decisiones y la cultura organizacional de las fuerzas armadas latinoamericanas. Inició su carrera como docente en el Cuerpo de Paz en la República Dominicana, donde trabajó en proyectos de alfabetización y desarrollo comunitario. Posteriormente, en Bogotá, Colombia, se desempeñó como investigador en un centro de estudios económicos, enfocado en el comercio energético colombiano, las insurgencias armadas y los problemas de seguridad vinculados con las economías ilícitas. En la actualidad, es investigador asociado en el Centro de Estudios de Defensa Hemisférica William J. Perry, perteneciente a la Universidad Nacional de Defensa, en Washington D. C. Su labor investigadora abarca la dinámica de la delincuencia transfronteriza, el lavado de dinero, la trata de personas y las estrategias antiterroristas.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Resumen

La guerra moderna abarca tanto el ámbito físico como el cibernético. Las fuerzas armadas actuales enfrentan amenazas en múltiples dominios, tales como: tierra, mar, aire, espacio y el ciberespacio. Por ello, integrar las operaciones cibernéticas con las operaciones en los dominios físicos se ha vuelto esencial para lograr ventajas en el campo de batalla. La doctrina estadounidense de Operaciones Multidominio (OMD) plantea contrarrestar amenazas simultáneas en todos los dominios de la guerra mediante la convergencia de efectos y fuerzas. Sin embargo, muchos países aliados aún enfrentan desafíos para incorporar plenamente las capacidades cibernéticas a sus operaciones convencionales. Este artículo analiza la importancia de integrar el dominio cibernético con los dominios físicos en las operaciones de seguridad y defensa, apoyándose en la doctrina de Operaciones Multidominio (OMD) de EE. UU., estudios de caso regionales y tendencias hemisféricas, con el fin de orientar a los países de América Latina y el Caribe en la construcción de capacidades multimisión frente a amenazas híbridas.

Palabras clave: Dominio, operaciones multidominio (OMD), guerra cibernética, sistemas ciberfísicos (SCF), inteligencia artificial generativa (IAG)

Abstract

Modern warfare encompasses both the physical and cybernetic realms. Today's armed forces face threats in multiple domains, such as land, sea, air, space, and cyberspace. As such, integrating cyber operations with operations in the physical domains has become essential to achieving advantages on the battlefield. The U.S. doctrine of Multi-Domain Operations (MDO) proposes countering simultaneous threats in all domains of warfare through the convergence of effects and forces. However, many allied countries still face challenges in fully incorporating cyber capabilities into their conventional operations. This article analyzes the importance of integrating the cyber domain with the physical domains in security and defense operations, based on the U.S. Multi-Domain Operations (MDO) doctrine, regional case studies, and hemispheric trends, in order to guide Latin American and Caribbean countries in building multi-mission capabilities against hybrid threats.

Keywords: Domain, Multi-Domain Operations (OMD), Cyber Warfare, Cyber-Physical Systems (SCF), Generative Artificial Intelligence (IAG)

Introducción

En la era de la guerra cibernética y la IAG, las principales potencias y otros Estados han aumentado sus arsenales con capacidades cibernéticas cuya utilidad se deriva en gran medida de su opacidad y negabilidad, y en algunos casos, de su actuación en los ambiguos límites de la desinformación, la recopilación de inteligencia, el sabotaje y el conflicto tradicional, creando estrategias sin doctrina reconocida. Sin embargo, cada avance ha ido acompañado de vulnerabilidades (Kissinger, Schmidt & Huttenlocher, 2021). En el contexto de la defensa y la seguridad, un dominio se refiere a una esfera o medio especifico en el que se llevan a cabo actividades militares o de seguridad para alcanzar objetivos este concepto es fundamental para la estrategia militar moderna, en particular en el marco de las operaciones multidominio.

El mundo de tecnologías digitales emergentes, aceleradas y convergentes actual, el concepto de seguridad ha evolucionado para abarcar no solo las amenazas digitales, sino también las vulnerabilidades físicas. Esta convergencia de la seguridad digital y física se materializa con la aparición de los sistemas SCF. Comprender sus complejidades es crucial para la integración del dominio cibernético con los dominios físicos.

La protección de nuestra sociedad cada vez es más compleja y vulnerable. En esencia, sistema ciberfísico consta de tres elementos esenciales: infraestructura física, infraestructura informática y redes de comunicaciones que facilitan la integración de procesos informáticos y físicos que combinan sensores, actuadores y comunicación en red para monitorizar y controlar entidades físicas. Esta fusión fluida de los dominios digitales y físicos permite la creación de sistemas inteligentes e interconectados que pueden interactuar fluidamente con el mundo físico (Blue Goat Cyber, 2025).

En los dominios físicos los sistemas de armas representan los elementos tangibles como armas, barcos de guerra y aviones de combate que funcionan en forma inteligente por estar equipados con sensores que recopilan datos sobre su entorno y actuadores que les permiten interactuar en el mundo físico. El dominio cibernético abarca los componentes de software y hardware que permiten el procesamiento y análisis de datos y comunicaciones.

La creciente complejidad de las operaciones modernas de seguridad y defensa ha exigido una transición hacia una seguridad integrada en múltiples dominios operativos. El concepto de misiones multidominios se centra en la sincronización de las iniciativas de ciberseguridad en entornos aéreos, terrestres, marítimos, espaciales y cibernéticos. Con el auge de las amenazas híbridas, los ataques ciberfísicos y la guerra electrónica, las organizaciones de defensa deben adoptar un enfoque holístico de la defensa que garantice la interoperabilidad fluida, el intercambio de inteligencia y la mitigación de amenazas (Verma, 2025).

El ataque de Estados Unidos a las instalaciones nucleares iraníes, conocido como Operación Martillo de Medianoche, ocurrido el 22 de junio, a las 2:15 a.m. hora de Irán se desarrolló bajo la doctrina de Operaciones Multidominio (OMD) las fuerzas armadas de los Estados Unidos plantean que el éxito en los conflictos actuales y futuros depende de la integración estrecha de todos los dominios, incluyendo el ciberespacio y el espectro electromagnético. Esta convergencia exige superar la tradicional separación entre operaciones físicas y cibernéticas, adoptando estructuras organizativas y conceptuales que

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

permitan acciones coordinadas en tiempo real a través de distintos entornos operativos (Perkins, 2018).

La integración de las capacidades cibernéticas con los dominios físicos tradicionales (aire, tierra, mar, espacio) se ha vuelto crucial para los sistemas de defensa modernos, ya que los adversarios explotan cada vez más las vulnerabilidades en la intersección de la infraestructura digital y física. Este artículo tiene como objetivo hacer un análisis estratégico para examinar la convergencia de la seguridad y defensa ciberfísica, sus desafíos y las soluciones emergentes para la resiliencia de misiones multidominio con una perspectiva hemisférica.

En este contexto, los conflictos modernos evidencian que ninguna misión de seguridad o defensa puede ignorar la dimensión cibernética: los ataques informáticos pueden paralizar infraestructuras críticas, socavar la confianza pública y extender los efectos de un conflicto más allá del campo de batalla tradicional El dominio cibernético abarca los componentes de software y hardware que permiten el procesamiento y análisis de datos, así como las capacidades de ataque y defensa en el ámbito digital (Vergara Cobos & Diao, 2024).

El concepto de seguridad ha evolucionado para abarcar no solo las amenazas digitales, sino también las vulnerabilidades físicas, dando lugar a la convergencia ciber-física. Esta se materializa con los sistemas SCF, que combinan infraestructura física, infraestructura informática y redes de comunicación para controlar entidades físicas mediante sensores y actuadores. La integración fluida entre lo digital y lo físico permite la creación de sistemas inteligentes e interconectados con aplicaciones militares estratégicas. En los dominios físicos, los sistemas de armas modernos están cada vez más equipados con sensores y capacidades de inteligencia artificial que dependen de la robustez de su integración con redes cibernéticas seguras.

La creciente complejidad de las operaciones de defensa exige una transición hacia una seguridad multidominio. Esta se basa en la sincronización entre dominios terrestre, marítimo, aéreo, espacial y cibernético para garantizar interoperabilidad, intercambio de inteligencia y respuestas efectivas ante amenazas híbridas. La integración de las capacidades cibernéticas con los dominios físicos tradicionales se ha vuelto esencial, ya que los adversarios explotan cada vez más las vulnerabilidades en la intersección entre infraestructuras digitales y físicas.

En América Latina y el Caribe (ALC), la rápida digitalización ha incrementado la exposición a Ciberamenazas, pero la mayoría de los países aún no ha consolidado capacidades cibernéticas robustas ni logrado una integración efectiva con sus estructuras de defensa física. La región ha experimentado un rápido aumento de incidentes cibernéticos —con una tasa anual de crecimiento del 25% en la última década— al mismo tiempo que exhibe rezagos significativos en sus niveles de protección (Vergara Cobos & Diao, 2024).

Esta combinación convierte al ciberespacio en un frente atractivo para actores maliciosos, como cibercriminales, grupos insurgentes, organizaciones criminales transnacionales o incluso Estados que emplean medios híbridos. Casos recientes, como el ciberataque masivo de ransomware contra Costa Rica en 2022 – que llevó a declarar un estado de emergencia nacional sin precedente – demuestran que las agresiones digitales pueden traducirse en crisis de seguridad nacional con impacto tangible en la economía, la gobernanza y la confianza institucional (Collier, 2022).

Desarrollo

El Ejército de EE. UU. adopta nueva doctrina de operaciones multidominio

Las doctrinas militares de EE. UU. ofrecen una base para integrar eficazmente la dimensión cibernética. Manuales y publicaciones conjuntas del Ejército reconocen al ciberespacio como un dominio operativo más. El concepto de Multi Domain Operations (OMD), según el manual del 1 de octubre de 2022, busca integrar todos los dominios (tierra, mar, aire, espacio y ciberespacio) para enfrentar adversarios pares. Esta integración combina ciberataques, guerra electrónica, información, fuego convencional y maniobra física. Unidades especializadas como los 'Multi-Domain Task Forces' ejemplifican esta visión. Estos batallones integran inteligencia de señales, espacio y ciberespacio para apoyar a fuerzas convencionales. El objetivo: generar efectos coordinados y multiplicar el poder en tiempo real.

Sin embargo, las doctrinas por sí solas no ganan batallas. Persisten desafíos en interoperabilidad tecnológica, estructura de mando, y formación de personal. Muchos ejércitos aliados carecen de una estructura organizativa que vincule estrechamente a los comandantes de operaciones cibernéticas con los comandantes de fuerzas terrestres, aéreas, navales o espaciales. Del mismo modo, la capacitación tradicional suele aislar la seguridad cibernética en unidades de IT, en lugar de entrenar a todos los niveles en escenarios donde lo cibernético y lo físico convergen. Este desfase doctrinal y organizativo puede llevar a demoras en la respuesta ante ciberamenazas durante combates convencionales, o a una falta de comprensión y comunicación mutua entre expertos técnicos y comandantes tácticos (Feickert, 2024).

Situación actual del dominio cibernético en América Latina y el Caribe

América Latina y el Caribe enfrentan una encrucijada en ciberseguridad. La digitalización ha generado sociedades interconectadas, pero la capacidad institucional no ha crecido al mismo ritmo. Informes destacan que ALC es la región con mayor crecimiento en incidentes cibernéticos divulgados, con un aumento anual del 25% en la última década. A la vez, es una de las menos preparadas: según el Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones, su puntaje promedio en ciberseguridad es 10.2 de 20. Esta brecha ha convertido al ciberespacio regional en un "campo de batalla", explotado por actores maliciosos. Las vulnerabilidades técnicas e institucionales son el blanco principal (Vergara Cobos & Diao, 2024).

Los ciberataques en ALC no solo aumentan en número, sino que son más disruptivos y con fines más amplios que el lucro financiero. Un 59% tienen motivaciones políticas, lo que refleja una transición hacia amenazas híbridas con fines de desestabilización. Ejemplos recientes lo demuestran: en 2022, Costa Rica sufrió un ataque con ransomware que generó pérdidas del 2,4% del PIB; en Ecuador y Argentina, filtraciones masivas expusieron datos sensibles; en Chile, un ataque con malware cerró temporalmente un banco estatal; y en 2023, un ataque impidió el voto en el extranjero en Ecuador. Estas agresiones digi-

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

tales generan impactos físicos graves (Vergara Cobos & Diao, 2024).

Pese al panorama crítico, la respuesta institucional en ALC ha sido desigual. Algunos países, como Chile, Colombia, Costa Rica, República Dominicana, México, Panamá y Perú, ya cuentan con Estrategias Nacionales de Ciberseguridad activas, lo que permite coordinación y asignación de recursos. Otros, como Bolivia, El Salvador y Honduras, carecen aún de estrategias integrales o están en fase de elaboración. Esto refleja una baja prioridad política en seguridad digital. Además, la región enfrenta escasez de talento especializado e inversión en infraestructura, lo que limita su capacidad de respuesta (Ciberlatam, 2024).

En 2024, la República Dominicana fue elegida para presidir el Grupo de Trabajo sobre Medidas de Fomento de la Confianza en el Ciberespacio (CBMs) de la OEA, consolidándose como uno de los pocos países caribeños con liderazgo hemisférico en ciberseguridad. Además, su CSIRT-RD, miembro del Forum of Incident Response and Security Teams (FIRST) desde 2020, ha fortalecido su integración en la comunidad internacional de respuesta a incidentes, lo que le permite acceder a apoyo técnico y participar activamente en el desarrollo de normativas globales sobre estabilidad en el ciberespacio (Presidencia de la Republica Dominicana, 2024a).

En esencia, el dominio cibernético en ALC se caracteriza actualmente por alto riesgo y preparación dispar. La creciente conectividad y digitalización amplían la superficie de ataque y atraen tanto a ciberdelincuentes oportunistas como a actores más sofisticados (incluyendo grupos auspiciados por Estados) que emplean tácticas híbridas. Si bien los gobiernos han comenzado a reaccionar mediante estrategias, leyes y mayor cooperación, persiste la necesidad de fortalecer integralmente las capacidades cibernéticas nacionales. Este fortalecimiento abarca no solo la dimensión técnica, sino también el desarrollo doctrinal, la capacitación de recursos humanos, la sensibilización política sobre el tema y la integración del ciberespacio dentro del planteamiento general de defensa y seguridad.

Conceptualización del dominio cibernético y estructura integradora

En el ámbito militar, el término dominio se refiere a un entorno o ámbito —físico o virtual— en el que se llevan a cabo operaciones y sobre el cual se busca ejercer cierto grado de control o superioridad. Tradicionalmente, las Fuerzas Armadas han reconocido dominios de la guerra como la tierra, el mar, el aire e, incluso desde fines del siglo XX, el espacio ultraterrestre. Desde inicios del siglo XXI, el ciberespacio ha sido ampliamente aceptado como un quinto dominio de las operaciones militares, con características propias pero complementarias a las de los dominios físicos (Pelcastre, 2019; Perkins, 2018). En Latinoamérica y el Caribe, numerosos países se han alineado con esta visión, denominando al ciberespacio como un dominio operacional comparable a los tradicionales. Por ejemplo, doctrinas militares regionales emplean ya el término dominio cibernético o espacio ciber para enmarcar las acciones de defensa y seguridad en entornos digitales (Saavedra, 2019).

Definir conceptualmente el dominio cibernético es esencial para delimitar su alcance y articular cómo interactúa con los demás dominios. De acuerdo con la Real Academia Española (2014), dominio es un ámbito, real o imaginario, de una actividad, mientras que ciberespacio se describe como un ámbito

virtual creado mediante medios informáticos interconectados. Desde el plano doctrinal, el profesor Daniel T. Kuehl ha ofrecido una definición operativa del ciberespacio, al describirlo como "un entorno operativo que consiste en la red interdependiente de sistemas de información conectados al Internet, incluyendo las infraestructuras informáticas y de telecomunicaciones, así como los datos que allí residen" (Saavedra, 2019). Con esta concepción, el ciberespacio, si bien intangible a simple vista, tiene una base física real (servidores, cables, enrutadores, dispositivos) y produce efectos medibles en el mundo.

El Comando Cibernético de Estados Unidos (USCYBERCOM) define el ciberespacio como un dominio con tres capas: física (infraestructura, hardware, cables, satélites), lógica (protocolos, software, algoritmos) y de ciberpersona (identidades digitales, redes sociales, interacciones humanas) (2018). Esta última, aunque abstracta, es clave porque refleja la actividad humana en línea. Estas capas demuestran que el ciberespacio no es uniforme, sino una red compleja de tecnología y personas. Protegerlo implica acciones diferenciadas: asegurar la infraestructura, optimizar los sistemas lógicos (ciberdefensa, actualizaciones, detección de intrusos) y gestionar la información e influencia digital (contrarrestar desinformación, proteger datos, educar usuarios).

Un elemento clave al conceptualizar un dominio es definir qué implica ejercer superioridad en él. En los ámbitos físicos, esto significa emplearlo libremente para operaciones propias mientras se restringe su uso al enemigo. En el dominio cibernético, este concepto se complica por su carácter difuso y la presencia de actores estatales y no estatales. Aun así, puede hablarse de superioridad cibernética como la capacidad de proteger redes propias y mantener la posibilidad de generar efectos ofensivos en el ciberespacio. Esto exige adaptar principios clásicos de la guerra —como sorpresa, seguridad, unidad de comando— al entorno digital, mediante ataques difíciles de atribuir y defensas sólidas (Saavedra, 2018).

Una consideración doctrinal clave es el rol del sector privado en el dominio cibernético. A diferencia de otros dominios controlados por el Estado (como el espacio aéreo o las fronteras), en el ciberespacio más del 90 % de la infraestructura y servicios depende de actores privados. Por tanto, ninguna estrategia de defensa cibernética puede excluir la cooperación público-privada. Militares y agencias deben trabajar con proveedores de Internet, empresas tecnológicas, de telecomunicaciones y del sector financiero para compartir información, definir estándares y coordinar respuestas. En América Latina, esta colaboración se ha formalizado mediante centros nacionales de ciberseguridad o equipos CERT/CSIRT con participación conjunta.

El dominio cibernético puede entenderse doctrinalmente como un entorno operativo multidimensional (físico, lógico y humano) donde se libran acciones de guerra y seguridad. Su control exige capacidades especializadas y la adaptación de principios militares tradicionales. Esta comprensión estructural es esencial para integrarlo con los dominios físicos. Solo entendiendo su alcance, funcionamiento interno y desafíos —como el rol del sector privado, la atribución de ataques o la velocidad de innovación— se pueden diseñar estrategias efectivas. Los casos de Costa Rica, República Dominicana y Colombia muestran cómo algunos gobiernos de la región ya integran el ciberespacio en sus estructuras de seguridad ante amenazas que superan lo físico.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Integración de dominios en misiones multidominio - iniciativas actuales

El concepto de Operaciones Multidominio (OMD), originado en la doctrina militar estadounidense, postula que las fuerzas conjuntas deben ser capaces de integrar capacidades en todos los dominios de forma coordinada para alcanzar la superioridad sobre adversarios cada vez más versátiles (Perkins, 2018). En la práctica, esto significa que una misión de defensa o seguridad no se circunscribe a un solo entorno (por ejemplo, terrestre), sino que involucra simultáneamente acciones terrestres, aéreas, navales, espaciales y cibernéticas, todas sincronizadas hacia el mismo objetivo operacional. Lograr tal convergencia requiere no solo cambios doctrinales, sino también innovaciones tecnológicas, entrenamientos conjuntos y nuevas estructuras de mando que permitan la comunicación fluida entre unidades de distintos dominios.

A nivel global, varias iniciativas actuales ejemplifican esfuerzos por materializar las operaciones multidominio. En Estados Unidos, las Fuerzas Armadas han implementado programas experimentales como Project Convergence (del Ejército) y Exercises Red Flag (Fuerza Aérea y Espacial) que integran sensores, plataformas de armas y redes de mando y control en escenarios simulados donde intervienen todos los dominios. La esencia es acortar el ciclo de decisión: que datos recolectados por satélites o ciberinteligencia alimenten en segundos decisiones de maniobra en tierra o ataques de precisión desde el aire, por ejemplo. Esto se soporta en la iniciativa de JADC2 (Joint All-Domain Command and Control), un sistema unificado de mando que conecta a todas las ramas militares en un solo tejido de información. Tales desarrollos están todavía en fases de prueba, pero han arrojado resultados prometedores en ejercicios contra amenazas convencionales y híbridas.

En América Latina, varios países avanzan hacia la integración multidominio en seguridad y defensa. Destaca el Ejercicio Conjunto Multidominio de Ciberdefensa y Guerra Electrónica (denominado *Ejercicio "Beato Carlo Acutis I"*), realizado por Argentina en 2022. Por primera vez, sus Fuerzas Armadas simularon un ataque combinado —sabotaje de cables submarinos y ciberataques a redes terrestres— para interrumpir la conectividad del país. La respuesta integró navíos como el ARA Piedrabuena, tropas terrestres, defensa aérea con sistemas RBS 70 y equipos de ciberdefensa y guerra electrónica. El objetivo fue sincronizar fuerzas convencionales y capacidades cibernéticas, actualizar procedimientos y extraer lecciones doctrinarias. Participaron más de 400 efectivos y múltiples plataformas aéreas, marítimas y terrestres (Mary, 2022).

Otro ejemplo relevante es la integración entre ciberdefensa y defensa aeroespacial en el ejercicio multinacional CRUZEX 2024, liderado por Brasil. Tradicionalmente enfocado en operaciones aéreas combinadas, esta edición incorporó por primera vez el componente CRUZEX Cyber, una simulación tipo "Captura la Bandera" (CTF) para entrenar en protección y ataque de sistemas virtuales de apoyo aeroespacial. Participaron más de 3.500 militares de 16 países en escenarios de conflicto regional, promoviendo interoperabilidad y actualización táctica entre fuerzas aéreas. La inclusión de capacidades cibernéticas, aeroespaciales y antiaéreas apuntó a reforzar la preparación operativa en entornos multidominio (Santos, 2024).

Más allá de ejercicios, también hay iniciativas en doctrina y educación para la integración multidominio. Varios países latinoamerica-

nos han actualizado sus documentos doctrinarios conjuntos para incluir explícitamente el concepto de Operaciones Multidominio. Por ejemplo, fuerzas armadas de Chile y Brasil han estudiado las OMD estadounidenses para adaptarlas a sus realidades, especialmente en escenarios como operaciones de paz donde las amenazas pueden ser híbridas. En la educación militar, seminarios y cursos sobre multidominio empiezan a ofrecerse en academias de guerra de la región, a menudo con cooperación de países de la OTAN o el Comando Sur de EE. UU.

En materia de mando, algunos países han establecido comandos conjuntos para integrar dominios. Colombia creó el Comando Conjunto Cibernético (CCOC), que coordina ciberdefensa entre Ejército, Armada y Fuerza Aérea, permitiendo operar el ciberespacio como dominio estratégico junto a otras fuerzas estatales (Villanueva Mendes, 2015). Brasil fundó en 2016 el Comando de Defensa Cibernética (CD Ciber), integrado por sus tres fuerzas, con la misión de proteger infraestructuras críticas y coordinar defensa cibernética. Durante los Juegos Olímpicos de Río 2016, el CD Ciber apoyó la seguridad digital. Desde entonces, ha ampliado su alcance y colabora con la ABIN, consolidando un modelo de integración entre inteligencia y ciberdefensa (EpEx, 2023).

Aunque los avances en ciberdefensa en América Latina varían, comparten un objetivo común: preparar fuerzas que operen integradas en todos los dominios. Ejercicios con componentes cibernéticos, reformas doctrinales y comandos especializados marcan una ruptura con las estructuras tradicionales. A medida que se acumulan experiencias —y se observan conflictos híbridos en otras regiones—, estos esfuerzos probablemente se expandan. La interoperabilidad multidominio no es solo una mejora táctica; es una necesidad estratégica frente a amenazas difusas donde lo civil y lo militar, lo legal y lo ilícito, se entrecruzan.

Estudios de caso: Costa Rica, República Dominicana y Colombia

Para ilustrar la realidad latinoamericana en la integración del dominio cibernético con los dominios físicos, se presentan a continuación tres casos nacionales. Cada caso refleja distintos niveles de desarrollo institucional, diferentes experiencias frente a amenazas cibernéticas y aproximaciones particulares para incorporar el ciberespacio en las misiones de seguridad y defensa.

Costa Rica: Respuesta nacional a una crisis cibernética sin Fuerzas Armadas

Costa Rica, un país sin ejército desde 1949, delega su seguridad nacional en cuerpos civiles y policiales. Sin embargo, en 2022, enfrentó una de las amenazas cibernéticas más graves del hemisferio cuando el grupo Conti lanzó ataques simultáneos contra casi 30 instituciones públicas, incluyendo ministerios clave como Hacienda y Ciencia y Tecnología, así como empresas estatales de servicios (Revista Summa, 2024). Ante la negativa a pagar rescate, se filtraron datos sensibles, lo que llevó al presidente Rodrigo Chaves a declarar estado de emergencia nacional—la primera vez que el país activaba ese mecanismo por una amenaza digital (Collier, 2022). Hubo interrupciones de servicios, parálisis fiscal y semanas de incertidumbre mientras el gobierno, con apoyo internacional, intentaba contener la crisis.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

La respuesta de Costa Rica evidenció tanto las debilidades como la resiliencia institucional de un país sin fuerzas armadas ante un ciberataque de gran escala. En ausencia de un comando militar de ciberdefensa, la gestión de la crisis recayó en el Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT-CR) nacional, y en el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) con el respaldo de cooperación internacional, incluyendo asistencia técnica de Estados Unidos. Se activaron protocolos de contingencia para mantener operativos servicios esenciales, se aislaron redes comprometidas y se fortaleció el monitoreo de infraestructura crítica, con especial énfasis en la protección de la red eléctrica y las telecomunicaciones para evitar efectos en cascada (Revista Summa, 2024).

Después de contener la crisis inmediata, Costa Rica dio pasos decisivos para fortalecer su ciberseguridad. Se aceleró la implementación de su Estrategia Nacional de Ciberseguridad 2017–2021, hasta entonces rezagada, y se iniciaron planes para una nueva estrategia a largo plazo. En 2023, el país lanzó oficialmente la Estrategia Nacional de Ciberseguridad 2023–2027, lo que marcó un giro hacia una planificación más sostenida. Para 2024, analistas locales destacaban avances notables: mayor presupuesto, autenticación multifactorial en sistemas gubernamentales y ejercicios regulares de simulación de ciberataques. Costa Rica también buscó apoyo internacional, uniéndose a iniciativas del Banco Mundial y foros hemisféricos de ciberresiliencia (Revista Summa, 2024).

El caso de Costa Rica demuestra que, incluso sin fuerzas armadas, un Estado puede (y debe) integrar el dominio cibernético en su estrategia de seguridad nacional, movilizando agencias civiles, fuerzas policiales e inteligencia en torno a un objetivo común. La convergencia ciber-física aquí se refleja en cómo un ataque digital afectó severamente funciones físicas del Estado (recaudación fiscal, atención de salud, etc.), y cómo la respuesta involucró tanto medidas técnicas en redes como acciones legales, diplomáticas y de seguridad pública. Para los países latinoamericanos, Costa Rica sirve de ejemplo de la importancia de prepararse ante Ciberamenazas sistémicas: contar con planes de contingencia, claridad en la cadena de mando (¿quién lidera en caso de ciber crisis?) y alianzas internacionales puede marcar la diferencia cuando la infraestructura digital de la nación está bajo asedio.

República Dominicana: Construcción de ciberresiliencia y liderazgo regional

La República Dominicana ha emergido como un actor clave en la ciberseguridad del Caribe, desarrollando una arquitectura institucional sólida y participando activamente en foros internacionales. Aunque posee Fuerzas Armadas, ha delegado la gestión del ciberespacio en entidades civiles, reconociendo la necesidad de coordinación público-privada. En 2018, adoptó su primera Estrategia Nacional de Ciberseguridad (2018–2021), y en 2022 aprobó la Estrategia Nacional de Ciberseguridad 2030, que orienta su visión a largo plazo. El Centro Nacional de Ciberseguridad (CNCS), bajo el Ministerio de la Presidencia, coordina acciones, supervisa la estrategia y responde ante incidentes (Ciberlatam, 2023).

Un hito importante fue la emisión del Decreto 685-22 de Ciberseguridad en 2022, que estableció obligaciones concretas para las instituciones de la administración pública en materia de protección cibernética. Este decreto insti-

tucionaliza la notificación obligatoria de incidentes: todos los organismos públicos deben reportar eventuales ciberataques o brechas de seguridad al CNCS y al CSIRT sectorial correspondiente en un plazo máximo de 24 horas. Asimismo, fija principios y lineamientos para elevar la madurez de ciberseguridad en el sector público, exige la adopción de estándares internacionales, la gestión proactiva de riesgos y la compartición de información sobre amenazas. En efecto, la República Dominicana está construyendo una cultura de ciberseguridad gubernamental, con reglas claras y canales formales de coordinación, lo que redunda en mayor integración del dominio cibernético en las operaciones cotidianas del Estado (Ciberlatam, 2023).

Aunque la República Dominicana no ha enfrentado un ataque tan disruptivo como el de Costa Rica, sí ha gestionado incidentes significativos. Entre 2021 y 2022, el CNCS reportó cerca de 980 eventos en instituciones del Estado, contenidos sin consecuencias graves gracias al trabajo del CSIRT-RD y al monitoreo activo de redes (Presidencia de la República Dominicana, 2023). Además, se registraron más de 4 mil millones de intentos de ciberataques, lo que confirma la presión constante sobre la infraestructura digital pública. En 2023, el gobierno lanzó un sistema de alerta automática de vulnerabilidades para instituciones públicas, fortaleciendo la capacidad preventiva del país (Presidencia de la República Dominicana, 2025).

En el frente militar, si bien la ciberdefensa en la República Dominicana es liderada por entidades civiles como el Centro Nacional de Ciberseguridad (CNCS), las Fuerzas Armadas han comenzado a integrar el componente cibernético en su planificación estratégica. Según el ministro de Defensa, teniente general Carlos Antonio Fernández Onofre, la modernización militar desde 2022 ha incluido inversiones significativas en tecnología, inteligencia y mejoras en los controles para fortalecer la ciberseguridad institucional, como parte de un plan amplio de fortalecimiento del aparato militar nacional (Villegas, 2025).

La Estrategia Nacional de Ciberseguridad 2030 (2022), establecida por el Decreto 313-22, reconoce la dimensión de defensa cibernética como un componente estratégico, con responsabilidades compartidas entre el Ministerio de Defensa, el Departamento Nacional de Investigaciones (DNI), y otras agencias relevantes. La estrategia enfatiza la protección de infraestructuras críticas y la prevención del ciberterrorismo mediante políticas coordinadas, capacitación especializada y la integración de estándares internacionales. Estas acciones se complementan con el liderazgo del Centro Nacional de Ciberseguridad (CNCS), que supervisa la implementación general y fomenta la colaboración público-privada para fortalecer la ciberresiliencia nacional.

Además, el presidente Luis Abinader anunció en 2022 una histórica inversión en defensa, que incluyó la adquisición de helicópteros, aeronaves de vigilancia, vehículos blindados, y la instalación de una valla fronteriza inteligente con Haití equipada con sensores, cámaras y drones militares. Aunque no se detalla públicamente, la ciberseguridad de estos sistemas de vigilancia fronteriza presumiblemente forma parte de los esfuerzos integrales para proteger las capacidades tecnológicas del Estado (HaitiLibre, 2022).

Un rasgo distintivo del caso dominicano es su liderazgo regional e internacional en temas ciber. Además de participar en el grupo de la OEA mencionado, la República Dominicana ha sido sede de reuniones hemisféricas de

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

equipos CSIRT (en agosto de 2024 organizó la primera reunión de trabajo para desarrollar un protocolo regional de asistencia inmediata ante crisis cibernéticas) (Presidencia de la Republica Dominicana, 2024b). Tal liderazgo tiene beneficios tangibles: ante un incidente grave, la República Dominicana puede recurrir con facilidad a sus contrapartes internacionales para recibir apoyo técnico; del mismo modo, su voz tiene peso en la discusión de normativas globales sobre estabilidad en el ciberespacio.

La experiencia dominicana demuestra que, incluso con recursos limitados, un país de ingresos medios puede integrar el dominio cibernético en su arquitectura de seguridad si hay voluntad política y una estrategia clara. La Estrategia 2030, el CNCS y normativas como el Decreto 685-22 han establecido un marco institucional exigente. Su proyección internacional revela una comprensión madura del ciberespacio como un entorno interdependiente, donde la cooperación es clave. Para países con condiciones similares, este enfoque resalta la importancia de institucionalizar buenas prácticas, como el reporte de incidentes, y asumir un rol activo en la comunidad internacional de ciberseguridad.

Colombia: Militarización del ciberespacio y combate a amenazas híbridas

Colombia, con un extenso historial de desafíos de seguridad internos (conflicto con guerrillas, narcotráfico, crimen organizado), ha reconocido tempranamente el ciberespacio como un frente más de confrontación contra amenazas tanto estatales como no estatales. A diferencia de Costa Rica o República Dominicana, Colombia ha militarizado en buena medida la gestión del dominio cibernético, creando estructuras dedicadas de ciberdefensa en el seno de sus Fuerzas Militares y articulándolas con sus estrategias de seguridad nacional. Este enfoque se explica, en parte, porque el país ha sufrido no solo ataques cibernéticos del tipo convencional (fraudes financieros, ransomware, etc.) sino también campañas de ciberterrorismo y desinformación vinculadas con actores armados ilegales y con injerencias externas en su panorama de conflicto interno (Pelcastre, 2019).

El pilar de la integración ciber-física colombiana es el Comando Conjunto Cibernético (CCOC) de las Fuerzas Militares, creado oficialmente a inicios de la década de 2010 como primera línea de defensa en el quinto dominio. Su misión es planear y conducir operaciones militares en el ciberespacio para contrarrestar amenazas a la seguridad nacional, desde la protección de redes institucionales hasta el análisis forense digital y la implementación de protocolos de defensa informática (Cruz Rubio, 2021).

Si bien no se han documentado públicamente operaciones ofensivas contra infraestructuras específicas de grupos armados, documentos doctrinales confirman que las capacidades del CCOC incluyen operaciones ofensivas diseñadas para interrumpir, degradar o destruir redes informáticas y sistemas del adversario cuando sea necesario. Estas acciones buscan afectar el normal funcionamiento de las operaciones enemigas, como parte integral del poder militar en el ciberespacio. En contextos de operaciones especiales, incluso se plantea la incorporación táctica de agentes cibernéticos para insertar código malicioso en redes hostiles, lo que permite neutralizar o interrumpir comunicaciones críticas bajo presión operativa (Cruz Segura & Di Genaro, 2024).

Además, el CCOC monitorea redes sociales y espacios digitales para detectar campañas

de desinformación o propaganda destinadas a socavar la estabilidad del Estado. Este enfoque responde a la comprensión de que las guerras modernas se libran también con narrativas e influencia sobre la opinión pública. Las operaciones cibernéticas de Colombia, tal como lo definen documentos institucionales, abarcan todo el ciclo de prevención, vigilancia, neutralización y recuperación en caso de incidentes, con un énfasis especial en proteger la infraestructura crítica nacional que sustenta servicios esenciales como energía, salud, telecomunicaciones y defensa (Cruz Segura & Di Genaro, 2024).

Operativamente, el Comando Conjunto Cibernético (CCOC) colombiano se ha dotado de capacidades especializadas en ciberdefensa, incluyendo plataformas tecnológicas, personal entrenado, y coordinación con entidades como colCERT y el Centro Cibernético Policial. Entre sus funciones está proveer ciberinteligencia, proteger infraestructuras críticas y liderar la respuesta ante incidentes que comprometan la seguridad nacional (Mora Gámez, & Baquero, 2022, pp. 125-139). Durante las protestas sociales de 2021, grupos hacktivistas como Anonymous vulneraron sitios gubernamentales clave; la respuesta técnica para mitigar estos ataques involucró al ecosistema de ciberdefensa del país, incluyendo al CCOC en colaboración con otras entidades como ColCERT y CCP (Mora Gámez, & Baquero, p. 127).

Los resultados de esta estrategia se observan en varios planos. Colombia ha logrado frustrar ciberataques significativos y mitigar su impacto. Entre 2017 y 2019, el país registró más de 53.000 incidentes de seguridad informática atribuidos a crimen organizado transnacional (principalmente robo de dinero e identidad), pero gracias a una postura proactiva ("mantener nunca la defensa abajo" en palabras de un oficial), no se han materializado daños catastróficos en infraestructuras críticas (Pelcastre, 2019).

En respuesta a la ofensiva del ELN en la región del Catatumbo a inicios de 2025, el Ejército colombiano desplegó 300 soldados con apoyo de la Fuerza Aeroespacial para neutralizar los enfrentamientos con disidencias de las FARC y proteger a la población civil, incluyendo la evacuación de heridos y la asistencia a familias desplazadas (Xinhua Español, 2025). Estas operaciones ofensivas también buscaron controlar corredores de movilidad clave y restablecer la seguridad en centros urbanos como Tibú, epicentro de una de las crisis humanitarias más graves desde el acuerdo de paz de 2016 (SWI, 2025).

En términos normativos, Colombia también ha avanzado: su documento de política CONPES 3701 de 2011 ya delineaba la necesidad de integrar ciberseguridad y ciberdefensa, y fue actualizándose con una Política de Seguridad Digital 2020–2022. Actualmente, se discute en el Congreso el proyecto de ley 023 de 2023 que crearía la Agencia Nacional de Seguridad Digital, con el objetivo de coordinar y centralizar funciones dispersas entre el Ministerio de Defensa, la Policía Nacional, la Fiscalía y otros actores institucionales, optimizando la respuesta del Estado ante incidentes cibernéticos (Mejía Marulanda, 2024). De lograrse, esta agencia civil se complementaría con el Comando Conjunto Cibernético ya existente, fortaleciendo el ecosistema nacional de ciberseguridad.

En conclusión, Colombia ofrece un ejemplo de integración ciber-física como parte de una estrategia de defensa nacional consolidada. El país ha desarrollado capacidades multimisión en el dominio cibernético, usándolas tanto para proteger sus infraestructuras y redes gu-

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

bernamentales como para apoyar operaciones contra amenazas tradicionales (guerrilla, terrorismo, crimen organizado). Al tratar al ciberespacio como otro frente de su prolongado conflicto interno, Colombia ha innovado en tácticas conjuntas, combinando acciones cinéticas con operaciones en línea. La experiencia colombiana ofrece lecciones útiles para países que enfrentan amenazas híbridas, al subrayar el valor de contar con unidades especializadas, fusionar inteligencia digital y convencional, y adaptar la doctrina militar a la realidad del conflicto virtual.

Capacidades multimisión ante amenazas híbridas - recomendaciones y casos destacados

Las amenazas híbridas son un desafío cada vez más común en la seguridad global y regional, caracterizado por la combinación de métodos convencionales e irregulares con fines estratégicos. El concepto alude a la articulación de capacidades regulares e irregulares —acciones militares abiertas junto con tácticas encubiertas o no militares— dirigidas a un mismo objetivo (Fernández Córdoba, 2024). En lugar de un enfrentamiento directo, los actores hostiles (estatales o no) explotan vulnerabilidades en varios dominios: lanzan ciberataques, fomentan disturbios, difunden propaganda, emplean proxis para sabotaje y recurren al crimen organizado o al terrorismo. El resultado es un entorno difuso, donde la línea entre guerra y paz se desdibuja y las instituciones deben responder en varios frentes a la vez.

Frente a estas amenazas híbridas, las naciones necesitan desarrollar capacidades multimisión, entendidas como la aptitud de sus fuerzas de seguridad y defensa para cumplir misiones diversas y simultáneas en diferentes dominios. A continuación, se presentan recomendaciones estratégicas para fortalecer dichas capacidades en el contexto latinoamericano, acompañadas de ejemplos de países que están encabezando esfuerzos en cada aspecto:

1. Adoptar un enfoque integral de seguridad nacional. Las estructuras estatales deben evitar divisiones estrictas entre seguridad interna (a cargo de policías) y defensa externa (a cargo de militares) cuando enfrentan amenazas híbridas, ya que estas desdibujan dicha frontera. Se recomienda establecer marcos de coordinación inter agencial permanentes (ej. comités nacionales de seguridad cibernética e híbrida) que integren a militares, policías, inteligencia civil, autoridades regulatorias y sector privado. Por ejemplo, Colombia ha integrado sus esfuerzos contra la desinformación combinando recursos de inteligencia militar (CCOC) con su Centro Cibernético Policial, logrando respuestas unificadas a campañas de influencia malignas.

2. Fortalecer la ciberdefensa como componente central de la defensa nacional. Más allá de la inversión en tecnología, esto requiere contar con equipos de respuesta rápida, analistas en inteligencia de señales, hackers éticos y un marco legal claro que defina las reglas de operación en el ciberespacio. Estados Unidos y las naciones de la OTAN han establecido Ciber comandos con mandato tanto defensivo como ofensivo, que en los últimos conflictos (por ejemplo, frente a amenazas rusas) han realizado operaciones de "caza hacia adelante" desarticulando malware antes de que ataque sus redes (Pomerleau, 2025). En América Latina, Brasil con su Comando de Defensa Cibernética, ha invertido en simuladores y ejercicios in-

ternacionales (como los mencionados CRUZEX Cyber) para preparar a su personal. Cada país debería considerar la creación o el fortalecimiento de comandos conjuntos de ciberdefensa, con una línea directa al más alto nivel militar para asegurar su peso en la planificación estratégica.

3. Desarrollar fuerzas flexibles y versátiles. Las amenazas híbridas pueden exigir, por ejemplo, que en una misma misión humanitaria las tropas deban lidiar con desinformación en redes locales, protegerse de drones comerciales armados y mantener redes de comunicación seguras frente a hackeos. Para ello, es necesario que las unidades militares y policiales sean versátiles o cuenten con destacamentos especializados integrados. Una buena práctica la ofrece Francia con su concepto de "GTIA aéroterrestre" usado en operaciones en África, donde cada Grupo Táctico incluye no solo infantería y blindados, sino especialistas en guerra electrónica e inteligencia de señales para contrarrestar los artefactos explosivos improvisados detonados vía celular por terroristas. Trasladado a Latinoamérica, cuando las fuerzas mexicanas o centroamericanas enfrentan carteles de la droga (que a veces emplean tácticas híbridas con corrupción de información, comunicaciones cifradas, etc.), deberían desplegar ya con equipos de ciberinteligencia y guerra electrónica que intercepten y bloqueen las comunicaciones enemigas. Argentina, con el ejercicio en Las Toninas, ya probó la eficacia de combinar tropas convencionales con expertos de ciber/electrónica en un solo operativo. La recomendación es institucionalizar estas unidades conjuntas multidominio a nivel táctico, para que se entrenen juntas de antemano y tengan procedimientos estandarizados.

4. Aumentar la cooperación internacional y regional. Ningún país puede abordar solo amenazas que, por naturaleza, atraviesan fronteras (virus informáticos globales, campañas de desinformación que ignoran límites geográficos, redes criminales transnacionales). Es crucial aprovechar marcos multilaterales. La OEA ya trabaja en confianza cibernética, pero podría expandir sus ejercicios de simulación híbrida. Mediante su Programa de Ciberseguridad y la resolución CICTE/RES.1/17, la OAE ha promovido medidas de cooperación técnica entre sus Estados miembros. También existen centros de excelencia como el Centro Europeo de Excelencia contra Amenazas Híbridas (COE en Finlandia), con el cual países americanos pueden colaborar para intercambiar lecciones aprendidas de escenarios en Europa del Este. Estados Unidos ha potenciado la asistencia en ciberseguridad a sus aliados latinoamericanos a través del Comando Sur (USSOUTHCOM), mediante acuerdos de cooperación, ejercicios conjuntos y revisiones técnicas en países como Costa Rica, Paraguay, Panamá, El Salvador y Argentina (Hamilton & Ruiz, 2023; Thomas, 2022; U.S. Southern Command, 2024). Esta colaboración incluye actividades como el fortalecimiento de centros de operaciones cibernéticas, intercambios de expertos en defensa cibernética con Argentina, y ejercicios como CENTAM Guardian, donde equipos de ciberdefensa de Guatemala, El Salvador y Honduras practicarán en redes simuladas (Nelson, 2022; Thomas, 2022). Asimismo, espacios regionales como la conferencia CENTSEC han incorporado temas de ciberseguridad en sus agendas,

consolidándose como foros clave para enfrentar amenazas emergentes y fortalecer capacidades compartidas (Pelcastre, 2025). Se recomienda formalizar alianzas regionales enfocadas en amenazas híbridas, que complementen los mecanismos de defensa existentes e integren actores civiles—como un Task Force hemisférico contra la desinformación electoral.

5. Invertir en inteligencia estratégica y anticipación. Las amenazas híbridas suelen gestarse silenciosamente antes de desencadenarse abiertamente. Un Estado debe poder detectar signos tempranos en múltiples dominios: rumores en la Deep web de un ataque inminente, movimientos financieros inusuales, agrupación de fuerzas paramilitares, campañas mediáticas sospechosas. Esto requiere una inteligencia fusionada que combine fuentes tradicionales (humanas, señal, geoespaciales) con ciberinteligencia e inteligencia artificial para analizar grandes datos. En América Latina, un caso emergente es Chile, que en su reciente Política Nacional de Ciberseguridad 2023–2028 priorizó el fortalecimiento de la infraestructura institucional y técnica, incluyendo la creación de una Agencia Nacional de Ciberseguridad (ANCI), aunque sin contemplar aún un centro dedicado exclusivamente al análisis de amenazas híbridas (IMF, 2024; Biblioteca del Congreso Nacional del Chile, 2023). Se recomienda a los países destinar parte de sus fondos de seguridad y defensa a herramientas analíticas avanzadas (por ejemplo, sistemas de Big Data para redes sociales que alerten sobre campañas coordinadas) y entrenar analistas con mentalidad "híbrida" capaces de correlacionar eventos dispersos.
6. Fortalecer la resiliencia societal y la comunicación estratégica. Las amenazas híbridas apuntan a explotar fracturas dentro de la sociedad objetivo (divisiones políticas, desconfianza en instituciones) y provocar reacciones desproporcionadas. Por ello, la respuesta no es solo militar/policial, sino que involucra la resiliencia de la población y una hábil gestión de la información por parte del gobierno. Programas educativos de ciber higiene, alfabetización mediática para reconocer noticias falsas, protocolos para continuidad de negocios en sector privado, son parte de las capacidades multimisión menos tangibles pero cruciales. Varios países europeos han implementado conceptos de "defensa total" que involucran a la ciudadanía en la protección del país (por ej., Finlandia y Estonia, muy conscientes de la amenaza híbrida rusa, donde cada ciudadano tiene un rol en resiliencia). En Latinoamérica, se podría emular en contextos locales: Costa Rica, tras su ataque de 2022, ha fomentado fuertemente la cultura de la ciberseguridad en sector público y privado , mientras Colombia ha desplegado campañas para fortalecer la confianza en la Fuerza Pública ante la propaganda hostil. La recomendación es elaborar planes nacionales de resiliencia híbrida, que incluyan desde respaldos energéticos para cortes de luz intencionales, hasta manuales de comportamiento ciudadano ante campañas de miedo o caos fomentadas artificialmente.

En cuanto a países que destacan en el desarrollo de capacidades multimisión contra amenazas híbridas en el hemisferio occidental, además de los casos ya mencionados de Colombia, Brasil, República Dominicana y Argentina, cabe resaltar a Estados Unidos y Canadá como referentes por sus avanzadas

doctrinas y recursos. Estados Unidos, mediante su concepto de Deterrence by Denial en ciberespacio y la implementación de fuerzas de tarea multidominio en unidades del Ejército, está marcando pautas que aliados cercanos como Colombia buscan seguir (Lane, 2023). Canadá, a través de su enfoque de seguridad nacional integral (incluyendo protección de procesos electorales contra injerencia extranjera y un centro de ciberseguridad puntero), ofrece un modelo adaptado a un país con población y extensión moderada, similar a muchos latinoamericanos.

En el contexto latinoamericano, México empieza a dar señales de abordar amenazas híbridas ligadas al crimen organizado al integrar inteligencia financiera, ciberinteligencia e incursiones armadas de manera más sincronizada contra cárteles. Perú y Ecuador, tras experiencias de crisis política acompañadas de ciberataques (por ejemplo, los ataques del grupo Guacamaya que expusieron miles de documentos militares en 2022), están reestructurando sus sistemas de inteligencia y ciberdefensa para no ser sorprendidos de nuevo. En suma, la región en su conjunto se halla en distintas etapas, pero la tendencia es clara: las capacidades multimisión dejarán de ser una opción deseable para convertirse en una necesidad estratégica ineludible ante la realidad de las amenazas híbridas.

Imperativos operacionales para la integración

1. Neutralización de Amenazas Híbridas

   Los conflictos modernos combinan ciberataques con ataques cinéticos, como el incidente del gusano Stuxnet (que atacó sistemas de control industrial) y las interrupciones en activos militares dependientes del GPS. La integración entre dominios permite respuestas sincronizadas a estas amenazas multivectoriales.

2. Interdependencia de la Infraestructura

   Las comunicaciones espaciales, las redes inteligentes y los sistemas de armas autónomos dependen de arquitecturas ciberfísicas interconectadas. Por ejemplo: un BESS (Sistema de Almacenamiento de Energía de Baterías) comprometido podría desestabilizar las redes eléctricas o los sistemas de propulsión naval, lo que podría generar riesgos con efectos en cascada.

3. Interoperabilidad Aliada

   Iniciativas como las Operaciones Multidominio de la OTAN y el JADC2 (All-Domain Command and Control) del Departamento de Defensa de EE. UU. hacen hincapié en protocolos estandarizados para el intercambio seguro de datos en los dominios aéreo, terrestre, marítimo, espacial y cibernético.

Desafíos claves

- Integración de Sistemas diferentes con protocolos incompatibles dificultan la fusión de datos en tiempo real. Esto demanda actualizaciones modulares de las puertas de enlace de las aplicaciones de la interfaz de programación de aplicaciones (API).
- Vulnerabilidades de la cadena de suministro Los componentes comprometidos (por ejemplo, unidades de BESS (Battery Energy Storage Systems) fabricadas en China tienen una arquitectura de puertas traseras de confianza cero, auditorías de hardware.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

- Ampliación de la superficie de ataque mediante los dispositivos conectados por Internet de las cosas y operaciones tecnológicas. (IoT/OT) en sistemas navales y de aviación crean puntos de entrada. La Segmentación de red, detección de anomalías mediante el empleo de IAG.
- Disyuntiva entre velocidad y seguridad por los retrasos en el cifrado de las comunicaciones en el campo de batalla. El empleo de algoritmos resistentes a la tecnología cuántica y computación muy sofisticada.

Recomendaciones estratégicas

1. Estructuras de mando unificadas

   Establecer grupos de trabajo ciberfísicos conjuntos (p. ej., la Agencia Cibernética de Defensa de la India) para supervisar las operaciones Inter dominio.

2. Armonización de estándares

   Adoptar los marcos de operaciones multidominio por ejemplo en la OTAN para la comunicación cifrada Inter dominio y los manuales de respuesta a incidentes.

3. Fortalecimiento de la cadena de suministro

   Exigir certificaciones de componentes de terceros y fabricación local para sistemas críticos como los BMS (sistemas de gestión de baterías).

4. Entrenamiento basado en simulación

Realizar simulacros de guerra que simulen ataques cibernéticos coordinados contra infraestructuras multidominio. La fusión de la ciberseguridad y la seguridad física ya no es opcional, sino un imperativo estratégico. Aprovechar la arquitectura interoperable, la criptografía avanzada y los sistemas de comando potenciados por IAG, las organizaciones de defensa pueden lograr resiliencia ante las amenazas híbridas en constante evolución. El éxito dependerá de romper los silos o situaciones Inter dominio que puedan obstaculizar las comunicaciones entre los equipos de ciberseguridad y seguridad física, como lo demuestran iniciativas de primera línea como JADC2 de los EE. UU y el Comando Espacial Integrado de la India.

Conclusiones

Integrar plenamente el dominio cibernético con los dominios físicos es hoy un imperativo estratégico para las fuerzas armadas del siglo XXI. Las operaciones cibernéticas ya no son un complemento, sino un multiplicador de poder que puede inclinar la balanza en conflictos modernos. La sinergia entre acciones cinéticas y digitales permite responder de manera más eficaz ante amenazas híbridas, mientras que su ausencia puede generar vacíos operacionales críticos.

En América Latina y el Caribe, la creciente exposición a Ciberamenazas contrasta con capacidades defensivas aún desiguales. El análisis regional evidencia que los países mejor preparados —como Colombia, República Dominicana o Brasil— han comenzado a consolidar estructuras ciberfísicas integradas, aunque en diferentes etapas de madurez. Estas experiencias demuestran que no existe una fórmula única, pero sí principios comunes: planificación interinstitucional, entrenamiento conjunto, y adopción de doctrinas operativas que incorporen al ciberespacio desde la fase táctica.

Asimismo, la integración de dominios no debe limitarse al ámbito militar. Las amenazas

híbridas actuales atacan infraestructura crítica, redes sociales, procesos democráticos y cohesión social. Por ello, las capacidades multimisión deben incluir no solo fuerzas armadas entrenadas en operaciones multidominio, sino también ciudadanía informada, marcos legales modernos y alianzas público-privadas. La defensa efectiva frente a estos retos exige una respuesta convergente, coordinada y adaptada a las realidades del hemisferio.

En resumen, avanzar hacia una convergencia ciber-física no es solo una aspiración técnica, sino una necesidad estratégica para preservar la soberanía, la seguridad y la estabilidad regional. Al adaptar los principios de las Operaciones Multidominio (OMD) a los contextos latinoamericanos, los países del hemisferio podrán fortalecer su interoperabilidad, disuadir agresiones y responder con mayor resiliencia a las complejidades del entorno operativo contemporáneo.

Referencias

Biblioteca del Congreso Nacional de Chile. (2023). *Construyendo la ciberseguridad en Chile*. Comisión Desafíos del Futuro, Ciencia, Tecnología e Innovación. https://www.forociber.cl/foro/site/docs/20240322/20240322150520/edicion_construyendo_la_ciberseguridad_en_chile_v2.pdf

Blue Goat Cyber. (2025). *Cyber-Physical Systems: Bridging Digital and Physical Security [Sistemas ciberfísicos: Tendiendo puentes entre la seguridad digital y la física]*. https://bluegoatcyber.com

Ciberlatam. (2023). República Dominicana publica el decreto 685-22 de ciberseguridad. *Segurilatam*. https://www.segurilatam.com/actualidad/republica-dominicana-publica-el-decreto-685-22-de-ciberseguridad_20230103.html

Ciberlatam. (2024). Estas son las estrategias nacionales de ciberseguridad de los países latinoamericanos. *Segurilatam*. https://www.segurilatam.com/ciberilatam/estas-son-las-estrategias-nacionales-de-ciberseguridad-de-los-paises-latinoamericanos_20240514.html

Collier, K. (2022, 8 de mayo). Costa Rica declara estado de emergencia ante ataque cibernético masivo estilo ransomware. *NBC News*. https://www.nbcnews.com/tech/tech-news/costa-rica-declares-state-emergency-ransomware-attack-rcna28415

Cruz Rubio, J. (2021). *Defendiendo el ciberespacio: Una aproximación al estado de Colombia frente a la ciberdefensa* [Tesis de maestría, UniversidadMilitarNuevaGranada].Repositorio Institucional UMNG. https://repository.umng.edu.co/server/api/core/bitstreams/67dd16a6-dfb8-4244-961e-8cd887469aba/content

Cruz Segura, J. G., & Di Genaro, R. (2024). Soporte cíber a Fuerzas Especiales del Ejército colombiano en ambiente táctico. En L. Montero Moncada & O. A. Garzón Gómez (Eds.), *Comandos: Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea* (pp. 163-188). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602809.07

Estrategia Nacional de Ciberseguridad 2022. Gobierno de República Dominicana. https://cncs.gob.do/wp-content/uploads/2022/07/Decreto-313-22.pdf

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

EpEx. (2023). *Consolidação do Comando de Defesa Cibernética*. Exército Brasileiro. http://www.epex.eb.mil.br/index.php/ultimas-noticias/497-consolidacao-do-comando-de-defesa-cibernetica

Feickert, A. (2024). *Defense primer: Army multi-domain operations (MDO) [Manual de defensa: Operaciones multidominio del Ejército]*. Congressional Research Service. https://www.congress.gov/crs_external_products/IF/PDF/IF11409/IF11409.13.pdf

Fernández Córdoba, J. (2024, 4 de febrero). La tecnología multidominio y la amenaza híbrida: el enemigo invisible ya está aquí. *El Confidencial*. https://www.elconfidencial.com/espana/2024-02-04/foro-desafios-defensa-amenaza-híbrida-guerra-multidominio_3823290/

HaitiLibre. (2022, 7 de junio). Haiti - Security: Very important purchases of military equipment in the Dominican Republic [Haití - Seguridad: Compras muy importantes de material militar en la República Dominicana]. *HaitiLibre*. https://www.haitilibre.com/en/news-37851-haiti-security-very-important-purchases-of-military-equipment-in-the-dominican-rep.html

Hamilton, J., & Ruiz, V. (2023). Employing strategic cyber competition in Latin America [Emplear la cibercompetencia estratégica en América Latina]. *Journal of the Americas,* 5(2), 274-298. https://www.airuniversity.af.edu/Portals/10/JOTA/journals/Volume-5_Issue-2/23-Hamilton-Ruiz_eng-w.pdf

International Monetary Fund. [IMF] (2024). *Cybersecurity and financial stability: Considerations for Chile [Ciberseguridad y estabilidad financiera: Consideraciones para Chile]*. https://www.elibrary.imf.org/view/journals/002/2024/042/article-A002-en.xml

Kissinger, H. A., Schmidt, E., & Huttenlocher, D. (2021). *The age of AI and our human future [La era de la inteligencia artificial y nuestro futuro humano]*. Little Brown.

Lane, G. (2023). Operationalizing deterrence by denial in the cyber domain [Operacionalización de la disuasión por denegación en el ciberespacio]. *Military Cyber Affairs*, 6(1). https://scholarcommons.usf.edu/mca/vol6/iss1/

Mary, G. (2022, 15 de julio). Argentina realiza el primer ejercicio conjunto de ciberdefensa y guerra electrónica. *InfoDefensa*. https://www.infodefensa.com/texto-diario/mostrar/4076957/argentina-realiza-primer-ejercicio-conjunto-multidominio-ciberdefensa-guerra-electronica

Mejía Marulanda, M. (2024, 28 de septiembre). Sin haberse creado la Agencia de Seguridad Digital ya genera polémica: congresistas denuncian posible 'mico'. *Infobae*. https://www.infobae.com/colombia/2024/09/28/sin-haberse-creado-la-agencia-de-seguridad-digital-ya-genera-polemica-congresistas-denuncian-posible-mico/

Mora Gámez, I. H., & Baquero Valdés, F. (2022). Capacidades del Estado colombiano para combatir las amenazas y los desafíos multidimensionales en los dominios aéreo y ciberespacial. En F. Baquero Valdés (Ed.), *Poder aéreo, espacial y ciberespacial frente a desafíos y amenazas multidimensionales que afectan al Estado colombiano* (pp. 109-151). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602106.03

Nelson, V. (2022, 20 de diciembre). NH Guard, Salvadoran cyber teams strengthen partnership [La Guardia Nacional y los equipos cibernéticos salvadoreños refuerzan su colaboración]. *U.S. Southern Command*. https://www.

southcom.mil/MEDIA/NEWS-ARTICLES/Article/3258497/nh-guard-salvadoran-cyber-teams-strengthen-partnership/

Pelcastre, J. (2019, 12 de junio). Militares colombianos en guerra contra cibercriminales. *Diálogo Américas*. https://dialogo-americas.com/es/articles/militares-colombianos-en-guerra-contra-cibercriminales/

Pelcastre, J. (2025, 1 de abril). Central America builds on CENTSEC for security [Centroamérica se apoya en CENTSEC para su seguridad]. *Diálogo Américas*. https://dialogo-americas.com/articles/central-america-builds-on-centsec-for-security/

Perkins, D. G. (2018). Preparándonos para combatir hoy: Las operaciones multidominio y el Manual de Campaña 3-0. *Military Review,* (3), 2-12. https://www.armyupress.army.mil/Journals/Edicion-Hispanoamericana/Archivos/Tercer-Trimestre-2018/Preparandonos-para-combatir-hoy/

Pomerleau, M. (2025, 1 de abril). Cybercom discovered Chinese malware in South American nations—Joint Chiefs chairman nominee [El Cibercomando descubrió malware chino en países sudamericanos]. *DefenseScoop*. https://defensescoop.com/2025/04/01/cybercom-chinese-malware-south-america-dan-caine-joint-chiefs-trump/

Presidencia de la República Dominicana. (2023, 7 de noviembre). El Centro Nacional de Ciberseguridad ha atendido alrededor de 980 incidentes cibernéticos en instituciones del Estado. *Ministerio de la Presidencia*. https://minpre.gob.do/comunicacion/notas-de-prensa/el-centro-nacional-de-ciberseguridad-ha-atendido-alrededor-de-980-incidentes-ciberneticos-en-instituciones-del-estado

Presidencia de la República Dominicana. (2024a, 19 de febrero). *República Dominicana lidera el Grupo de Trabajo de Medidas de Fomento de la Confianza en el Ciberespacio de la OEA*. https://presidencia.gob.do/noticias/republica-dominicana-lidera-el-grupo-de-trabajo-de-medidas-de-fomento-de-la-confianza-en

Presidencia de la República Dominicana. (2024b, 9 de mayo). *República Dominicana reúne a líderes de los Equipos de Respuesta ante Incidentes Cibernéticos (CSIRT) nacionales de América Latina y el Caribe*. https://presidencia.gob.do/noticias/republica-dominicana-reune-lideres-de-los-equipos-de-respuesta-ante-incidentes

Presidencia de la República Dominicana. (2025, 3 de abril). *La República Dominicana es sede de evento internacional sobre ciberseguridad y diplomacia cibernética*. https://presidencia.gob.do/noticias/la-republica-dominicana-es-sede-de-evento-internacional-sobre-ciberseguridad-y-diplomacia

Real Academia Española. (2024). *Diccionario de la lengua española* (23.ª ed.). https://dle.rae.es/dominio

Revista Summa. (2024, 20 de marzo). ¿Cómo ha avanzado Costa Rica en ciberseguridad tras la ola de ataques del 2022? *Revista Summa*. https://revistasumma.com/como-ha-avanzado-costa-rica-en-ciberseguridad-tras-la-ola-de-ataques-del-2022/

Saavedra, B. (2019, 11 de junio). El papel de los militares en el ciberespacio como dominio: implicancias, retos y oportunidades. *CEEEP*. https://ceeep.mil.pe/2019/06/11/el-papel-de-los-militares-en-el-ciberespacio-como-dominio-implicancias-retos-y-oportunidades/

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Santos, E. (2024, 13 de noviembre). Fuerza Aérea Brasileña inicia Ejercicio CRUZEX 2024. *Diálogo Américas*. https://dialogo-americas.com/es/articles/fuerza-aerea-brasilena-inicia-ejercicio-cruzex-2024/

SWI. (2025, 12 de enero). Colombia anuncia inicio de 'operaciones ofensivas' en zona afectada por ataques del ELN. *Swissinfo*. https://www.swissinfo.ch/spa/colombia-anuncia-inicio-de-%22operaciones-ofensivas%22-en-zona-afectada-por-ataques-del-eln/88765163

Thomas, L. (2022, 20 de mayo). U.S. Army South, Argentine army work to strengthen cybersecurity capabilities [El Ejército Sur de EE. UU. y el Ejército argentino trabajan para reforzar capacidades en ciberseguridad]. *U.S. Southern Command*. https://www.southcom.mil/MEDIA/NEWS-ARTICLES/Article/3056987/us-army-south-argentine-army-work-to-strengthen-cybersecurity-capabilities/

U.S. Southern Command. (2024, 11 de marzo). U.S. Strengthens cybersecurity partnership with Paraguay [EE. UU. refuerza su alianza con Paraguay en seguridad cibernética]. https://www.southcom.mil/MEDIA/NEWS-ARTICLES/Article/3979394/us-strengthens-cybersecurity-partnership-with-paraguay/

Vergara Cobos, E., & Diao, H. (2024, 3 de abril). De la ficción a la realidad: cómo América Latina se convirtió en el campo de batalla cibernético más crítico del mundo. *Banco Mundial Blogs*. https://blogs.worldbank.org/es/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe

Verma, D. (2025, 5 de enero). Cross-domain security: Integrating air, land, sea, and space cyber defense [Seguridad entre dominios: Integración de la ciberdefensa aérea, terrestre, marítima y espacial]. *LinkedIn*. https://www.linkedin.com/pulse/cross-domain-security-integrating-air-land-sea-space-cyber-verma-aepcc

Villanueva Mendes, J. C. (2015). *La ciberdefensa en Colombia* [Tesis de maestría, Universidad Piloto de Colombia]. http://polux.unipiloto.edu.co:8080/00002646.pdf

Villegas, L. (2025, 12 de mayo). Military institutional strengthening, pivotal goal of Dominican Defense Minister Onofre [El fortalecimiento institucional militar, objetivo central del ministro de Defensa dominicano Onofre]. *Diálogo Américas*. https://dialogo-americas.com/articles/military-institutional-strengthening-pivotal-goal-of-dominican-defense-minister-onofre/

Xinhua Español. (2025, 19 de enero). Ejército colombiano refuerza operaciones contra guerrilla ELN tras ataques. *Xinhua*. https://spanish.xinhuanet.com/20250119/87e0c56f-2d4149928a3c638979447332/c.html

De la mar a la nube: Guerra naval e integración de dominios en Ucrania

From the sea to the cloud: naval warfare and domain integration in Ukraine

Recibido: 30/ 04 / 2025 | Revisado: 05 / 07 / 2025 | Aprobado: 16 / 09 / 2025
DOI: https://doi.org/10.59794/rscd.2025.v11i11.150

Capitán de fragata Augusto Conte de los Ríos, AE
España

Correo: augusto.conte@um.es.

ORCID: https://orcid.org/0000-0003-4473-7605

Afiliación: Universidad de Murcia

El autor es capitán de fragata de la Armada Española. Doctor en Historia; Máster en Paz, Seguridad y Defensa (UNED); Máster en Historia y Patrimonio Naval (UMU); Máster en Educación y Museos (UMU); Máster en Alta Dirección Pública (UIMP); Máster en Archivos y Bibliotecas (UC3M); Máster en Dirección y Gestión de Adquisiciones de Sistemas para Defensa (UNIZAR); Máster en Técnicas de Ayuda a la Decisión (UPCT); Máster en Prevención de Riesgos Laborales (UNED); Máster en Gestión de Seguridad, Crisis y Emergencias (URJC). Ha cursado, además, estudios de especialización y altos estudios en diversos centros de la Armada y las Fuerzas Armadas. Durante el desarrollo de su carrera militar ha ocupado numerosas funciones de relevancia tales como: Comandante del Patrullero Formentor; Segundo Comandante del Submarino Siroco; Jefe del Área de Submarinos en el Centro de Evaluación para el Combate de Cartagena; Jefe de Órdenes del Mando de Cartagena (MARCART); Segundo de la Comandancia Naval de Cartagena; Subdirector de la Escuela de Submarinos de la Armada; y actualmente Jefe de Integración y Reclutamiento en el Organismo de Apoyo al Personal en Cartagena. Es miembro de la Cátedra de Historia y Patrimonio Naval (UMU-ARMADA) y coordinador de la Cátedra «Jerónimo de Ayanz» (UPCT-ARMADA). Asimismo, colabora habitualmente con la Revista Ejércitos, la Revista General de Marina, Proceedings del US Naval Institute, Warships International Fleet Review, Boletín y Revista del Instituto Español de Estudios Estratégicos (IEEE), y es analista del Centro de Pensamiento Naval de la Armada. Participa como experto en el Proyecto Anti-Access/Area Denial (A2/AD) del Centro Conjunto de Desarrollo de Conceptos del EMAD, y es miembro de ICOMOS e ICOFORT. A través de sus años de servicio ha adquirido una gran experiencia como submarinista, analista naval y en temas relacionados con la estrategia naval y la geopolítica. Ha sido condecorado y reconocido en múltiples ocasiones por su desempeño, servicios prestados y desarrollo de su carrera militar.

Resumen

La guerra en Ucrania ha transformado los paradigmas tradicionales de la guerra naval, destacando la importancia de integrar dominios (físico, digital y cognitivo) y capacidades multimisión en conflictos asimétricos contemporáneos. En el teatro del mar Negro, la estrategia ucraniana basada en la «flota mosquito» —concepto recogido en su «Nueva Estrategia Naval hasta 2035»— ha demostrado la eficacia de unidades pequeñas, rápidas y bien equipadas frente a plataformas tradicionales de gran tamaño. Este estudio analiza cómo Ucrania, mediante sistemas no tripulados (USV y UAV), tácticas de denegación marítima e integración de dominios, ha contrarrestado la superioridad material de la Flota rusa del mar Negro. El hundimiento del crucero Moskva, los ataques en Sebastopol y la reconquista de la isla de las Serpientes evidencian un cambio de paradigma: el control del mar ya no depende exclusivamente del dominio físico, sino de la sincronización de efectos en todos los espacios de batalla. El análisis, enmarcado en los postulados de Julian Corbett sobre el poder marítimo como parte de la estrategia global, demuestra que la innovación tecnológica y doctrinal puede revertir desequilibrios cuantitativos. Así, el enfoque multimisión y la flexibilidad operativa emergen como factores esenciales frente a las amenazas híbridas del siglo XXI. Se concluye que el conflicto en el mar Negro ofrece lecciones estratégicas de alcance global, subrayando que la superioridad marítima contemporánea exige capacidades distribuidas, resiliencia tecnológica, integración multisectorial y adaptación doctrinal profunda. La experiencia ucraniana inaugura un modelo emergente donde la «nube» y el «mar» convergen para redefinir el poder naval.

Palabras clave: Integración, multidominio, fuerzas marinas, guerra Ucrania, mar Negro

Abstract

The war in Ukraine has transformed traditional paradigms of naval warfare, highlighting the importance of integrating domains (physical, digital, and cognitive) and multi-mission capabilities in contemporary asymmetric conflicts. In the Black Sea theatre, the Ukrainian strategy based on the "mosquito fleet" – a concept included in its "New Naval Strategy until 2035" – has demonstrated the effectiveness of small, fast and well-equipped units against large, traditional platforms. This study analyzes how Ukraine, through unmanned systems (USVs and UAVs), maritime denial tactics, and domain integration, has countered the material superiority of the Russian Black Sea Fleet. The sinking of the cruiser Moskva, the attacks on Sevastopol and the reconquest of Snake Island are evidence of a paradigm shift: control of the sea no longer depends exclusively on physical dominance, but on the synchronization of effects in all battle spaces. The analysis, framed in Julian Corbett's postulates on maritime power as part of the global strategy, demonstrates that technological and doctrinal innovation can reverse quantitative imbalances. Thus, the multi-mission approach and operational flexibility emerge as essential factors in the face of the hybrid threats of the 21st century. It concludes that the conflict in the Black Sea offers strategic lessons of global scope, underlining that contemporary maritime superiority requires distributed capabilities, technological resilience, multisectoral integration and deep doctrinal adaptation. The Ukrainian experience inaugurates an emerging model where the "cloud" and the "sea" converge to redefine naval power.

Keywords: Integration, multi-domain, marine forces, war Ukraine, Black Sea

Introducción

La guerra en Ucrania ha redefinido los paradigmas de la operatividad naval moderna, evidenciando cómo la integración de dominios (físico, digital, cognitivo) y las capacidades multimisión son críticas en escenarios asimétricos. Este análisis se centra en el mar Negro, donde la Flota rusa y las innovaciones ucranianas han escrito un capítulo decisivo en la historia militar contemporánea.

Las condiciones militares y estratégicas del mar son diferentes de las de tierra firme, el mar no puede ocuparse en el sentido militar de la palabra; no hay líneas de frente y la defensa no puede basarse en fortificaciones del mismo modo que en tierra. El Báltico y el mar Negro son mares semicerrados con un importante flujo marítimo. En ambos casos, la Federación Rusa constituye una potencia dominante y una amenaza permanente (Wedin, 2015).

La guerra naval en el mar Negro, impulsada por el conflicto entre Ucrania y la Federación Rusa, ha significado un cambio de paradigma en la conducción de operaciones navales. La respuesta ucraniana ante el dominio inicial ruso no fue replicar la superioridad convencional en términos de tonelaje o grandes unidades navales, sino que se basó en una estrategia radicalmente distinta: la «flota mosquito», una doctrina ya prevista en su "Nueva Estrategia Naval hasta 2035" (Ukrainian Navy, 2019).

Esta estrategia consiste en la introducción masiva de unidades pequeñas, rápidas y bien armadas, apoyadas por la integración de capacidades aéreas, navales y cibernéticas, con un enfoque prioritario en misiones de negación del mar y operaciones multimisión. Se buscaba compensar la inferioridad cuantitativa frente a la Flota rusa del mar Negro mediante la agilidad, el sigilo, el bajo coste y el uso intensivo de nuevas tecnologías.

El término estrategia, afirmaba Bordejé, implica los conocimientos necesarios para dirigir combates. A pesar de numerosas publicaciones, la estrategia sigue siendo un concepto ambiguo, especialmente en el ámbito naval, donde se entrelazan la estrategia operativa y la de recursos. Su fundamento teórico aún descansa en un conjunto limitado de obras que continúan influyendo en la comprensión actual del concepto (Bordejé, 1982).

Dentro de la historiografía del pensamiento marítimo, los nombres que destacan con mayor frecuencia son los del almirante estadounidense Alfred Mahan (1840-1914), cuya obra sigue teniendo un impacto significativo (Baqués, 2024), y el del historiador británico Julian Corbett (1854-1922), quien, pese a su relevancia, es menos conocido por el público general (Henrotin, 2013). Menos conocido aún, pero de notable influencia por su relación con el almirante Carrero Blanco, es el capitán de fragata Mateo Mille García, quien, a través de sus obras y conferencias impartidas en la Escuela de Guerra Naval durante la década de 1930, sentó en España las bases de la estrategia naval (Mille García, 1926).

Corbett, reconocido por integrar las estrategias marítima y naval dentro del marco más amplio de la estrategia general, ofreció una interpretación innovadora y dinámica del pensamiento estratégico. Su legado proporciona una visión moderna y accesible no solo sobre el arte de la guerra en el ámbito marítimo, sino también sobre su vinculación con la estrategia en sentido

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

amplio, aspectos que hoy en día siguen teniendo gran vigencia.

El contraste clásico entre control y negación del mar resulta insuficiente para explicar las realidades contemporáneas. Bernard Brodie anticipó esta limitación al reformular la dicotomía hacia una entre control marítimo e interdicción. Esta última, menos exigente, otorga libertad de acción a las flotas mediante sensores y sistemas de armas de largo alcance, ampliando así las zonas efectivamente controladas (Lavernhe & Corman, 2023).

La estrategia Anti-Acceso/Denegación de Área (A2/AD) es un enfoque defensivo destinado a impedir el acceso enemigo a zonas clave. En el 480 a.C., las ciudades-estado griegas emplearon una forma temprana de esta estrategia contra Jerjes, usando islas como barreras naturales y estrangulando sus líneas de suministro marítimo, lo que provocó su retirada y el colapso logístico de su ejército (Russell, 2017).

Este ejemplo evidencia cómo la estrategia A2/AD puede debilitar fuerzas superiores sin combates decisivos, usando el tiempo, el desgaste y la geografía como aliados. En la actualidad, esta lógica permanece vigente, con Estados Unidos beneficiándose de sus océanos como defensas naturales, mientras el control marítimo moderno exige dominio también del espacio aéreo y del entorno submarino (Espinosa Rubio, 2025).

La guerra de Ucrania en el mar Negro ha puesto en primer plano la importancia de la integración de dominios y la necesidad de ejércitos multimisión en los conflictos contemporáneos. El teatro naval ucraniano, lejos de ser un escenario secundario, ha demostrado que la coordinación efectiva entre fuerzas terrestres, aéreas, navales, cibernéticas y espaciales es crucial para alcanzar objetivos estratégicos y adaptarse a entornos operativos complejos y cambiantes (Conte de los Ríos, 2024).

En este contexto, el dominio conjunto se revela como factor decisivo: la Marina rusa, aunque inicialmente superior en medios, ha visto limitadas sus capacidades por la acción combinada de los ucranianos y el uso innovador de tecnologías disruptivas, como drones navales y misiles de precisión. La respuesta ucraniana, basada en una estrategia de negación del mar y en la integración ágil de recursos y saberes, ha logrado infligir daños significativos a la Flota del mar Negro y modificar el equilibrio de poder en la región.

El propósito de este artículo es analizar cómo la Marina ucraniana ha transformado su estrategia naval frente a la superioridad convencional rusa mediante la integración de dominios (físico, digital y cognitivo) y el empleo de capacidades multimisión en el mar Negro. El estudio se enfoca en el periodo 2022–2024, con especial atención a las implicaciones estratégicas del uso de sistemas no tripulados, la doctrina de negación del mar y las lecciones aplicables a conflictos navales de alta intensidad en entornos confinados.

Al mismo tiempo, esta guerra ha evidenciado que el éxito en el ámbito naval no depende únicamente del control físico del mar, sino de la capacidad para sincronizar efectos en todos los dominios y proyectar poder más allá de las fronteras tradicionales. Así, la experiencia ucraniana subraya la necesidad de fuerzas armadas flexibles, capaces de operar de manera conjunta y multimisión, adaptándose rápidamente a los desafíos de la guerra moderna y aprovechando la convergencia de capacidades tecnológicas, doctrinales y humanas (Romero Sobrino, 2024).

El caso del mar Negro ilustra cómo la integración de dominios y el enfoque multimisión no solo multiplican la eficacia militar, sino que resultan imprescindibles para afrontar las amenazas híbridas y los escenarios de alta intensidad actuales. Corbett y algunos autores españoles, nos ayudarán a comprender mejor el papel de las fuerzas navales en el futuro venidero (Mille García, 1926).

Mar Negro, geopolítica y dominio ruso

El mar Negro, situado entre Europa y Asia, posee una importancia estratégica clave, pues conecta con el Mediterráneo por los estrechos turcos y con el mar de Azov por el de Kerch. Su geografía y su entorno político, con países ribereños pertenecientes a la OTAN y otros aliados o adversarios de Rusia, lo convierten en un escenario central de rivalidad geopolítica. Rusia, lo considera vital para su proyección regional y se enfrenta a un entorno cada vez más disputado (Gollnisch, 2022).

Otro factor geopolítico importantísimo son las restricciones impuestas por la Convención de Montreux, uno de los tratados internacionales más antiguos que ha resistido vientos y mareas como la Segunda Guerra Mundial, y que regula el tránsito naval por los estrechos, limita la presencia de potencias extranjeras, favoreciendo el predominio de los países ribereños y, en particular, de Rusia, cuyo control sobre el área ha sido objetivo estratégico permanente (Conte de los Ríos, 2015, 2019, 2022, 2023 y 2024).

Desde la disolución de la URSS, Rusia ha intentado revertir la pérdida de influencia, especialmente tras la expansión de la OTAN hacia el este. El control de la cuenca del mar Negro, puente entre Europa y Asia, ha sido históricamente un objetivo estratégico para Moscú, que busca asegurar su proyección hacia el Mediterráneo y contener a la OTAN (Monaghan & Connolly, 2023). La anexión de Crimea en 2014 permitió a Moscú consolidar bases como Sebastopol, pero la invasión de 2022 reveló vulnerabilidades inesperadas (Patalano, 2024):

- Dominio físico: La captura inicial de la isla de las Serpientes (24/02/2022) facilitó el bloqueo naval ruso, pero la resistencia ucraniana convirtió la costa de Odesa en un "nido de avispas" con baterías móviles de misiles Neptune y armas de gran alcance.
- Dominio cibernético: Ucrania empleó drones aéreos y navales (como el Magura V5) coordinados con inteligencia satelital occidental, desafiando la superioridad convencional rusa.

La invasión de Ucrania en 2022 persiguió asegurar el dominio marítimo y terrestre, controlar la costa del mar de Azov, establecer un corredor hacia Crimea y debilitar Ucrania, a fin de consolidar un bloqueo sobre la región de Odesa. La Flota del mar Negro ha actuado como apoyo a las operaciones terrestres rusas, imponiendo bloqueos, lanzando misiles de crucero y amenazando con desembarcos (Conte de los Ríos, 2024).

No obstante, ha sufrido pérdidas importantes, incluyendo el hundimiento del Moskva, lo que ha evidenciado fallos estructurales en sus defensas y vulnerabilidades ante ataques con misiles y drones (ver Tabla 1). Ucrania, con medios asimétricos, ha logrado dañar significativamente a la flota rusa, destacando el uso de vehículos de superficie no tripulados, misiles costeros y drones aéreos, lo que ha obligado a Rusia a adoptar una estrategia cautelosa de disuasión más que de confrontación directa.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Tabla 1
Resumen de las bajas navales rusas el primer año

Categoría	Clase	Detalles
Crucero misiles guiados	Proyecto 1164 Clase Slava	1, Moskva, hundido por misil Neptune AShM
Submarinos	Proyecto 636.3 Clase Kilo mejorada	1, Rostov-na-Donu, dañado irreparablemente por misil
Buques de desembarco	Proyecto 1171 Clase Tapir	1, Saratov, destruido por Tochka-U
	Proyecto 775 Clase Ropucha	3: Minsk (irrecuperable), Novocherkassk (destruido), Caesar Kunikov (destruido)
	Proyecto 11770 Clase Serna	2: 1 destruido por TB2, 1 dañado
	Proyecto 1176 Clase Ondatra	1, dañado
Corbetas	Proyecto 22800 Clase Karakurt	1, Askold, destruido
	Proyecto 12411 Clase Tarantul-III	1, Ivanovets, destruido
Dragaminas	Proyecto 266M Clase Natya	1, dañado por USV
Patrulleros	Proyecto 22160 Patrullero grande	1, Sergey Kotov, destruido
	Proyecto 03160 Clase Raptor	5: 3 destruidos (TB2), 1 dañado (TB2), 1 dañado (ATGM)
Lanchas	Proyecto 02510 Lancha rápida BK-16	1, destruido por TB2
	Proyecto 640 Bote pequeño	1, destruida por TB2
Buques auxiliares	Proyecto 22870 Remolcador rescate	1, Vasily Bekh, destruido por TB2 + Harpoon
Buques reconocimiento	Proyecto 18280 Clase Yuri Ivanov	1, Ivan Khurs, dañado

Nota. Oryx y elaboración propia.

Rusia ha adoptado una estrategia integral para reforzar su proyección en el dominio marítimo, articulada a través de tres documentos clave que conforman el núcleo de su planificación naval: la *Doctrina Marítima de la Federación Rusa (2022), los Fundamentos de la Política Estatal en el Campo de las Operaciones Navales hasta 2030 (2017) y la Estrategia para el Desarrollo de las Actividades Marítimas de Rusia hasta 2030*. Esta arquitectura estratégica se complementa con planes regionales específicos que subrayan la prioridad geopolítica que Moscú otorga a esta región (Conte de los Ríos, 2022, 2023 y 2024).

Rusia percibe que la OTAN trata de encerrarla estratégicamente mediante una guerra híbrida marítima que combina guerra regular e irregular, diplomática y económica, táctica y estratégica. Esta amenaza se articula como un sistema unificado de desafíos del siglo XXI, aplicable incluso en tiempos de paz, mediante medios directos e indirectos, como empresas militares privadas, ataques cibernéticos y operaciones encubiertas en espacios maríti-

mos y puntos críticos (Mikhlin, Molochny, & Koemets, 2023).

La guerra también refleja un cambio en la naturaleza de los combates, donde tecnologías asimétricas pueden desequilibrar el poder marítimo convencional, obligando a adaptaciones tácticas y doctrinales en todos los frentes del conflicto. Los rusos trataron de reponerse, retrasaron sus líneas y se focalizaron en el empleo de sus submarinos con el lanzamiento de misiles de crucero Kalibr, siguieron ejerciendo presión sobre el tráfico marítimo ucraniano, y aumentaron los bombardeos sobre la línea de Odesa y la desembocadura del Danubio.

En el plano conceptual, la doctrina cumple una función cohesionadora entre el pensamiento estratégico y la acción táctica. Tal como señalan Hughes y Girrier (2018), la doctrina actúa como el elemento estructurador que da coherencia a la maniobra táctica, proporcionando unidad operativa en entornos marcados por el caos y la incertidumbre. Bajo esta lógica, la nueva doctrina marítima rusa busca justamente consolidar la expansión del poder naval ruso en múltiples teatros, integrando medios, objetivos y entornos operacionales bajo una misma arquitectura doctrinal.

Moscú después de 2022, impuso un bloqueo a todos los puertos ucranianos en la región, lo que provocó la interrupción total del tráfico marítimo y de las operaciones de importación y exportación del país. Esta medida impactó tanto en el mar Negro como al mar de Azov, dominio absoluto ruso cerrado por el puente sobre el estrecho de Kerch. Ante esta situación, Ucrania se vio obligada a recurrir al uso de puertos alternativos en la zona del Danubio y a reforzar el transporte ferroviario ante su bloqueo en aguas restringidas (Vego, 2003).

Nueva estrategia naval de Ucrania hasta 2035

La «Nueva Estrategia Naval de Ucrania hasta 2035», presentada por el almirante Ihor Voronchenko en noviembre de 2018, define la hoja de ruta para el fortalecimiento de las Fuerzas Navales de Ucrania (Kabanenko, 2019). Esta estrategia, elaborada con el apoyo de expertos occidentales, tiene como objetivo principal lograr la interoperabilidad con la OTAN y desarrollar capacidades navales reales para hacer frente a las amenazas marítimas de Rusia (Patalano & Hallett, 2025).

La modernización de la marina ucraniana está orientada hacia la protección de su soberanía marítima, particularmente tras la pérdida de Crimea en 2014, y la creciente militarización rusa del mar Negro. La estrategia se organiza en tres componentes esenciales del potencial de combate naval —físico, conceptual y moral—, alineados con la Doctrina Conjunta Aliada AJP-01 de la OTAN, y se implementa en tres etapas definidas (Ukrainian Navy, 2019):

1. Primera etapa (hasta 2025): El objetivo es el control efectivo de las aguas territoriales ucranianas hasta 40 millas náuticas, garantizando la defensa del litoral cercano.

2. Segunda etapa (2025-2030): El foco está en proteger los intereses nacionales en la Zona Económica Exclusiva (ZEE) de Ucrania, extendiendo la defensa hasta las 200 millas náuticas.

3. Tercera etapa (2030-2035): La estrategia apunta a expandir las capacidades para proteger los intereses ucranianos más allá

de las aguas regionales, en el ámbito oceánico, con proyección global.

A corto plazo, Ucrania apuesta por una «flota mosquito» compuesta por embarcaciones pequeñas, rápidas y bien equipadas. Además, se están estableciendo acuerdos con otros países para la construcción de buques patrulleros adicionales. Estas embarcaciones están diseñadas para ser ágiles y para operar en zonas de acceso restringido, adaptándose a la necesidad de enfrentarse a una flota rusa más poderosa, sin la capacidad de una confrontación directa con buques de gran tonelaje (Kollakowski, 2025).

A nivel estratégico, la recuperación del potencial naval en el mar Negro se presenta como una prioridad. Este objetivo se implementará siguiendo la metodología DOTMLPF de la OTAN, que abarca áreas clave como Doctrina, Organización, Formación, Material, Liderazgo, Personal y las Instalaciones necesarias para una defensa efectiva. Sin embargo, este proceso se enfrenta a desafíos significativos (Ukrainian Navy, 2019).

La reacción ucraniana al agresor ruso se ha desplegado en tres grandes ejes operacionales: la implantación de sistemas no tripulados, la negación del mar y la integración de dominios. Ucrania ha desarrollado y utilizado de manera efectiva USV como el Magura V5, así como UAV, para ejecutar ataques de precisión sobre buques, bases y plataformas logísticas rusas. Esta táctica asimétrica ha sido esencial para contrarrestar la superioridad numérica y tecnológica de la flota rusa (Conte de los Ríos, 2024).

Ucrania abandonó la lógica de dominación naval clásica, centrando sus esfuerzos en dificultar o impedir el uso efectivo del espacio marítimo por parte de Rusia. Este enfoque se ha traducido en una serie de acciones continuas sobre la isla de las Serpientes, el hundimiento del crucero Moskva, ataques a la base naval de Sebastopol y a buques en Novorossiysk. Al priorizar la negación del acceso marítimo mediante una combinación de ataques asimétricos, ha alterado las dinámicas de poder en el mar Negro.

La interacción entre sistemas de superficie, aéreos y, en menor medida, submarinos no tripulados, ha creado un efecto multiplicador en la estrategia ucraniana. La guerra electrónica, el intercambio de información en tiempo real y el empleo coordinado de drones de reconocimiento y ataque han transformado la naturaleza de la guerra naval en la región, demostrando que la supremacía naval ya no depende exclusivamente de grandes unidades de superficie, sino de la capacidad para operar de manera distribuida y autónoma.

Este nuevo paradigma operacional demuestra que el control efectivo del mar ya no se basa únicamente en grandes unidades navales. La capacidad de negar el acceso al adversario mediante plataformas distribuidas y autónomas se ha convertido en un factor clave. Las tradicionales fuerzas navales basadas en grandes buques de guerra han quedado vulnerables ante enjambres de drones baratos y veloces, difíciles de detectar y neutralizar en espacios marítimos confinados como el mar Negro.

La estrategia ucraniana también ha puesto de relieve la vulnerabilidad inherente a las bases navales fijas, lo que obligó a Rusia a redesplegar parte de su Flota del mar Negro desde Crimea hacia otros puertos como Novorossiysk. A través de una combinación de drones, minas y ataques con misiles, Ucrania logró romper el bloqueo marítimo ruso, reabriendo corredores de exportación vitales para su economía,

especialmente en el sector de granos (Wolkov, Mealie & Stepanenko, 2023).

Este cambio estratégico no implica la desaparición de las fuerzas tradicionales, sino su adaptación a un entorno donde la supremacía aérea, cibernética y de información son esenciales. La guerra en el mar Negro sugiere que el futuro de la guerra naval se encuentra en la integración de dominios, la interoperabilidad entre sistemas tripulados y no tripulados y la ejecución de operaciones multimisión ágiles y dinámicas. Esto marca un salto cualitativo respecto a las doctrinas navales clásicas, las cuales estaban basadas en la supremacía de grandes buques de guerra.

Aunque la estrategia asimétrica ha mostrado resultados exitosos en el mar Negro, el liderazgo naval de Ucrania, encabezado por el almirante Neizhpapa, ha subrayado la necesidad de desarrollar capacidades convencionales de flota. Para ello, se ha establecido colaboración con Reino Unido y Noruega en el marco de la Iniciativa de Capacitación Marítima, buscando no solo la mejora de la capacidad defensiva, sino también la posibilidad de realizar operaciones más complejas, como un posible bloqueo naval en las costas rusas del mar Negro (Kollakowski, 2025).

Las capacidades de Ucrania para negar el acceso al mar Negro se han visto potenciadas por el uso de vehículos no tripulados (UAV y USV) y ataques de largo alcance, lo que demuestra la importancia de la guerra tecnológica. Este enfoque de "denegación de mar" ha sido fundamental para neutralizar las fortalezas de la flota rusa, limitando su efectividad, especialmente en el contexto de ataques a infraestructuras estratégicas, como la destrucción de un submarino ruso en 2024.

El debate interno sobre el futuro de la flota ucraniana refleja una clara tensión entre el deseo de mantener una flota convencional fuerte y la necesidad de seguir desarrollando una capacidad asimétrica eficaz. Muchos analistas como Tobias Kollakowski, advierten sobre los elevados costos de una flota convencional, sugiriendo que los recursos disponibles deberían destinarse a reforzar la estrategia de negación del mar, utilizando activos más ágiles y menos costosos, como las lanchas rápidas y los drones (Kollakowski, 2023a, 2023b y 2025).

Este enfoque se alinea con la doctrina *jenecolista*,[1] que aboga por el uso de pequeños, pero bien armados barcos capaces de llevar a cabo operaciones de guerra asimétrica y perturbar las líneas de comunicación marítima del enemigo. Aunque, en el caso de Ucrania vemos que es una nueva estrategia multidominio y escorada hacía el A2/AD (Conte de los Ríos, 2024).

Transformación del campo de batalla: autonomía, innovación y adaptabilidad

Los conflictos armados contemporáneos están experimentando una evolución acelerada hacia la automatización y la integración de sistemas no tripulados. La rápida transformación tecnológica no solo está redefiniendo las capacidades militares, sino que también está generando una continua interacción entre amenazas emergentes y respuestas defensivas adaptativas. En este escenario, la velocidad de innovación y la capacidad de adaptación táctica se han consolidado como factores críticos de ventaja operativa.

1 El término jenecolista, utilizado por los autores españoles, se refiere a la teoría del almirante Théophile Aube (1826-1890) de finales del siglo XIX, denominada Jeune École.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Como señaló Liddell Hart, todo plan debe considerar las capacidades y el poder del adversario para anticipar y frustrar sus acciones. Bourcet, en el siglo XVIII, destacó este principio con su axioma: "Todo plan de campaña debe tener varias ramificaciones que aseguren el triunfo sin error". Esta filosofía, adoptada por Napoleón, quien siempre buscaba "faire son thème en deux façons", subraya la necesidad de planes flexibles que se adapten a las circunstancias cambiantes del conflicto (Liddell Hart, 2023).

Los sistemas no tripulados se están utilizando cada vez más en espacios marítimos confinados para tareas de vigilancia, protección y acciones tácticas de combate. El éxito de los drones en la guerra de Ucrania ha impulsado una rápida innovación y el desarrollo de nuevas tácticas. Su uso en los mares Negro y Rojo demuestra su efectividad en espacios marítimos limitados, ya que permiten llevar a cabo operaciones de larga duración y bajo coste sin poner en riesgo los recursos humanos. Esta tendencia subraya la creciente importancia de los sistemas no tripulados en la guerra moderna (Toma, 2024).

Según Mahan, la geografía puede influir en la necesidad de concentrar o dispersar las fuerzas navales, una consideración crucial para la Marina rusa, que enfrenta el desafío de gestionar cuatro flotas en diferentes mares. La táctica sugerida es la que Hattendorf describe como "Fleet in being", un concepto introducido por Arthur Herbert. Esta estrategia es empleada por una flota que, al no tener la capacidad de enfrentarse a una flota enemiga debido a la desventaja numérica o igualdad de fuerzas, decide permanecer en puerto, donde está protegida desde un punto de vista táctico (Hattendorf, 2014).

En este contexto, Ucrania ha ejemplificado de forma notable la aplicación de una estrategia asimétrica de negación multidominio. Sin contar con una armada tradicional comparable a la rusa, empleó vehículos no tripulados de superficie para atacar objetivos distantes, como Novorossiysk, demostrando que la distancia dejó de ser una garantía de seguridad. La combinación de ataques electrónicos y cinéticos, como el hundimiento del Moskva, subraya la eficacia de operaciones integradas en múltiples dimensiones del espacio de batalla.

Este paradigma militar, marcado por la autonomía y la guerra multidominio, privilegia la explotación de vulnerabilidades específicas del adversario sin recurrir necesariamente a grandes plataformas convencionales. El ingenio táctico y la innovación tecnológica permiten generar efectos operativos disruptivos mediante recursos limitados, forzando una redefinición de las reglas tradicionales del combate y de la estructura doctrinal de las fuerzas armadas (Kollakowski, 2025).

A escala estratégica, Kiev logró degradar sustancialmente la Flota del mar Negro en menos de tres años de guerra. Forzó su repliegue hacia puertos más lejanos y redujo significativamente su capacidad de proyección. Esta transformación ilustra cómo una fuerza menor, adaptativa y tecnológicamente ágil puede neutralizar componentes esenciales del poder naval de un adversario superior en medios convencionales.

Frente a esta presión, la doctrina rusa de disuasión, centrada en submarinos y misiles de largo alcance, encontró limitaciones. La exposición de infraestructuras logísticas críticas, como el dique seco de Sebastopol, y la incapacidad de responder de forma efectiva a amenazas no tripuladas, revelaron vulnerabi-

lidades estructurales en la organización naval rusa. Además, la sobrecarga de funciones —bloqueo naval, apoyo terrestre y disuasión estratégica— tensionó una flota diseñada para escenarios lineales más tradicionales.

La respuesta ucraniana ofrece lecciones fundamentales para las fuerzas multimisión del futuro. Destaca especialmente la construcción de una interoperabilidad táctica efectiva, en la que se integran unidades de drones, inteligencia de señales y artillería costera bajo un mando conjunto. Este modelo, similar a la guerra en red, incrementa la eficiencia de las acciones coordinadas con pocos recursos. Kiev apostó decididamente por una estrategia de eficiencia asimétrica mediante el desarrollo de una «flota mosquito» de bajo coste que permite infligir daños a unidades de alto valor estratégico, cuestionando la lógica clásica de la superioridad basada en el volumen y la masa convencionales (Patalano & Hallett, 2025).

Sin embargo, los rusos aplicaron la mencionada estrategia "Fleet in Being", una flota que, sin salir de puerto, ejerce influencia sobre el enemigo, negándole el control del mar. Su existencia obliga a destinar recursos para contenerla. Esta táctica de negación, popularizada por Colomb & Corbett, busca mantener los medios para contrarrestarla de forma activa, hostigando al enemigo hasta que surjan mejores oportunidades. El propósito es mantener la flota como un factor constante en los cálculos del enemigo (Ribera y Egea, 1930).

El modelo de guerra basado en agilidad operativa, innovación descentralizada e integración multisectorial está redefiniendo el arte militar contemporáneo. La experiencia ucraniana confirma que el futuro de los conflictos no se ganará con superioridad numérica o de plataformas pesadas, sino con inteligencia táctica, capacidad de adaptación rápida y dominio simultáneo de múltiples dimensiones operativas.

La guerra en Ucrania, además, ha catalizado cambios doctrinales profundos. Lo que inicialmente se percibía como una guerra convencional de grandes formaciones terrestres y supremacía aérea, pronto evolucionó hacia un conflicto caracterizado por el desgaste tecnológico. La utilización de drones, municiones merodeadoras y ataques de precisión asequibles evidenció la vulnerabilidad de sistemas de alto coste y alta exposición.

Se ha demostrado que las grandes plataformas —ya sean navales, aéreas o terrestres— pueden volverse inoperativas en entornos altamente contestados dominados por tecnologías A2/AD. Dentro de estas tecnologías, los sistemas no tripulados han adquirido protagonismo por su bajo coste, facilidad de despliegue y capacidad para operar en el espacio tridimensional, ofreciendo una movilidad y persistencia inalcanzables para sistemas tradicionales.

Este fenómeno ha obligado a muchos Estados, en particular a los aliados de la OTAN, a revisar sus doctrinas y adaptarlas a las nuevas exigencias de los conflictos asimétricos y multidominio (Pulido, 2021). La principal lección estratégica es que la superioridad no se logra únicamente mediante la acumulación de plataformas, sino mediante la comprensión profunda de las dinámicas del campo de batalla, la capacidad de innovar doctrinas y la flexibilidad para integrar rápidamente nuevas tecnologías en las operaciones militares.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Conclusiones

La guerra en Ucrania ha impulsado una transformación fundamental en la estrategia naval, destacando la necesidad urgente de integrar dominios operativos diversos y de adoptar enfoques multimisión. En un contexto de conflicto asimétrico, la estrategia naval de Ucrania ha demostrado ser un referente para el futuro de la guerra naval, especialmente mediante la implementación de tecnologías avanzadas como los sistemas no tripulados (USVs y UAVs). Esto ha permitido a Ucrania desafiar la superioridad numérica rusa de su Flota del mar Negro, subrayando que la capacidad para integrar dominios (físico, digital y cognitivo) es crucial para la eficacia operativa.

La «Nueva Estrategia Naval de Ucrania hasta 2035" pone de manifiesto la necesidad de mejorar la interoperabilidad de las fuerzas navales con otras ramas de las fuerzas armadas, no solo a nivel nacional sino también a nivel internacional, en colaboración con aliados clave como la OTAN. La evolución de su flota, centrada en embarcaciones rápidas y ágiles, junto con el uso de plataformas no tripuladas, refleja un cambio hacia un modelo de guerra naval distribuida y altamente adaptable, donde la flexibilidad y la innovación tecnológica son los principales activos.

Además, la guerra en el mar Negro ha mostrado que el control del mar ya no depende exclusivamente del dominio físico, sino que se basa en la sincronización de los efectos en todos los dominios de la batalla. Esto implica que las fuerzas navales del futuro deberán estar preparadas para operar en un entorno multidominio, integrando capacidades navales, aéreas, cibernéticas y de inteligencia, a fin de ejecutar operaciones multimisión de forma eficiente y en tiempo real.

La experiencia ucraniana resalta la adaptabilidad doctrinal como un factor clave para hacer frente a fuerzas superiores. Las tácticas de denegación del mar, centradas en la negación del acceso al adversario, se combinan con el uso de plataformas de bajo coste y alta efectividad, como los drones, para contrarrestar el poder naval convencional. Esta transición hacia una guerra naval más asimétrica y flexible sugiere que las fuerzas navales del futuro necesitarán integrar de forma efectiva sistemas no tripulados y adaptarse rápidamente a las nuevas tecnologías y tácticas, garantizando una capacidad de respuesta ante cualquier tipo de amenaza, desde la guerra electrónica hasta los ataques cinéticos de precisión.

La guerra naval en el mar Negro confirma la vigencia de Corbett: el control del mar ya no es solo físico, sino sincronizado en múltiples dominios. La integración de «mar y nube», combinada con capacidades multimisión, redefine el poder naval, imponiendo flexibilidad, innovación tecnológica y adaptación doctrinal frente a amenazas híbridas contemporáneas. En conclusión, la evolución de la estrategia naval tras la guerra en Ucrania apunta a la creación de fuerzas armadas multimisión, con una integración eficaz de tecnologías emergentes. Esto no solo garantizará un mayor control en conflictos futuros, sino que también permitirá a las fuerzas navales operar de manera más eficiente en escenarios de guerra multidominio, donde la capacidad de adaptarse rápidamente y aprovechar las ventajas tecnológicas será decisiva para el éxito estratégico.

Referencias

Baqués, J. (2024). Los axiomas de la guerra naval, según Mahan. *Global Strategy Report,* (11/2024).

Bordejé, F. (1982). Importancia de los estudios estratégicos y de los factores geográficos. En *España, poder marítimo y estrategia naval* (pp. 17-24). Editorial Naval.

Conte de los Ríos, A. (2015). El Tratado de Montreux y el conflicto de Ucrania. *Revista General de Marina,* 268(1), 43-56.

Conte de los Ríos, A. (2019). La base naval de Sebastopol tras la anexión rusa de Crimea. *Revista General de Marina*, 276(3), 467-483.

Conte de los Ríos, A. (2022). La nueva Doctrina Marítima de la Federación Rusa. *Revista Ejército*.

Conte de los Ríos, A. (2023). El dominio ruso del mar Negro a la sombra del conflicto de Ucrania. Bie3*: Boletín IEEE,* (29), 595-614.

Conte de los Ríos, A. (2024). La guerra de Ucrania en su vertiente naval. En B. Cózar Murillo & C. D. Villanueva López (Eds.), *La guerra de Ucrania III: De la reconquista de Jersón al estancamiento* (pp. 155-175). Editorial Catarata.

Espinosa Rubio, A. (2025). Los sistemas A2/AD y la guerra naval. *XXV CEMFAS*. CESEDEN.

Gollnisch, A. (2022). Enseignements navals et maritimes de la guerre en Ukraine. *Revue Défense Nationale*, 853(8), 13-18.

Hattendorf, J. B. (2014). The idea of a fleet in being in historical perspective. *Naval War College Review*, 67(1), 43-60.

Henrotin, J. (2013). *Julian Corbett: Renouveler la stratégie maritime*. Argos.

Hughes, W., & Girrier, R. (2018). *Fleet tactics and naval operation*s (3.ª ed.). US Naval Institute Press.

Kabanenko, I. (2019, 21 de febrero). New naval strategy of Ukraine to 2035: Implications and challenges. *Eurasia Daily Monitor,* 16(23).

Kollakowski, T. (2023a). Interpreting Russian aims to control the Black Sea region through naval geostrategy (Part One): The Azov-Black Sea basin as a whole [...] This is, in fact, a zone of our strategic interests. *The Journal of Slavic Military Studies*, 36(1), 57-72.

Kollakowski, T. (2023b). Interpreting Russian aims to control the Black Sea region through naval geostrategy (Part Two): "Establishing full control over Southern Ukraine and the Donbas is one of the tasks of the Russian Army". *The Journal of Slavic Military Studies*, 36(2), 119-138.

Kollakowski, T. (2025). War in the Black Sea: The revival of the Jeune École? *Journal of Strategic Studies*, 1-33.

Lavernhe, T., & Corman, F. O. (2023). *Vaincre en mer au XXIe siècle – La tactique au cinquième âge du combat naval.* Éditions Des Équateurs.

Liddell Hart, B. H. (2023). Fundamentos de estrategia: *¿Por qué no aprendemos de la historia?* Arzalia Ediciones.

Mikhlin, A. A., Molochny, V. V., & Koemets, T. M. (2023, 30 de septiembre). Maritime hybrid warfare in US and NATO strategies:

Essence, content, possible countermeasures. *Military Thought*.

Mille García, M. (1926). *Geografía estratégica y posiciones marítimas*. Escuela de Guerra Naval.

Monaghan, A., & Connolly, R. (Eds.). (2023). *The sea in Russian strategy*. Manchester University Press.

Patalano, A. (2024). *The maritime war in Ukraine: The limits of Russian sea control?* The Hague Centre for Strategic Studies.

Patalano, A., & Hallett, D. (2025). The strategic significance of the maritime theatre in the Russia–Ukraine war. *The RUSI Journal*.

Pulido, G. (2021). *Guerra multidominio y mosaico: El nuevo pensamiento militar estadounidense*. Editorial Catarata.

Ribera & Egea, J. L. (1930). *Concepto del dominio del mar: Origen y significado de la locución Fleet in being*. Escuela de Guerra Naval.

Romero Sobrino, F. J. (2024). *La flota del mar Negro en la guerra de Ucrania: Impacto en la campaña operacional*. XXV CEMFAS. CESEDEN.

Russell, A. (2017). Historical perspective of A2/AD strategy. *En Strategic A2/AD in Cyberspace* (pp. 11-25). Cambridge University Press.

Toma, V.-M. (2024). The use of unmanned systems in maritime confined spaces. *Romanian Military Thinking International Conference*.

Ukrainian Navy. (2019). *Strategy of the Naval Forces of the Armed Forces of Ukraine 2035*. https://navy.mil.gov.ua/en/strategiya-vijskovo-morskyh-syl-zbrojnyh-syl-ukrayiny-2035/

Vego, M. N. (2003). *Estrategia naval y operaciones en aguas restringidas* (1.ª ed.). Colección Defensa.

Wedin, L. (2015). *Les stratégies maritimes au XXIe siècle: L'apport de l'amiral Castex*. Nuvis.

Wolkov, N., Mealie, D., & Stepanenko, K. (2023, 16 de diciembre). Ukrainian strikes have changed Russian naval operations in the Black Sea. *Institute for the Study of War*. https://www.understandingwar.org/backgrounder/ukrainian-strikes-have-changed-russian-naval-operations-black-sea

De la guerra tradicional a la multimisión, integración de dominios y capacidades militares en Ecuador

From traditional to multi-mission warfare, integration of domains and military capabilities in Ecuador

Recibido: 14/ 05 / 2025 | Revisado: 17 / 07 / 2025 | Aprobado: 09 / 09 / 2025
DOI: https://doi.org/10.59794/rscd.2025.v11i11.154

Coronel Manuel Alfonso Querembás Altamirano, EE
Ecuador

Correo: maquerembasa@ejercito.mil.ec
mquerembas@gmail.com

ORCID: https://orcid.org/0000-0003-2011-7946

Afiliación: Academia de Guerra del Ejército del Ecuador

El autor es coronel de Estado Mayor Conjunto del Ejército de Ecuador. Coronel diplomado como oficial de Estado Mayor Conjunto de las FF. AA. del Ecuador. Posee los siguientes cursos: Curso Avanzado de Ingeniería Militar ECCC 2013, Fort Leonard Wood, Mo. EE. UU. Curso de Operaciones Conjuntas JTO 2018, Fort Benning, Ga. EE. UU. Pro eficiencia militar de Alemania. Curso de Formación de instructores desminado, España. Instructor de instructores militares Universidad militar de España y Diplomado internacional de Manejo y defensa de los DD. HH. Es además Ingeniero Civil e Ingeniero Comercial. Máster en Estrategia militar terrestre. Magister en Educación, mención gestión del aprendizaje mediado por TIC. UIDE y Magister en Educación, mención gestión de la investigación. UNISAN (México) Diplomado en pedagogía. Administración de la construcción, TEC-Monterrey México. Oficial de Operaciones de la Compañía de ingenieros militares ECUADOR-CHILE, Haití. Ha sido director de la Escuela de Ingenieros Militares "Grab. Guillermo Rodríguez Lara". Director del Centro de Educación Militar CEDMIL. Profesor de la Academia de Guerra del Ejército y Jefe de la Sección de visión y prospectiva del Ejército (Cargo Actual).

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Resumen

El presente estudio analiza los dominios de la guerra, y la transformación del ejército ecuatoriano hacia una fuerza multimisión, se destaca la necesidad de adaptación y flexibilidad en una sociedad gaseosa que afecta las misiones militares, se explora la integración de los dominios tradicionales: terrestre, marítimo, aéreo; y modernos: espacial y ciberespacio; como también la influencia de las dimensiones físicas, humanas y de información en las operaciones del Ejército; para el estudio se prioriza el dominio terrestre como base para ejemplificar su evolución, desde la guerra de desgaste, la guerra de maniobras, el concepto de armas combinadas, los sistemas operativos en el campo de batalla, hasta las operaciones multidominio, integrales, interagenciales, internacionales; desarrollando las capacidades militares, mejorando sus medios, infraestructura, recursos, adoctrinamiento, doctrina y organización, que permiten perfeccionar la eficiencia en el campo de batalla; asimismo, se investiga cómo los ejércitos han ampliado su rango de operaciones militares al incluir la lucha contra el terrorismo, crimen organizado y otras amenazas internas, además de sus misiones tradicionales de defensa externa. Finalmente, se reflexiona sobre la importancia de la comprensión, coordinación y sistematización de la integración de dominios y los ejércitos multimisión, destacando la necesidad de un enfoque flexible y modular para enfrentar los desafíos futuros, en donde la dimensión humana es y seguirá siendo el centro de gravedad de las Fuerzas Armadas ecuatorianas, priorizando el liderazgo y la educación militar para el desarrollo de un adecuado perfil del soldado del mañana.

Palabras Clave: Dominios físicos, dominios virtuales, dimensiones, fuerzas armadas, terrorismo, conflicto armado interno, operaciones multimisión

Abstrac

This present study analyzes the domains of war, and the transformation of the Ecuadorian army into a multi-mission force, highlights the need for adaptation and flexibility in a gaseous society that affects military missions, explores the integration of traditional domains: land, sea, air; and modern: space and cyberspace; as well as the influence of the physical, human and information dimensions on the Army's operations; For the study, the ground domain is prioritized as a basis to exemplify its evolution, from the war of attrition, the war of maneuvers, the concept of combined arms, operational systems on the battlefield, to multi-domain, integral, interagency, international operations; developing military capabilities, improving their means, infrastructure, resources, indoctrination, doctrine and organization, which allow improving efficiency on the battlefield; It also investigates how militaries have expanded their range of military operations to include the fight against terrorism, organized crime and other internal threats, in addition to their traditional external defense missions. Finally, it reflects on the importance of understanding, coordination and systematization of the integration of domains and multi-mission armies, highlighting the need for a flexible and modular approach to face future challenges, where the human dimension is and will continue to be the center of gravity of the Ecuadorian Armed Forces, prioritizing leadership and military education for the development of an adequate profile of the soldier of tomorrow.

Keywords: Physical domains, virtual domains, dimensions, armed forces, terrorism, internal armed conflict, multi-mission operations

DOI: https://doi.org/10.59794/rscd.2025.v11i11.154

Introducción

Objetivo General

Analizar la evolución de los dominios de la guerra y la transformación de las Fuerzas Armadas hacia un modelo de operaciones multimisión, en el contexto de los desafíos contemporáneos.

Objetivos Específicos

1. Examinar la integración de los dominios físicos y virtuales en el planeamiento y ejecución de operaciones militares.
2. Analizar el impacto de las dimensiones humanas, tecnológicas y de información en la eficacia operativa.
3. Proponer un enfoque flexible y modular para el desarrollo de capacidades militares adaptadas a escenarios cambiantes.
4. Evaluar la experiencia del Ejército del Ecuador en su proceso de transformación hacia una fuerza multimisión, en respuesta a amenazas internas como el terrorismo y el crimen organizado.

Google, tiene en sus instalaciones un Tiranosaurio Rex (T-rex), un colosal espécimen que estuvo a la cabeza de la cadena alimenticia por siglos, para reflexionar que hasta el más poderoso, requiere de adaptación, cambio y flexibilidad, o está condenado a desaparecer.

De acuerdo con De Crescenzo (2020), Heráclito de Éfeso hizo célebre la expresión "panta rei" (todo fluye), para Bauman (2017) con el concepto de la "sociedad líquida", y en concordancia con Innerarity (2020), "la sociedad gaseosa", es claro afirmar que "lo único permanente es el cambio".

Por otra parte, el cuadro de Escher (1953), llamado "Relatividad" refleja un mundo inquietante, un mundo VICA: Volátil, por la fragilidad de la paz y la espontanea reacción de las masas; Incierto, por el permanente cambio en las variables operacionales; Complejo, porque el manejo de la información es manipulable, hay una multidimensionalidad de los problemas y Ambiguo, porque a cada necesidad se le crea una teoría; incluso este concepto ha evolucionado a un mundo frágil, ansioso, no lineal e incomprensible (Brittle, Anxious, Nonlinear, Incomprehensible; BANI, por sus siglas en inglés): Frágil, porque las estructuras sociales y el equilibrio se puede romper fácilmente; Ansioso, ya que la rapidez de los cambios generan estrés que afectan la estabilidad emocional y operativa; No lineal, ya que no existe la relación directa entre la causa y la consecuencia:[2] Incomprensible, ya que es cada vez más complejo, con información confusa y contradictoria.

Por lo tanto, se refuerza la teoría del permanente cambio en un mundo cada vez más fluido y menos estable, repercutiendo principalmente, desde el punto de vista militar, en desafíos de seguridad; es claro que la sociedad muta, el conocimiento se transforma, las misiones militares han permutado, el T-rex

2 El lector puede analizar el efecto mariposa, donde todo tiene una reacción sin aparente relación entre el origen y la consecuencia, ni e tiempo ni espacio. De igual forma el efecto Dominó, donde hay una secuencia temporal de acciones y consecuencias. En esta sociedad gaseosa es cada vez mucho más errática esta correspondencia.

es un recordatorio de la obligatoriedad de aceptar el cambio en la sociedad que Bauman (2017) la sintetiza así:

> Hoy vivimos en un mundo de aislamiento y atomización en el que la gente desconfía de sus propias instituciones. En tales circunstancias, muchas personas reaccionan a la impotencia con actos de autodestrucción carentes de sentido. En los territorios palestinos, por ejemplo, hay jóvenes que ni se organizan ni colaboran con sus Gobiernos para mejorar sus perspectivas de futuro. Prefieren entrar en Israel, intentar apuñalar a un soldado o a una mujer embarazada y que les disparen o los arresten, una y otra vez. Tiran así sus vidas por un momento absurdo y, por lo general, fallido de terrorismo.

En este mundo de incertidumbres (VICA o BANI), es donde el militar debe tener pensamiento crítico, analizar mucha información en tiempos cortos y bajo mucha presión, tomar decisiones, liderar y sobre todo cumplir la misión que le demanda la sociedad, sin descuidar a sus subordinados, y el cumplimiento cabal de la normativa legal vigente (Querembás, 2020).

Ante esta caótica realidad, las Fuerzas Armadas, requieren adaptarse y extender su mirada hacia el futuro, en el caso del Ejército ecuatoriano según la Dirección de Transformación y Desarrollo Militar (DTDM) (2020), siguiendo procesos de: nacionalización, estructuración, profesionalización, adaptación tecnológica, fortalecimiento del ejército, modernización, fortalecimiento de capacidades, restructuración y transformación; todo esto para desarrollar capacidades flexibles, modulares, dinámicas, que le permitan enfrentar los retos venideros, convirtiéndose en ejércitos multimisión, en donde, de acuerdo con Arce (2019) el centro de gravedad es y seguirá siendo la dimensión humana; cuya polivalencia del profesional militar, le permitirá enfrentar escenarios complejos mediante una toma de decisiones respaldada en el conocimiento.

En este artículo se analizarán los cambios en los dominios de la guerra, desde dominios físicos tradicionales como terrestre, marítimo, aéreo; hasta los dominios virtuales (Ciberespacio) y las dimensiones: físicas, humanas y de información, que transversalmente los afectan; además, la integración de dominios como: el espacio exterior, el subsuelo terrestre y marino, detallado en la Tabla 1. Adicional, la participación de los ejércitos en un rango cada vez más amplio de operaciones, que nacen de las necesidades sociales, considerando lo expresado por Bush (2001) en su discurso ante la sesión conjunta del Congreso y el pueblo estadounidense, luego del ataque a las Torres Gemelas el 11 de septiembre del 2001, en donde expresa “Our war on terror begins with al Qaeda, but it does not end there.”

Nuestra guerra contra el terrorismo comienza con Al Qaeda, pero no termina allí, impulsando de inmediato el giro en las misiones de Fuerzas Armadas a nivel mundial, hacia un combate asimétrico con fuerzas no estatales; esto provocó que los ejércitos estén más compenetrados con la seguridad interna, apoyando las funciones tradicionales de la policía, pero con un enfoque de combate al terrorismo y al crimen organizado transnacional.

Finalmente, se reflexiona sobre la importancia de comprender, coordinar y sistematizar la integración de dominios en ejércitos multimisión; se analizará cómo esta integración

de dominios ha influido en el empleo de los ejércitos, obligándolos a transformarse para mejorar sus capacidades, a fin de tener el ejército que la sociedad necesita.

Desarrollo

Lo que las batallas tienen en común es el factor humano: el comportamiento de los hombres luchando para reconciliar sus instintos de auto conservación, su sentido del honor, y el logro de una meta, a causa de la cual, otros hombres son capaces de matarlos. El estudio de la batalla es siempre un estudio del miedo, y generalmente de la valentía; siempre del liderazgo, generalmente de obediencia; siempre de compulsión, a veces de insubordinación, siempre de ansiedad, a veces de euforia o catarsis, siempre de incertidumbre y dudas, desinformación y malentendidos, usualmente también de fe y a veces de visión; siempre de violencia, a veces también de crueldad, abnegación, compasión' y sobre todo, es siempre un estudio de la solidaridad y usualmente también de la desintegración – porque la batalla está dirigida hacia la desintegración de los grupos humanos (Keegan, 1976).

La sección de desarrollo se estructura en dos grandes apartados: el primero aborda la integración de los dominios de la guerra, desde los tradicionales hasta los emergentes, y su relación con las dimensiones operacionales; el segundo analiza el concepto de ejército multimisión, su evolución doctrinal, legalidad y operatividad, así como las capacidades necesarias para enfrentar los desafíos contemporáneos y futuros.

Integración De Dominios.

Históricamente, se reconocen los dominios y su integración en completa correlación con el avance tecnológico de la humanidad.

Tabla 1
Dominios Contemporáneos

Dominio	Definición
Terrestre	El área sobre la superficie de la tierra que termina en la línea de pleamar y que se superpone al dominio marítimo en el segmento terrestre de los litorales. Fuente JP 3-31 (2019)
Marítimo	Los océanos, mares, estuarios, islas áreas costeras y el espacio aéreo sobre este, incluyendo los litorales. Fuente JP 3-32 (2021)
Aéreo	La atmósfera, desde la superficie de la tierra, extendiéndose hacia la altitud donde sus efectos en las operaciones son insignificantes. Fuente JP 3-30 (2019)
Espacial	Un medio como el terrestre, marítimo y aéreo en el cual se pueden realizar operaciones militares para conseguir los objetivos de la seguridad nacional de EE.UU. Fuente JP 1-02 (2016)
Ciberespacio Espacio Electromagnético (EMM)	Un dominio global dentro que consistente en la red interdependiente de infraestructuras de tecnologías de la información y datos residentes, incluyendo Internet, redes de telecomunicaciones, sistemas computacionales y los procesadores y controladores integrados. Fuente JP 3-12 (2018)

Nota. Esta tabla ilustra la evolución de dominios y como se han incorporado cronológicamente a los contextos contemporáneos. Posteriormente, se abordarán las dimensiones que influyen, modifican y potencian estos dominios.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

El dominio terrestre se basa en el control del espacio vital, desde la prehistoria, cuando los pueblos sedentarios se enfrentaban constantemente con los nómadas, por comida y territorio. A partir de estas confrontaciones, la guerra ha sido una constante para la humanidad, lo que llevó al desarrollo de armamento, equipo, tácticas y técnicas en un entorno que es natural para el ser humano.

En el dominio marítimo, la invención de los barcos expandió significativamente el mundo conocido. Durante esa época, el control del mar equivalía al dominio global, con Inglaterra y España estableciéndose como las principales hegemonías. En el dominio aéreo, un avance significativo ocurrió durante la Segunda Guerra Mundial con la producción masiva de aviones de combate. Alemania logró dominar los cielos y formó la fuerza aérea de ataque más grande del mundo.

El desarrollo del dominio terrestre se amplía, ya que es el entorno natural de los seres humanos, donde tienen una presencia permanente. Los otros dominios físicos son alcanzados temporalmente mediante el uso de tecnología y máquinas, pero siempre se retorna al dominio terrestre. En tierra, se analiza la conformación de los grandes ejércitos, que en la llamada "guerra de desgaste" emplearon millones de soldados. En esta guerra, los recursos empleados eran ingentes y la victoria dependía de quién poseía más recursos y podía mantener el esfuerzo del combate por más tiempo. Literalmente, los ejércitos chocaban en grandes masas con el objetivo de reducir los recursos logísticos y humanos del adversario para vencer.

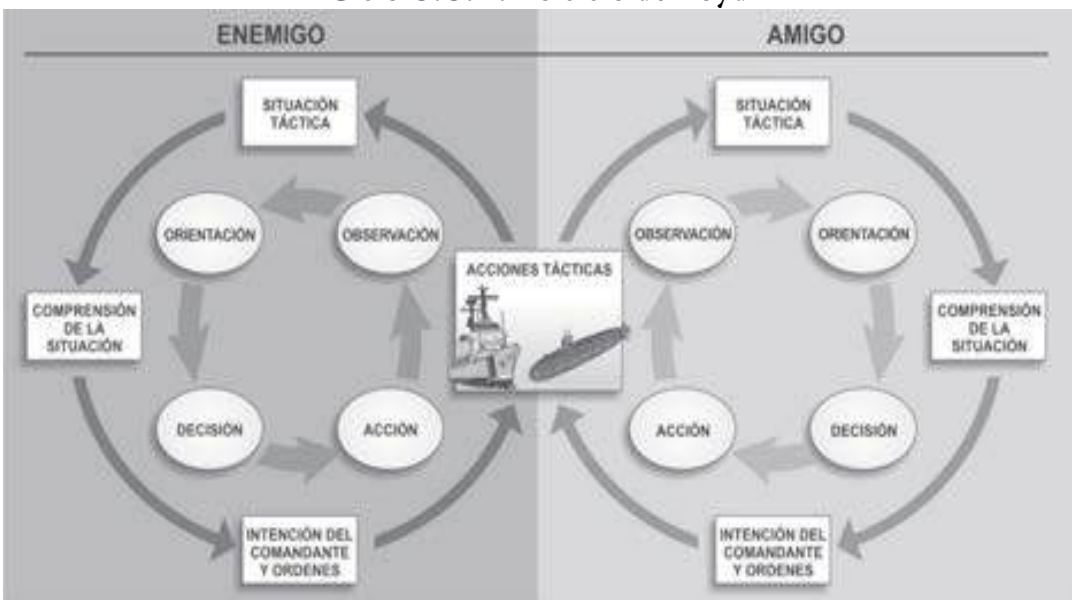
La evolución de la guerra de desgaste, según Luttwak (2001), se produce cuando los ejércitos comienzan a considerar el costo de la guerra y reconocen que la eficiencia es fundamental. Así, el conflicto se conduce mediante la Guerra de Maniobras aplicando los principios descritos por Sun Tzu (5th century BCE) como "la rapidez y la letalidad del ataque, aprovechando la falta de preparación del enemigo; aproxímate por rutas inesperadas y golpéalo donde no haya tomado precauciones". La Guerra de Maniobras, en concordancia con Segura (2012), busca dejar al adversario sin ideas, romper su ciclo de decisión y destruir su capacidad de reacción antes que su destrucción física, Boyd, citado por De Izcue, et al. (2020), expresa este concepto mediante el ciclo de observaciones, orientaciones, decisiones y acciones como se observa en la Figura 1. Ciclo O.O.D.A o ciclo de Boyd.

Según el enfoque norteamericano, de acuerdo con Lind (1985), la Guerra de Maniobra se basa en la integración y entendimiento de cuatro conceptos clave: Centro de Gravedad, Vulnerabilidad Crítica, Centro del Esfuerzo y Esfuerzo Principal. Para resolver estos aspectos, se requiere una secuencia de acciones, rápida, flexible y oportuna en completa sincronía con la Intención del comandante.

La historia, según Lind (1991), relata el uso de la Guerra de Maniobras desde las batallas de Leuctra, Cannae, Vicksburg, Blizkrieg, Verdún y el canal de Suez, que son fundamentales para la siguiente etapa en las guerras contemporáneas. Las Fuerzas del Ejército enfrentan enemigos igualmente inteligentes; a medida que un lado adopta acciones, el otro reacciona, aprende y se adapta. Apreciar estas relaciones entre las voluntades humanas es esencial para entender la naturaleza dinámica de un ambiente operacional, donde es difícil determinar la relación entre la causa y efecto, lo que contribuye a la incertidumbre de las operaciones militares.

El azar y la fricción contribuyen a la naturaleza incierta de las operaciones, de acuerdo a Clausewitz (2010), la Fricción se produce por ejemplo en el cambio de órdenes, planes muy complejos, fallas de equipo, etc. Los comandantes buscan contrarrestar la incertidumbre de las operaciones potenciando a los subordinados en la toma de decisiones, actuando y adaptándose rápidamente a las circunstancias cambiantes, mucho más rápido que el enemigo y se expresa este concepto mediante el ciclo de observaciones, orientaciones, decisiones y acciones como se observa en la Figura 1. Ciclo O.O.D.A o ciclo de Boyd.

Figura 1
Ciclo O.O.D.A o ciclo de Boyd



Nota. Apuntes de estrategia operacional. De Izcue, et al. (2020)

La evolución de la guerra de maniobras ha dado lugar al concepto de armas combinadas, donde se refuerza las características de velocidad y sorpresa, flexibilidad y capacidad de desorganizar al enemigo. Este enfoque potencia la combinación de las capacidades individuales de las armas tradiciones, como la infantería, caballería, artillería, ingeniería y comunicaciones. Por ejemplo, el uso de la artillería para debilitar al enemigo antes del ingreso de la infantería, seguido del choque de la caballería, habilitada por la movilidad establecida por los ingenieros militares, según Querembás (2018), resulta en un empleo eficiente de sus capacidades, logrando una suma mayor al esfuerzo individual de las partes.

El empleo de armas combinadas, explicado por Pineda, et al. (2019) se traduce en dos efectos principales: la complementariedad de armas, que consiste en la suma de sus capacidades para mejorar sus efectos, como la ingeniería militar en combinación con la maniobra; y el reforzamiento, que implica aumentar una capacidad similar para incrementar su letalidad, como el apoyo de la artillería de campo con la artillería antiaérea. Basándose en esta característica de organización combinada y con el avance de la tecnología armamentista, según el Ejército ecuatoriano (2020) se inician los Sistemas Operativos en el Campo de Batalla (SOCB), que agrupan la maniobra, el mando y control, los apoyos y la logística.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

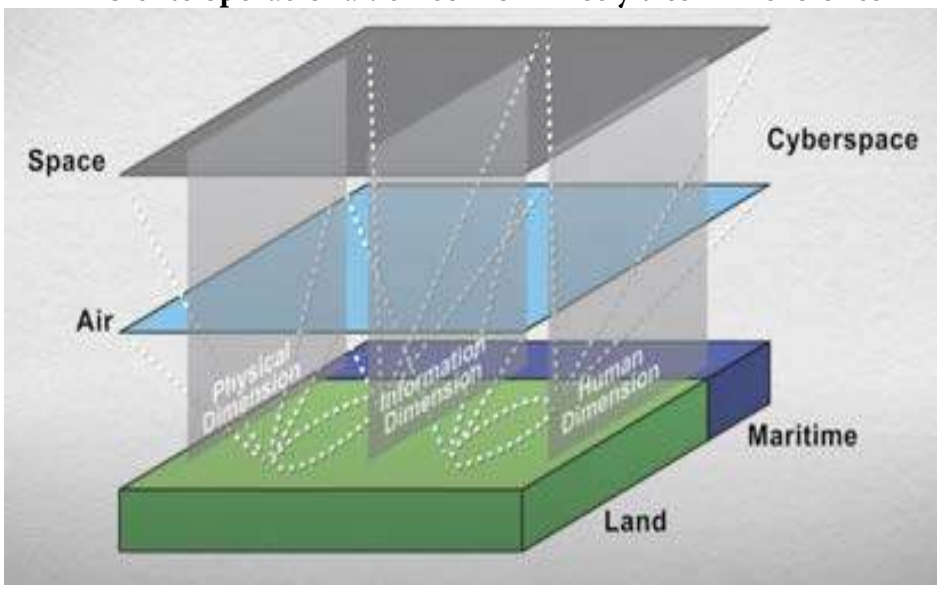
Las fuerzas no actúan como capacidades independientes, sino que se integran en sistemas completos y complejos, lo que permiten una mejor coordinación, un empleo eficiente y una economía de medios en las operaciones terrestres unificadas. En la actualidad estos SOCB incorporan los otros dominios físicos, y se han convertido en multidominios. Según Querembás (2020), esto ha permitido una fuerte integración interna de las Fuerzas Armadas, incluyendo el ejército, marina y aviación, así como otros organismos estatales y no estatales, organizaciones internacionales, privadas, públicas, académicas y técnicas. Esta evolución ha llevado a operaciones conjuntas unificadas, interagenciales, interestatales e integrales.

Siguiendo la línea de evolución, los dominios físicos han expandido su alcance al espacio exterior (órbita geoestacionaria internacional), donde se ha masificado el uso de satélites de comunicación y meteorológicos, que discretamente integran operaciones de inteligencia. Además, el dominio físico de los subsuelos, tanto en tierra como en el mar, ha revelado importantes recursos naturales a grandes profundidades. Con el rápido avance de la tecnología en todos los ámbitos del ser humano, los conflictos también han evolucionado, creando un dominio virtual o no físico conocido como ciberespacio. En este dominio, las capacidades del enemigo pueden ser horizontalizadas, haciendo la guerra aún más asimétrica. Por ejemplo, un solo operador capacitado con un equipo adecuado podría colapsar una organización completa desde cualquier parte del mundo.

Se puede identificar cinco dominios en total: los dominios físicos (aire, mar, que incluye el subsuelo marino, tierra, que incluye el subsuelo terrestre, y espacio exterior) y el dominio no físico del ciberespacio. Cada uno de estos dominios tiene la capacidad de modificar los resultados de la guerra.

Según el manual de campo sobre las operaciones multidominio del Departamento of the army. (2022), estos dominios están correlacionados en el ambiente operacional con tres dimensiones fundamentales que influyen decisivamente en el éxito o fracaso de las misiones. Estas dimensiones son: humanas, físicas y de información, como se demuestra en Figura 2. Ambiente operacional: cinco Dominios y tres Dimensiones.

Figura 2
Ambiente operacional: cinco Dominios y tres Dimensiones



Nota. Centro de armas combinadas de los EE. UU. (2022)

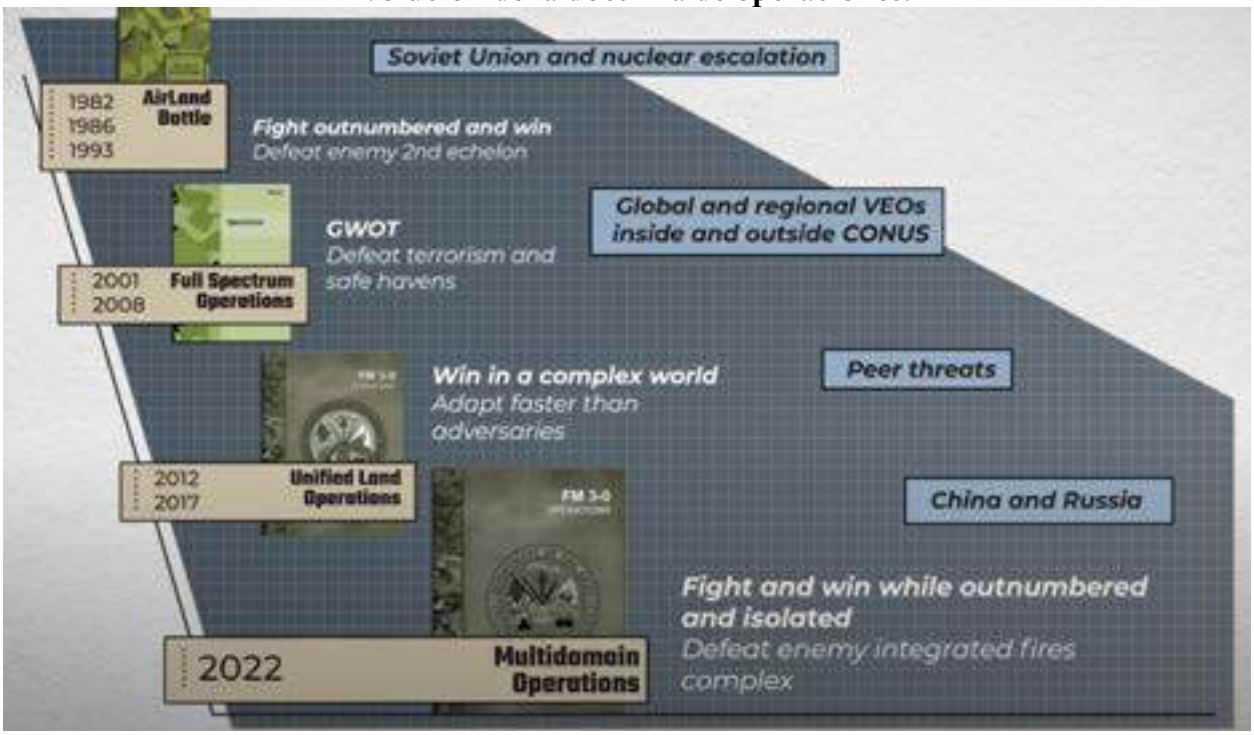
DOI: https://doi.org/10.59794/rscd.2025.v11i11.154

Las dimensiones físicas, de información y humanas en cada dominio proporcionan al comandante y su estado mayor una evaluación integral, permitiéndoles anticiparse al impacto en sus operaciones. Es vital entender la influencia de estas dimensiones. Por ejemplo, en el caso de la información, los medios de comunicación actuales permiten que un teléfono celular se convierta en un arma. Esto refleja el efecto que puede tener "el soldado estratégico", al hablar de las acciones de un solo soldado en el campo de batalla, transmitidas como información pública, que llegan a tener efectos estratégicos en las operaciones, ya sean positivos o negativos.

Paralelamente a lo descrito, la doctrina ha evolucionado para responder a las preguntas recurrentes de la sociedad en cada época de conflicto. Un ejemplo de esto es la evolución de la doctrina de operaciones del Ejército de los EE. UU., específicamente en el manual de campo FM 3-0, como se muestra en Figura 3. Evolución de la doctrina de operaciones. Se infiere, por lo tanto, que las operaciones multidominio implican el empleo combinado de las capacidades conjuntas de los SOCB de las Fuerzas Armadas. Este enfoque busca crear y explotar ventajas para alcanzar los objetivos y derrotar a las fuerzas opuestas con la mayor eficiencia en las operaciones.

Asimismo, se deduce que el ejército tiene la prioridad en la planificación de las operaciones, siendo responsable de organizar el empleo ordenado y coordinado de los recursos de las otras fuerzas. Por ejemplo, en ejércitos desarrollados como el de los Estados Unidos de Norteamérica, la Fuerza Terrestre recibe las capacidades de las otras fuerzas (llamadas servicios en ese país) para conducir las operaciones a nivel global.

Figura 3
Evolución de la doctrina de operaciones.



Nota. Centro de armas combinadas de los EEUU. (2022)

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Las operaciones multidominio se caracterizan por lo siguiente:

- Utilizan las capacidades asignadas, junto con las capacidades solicitadas por los comandantes según las necesidades de las operaciones, para generar un efecto multiplicador. Esto crea ventajas sobre las debilidades del enemigo a través de las dimensiones físicas, informativas y humanas. Por ejemplo, una brigada de maniobra que requiere un rápido despliegue en el campo de batalla solicita medios para ser aerotransportada, además incluye en sus tropas de infantería escuadras de robots que disminuyen el estrés físico y las bajas tempranas de sus hombres, mientras que se ejecutan acciones sicológicas en el enemigo, mediante operaciones de información en las que se maximiza la letalidad de las tropas propias como se observa en Figura 4. Operaciones Multidominio.
- El elemento integrador de los cinco dominios es la fuerza terrestre, ya que la influencia y el resultado del combate tendrá un efecto final en el dominio terrestre.
- El ejército aplica sus capacidades orgánicas y agregadas en todos los escalones de combate y en todos los dominios para vencer al oponente en los campos que este no domina, como las capacidades de comunicación satelital y las operaciones de interdicción.
- Prepararse para la guerra mediante ejercicios conjuntos permanentes, con el fin de potenciar las capacidades militares en tiempo de paz y mejorar la eficiencia en combate.
- El análisis de las debilidades del enemigo puede permitir a las fuerzas propias alcanzar objetivos rentables que faciliten la desarticulación, destrucción, aislamiento o derrota del oponente de forma temprana, por ejemplo, destruyendo sus SOCB.

Figura 4
Operaciones Multidominio

Nota. Revista profesional del Ejército de los EEUU. (2025)

Se puede razonar, por lo tanto, que en la actualidad todas las operaciones del ejército son operaciones multidominio. Para el futuro de las guerras, podemos inferir que tanto los dominios como sus dimensiones seguirán cambiado. Habrá más dominios físicos y no físicos por explorar, como la órbita geoespacial, el subsuelo profundo, el fondo marino y las nuevas tecnologías. En el futuro, no solo deberán unirse en las operaciones conjuntas los ejércitos, sino también las organizaciones no gubernamentales, el Estado y la empresa privada, considerando que la seguridad es una responsabilidad de todos. Estos actores estarán afectados por las variables políticas, económicas, sociales, militares, académicas, culturales, ecológicas, industriales, tecnológicas y legales (PEMESITL), especialmente en la producción y desarrollo de la industria de la defensa, la academia para la innovación militar y las relaciones internacionales para el intercambio de la información e inteligencia.

Ejército Multimisión

La forma de empleo de las Fuerzas Armadas evoluciona al ritmo de los avances tecnológicos y científicos en el ámbito militar, permitiendo la gestión de operaciones en múltiples dominios de manera simultánea. Este enfoque ha dado lugar al concepto de operaciones multidominio (Townsends, 2018), que abarcan un nuevo y amplio rango de operaciones militares, cada vez más demandantes. Según Keegan (1976), la planificación militar siempre prioriza el dominio terrestre, dado que es el hábitat natural de los seres humanos. Los otros dominios se alcanzan temporalmente mediante el uso de tecnología y máquinas. Esto implica que todas las operaciones comienzan y terminan en tierra, sin menospreciar la importancia de los demás dominios, cuya evolución ha transformado el poder hegemónico a lo largo de la historia universal.

Tradicionalmente, la planificación estratégica de los ejércitos se desarrollaba a partir de hipótesis que consideraban una guerra formal entre países, es decir, conflictos entre Estados. Este enfoque definía el diseño de la fuerza, la organización y el equipamiento, y las misiones de las Fuerzas Armadas, centradas en la defensa de la soberanía nacional frente a un oponente externo de características similares. Por lo tanto, la seguridad interna era responsabilidad de las Fuerzas Policiales, las cuales, en muchos países, tuvieron orígenes y formación militar. Por ejemplo, en Ecuador, la Policía Nacional fue formada y adoctrinada por el ejército.

A partir del 11 de septiembre de 2001, tras el catastrófico ataque a las Torres Gemelas y otros cinco objetivos políticos e icónicos de los Estados Unidos, llevó a Bush (2001) a declarar "Our war on terror begins with al Qaeda". Este discurso influyó globalmente en la inclusión de los ejércitos en la lucha contra el terrorismo, ampliando su accionar a guerras asimétricas, guerras irrestrictas, guerras remotas, guerras híbridas. Esto incrementó significativamente el apoyo de las Fuerzas Armadas a la seguridad interna, en complementariedad con la policía nacional y otras instituciones del Estado.

De acuerdo con el artículo 158 de la Constitución de la República del Ecuador (2008), Fuerzas Armadas tienen la misión fundamental de la defensa de la soberanía y la integridad territorial. Además, por referéndum, cumple con el apoyo complementario a la Policía Nacional en la lucha contra el

DOI: https://doi.org/10.59794/rscd.2025.v11i11.154

crimen organizado. También presta su contingente en actividades de desarrollo y apoya a otras instituciones del Estado en casos de desastres naturales y antrópicos, emergencias sanitarias, control de armas, entre otras, que se resumen en Figura 5. Misiones constitucionales que definen el empleo de FF. AA. del Ecuador.

Figura 5
Misiones constitucionales que definen el empleo de FF. AA. del Ecuador.

Nota. Sección de Visión y Prospectiva del Ejército del Ecuador.

En Ecuador, después del conflicto del Cenepa en 1995, se mantuvieron las misiones constitucionales enmarcadas en cuatro campos: la defensa de la soberanía e integridad territorial, el apoyo a la acción del estado, el apoyo al desarrollo nacional y la cooperación internacional. Sin embargo, la naturaleza del conflicto fue cambiando, como se observa en Figura 6. Modificación de la Naturaleza del Conflicto en el caso de Ecuador. El enfoque pasó de ser interestatal con amenazas simétricas, con balance de poder y teniendo al estado como blanco principal, a un conflicto intraestatal con amenazas asimétricas, actores no estatales y la población civil como blanco principal; finalmente se llegó a los conflictos intermésticos, donde los oponentes son grupos terroristas, el crimen organizado, el narcotráfico entre otros. De esta manera, el tipo, la cantidad y el alcance de las operaciones de Fuerzas Armadas han ido cambiando en el tiempo hasta llegar a ocupar hoy en día, el mayor esfuerzo del ejército, en las operaciones de ámbito interno, como se puede observar en la Figura 7.

El enfoque de la lucha en contra el terrorismo en el Ecuador tomó más tiempo, considerando que, según García (2007), los tres pilares fundamentales de una transformación militar son: la naturaleza del conflicto (tipo, cantidad, magnitud y alcance de las misiones), las normas jurídicas y las capacidades con las que cuenta una fuerza militar. De acuerdo con Querembás (2020), las capacidades se expresan en términos de materiales, infraestructura, recursos, adiestramiento, doctrina y organización (MIRADO). Por lo tanto, si uno de los tres pilares fundamentales cambia, se deben planificar rápidamente procesos de adaptación, modernización o transformación.

DOI: https://doi.org/10.59794/rscd.2025.v11i11.154

Figura 6
Modificación de la Naturaleza del Conflicto en el caso de Ecuador

Nota. Sección de Visión y Prospectiva del Ejército del Ecuador

Figura 7
Empleo histórico de las Fuerzas Armadas ecuatorianas

Nota. Creación del autor.

Figura 8
Los tres pilares fundamentales de la transformación

Nota. Military Review 2007.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

El empleo del ejército en el ámbito interno ha cambiado la "naturaleza" de sus operaciones, lo que requiere una modificación en el marco legal y las capacidades de estas fuerzas. Como se ha mencionado, el desarrollo de las capacidades se logra mediante la suma de los componentes del MIRADO. Sin embargo, es importante considerar la experiencia estadounidense, según el concepto funcional de sostenimiento TRADOC (2017) que utiliza: doctrina, organización, entrenamiento, materiales, liderazgo y educación, personal, infraestructura y políticas (doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy, DOTMLPF-P, por sus siglas en inglés). Este enfoque toma cuenta la dimensión humana, expresada a través del liderazgo y la educación.

Podemos deducir, que los escenarios futuros integran una participación más activa de los ejércitos, en el control de amenazas internas como el terrorismo, el narcotráfico, la minería ilegal, la tala de árboles, el tráfico de personas, la migración, y muchos otros delitos cometidos por bandas transnacionales que han perjudicado a las naciones. Además, se contempla la complementariedad con otras instituciones del Estado en casos de desastres naturales, crisis carcelarias, pandemias, entre otros.

Un aspecto crucial por analizar siempre será el presupuesto, para cumplir con la visión y con un enfoque prospectivo, los ejércitos a futuro deben ser adaptativos, flexibles y modulares, capaces de llevar a cabo un amplio rango de operaciones militares (ROM), es decir, ser multimisión, como se rescata del Manual Fundamental del Ejército Operaciones, Ejército Ecuatoriano (2020).

Esto también implica que el personal militar profesional debe ser polivalente, capaz de actuar en una variedad de funciones requeridas por la dinámica de las operaciones. En Ecuador, por ejemplo, se vive un conflicto armado interno, según el Decreto Ejecutivo No. 110 del 8 de enero (2024), que enfrenta a 22 grupos armados ilegales declarados como terroristas y actores no estatales beligerantes, acorde con el Decreto Ejecutivo No. 111 del 9 de enero (2024).

En este punto es importante anotar la visión institucional del Ejército del Ecuador, expresada en el plan de transformación de la DTDM (2020) que textualmente dice:

> Al 2033 ser una Fuerza Terrestre disuasiva, con características multimisión, con personal polivalente y medios multipropósito; promoviendo de forma permanente los principios, valores y comprometido con la sociedad, respetando los derechos humanos y garantías de los ciudadanos, contribuyendo a la integración, defensa, seguridad del Estado y posicionada en la cooperación internacional para el mantenimiento de la paz.

Se puede observar que las características enunciadas de un ejército del futuro se ajustan a todas las condiciones analizadas en el artículo, preparando a la institución castrense para las demandas sociales venideras. Esto se logra mediante una economía de medios que permita tener una "navaja Suiza" capaz de resolver todos los problemas militares, enmarcados en el concepto operacional amplio y flexible, según las capacidades militares futuras de la DTDM (2022) como se muestra en la Figura 9. Propósito del Concepto operacional.

Figura 9
Propósito del Concepto operacional

Nota. DTDM (2022). El concepto operacional sirve como un marco fundamental que orientará el empleo de estructuras militares flexibles, permitiendo responder eficazmente a las demandas de seguridad y defensa tanto actuales como futuras.

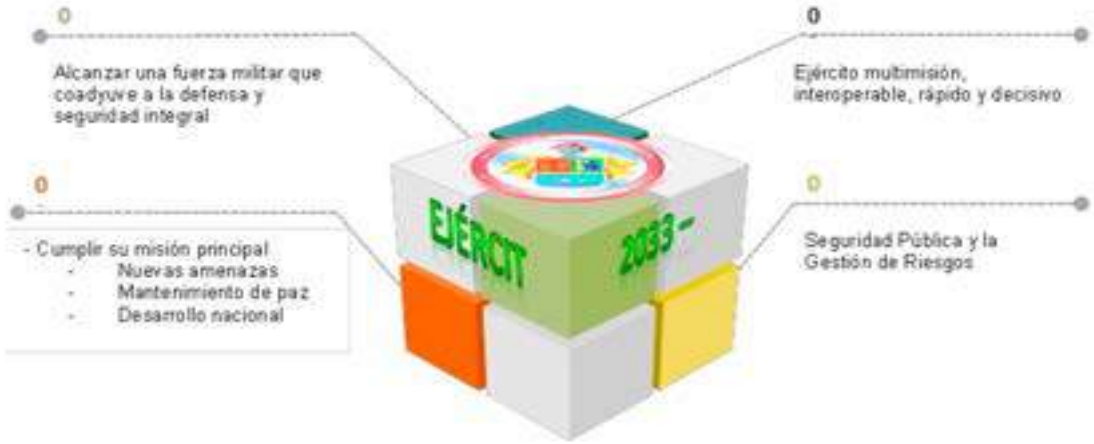
Para lograr estos propósitos los ejércitos deben profesionalizarse, especializarse, modernizarse y transformarse, basándose en el concepto operacional general, se debe diseñar una fuerza orientado a disponer unidades altamente entrenadas y equipadas para hacer frentes a las amenazas y riesgos, como se muestra en la Figura 10. Esquema que guía el diseño de fuerza en base al concepto operacional.

Este diseño de fuerza debe contribuir al desarrollo de capacidades mediante el análisis del MIRADO y considerando las capacidades militares futuras expuestas en la Figura 11. Capacidades militares futuras.

De esta manera, las fuerzas deben interconectarse para convertirse en multipropósito, es decir, para defensa externa, la gestión de riesgos y defensa interna, teniendo en cuanta los conflictos futuros por los recursos naturales. Además, deben ser multimisión, lo que implica que el ejército se empleará en tareas de seguridad, defensa, desarrollo, apoyo a otras instituciones del Estado, y en la asistencia durante desastres naturales y emergencias.

Figura 10

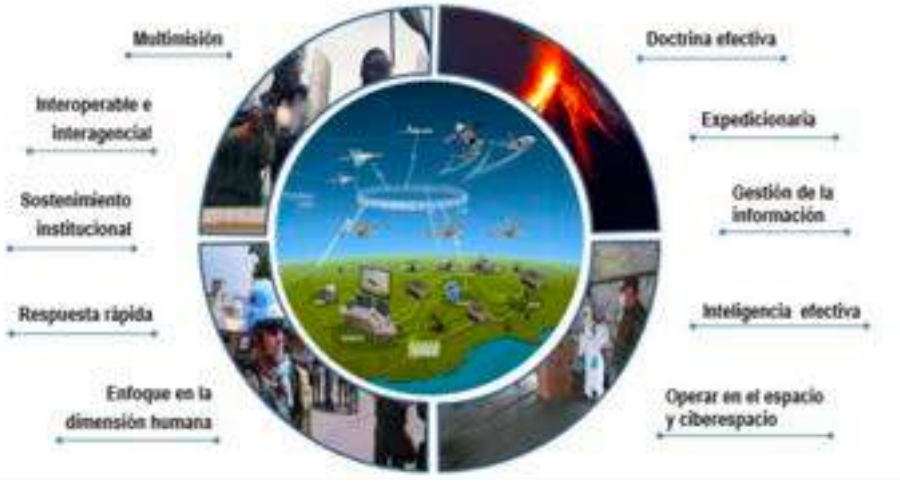
Esquema que guía el diseño de fuerza en base al concepto operacional



Nota. DTDM (2022).

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Figura 11
Capacidades militares futuras



Nota. DTDM (2022)

En todo el proceso, se destaca que el núcleo del desarrollo de capacidades es el talento humano, desarrollado a través de un perfil profesional que, en el futuro, deberá permitir la polivalencia de los soldados. Esto significa que puedan operar en todo tipo de circunstancias, reflejando la esencia misma de la profesión militar, donde un día se puede estar combatiendo y al siguiente desempeñando funciones de diplomacia militar.

El perfil profesional ha considerado las características humanas a desarrollar, como se observa en la Figura 12. Perfil profesional del profesional militar del futuro. Este estudio fundamenta su cumplimiento en el sistema de educación militar, que incluye los procesos de formación, perfeccionamiento, especialización y capacitación militar, abordados en la propuesta de Querembás (2021) sobre el complemento al modelo educativo de las Fuerzas Armadas para la modalidad de educación híbrida.

Figura 12
Perfil profesional del profesional militar del futuro

Nota. DTDM (2020)

Conclusiones

El análisis de la evolución de los dominios de la guerra y la transformación de los ejércitos hacia fuerzas multimisión, utilizando el caso del Ejército del Ecuador, revela varias conclusiones clave.

1. La adaptación y flexibilidad en una sociedad gaseosa, caracterizada por su inmediatez e inestabilidad en un mundo BANI, son fundamentales para el éxito de las misiones militares.

2. La integración del rango de operaciones militares para operar simultáneamente en los cinco dominios contemporáneos, junto con considerar la influencia de las dimensiones físicas, humanas y de información, son esenciales para mejorar la eficiencia operativa.

3. El estudio destaca la importancia del dominio terrestre como base para ejemplificar la evolución de las tácticas militares, desde la guerra de desgaste hasta las operaciones multidominio, integrales, interagenciales e internacionales.

4. La implementación de SOCB y la adopción de un enfoque integral, interagencial e internacional; han obligado que los ejércitos planifiquen el desarrollo de sus capacidades militares mediante planes de profesionalización, modernización y transformación.

5. La ampliación del rango de operaciones militares, al incluir la lucha contra el terrorismo, el crimen organizado y otras amenazas internas, junto con las misiones tradicionales de defensa externa, subraya la necesidad de un enfoque flexible y modular. Este enfoque debe priorizar la dimensión humana, reconociendo que el liderazgo y la educación militar son cruciales para desarrollar un perfil profesional polivalente en los soldados del futuro.

6. La comprensión, coordinación y sistematización de la integración de dominios y ejércitos multimisión son vitales para enfrentar los desafíos futuros. La capacidad de las Fuerzas Armadas para adaptarse y transformarse continuamente, garantizará su supervivencia en un mundo en constante cambio.

7. La dimensión humana no ha dejado de perder su preponderancia en el ámbito de la guerra, concluyendo que es prioritario el desarrollo de un perfil del soldado del mañana.

Referencias

Arce Ducassou, R. (2019). Capacidades militares para enfrentar los desafíos de las operaciones multidominio. *Revista Ensayos Militares,* 5(2), 57-81.

Bauman, Z. (2017). *Retrotopía*. Titivillus.

Bush, G. (2001). Discurso ante una sesión conjunta del Congreso y el pueblo estadounidense. En T. W. House (Ed.).

Clausewitz, C. (2010). *De la guerra*. Editorial Tecnos. https://doi.org/978-84-309-5118-5

Constitución de la República del Ecuador [Const.] (2008). Registro Oficial N.° 449, 20 de octubre de 2008. https://www.gob.ec/sites/default/files/regulations/2020-06/CONSTITUCION%202008.pdf

De Crescenzo, L. (2020). *Panta rei (tutto scorre)*. Arnoldo Mondadori Editorial.

Decreto Ejecutivo No. 110. Registro Oficial. Ecuador. 8 enero, 2024.

Decreto Ejecutivo No. 111. Registro Oficial. Ecuador. 9 enero, 2024).

De Izcue Arnillas, C., Arriarán Shaffer, A., & Tolmos Mantilla, Y. (2020). El ciclo O.O.D.A. y la guerra de maniobras. En *Apuntes de estrategia operacional* (pp. 71-74).

Department of the Army. (2022). *Field Manual No. FM 3-0: Operations. Headquarters, Department of the Army*. https://studylib.net/doc/27131729/fm-3-0-2022

Dirección de Transformación y Desarrollo Militar (DTDM). (2020). *Modelo de transformación del Ejército Ecuatoriano*. Instituto Geográfico Militar. https://ejercitoecuatoriano.mil.ec/images/IMAGENES/TRANSFORMACION/4_Modelo_transformacion.pdf

Dirección de Transformación y Desarrollo Militar (DTDM). (2022). *Capacidades militares futuras*. Instituto Geográfico Militar.

Ejército Ecuatoriano. (2020). *Manual Fundamental del Ejército: Operaciones*. Comando de Educación y Doctrina Militar Terrestre.

Escher, M. (1953). *Relatividad* [Litografía]. Museo Escher, La Haya.

García, J. (2007). Los tres pilares de la transformación. *Military Review,* 16-24.

Innerarity, D. (2020). *La sociedad invisible*. Galaxia Gutenberg.

Joint Force Development. (2018, junio 8). *Joint Publication* 3-12: Cyberspace operations. Department of Defense.

Joint Force Development. (2019, octubre 3). *Joint Publication* 3-31: Joint land operations. Department of the Army.

Joint Force Development. (2019, julio 25). *Joint Publication 3-30: Joint air operations*. Department of the Air Force.

Joint Force Development. (2021, septiembre 20). *Joint Publication 3-32: Joint maritime operations* (JP 3-32). Department of the Navy.

Joint Staff. (2016, febrero 15). *Joint Publication 1-02: Department of Defense dictionary of military and associated terms*. Department of Defense.

Joint Staff Force Development. (2016, enero 14). *Cross-domain synergy in joint operations: Planner's guide*. Cyber Vault Library.

Keegan, J. (1976). *El rostro de la batalla*. Viking Press.

Lind, W. (1985). *Maneuver warfare handbook*. Westview Press.

Lind, W. (1991). *Manual de la guerra de maniobras* (Vol. 1). Círculo Militar.

Ejército Ecuatoriano. (2020). *Manual Fundamental del Ejército*. Comando de Educación y Doctrina Militar Terrestre.

Pineda González, E., Rodríguez Melo, Y., Rivera Lozano, A., & Cruz González, D. (2019, octubre 25). Primer seminario de armas combinadas. *OSFHome*. https://doi.org/10.17605/OSF.IO/467QP

Querembás, M. (2018). Fuerzas armadas multifuncionales: La ingeniería militar como arma técnica multipropósito en el sismo del 16 de abril de 2016. *Revista de la Academia de Guerra del Ejército Ecuatoriano*, 93-98.

Querembás, M. (2020, junio 8). Nueva doctrina militar para los escenarios del siglo

XXI. *Revista de la Academia de Guerra del Ejército Ecuatoriano*, 13, 28-39. https://doi.org/10.24133/age.n13.2020.03

Querembás, M. (2021, noviembre). *Propuesta del complemento al modelo educativo de Fuerzas Armadas para la modalidad de educación híbrida.* Universidad Internacional del Ecuador.

Segura Flores, R. (2012). La teoría de la guerra de maniobra. *Military Review*, 64-71.

Townsend, S. (2018). Accelerating multi-domain operations: Evolution of an idea. *Military Review*, 6.

U.S. Army Training and Doctrine Command (TRADOC). (2017). *The U.S. Army functional concept for sustainment (AFCS) 2020-2040*. Department of the Army.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Guerra Cognitiva: El Dominio Cognitivo de la guerra, la mente humana como campo de batalla y su integración en los dominios

Cognitive Warfare: The Cognitive Domain of warfare, the human mind as a battlefield and its integration into the domains

Recibido: 20/ 04 / 2025 | Revisado: 14 / 07 / 2025 | Aprobado: 10 / 09 / 2025
DOI: https://doi.org/10.59794/rscd.2025.v11i11.138

Coronel (r)Alejandro Salas Maturana, FACh
Chile

Correo: alejandro_salas_m@hotmail.com

ORCID: https://orcid.org/0000-0002-6881-2158

Afiliación: Academia Nacional de Estudios Políticos y Estratégicos

El autor es coronel de Aviación de Chile en situación de retiro. Magíster en Ciencias de la Administración Militar de la Academia de Guerra Aérea y, Magíster en Seguridad y Defensa mención Gestión Político-Estratégica de Academia Nacional de Estudios Políticos y Estratégicos (ANEPE). Ingeniero de Ejecución en Sistemas Aeronáuticos mención Piloto de Guerra y especialista en Estado Mayor. Diplomado en "Gerencia de Recursos Humanos" de la Universidad de Chile y en "Estudios Políticos y Estratégicos" de la Academia Nacional de Estudios Políticos y Estratégicos (ANEPE). Especialista en "Política de Defensa y Amenazas Complejas" en el Centro de Estudios Hemisféricos de Defensa de la Universidad Nacional de la Defensa de Estados Unidos de Norteamérica. Se desempeñó por 15 años en la Academia Nacional de Estudios Políticos y Estratégicos, donde ejerció los cargos de jefe de Planificación Académica, jefe de Investigación, jefe del Centro de Investigaciones y Estudios Estratégicos y se desempeñó como profesor de "Conducción de la Defensa" y "Amenazas Multidimensionales". Es autor y coautor de numerosas publicaciones relacionadas con los fenómenos terrorista y de seguridad, donde destacan los libros "La amenaza terrorista para la seguridad internacional: estudio comparado de casos de tomas de rehenes", "La Defensa en perspectiva académica: historia y proyección", y "Gobernabilidad, Desarrollo y Seguridad en las Zonas Extremas de Chile". Integró grupos de trabajo de asesoría para la Subsecretaría de Defensa, formó parte del Grupo de Trabajo del Consejo Latinoamericano de Ciencias Sociales "Sociedad, Seguridad y Conflicto en América Latina", y fue vocal del Consejo Editorial de la revista Política y Estrategia de la Academia Nacional de Estudios Políticos y Estratégicos. Experto asociado de la revista digital, Defensa 21 LATAM – Seguridad y Defensa en América Latina.

DOI: https://doi.org/10.59794/rscd.2025.v11i11.138

Resumen

Hablar de los dominios de la guerra y, particularmente del multidominio, es un ejercicio desafiante para quienes estudian los conflictos y su evolución, pero aún más para quienes son responsables de concebir, planificar y conducir en sus diferentes niveles las capacidades de defensa de una nación. En relación con ello, en este artículo se aborda en términos generales el desafío que implica adentrarse en una temática nueva, que en muchos aspectos aún está en estudio, pero que, dada su relevancia en el marco de la guerra, requiere ser estudiado para comprender sus alcances e impacto en los conflictos actuales y futuros. Así entonces, pensar en la mente humana como campo de batalla genera un ambiente que, al no tener la tangibilidad de los dominios físicos, crea en un ambiente abstracto, aunque las consecuencias de lo que ocurra en ella los impactarán de manera relevante. En este contexto, la mente humana como escenario bélico empuja hacia lo cognitivo como un dominio más de la guerra, exigiendo también reflexionar sobre cómo se integra e impacta en el multidominio.

Palabras clave: Dominios de la guerra, multidominio, guerra cognitiva, mente humana, comportamiento humano

Abstract

Discussing the domains of warfare, but particularly the multi-domain, is a challenging exercise for those who study conflicts and their evolution, but even more for those responsible for conceiving, planning, and managing a nation's defense capabilities at their various levels. In this regard, in this article we will address in general terms the challenge of delving into a new topic, which in many aspects is still under study, but which, given its relevance in the context of warfare, requires study to understand its scope and impact on current and future conflicts. Thus, thinking of the human mind as a battlefield introduces us to an environment that, lacking the tangibility of physical domains, places us in an abstract context, although the consequences of what happens within it will significantly impact them. In this context, the human mind as a war theater pushes us toward the cognitive as another domain of warfare, also requiring us to reflect on how it integrates and impacts the multi-domain context.

Keywords: Domains of warfare, multidomain, cognitive warfare, human mind, human behavior

DOI: https://doi.org/10.59794/rscd.2025.v11i11.138

Introducción

Cuando se observa la guerra cómo un fenómeno eminentemente humano, se manifiesta lo mejor y lo peor de la naturaleza humana, reflejando tendencias sociales que se traducen en estrategias convencionales y no convencionales. En este plano, el ideal estratégico es la racionalidad y el equilibrio emocional que conduce a la victoria con el menor derramamiento de sangre y pérdida de recursos posible. En lo opuesto, una mente y un cerebro agobiados por la emoción, enraizada en el pasado sin ver el presente y, que no puede ver el mundo con claridad, producirá estrategias erradas (Greene, 2020) con una alta probabilidad de ser derrotada.

Cuando Sun Tzu señaló que "el supremo arte de la guerra es someter al enemigo sin combatir" (Griffith, 1971), no sólo expresaba una forma distinta de ver la guerra. El sentido de la frase plantea que, la clave para imponer la voluntad sobre un adversario sin emplear la fuerza letal está en el cerebro y la mente humana[1] que, a través de procesos cognitivos complejos hace sentir a su adversario que enfrentarlo por medios militares y/o no militares conlleva un precio tan alto que no se está dispuesto a pagar (Sabater, 2023). A riesgo de ser redundante, se dice entonces que, siendo el cerebro y la mente los que controlan las acciones humanas, en ellos está la llave de la victoria o la derrota en un conflicto.

Miles de años después, cuando el General André Beaufre en su obra *Introducción a la Estrategia (1977)* plantea citando a Foch que, "la esencia de la estrategia yace en el juego abstracto que resulta de la oposición de dos voluntades", y luego agrega que, la estrategia es el "arte de la dialéctica de las voluntades que emplean la fuerza para resolver su conflicto", (p. 18) se refiere a que en un conflicto, la voluntad de un individuo o un pueblo enfrentado otro, se genera en la mente y el cerebro de los seres humanos.

Refiriéndonos a Von Klausewitz (2002), se encuentran en su Trinidad elementos directamente vinculados al cerebro y a la mente humana. El ciego impulso natural que conduce al odio y a la violencia, el juego del talento y del valor en el dominio de las probabilidades del azar que depende del carácter del comandante en jefe de las fuerzas militares y, la definición de los objetivos políticos que incumben al gobierno, se generan primero en la mente humana antes de transformarse en estrategias y decisiones que requerirán de la disposición, tenacidad y energía individual y colectiva para materializar la imposición de la voluntad sobre el adversario y, con ello, el logro de la victoria.

En la vida diaria y, aún más en el conflicto y su expresión más extrema, la guerra, la incertidumbre es una constante. Bachs (2016) la define como una situación en la que se desconoce el resultado final, y tampoco se puede predecir en término de probabilidades objetivas. A su vez, según la Organización Internacional de Normalización (ISO, 2018),

1 Aunque tienen diferencias, el cerebro y la mente son dimensiones interconectadas siendo imposible separar la una de la otra. En el hecho, es común que se utilicen como términos intercambiables. El cerebro es el órgano físico encargado de las funciones cognitivas y corporales, mientras que la mente es el conjunto de procesos mentales y experiencias subjetivas que emergen de su funcionamiento. Entender esta distinción es fundamental para comprender cómo trabajan los seres humanos, y cómo las emociones, pensamientos y comportamientos están profundamente influenciados por la interacción entre ambos.

la incertidumbre es definida como un estado de conocimiento limitado o falta de certeza que impide describir con exactitud la situación existente o un resultado futuro, y por tanto, la planificación de la toma de decisiones. En relación con ello, Morin (2010) plantea que la condición humana está marcada por la incertidumbre cognitiva, que obedece a tres principios de incertidumbre en el conocimiento:

El cerebral, donde el conocimiento nunca refleja lo real, porque el cerebro lo traduce y lo reconstruye provocando riesgo de error; el psíquico, donde el conocimiento de los hechos es producto de la interpretación de la mente y, el epistemológico, que resulta de la crisis de los fundamentos de la certeza en filosofía y de la ciencia. Por ello, conocer y pensar no es llegar a una verdad absolutamente cierta, sino dialogar con la incertidumbre.

Todo lo planteado, conduce a abordar el conflicto con una perspectiva que se aleja de las miradas más comunes. Así entonces, al estudiar la guerra contemporánea, no se puede evitar observar que su evolución está mostrando un rápido desarrollo a partir de los nuevos escenarios que han surgido progresivamente junto a la multipolaridad derivada de la aparición de actores estatales y no estatales que, junto con cuestionar el statu quo, están incrementando la incertidumbre al generar un entorno operativo complejo y cambiante, obligando a su vez a redefinir el campo de batalla. Tal vez se estaría frente a la necesidad de proponer nuevos desarrollos conceptuales y estructurales en el diseño de las fuerzas, a fin de enfrentar con eficacia las amenazas actuales. Qué duda cabe, que en esta situación el desafío inmediato es ver formas distintas de pensar y hacer la guerra.

Respecto a este desafío inmediato, volviendo un instante a Sun Tzu (1971), Beaufre (1977) y Von Clausewitz (2002), se constata que el cerebro y la mente humana serían elementos decisivos al momento de enfrentar los desafíos que impone un conflicto, pero que no son factores únicos y aislados porque forman parte de un todo que dan sentido a la manera de pensar y hacer la guerra. En este sentido, también la incertidumbre es un factor que está presente como un fenómeno que afecta la mente incidiendo en las percepciones, creencias y juicios de las personas.

En este marco, aproximarse al concepto de dominios de la guerra, conduce al surgimiento de las operaciones multidominio, lo que impone ampliar su valoración que aproxima a la realidad compleja que implica el desarrollo de los conflictos actuales, donde las variables presentes en ellos y sus interacciones dan cuenta de las dificultades que se presentan al emprender los estudios teóricos y, más aún, en la aplicación práctica al momento de enfrentar y prevalecer en determinado conflicto, a través del logro de los objetivos establecidos por la política derivados de los intereses que cada país protege.

Junto con los cuatro dominios definidos por su entorno (terrestre, marítimo, aéreo, espacial y el ciberespacio que los conecta), lo cognitivo se considera un nuevo dominio que opera a nivel global por efectos de la conexión digital, que utiliza la tecnología de la información junto a herramientas, máquinas, redes y sistemas que la acompañan. Su campo de acción es la mente y el cerebro humano individual y colectivo donde se busca alterar o engañar a los integrantes de un gobierno, a la clase política y económica, a los miembros de las Fuerzas Armadas, y a la sociedad completa de un país o grupo de países en un tipo de agresión que no tendría límites.

DOI: https://doi.org/10.59794/rscd.2025.v11i11.138

De esta forma entonces, a partir del contexto propuesto, en primer lugar, en este trabajo se revisará la conceptualización de dominios de la guerra y multidominio, para luego analizar la conceptualización de la Guerra de la Información, la Guerra Cognitiva y la mente humana como campo de batalla, donde se expone por qué la mente humana es decisiva en el enfrentamiento de voluntades que se produce en una guerra, para finalmente explicar desde nuestra perspectiva, el comportamiento del Dominio Cognitivo y su relevancia en las operaciones multidominio durante el desarrollo de un conflicto.

Desarrollo

Dominios de la guerra y multidominio

Los debates en torno a los dominios de la guerra son esenciales para comprender la naturaleza evolutiva de los conflictos, y también para avanzar a partir de su alcance respecto de los ámbitos en que actúan. En esta conceptualización, actualmente se acepta la existencia de cinco dominios (Terrestre, Marítimo, Aéreo, Espacial y Ciberespacio) tal como lo considera la Organización del Tratado del Atlántico Norte (OTAN 2023). Esta categorización define los cuatro espacios físicos donde se realizan operaciones militares y, un espacio virtual, intangible y global que transversalmente afecta a los cuatro anteriores permeándolos e influenciándolos de manera profunda e imprevisible, mediante el uso de tecnologías informáticas, de la inteligencia artificial y de las neurociencias.[2]

En el contexto señalado, un programa informático tendría el potencial de dejar fuera de servicio infraestructuras críticas, pudiendo afectar a la generación de energía, los sistemas financieros, las redes de transporte y los servicios esenciales de un país, con graves consecuencias para su seguridad y bienestar. Recientemente ha surgido lo cognitivo estrechamente ligado a la información como un nuevo dominio no físico, estrechamente ligado al dominio cibernético. En este sentido, la manipulación cognitiva puede alterar las percepciones de un grupo humano, modificando su comportamiento y juicios, empujándolo a la toma de decisiones erradas afectando a la sociedad y a la estructura del Estado que la sustenta.

Se puede afirmar entonces, que un dominio de la guerra es un espacio físico o virtual donde se realizan operaciones militares, donde los actores involucrados se enfrentan para imponer su voluntad sobre su adversario, y que para ello necesitan dominarlo y controlarlo para maniobrar dentro y a través de él. No obstante, desde el fin de la Guerra Fría se ha estado desarrollando una evolución en el carácter de la guerra.

Los ataques de precisión a larga distancia con misiles, artillería y drones, las capacidades furtivas de aviones de combate y medios navales, la tecnología satelital usada en reconocimiento, vigilancia y obtención de

2 Las neurociencias son un conjunto de disciplinas científicas que estudian el sistema nervioso y todos sus aspectos, tales como la estructura, función, desarrollo ontogenético y filogenético, bioquímica, farmacología y patología, y cómo sus diferentes elementos interactúan, dando lugar a las bases biológicas de la cognición y la conducta.

información de inteligencia, sumados a las capacidades para utilizar el ciberespacio, han generado cambios a veces decisivos en la forma de hacer la guerra. Las operaciones en zona gris y la guerra híbrida también reflejan las nuevas formas de acción que los actores en conflicto utilizan para imponer su voluntad y lograr sus objetivos políticos.

Sin embargo, una nueva forma de guerra sería la culminación de la evolución en la manera en que los países pueden llevar a cabo operaciones militares, cuestionando la aplicación de la fuerza letal como la única necesaria para lograr los objetivos que se busca satisfacer. Se trata de la Guerra Cognitiva, forma de conflicto altamente disruptivo que pone en riesgo o amenaza a las instituciones democráticas y a la soberanía de los países, que obliga a mirar la guerra desde otras perspectivas que modifican de manera relevante su carácter. También afectaría la forma de mirarla y comprenderla (Bebber, 2024).

Shah (2024) citando a Krepinevich, autor del libro "Los orígenes de la victoria: cómo la innovación militar disruptiva determina el destino de las grandes potencias" (The Origins of Victory: How Disruptive Military Innovation Determines the Fates of Great Powers), señala que, en la actualidad, los avances desarrollados en tecnología de datos, en modelos basados en algoritmos, en las ciencias del cerebro, en la inteligencia artificial, la computación cuántica y la biología sintética estarían expandiendo los ámbitos que se podrían aprovechar para realizar ataques utilizando la manipulación cognitiva de las personas, lo que está transformando la dinámica de la guerra.

En este ámbito China y Rusia compiten con y, en algunos casos, superan con creces a las fuerzas militares estadounidenses con la ambición de transformar el orden global. Como se aprecia, se constata la presencia de un nuevo dominio de la guerra, que se agrega a los cinco dominios ya reconocidos por la OTAN, y que tendría una influencia decisiva en las operaciones multidominio.

Mirar lo que ha ocurrido y continúa pasando en torno a la guerra Ucrania-Rusia, en la guerra que enfrenta a Israel con Hamas, Hezbollah e Irán, y otros conflictos como el que enfrenta a los Hutíes de Yemen con occidente, entre otros de menor impacto en un escenario de mundo globalizado e hiperconectado, obliga a reconocer la necesidad de revisar la forma en que se conducen las operaciones militares, a partir de una ampliación de los ámbitos de acción en que estas se producen.

En este contexto, las nuevas tecnologías han ampliado los dominios físicos (tierra, mar, aire y espacio) y no físicos (ciberespacio y cognitivo) donde se suman como funciones transversales la información, el espectro electromagnético, la inteligencia artificial (IA), la nanotecnología y la interoperabilidad entre Estados y agencias. De esta manera, existe un espacio de batalla que se ha extendido por el mayor alcance de los sistemas de armas y dominios no físicos, generando un nuevo entorno operativo con efectos en todos los niveles de la conducción de una conflicto (Martínez-Valera, 2022).

La extensión del espacio de batalla conduce a abordar las Operaciones Multidominio que representan un cambio de enfoque que resulta fundamental particularmente para la OTAN. Con ello, la alianza tendría la capacidad de influir estratégicamente en los acontecimientos, coordinar esfuerzos con actores externos a ella, y provocar desafíos formidables a los adversarios. Implica disponer de las capacidades para realizar actividades militares en to-

dos los dominios y entornos operativos, con acciones sincronizadas con actividades no militares, crucial para las iniciativas de defensa y disuasión a largo plazo (NATO's Strategic Warfare Development Command, 2023).

De acuerdo con lo que señala Cannon en su artículo "La transición de la Alianza a operaciones multidominio: una perspectiva de AIRCOM" (The Alliance's Transition to Multi-Domain Operations: An AIRCOM Perspective) publicado en mayo de 2024 en la publicación "Revista del Centro de Competencia del Poder Aéreo Conjunto" (The Journal of Joint Air Power Competence Centre), materializar el concepto de Operaciones Multidominio se ha convertido en uno de los retos más desafiantes que la OTAN ha debido asumir, a partir de la necesidad de contrarrestar la amenaza rusa de Antiacceso/Negación de Área (A2/AD),[3] al surgir un campo de batalla futuro cambiante e impredecible.

Este sistema de sistemas multidominio, multicapa, multiamenaza, altamente dinámico, omnidireccional y de gran alcance (Shaun, 2023), obligó a la OTAN a replantear su enfoque para implementar de forma eficaz y eficiente el Instrumento Militar, donde la creciente competencia en los dominios cibernético y espacial plantea nuevas complejidades que deben abordarse durante las operaciones. Lo importante es, que los conceptos operativos deben garantizar que las tareas principales de la OTAN puedan ejecutarse en todo el espectro en tiempos de paz y conflicto en cualquier condición. Por ello, los miembros de la Alianza deben tener la capacidad de comprender permanentemente el entorno operativo cambiante, desarrollando estrategias para mantener las ventajas operativas.

Como se plantea en el documento OTAN (2023): "Explicación de Operaciones multidominio en la OTAN (Multi-Domain Operations in NATO – Explained), las Operaciones Multidominio se refieren esencialmente al esfuerzo por articular acciones militares en todos los dominios de la guerra, sincronizadas con actividades no militares, que contribuyen a que la alianza obtenga los resultados deseados en el momento y lugar más conveniente. Esto significa que, en el actual entorno estratégico caracterizado por la competencia en marcha entre las grandes potencias, las fuerzas militares deben adaptar sus actuales capacidades centradas en la contrainsurgencia y la lucha contra el terrorismo, para enfrentar a Fuerzas Armadas convencionales poseedoras de capacidades tecnológicas no demasiado distintas a las de la Alianza (Pulido, 2018).

La guerra ruso-ucraniana representa el caso más reciente de una realidad que inevitablemente se debe enfrentar. Es tal vez el mejor ejemplo que demuestra que la evolución conceptual en el tema operativo es una realidad tangible, que obliga a analizar y debatir cómo se debe afrontar al adversario en un campo de batalla que excede los límites del espacio de batalla donde ucranianos y rusos se enfrentan. A modo de paréntesis, es pertinente decir

3 Es un concepto de naturaleza militar y operacional que integra dos conceptos: el antiacceso que se refiere a acciones en profundidad que podrían impedir la movilidad de fuerzas adversarias hacia un teatro de operaciones y, la denegación de área, que se orienta a medidas para limitar la libertad de acción de fuerzas desplegadas en un teatro bajo el control de quien lo aplica. Ambos conceptos por tanto están directamente relacionados y pueden superponerse. Se identifica como un "sistema de sistemas" basado en la integración de éstos, y no en su sola superposición, uniendo acciones defensivas y también ofensivas que se aplican de forma gradual ante un adversario que tendría la iniciativa.

que tal vez no sería aventurado decir que en esta guerra también se enfrentan la Alianza Atlántica y Rusia, donde no hay enfrentamiento directo de fuerzas militares, pero sí una guerra política donde el protagonismo lo tienen los medios no militares.[4]

Volviendo a las Operaciones Multidominio y vinculado a lo dicho en el párrafo anterior, la OTAN se refiere a la importancia de la sincronización de las capacidades militares de los países miembros con los instrumentos de poder integrados de cada país, lo cual le permitiría emplear todas sus capacidades para responder a una amplia gama de amenazas. Ello significa que la aptitud para desarrollar capacidades multidominio no sólo recae en las entidades militares de sus miembros, si no que alcanza a todos sus instrumentos de Poder Nacional reflejados en los ámbitos político, diplomático, económico y social, cuya gestión corresponde a sus gobiernos.

Otro aspecto relevante que considerar, tiene relación con los rápidos cambios que se están produciendo en los ambientes operativos presentes en los dominios. Ello hace esencial comprender estos cambios, y anticipar sus efectos en las operaciones en todos ellos como un todo (Perkins, 2018). Ello necesariamente conduce a actualizar o en definitiva modificar la doctrina, lo que exige hacerlo antes de que se produzca el enfrentamiento con el o los adversarios, lo que es un ejercicio complejo, porque conlleva la observación de los nuevos escenarios de conflicto por venir, o las nuevas formas de combate que se podrían producir en dichos escenarios, ampliando la visión hacia nuevas condiciones estratégicas, operacionales y tácticas que afectarán o podrían afectar la evolución de los escenarios de guerra involucrados.

Ejemplos como el ataque de Hamas a Israel el 7 de octubre, la derrota sufrida por las columnas rusas en su ataque a Kiev al comienzo de la guerra ruso-ucraniana, y la pérdida del control del mar Negro por parte de la marina rusa, como consecuencia de las innovaciones ucranianas que a pesar de carecer capacidades navales comparables a las rusas provocaron graves pérdidas a su Armada, requieren ser analizados en profundidad y en su mérito.

El exceso de confianza en las capacidades propias, la subestimación de las capacidades del adversario y apreciaciones de inteligencia deficientes, finalmente conducen a derrotas y pérdidas dolorosas cuyas consecuencias persisten en el tiempo. Al final, todo tiene que ver con el mal manejo de la gestión de los dominios donde parece estar ausente la mirada integral que exigen las operaciones multidominio, provocando la descoordinación de sus

4 En mayo de 1948, el historiador y diplomático George F. Kennan, en ese momento Director de Planificación Política del Departamento de Estado (DoS), en su Policy Planning Staff Memorandum "The inauguration of organized political warfare.", definió la Guerra Política como la aplicación lógica del pensamiento de Clausewitz en tiempo de paz, señalando que "la guerra política es el empleo de todos los medios a disposición de una nación, excepto el empleo de la fuerza letal para lograr sus objetivos nacionales". Para Kennan las operaciones que se realizan al aplicar estrategias de Guerra Política consideran alianzas políticas, medidas económicas, propaganda, guerra sicológica, operaciones encubiertas de apoyo clandestino a elementos extranjeros amigos y, el estímulo a la resistencia clandestina en Estados hostiles.
A su vez Xi Jinping en su informe en el vigésimo Congreso Nacional del Partido Comunista Chino el 16 de octubre de 2022. Sugiere que China emplea la guerra política para preservar el gobierno del Partido Comunista Chino (PCC) y, asimismo, expandir el poder y la influencia china debilitando a sus adversarios, especialmente a los Estados Unidos. Estos tres objetivos están en línea con la estrategia nacional de China que conduce al "gran rejuvenecimiento de la nación china en todos los frentes", mediante el incremento de su poder e influencia política y sus capacidades militares, económicas, tecnológicas, comunicacionales y diplomáticas.

acciones, perdiendo la capacidad de maniobra y la superioridad en los dominios que hacen posible lograr los objetivos asignados.

Sin embargo, aún quedan interrogantes en el ambiente. A nuestro modo de ver, es trascendental preguntarse: ¿que causa el manejo inadecuado de la gestión de los dominios que limita la capacidad de derrotar al adversario? ¿Qué provoca los errores de juicio y la alteración de la voluntad, que conduce a tomar decisiones erradas a los responsables de liderar un conflicto en los distintos niveles de conducción?

La respuesta parece simple. La mente humana no sería capaz de procesar la complejidad e incertidumbre de los acontecimientos que ocurren en una guerra, generando percepciones erradas y/o alteraciones de juicio. Lo interesante radica en que dichas anomalías tienen un origen que pueden estar en las mismas personas, o podrían estar siendo provocadas por otros sujetos mediante acciones que utilizan tecnologías que aprovechan los sesgos cognitivos[5] que tienen todos los seres humanos. ¿Se puede estar hablar entonces de la mente humana como ámbito de guerra?

Guerra de la Información, Guerra Cognitiva y la mente humana como campo de batalla

La respuesta a la última pregunta realizada la entrega François du Cluzel en su texto "Guerra Cognitiva" (Cognitive Warfare). En dicho documento afirma que, ha surgido la "Guerra Cognitiva" como una nueva forma de guerra, en la cual la mente humana es un nuevo ámbito de guerra, siendo en la actualidad recurrente en la terminología militar actual (Cluzel, 2020). Robert Bebber se refiere a ella reafirmando el enfoque de Cluzel, al decir que este tipo de guerra es una amenaza única para Estados Unidos y sus aliados, porque manipula la mente de las personas para desestabilizar sus sistemas socioculturales, económicos, políticos y militares, intentando influir en cómo piensan, sienten y actúan las personas, alterando su espacio cognitivo desde el nivel individual, hasta el colectivo (Bebber, 2024).

Esto implica que, a través de la Guerra Cognitiva, a las personas se les perturba de manera progresiva y solapada su comprensión de las cosas, y la manera de reaccionar frente a los acontecimientos habituales, provocando efectos perjudiciales en el tiempo. En este contexto, está presente la Guerra de la Información que puede confundirse con la Guerra Cognitiva, por lo que es importante diferenciarlas, porque en una mirada son fácilmente asimilables. En la realidad, hay distinciones claves entre ambas, permitiendo que se puedan analizar desde sus propias particularidades.

De esta manera, el Programa de Mejora de la Educación en Defensa (Defense Education Enhancement Programme) de la OTAN (2005), señala que la Guerra de la Información no es un fenómeno nuevo, pero contiene elementos innovadores como resultado del desarrollo tecnológico, permitiendo la difusión de la información de manera más rápida y a mayor escala. En este marco, la Guerra de la

5 Un sesgo cognitivo es un error sistemático de pensamiento que se produce cuando las personas procesan e interpretan la información del mundo que les rodea y que afecta a las decisiones y juicios que emiten. El concepto de sesgo cognitivo fue introducido por los investigadores Amos Tversky y Daniel Kahneman en 1972, y desde entonces han descrito distintos tipos de sesgos que afectan a la toma de decisiones en una amplia gama de áreas, como el comportamiento social, la cognición, la economía conductual, la educación, la gestión, la sanidad, los negocios y las finanzas.

DOI: https://doi.org/10.59794/rscd.2025.v11i11.138

Información consiste en acciones que se llevan a cabo para obtener ventaja informativa sobre el oponente, controlando su propio espacio de información y protegiendo el acceso a la misma. Además, adquiriendo y utilizando la información del oponente, destruyendo a su vez sus sistemas de información logrando interrumpir el flujo de esta en su beneficio.

De acuerdo con Cluzel, en su esencia la Guerra de la Información busca controlar el flujo de información, con el fin de apoyar los objetivos definidos por la misión de las fuerzas militares, es decir, para producir efectos cinéticos letales en el campo de batalla, por lo que no está diseñada para lograr éxitos políticos duraderos (Cluzel, 2020).

Desde otra perspectiva, Delgado, Rodríguez y Solana (2024), plantean que la Guerra de la Información es un fenómeno multifacético que se ha vuelto cada vez más prominente en la era digital, caracterizándose por el uso estratégico de la información para influir en la opinión pública o en el comportamiento de un determinado grupo objetivo. Así entonces, definen a la Guerra de la Información como el uso y manejo de la información, con el objetivo de conseguir una ventaja competitiva sobre un oponente, con lo cual le otorgan un papel protagónico en el desarrollo de la guerra pudiendo incluso decidir el destino de un conflicto antes de que se inicien las actividades bélicas.

Bingle (2023), de la Henry Jackson School of International Studies define la Guerra de la Información como una lucha por controlar o negar la confidencialidad, integridad y disponibilidad de la información en todas sus formas, desde datos en bruto hasta conceptos e ideas complejas. Se trata de un enfrentamiento que puede concebirse como algo que ocurre en tres momentos, ya sea individualmente o en la combinación de ellos. Durante el flujo de la información desde su fuente hasta los tomadores de decisiones, durante el flujo de la información desde los tomadores de decisiones hasta los actores que deben ejecutarlas, y/o en el proceso de aprendizaje o interpretación de la información que ocurre dentro de cada uno de los nodos descritos anteriormente (fuente, tomador de decisiones, actor).

En las cuatro conceptualizaciones propuestas se observan como elementos claves, el control del flujo de la información propio y del o los oponentes, la decisiva presencia de la tecnología, la obtención de ventajas sobre el adversario para apoyar el cumplimiento de la misión de las fuerzas militares y, la ejecución de acciones vinculadas a la información en el nivel estratégico y táctico, que no provocan efectos duraderos en el ámbito político.

Complementado con lo anterior y, en estrecha relación con la Guerra de la Información, el ciberespacio es un ámbito relevante donde la ciberguerra se utiliza para neutralizar los sistemas de información del enemigo, y también para crear en las personas imágenes específicas del mundo donde se desenvuelven, en coherencia con los objetivos de la Guerra de la Información realizada por un país o actor determinado. En este sentido, actualmente el Portal del Programa de Mejora de la Educación en Defensa de la OTAN (Defence Education Enhancement Programme DEEP NATO 2005), señala que Internet es un espacio donde se materializan acciones de Guerra de la Información, porque permite la adquisición de datos, como también la defensa e interrupción de los flujos de información, dada la velocidad de la comunicación, y la amplia cobertura y bajo costo de las campañas de información.

DOI: https://doi.org/10.59794/rscd.2025.v11i11.138

Finalmente, la Guerra de la Información se aplica ofensivamente cuando los contendientes tratan de imponer la ventaja sobre la información de su enemigo, influyendo en cómo las personas o poblaciones objetivo interpretan o aprenden de la información que poseen o recopilan. La aplicación defensiva, se produce cuando las partes en conflicto buscan mantener la ventaja obtenida, conservando la capacidad de recopilar, interpretar y/o aprender libremente de la información disponible sin interferencia adversaria (Bingle, 2023).

Abordar la Guerra Cognitiva, es un ejercicio particularmente complejo. Esta idea la reafirma François du Cluzel (2020), al referirse a ella como la forma de utilizar el conocimiento y las ciencias cognitivas con un propósito conflictivo, que no se limita al mundo militar o institucional, y que, desde principios de la década de 1990, también se ha aplicado a los ámbitos político, económico, cultural y social. Como agrega Cluzel, esta utilización del conocimiento con propósitos conflictivos se dirige a todo el capital humano de una nación, por lo que cualquier usuario de las tecnologías de la información modernas es un objetivo potencial en la Guerra Cognitiva, donde el escenario de combate es la mente humana.

Bebber (2024) se refiere a la Guerra Cognitiva, señalando que en ella se manipula la cognición[6] para desestabilizar los sistemas socioculturales, económicos, políticos y militares de una nación, representando una amenaza para cualquier país expuesto a este tipo de guerra. Se diferencia a su vez de la Guerra de la Información, en que busca influir en cómo, y no en qué, piensan, sienten y actúan las personas, alterando el espacio cognitivo desde el individuo hasta la población total de un país o región del mundo. Agrega Bebber que, dentro de las características relevantes de la Guerra Cognitiva se incluyen su uso táctico y estratégico, la manipulación del pensamiento de las personas, la dependencia de la neurociencia y los datos y, la capacidad de emplear múltiples modos de interacción con los seres humanos.

Se hace evidente entonces, la posibilidad de que la Guerra Cognitiva esté presente en la vida diaria de las personas aún sin que estos se percaten que son parte en este conflicto. Siguiendo esta idea, la Guerra Cognitiva puede ser parte en un conflicto militar, aunque puede ejecutarse sin vinculación alguna con el empleo de las fuerzas militares, lo cual le agrega otra característica que se relaciona con la amplitud de su campo de acción. Por ello, su empleo puede ir más allá de los niveles estratégico y táctico, extendiendo su presencia al nivel político.

Esto se sustenta en el hecho de que, si es posible alterar el espacio cognitivo de las personas desde el individuo hasta la población total de un país, inevitablemente se verán afectados aquellos individuos que se desempeñan en los ámbitos de la administración estatal, particularmente aquellos que, por su ubicación en la estructura orgánica del Estado, tienen la responsabilidad de tomar las decisiones políticas.

A estas alturas, la conceptualización que plantea Bebber (2023) para la Guerra Cognitiva, señalando que en ella se emplea la ciencia y la tecnología para alterar la cognición en individuos, grupos y poblaciones, provocando cambios en la comprensión de las cosas, en las emociones y en el comportamiento humano. El objetivo que persigue es ejercer en

6 La cognición es el proceso mediante el cual se adquiere, se almacena, se recupera y se utiliza información en nuestra mente. Implica funciones mentales como la percepción, la atención, la memoria, el pensamiento y el lenguaje.

las personas una influencia disruptiva de propagación progresiva de manera directa o indirecta, alterando sus sensaciones, percepciones, creencias, patrones de pensamiento y emociones, afectando el comportamiento resultante de individuos y grupos de personas, para desestabilizar y manipular el statu quo sociocultural, económico, político y militar de una nación, permitiendo ejercer influencia y poder de manera intencionada.

Para lograr dicho objetivo, se aplican conocimientos y métodos avanzados de la neurociencia, se utilizan las ciencias vinculadas a las tecnologías de datos y computacionales, se usa el espectro electromagnético y las redes sociales impulsadas a diferentes velocidades y escalas para atacar a agentes, actores y organizaciones sociales clave que, a su vez, pueden tener comportamientos que amplifiquen los efectos disruptivos buscados en escalas y direcciones deseadas. Esto implica esfuerzos para desarrollar operaciones sin empleo de la fuerza letal dirigidas al ser humano, con efectos a todos los niveles, desde el individual hasta el sociopolítico.

Se está entonces frente a amenazas particularmente disruptivas para la seguridad global, con el surgimiento de nuevas formas de guerra que van más allá de la guerra tradicional. Esto no sería sorprendente, porque a pesar de las guerras en desarrollo, las potencias nucleares y no nucleares podrían estar buscando maneras de lograr sus objetivos políticos y estratégicos reduciendo el riesgo de un conflicto abierto y una posible escalada nuclear.

A nuestro parecer, tipos de conflicto como la Guerra Híbrida y la Guerra de Zona Gris no quedan obsoletos, sino que se podrían ver potenciados con estrategias que utilizan la Guerra Cognitiva. Esa complementariedad tiene un elemento particularmente importante. Los tipos de guerra que se han nombrado y, las estrategias que se emplean en las mismas intentan ocupar el espacio físico e influir en ámbitos de decisión política. No obstante, la Guerra Cognitiva no depende de la ocupación de espacios físicos, porque se desenvuelve en la mente de las personas en una dimensión no física.

Todo esto es posible debido al rápido avance en la comprensión del cerebro humano, y a la capacidad de operacionalizar dicha comprensión mediante la ciencia y la tecnología. El cambio más profundo entonces, tiene que ver con el nuevo campo de batalla que es el cerebro y la mente humana, que hace posible el uso de capacidades para realizar campañas de guerra no militar a través del acceso y afectación del espacio cognitivo de las personas. Esta situación genera y fundamenta la existencia del Dominio Cognitivo como un segundo dominio no físico de la guerra, además del Dominio Cibernético, con la misma importancia de los dominios físicos, donde también es posible maniobrar y conseguir objetivos estratégicos independientes tal como sucede en los dominios físicos y en el ciberespacio.

El Dominio Cognitivo en las operaciones multidominio

A riesgo de ser reiterativo, la comunidad internacional está en un momento de cambios en el carácter de la guerra, dado que las circunstancias en que esta se materializa muestran nuevas tendencias, condiciones y escenarios que obligan a replantear las estrategias que se utilizan y, la manera de conducirla. Es lo que ha estado ocurriendo con el surgimiento de las operaciones multidominio, y se reafirma con la incorporación del Dominio Cognitivo. Ello significa que se está produciendo un cambio de paradigma en el enfoque, planifi-

cación y ejecución de las operaciones militares, y desde una mirada más amplia, la necesidad de repensar como enfrentar la guerra, lo que impone la necesidad de actuar en todos los dominios de manera integrada.

Esto estaría indicando que, mantener enfoques clásicos en la conducción de la guerra es un riesgo enorme, porque siempre pueden surgir adversarios que han desarrollado aptitudes de innovación que, a no mediar una gran capacidad de adaptación, inevitablemente podrían derrotar a quienes mantienen actitudes conservadoras. El mensaje es claro, ningún país puede tener éxito en la guerra futura con enfoques del pasado, por lo que hoy debiesen concentrar sus esfuerzos en prepararse para el conflicto de mañana. Por sí mismo, esto es un desafío cognitivo enorme porque exige proyectar escenarios a futuro que no sólo se deben centrar en los dominios físicos, sino en aquellos no físicos que, a nuestro juicio, requieren mayor profundización porque todo indicaría que están menos estudiados respecto de su empleo bélico, particularmente el Dominio Cognitivo.

Rüştü (2024) en su artículo "Concepto fundamental de la guerra de la OTAN: ¿Cómo anticipar el carácter cambiante de la guerra?" (NATO's Warfighting Capstone Concept: ¿How Able to Anticipate the Changing Character of War?), propone varios aspectos relacionados con la visión futura de la guerra, a partir de supuestos que han apuntado a un entorno operativo más compacto y complejo en el tiempo, en el que los Estados rivales o casi rivales multidominio, sumado a grupos y organizaciones terroristas, seguirán planteando desafíos más amplios, al centrarse progresivamente en dimensiones de razonamiento y virtualidad. Esta propuesta pone en el centro de la atención al Dominio Cognitivo en las operaciones multidominio.

De manera complementaria, García y Calvo (2022) afirman que la redefinición de las operaciones militares bajo el prisma del Multidominio tiene su origen en una realidad que obliga a operar en todos los dominios, sin que puedan establecerse entre ellos líneas divisorias relevantes, porque los nuevos dominios, como el ciberespacio, el espacio exterior y el Dominio Cognitivo han adquirido la misma importancia que los tradicionales entornos físicos. Esto explica la necesidad de enfocar las operaciones militares con reglas nuevas y más amplias.

Enfocando la atención en el Dominio Cognitivo, parece importante recordar que, como derivación de la Guerra Cognitiva este concepto recoge ideas antiguas, que se originan en el uso de la desinformación y la propaganda pasando por las Operaciones Psicológicas como armas, que se potenciaron con los avances tecnológicos desarrollados particularmente a partir de la segunda mitad del Siglo XX. Como es posible observar, las nuevas tecnologías de la información permiten manipular la cognición de las personas a gran escala, a un costo mucho menor que cuando se creaban efectos para generar impactos a través de acciones no virtuales en el ámbito físico, sacando ventajas de los sesgos cognitivos que tienen las personas cuyos efectos se pueden extender a todos los grupos sociales de un país.

Basándonos en la propuesta de García y Calvo (2022) existen variables que son determinantes en el comportamiento del Dominio Cognitivo, las que forman parte de la conducta humana. Las percepciones, las creencias, los comportamientos y la toma de decisiones de las personas, afectadas por una incertidumbre constante, pueden ser sometidas a la influencia externa ejercida para ser modificadas. En ello, se considera a los seres huma-

nos en su doble vertiente de individuo y. a la vez, ser social integrado en una comunidad. Agregan los mencionados autores, que la actividad esencial en el Dominio Cognitivo es la influencia que los seres humanos y las sociedades reciben, la que se logra mediante la gestión de la información.

Desde lo expuesto la pregunta que surge es, en el "combate" en el Dominio Cognitivo: ¿cuál sería el objetivo fundamental por lograr? A nuestro juicio, lo esencial está en lograr la fractura de las organizaciones políticas, económicas, sociales, culturales y militares del adversario, a fin de someterlas a la propia voluntad y así crear las condiciones para lograr los objetivos políticos y estratégicos del conflicto. Para ello, se requeriría principalmente neutralizar las capacidades de tomar decisiones y aplicarlas en los diferentes estamentos de la administración del Estado, provocar la desconfianza y falta de credibilidad de la ciudadanía en los poderes político, económico, militar y social y, quebrar la moral de las fuerzas militares haciéndolas incapaces de cumplir su misión de forma efectiva. Esencialmente entonces, esta lucha se producirá en la mente humana convertida en un campo de batalla.

En una mirada más específica, para Du Cluzel (2020) es importante identificar la vulnerabilidad del adversario siendo la humana la principal. En este sentido, el primer propósito es comprender la psicología de los individuos porque ello conducirá a identificar a las personas objetivo, pudiendo anticipar sus reacciones y formas de actuar. En este aspecto, el ser humano es un blanco fácil porque proporcionan información sobre si mismos principalmente en las redes sociales, lo que contribuye a fortalecer la estrategia que se pretende aplicar, para erosionar la confianza en el contrato social que sustenta a la sociedad.

En la actualidad, el uso de la inteligencia artificial asociada a herramientas y técnicas automatizadas, contribuyen a que cualquier persona distorsione información socavando la confianza en otras, especialmente en las sociedades abiertas. Por ello, publicar noticias falsas y usar avatares digitales tienen el potencial de crear múltiples sospechas que se pueden explotar en beneficio del agresor. Es más fácil y económico para un adversario dañar la confianza del antagonista en sus propios sistemas que atacar sus redes eléctricas, fábricas o complejos militares.

Como se deduce de lo expuesto, los efectos de las acciones en el Dominio Cognitivo afectarían significativamente a los restantes cinco dominios de la guerra. Desde esta perspectiva, dicho dominio sería decisivo, justificando disponer de las capacidades para ejecutar operaciones de Guerra Cognitiva de manera independiente en etapas previas al empleo de las Fuerzas Armadas y, en estrecha relación con ellas durante el desarrollo de las operaciones militares.

Sin embargo, la relación de las operaciones multidominio con el Dominio Cognitivo no está exenta de dificultades que merecen ser analizadas. Todo estaría indicando, que en los nuevos escenarios de conflicto hay formas inéditas de enfrentamiento que exigen ampliar la visión respecto de la evolución de los escenarios de guerra. En consecuencia, frente a la línea cada vez más difuminada que separa lo militar y lo civil, se evidencia que, para ganar en un conflicto es necesario articular acciones civiles y militares en todos

DOI: https://doi.org/10.59794/rscd.2025.v11i11.138

los dominios de la guerra, asociándolos a los instrumentos de Poder Nacional.

Ello genera una primera dificultad, que radica precisamente en cómo coordinar dichas acciones, porque se requieren estructuras orgánicas militares y civiles vinculadas a dichos instrumentos. El desafío principal está en el diseño de las mencionadas estructuras, que deben ser capaces de idear, planificar y ejecutar operaciones de guerra cognitiva en los niveles de conducción político y estratégico. Lo importante para tener en cuenta, es que la concepción de una campaña de esta naturaleza se debe hacer en el nivel político, a la que las instituciones militares se subordinan manteniéndose en su área de responsabilidad.

La segunda dificultad es en nuestra opinión la más importante, se relaciona estrechamente con la anterior. Esta es no disponer de las personas idóneas y en cantidad suficiente que tripulen las estructura que deben hacer funcionar al Dominio Cognitivo. Las capacidades necesarias en este Dominio tienen que ver con la especialización, la que necesariamente exige equipos multidisciplinarios que incluyan profesionales civiles y militares[7], lo cual agrega un factor de complejidad que se requiere resolver.

Sin embargo, más allá de los inconvenientes, queda poco espacio para las dudas respecto a que los países necesitan mirar el futuro de los conflictos. Este no es un ejercicio fácil de realizar, porque exige salir de la zona de confort. Adentrarse en un ámbito tan incierto, como la Guerra Cognitiva y los retos que ocasionaría el Dominio Cognitivo en su funcionamiento, llama a superar las limitaciones que impone el pensamiento ortodoxo, abriendo la mente para comprender las posibilidades que ofrece el ámbito cognitivo usando la manipulación cognitiva como arma para explotar las fragilidades humanas contra el adversario, a la vez que se protegen las debilidades propias contra la acción enemiga.

Conclusiones

En los tiempos actuales, se ha hecho evidente que nuevas formas de guerra han tomado relevancia en el universo de los conflictos. Los avances de la tecnología informática, la inteligencia artificial, los modelos basados en algoritmos, las ciencias del cerebro, la computación cuántica y la biología sintética estarían creando nuevas posibilidades que se manifiestan en dominios no físicos como el cibernético y cognitivo. En este marco, la dinámica de la guerra está siendo transformada con la manipulación cognitiva, no solo afectando transversalmente a los dominios de la guerra sino también a las instituciones democráticas y a la soberanía de los países. Ello invita a mirar a la guerra con perspectivas más amplias, comprendiendo que la posibilidad de imponer la voluntad sobre un adversario sin usar la fuerza letal es una situación posible que se manifestara en la mente humana como campo de batalla.

Sin embargo, en este nuevo enfoque para mirar el desarrollo de los conflictos, resulta indispensable disponer de capacidades para realizar Operaciones Multidominio, articu-

7 Aquí debiesen estar presentes entre otros, sicólogos, sociólogos, historiadores, siquiatras, periodistas, informáticos, biólogos, comunicadores, analistas de inteligencia, oficiales de Estado Mayor, hackers, economistas, especialistas en guerra sicológica, etc.

lando acciones militares en todos los dominios de la guerra, sincronizándolas con actividades civiles comprometiendo a todos los instrumentos del Poder Nacional de una nación, tras el logro de los objetivos políticos y estratégicos que permitirían la prevalencia de los intereses nacionales.

Referido a la lucha en el ámbito de la cognición, la Guerra de la Información y la Guerra Cognitiva tienden a confundirse. Sin embargo, la diferenciación entre ambas es importante tenerla presente porque se manifiestan en ámbitos diferentes. La Guerra de la Información actúa esencialmente en apoyo a la misión de las fuerzas militares, sin efectos decisivos en el ámbito político y, la Guerra Cognitiva actúa a través de la manipulación de la mente de las personas para alterar su espacio cognitivo, a fin de desestabilizar los sistemas socioculturales, económicos, políticos y militares de un país, provocando efectos decisivos. Por ello entonces, quienes utilicen la Guerra Cognitiva de manera independiente o asociadas a estrategias híbridas, de zona gris o en una Guerra no Militar, se convierten en amenazas disruptivas con gran potencial de causar daños significativos a los países atacados.

Consecuencia de lo anterior, es que el nuevo escenario generado por la Guerra Cognitiva obliga a incorporar al Dominio Cognitivo como un sexto dominio de la guerra, incorporándolo en las operaciones multidominio. En esta perspectiva, la visión clásica para concebir, planificar y ejecutar las operaciones militares es superada, lo que conduce a la necesidad de repensar la forma de enfrentar un conflicto, considerando esencial la actuación en los dominios de manera integrada.

No obstante, la acción del Dominio Cognitivo en las Operaciones Multidominio enfrenta situaciones que requieren una reflexión profunda, como consecuencia de las múltiples variables en juego que necesitan ser armonizadas para provocar los efectos deseados durante el desarrollo de un conflicto. Siendo así, es importante el diseño de una estructura orgánica que permita aplicar una estrategia de Guerra Cognitiva en los niveles de conducción político y estratégico y, disponer de las personas idóneas y en cantidad suficiente que tripulen las estructuras que deben hacer funcionar al Dominio Cognitivo.

Si la esencia de la guerra es el enfrentamiento sociopolítico entre dos o más grupos humanos sean estos países, sociedades, organizaciones delictuales, insurgentes o terroristas, las estrategias, la voluntad, y la adaptación se reflejan en la evolución inevitable de sus métodos, lo que recuerda la importancia de innovar en un campo en constante transformación para responder a nuevos retos en ambientes muchas veces impredecible. El conflicto entendido de manera integral presenta oportunidades que no sólo tienen que ver con los avances tecnológicos en el campo bélico. También exige pensar en nuevas maneras de mirar la realidad de él, apuntando a las formas de lograr el sometimiento de enemigo sin usar la fuerza letal.

Acciones sutiles infiltrando la mente de las personas adversarias para romper el equilibrio social, creando realidades destructivas que socaven las bases que sustentan la moral de la sociedad, que dañen la confianza en el Gobierno, que provoque la desconfianza de este en las Fuerzas Armadas y viceversa y, la del pueblo en ambos, sería el primer paso hacia la victoria, antes de siquiera lanzar el primer disparo.

Referencias

Abogado, I. (2022). ¿Qué son los sesgos cognitivos? Aprende a identificarlos. *The Brain*. https://thebrain.blog/es/sesgos-cognitivos/

Bachs, J. (2016). Incertidumbre y neurociencias: Pilares en la adopción de decisiones. *Real Academia Europea de Doctores*. https://raed.academy/wp-content/uploads/2016/11/Incertidumbre-y-neurociencias-1.pdf

Bayorty, A. (2022). *La incertidumbre como motor de cambio y reflexión*. https://www.psicoadapta.es/blog/la-incertidumbre-como-motor-de-cambio-y-reflexion/

Beaufre, A. (1977). *Introducción a la estrategia* (2da ed.). Editorial Rioplatense.

Bebber, R. (2024). *Cognitive competition, conflict, and war: An ontological approach*. Andrew W. Marshall Scholar, Hudson Institute.

Bingle, M. (2023). What is information warfare. *The Henry Jackson School of International Studies, University of Washington*. https://jsis.washington.edu/news/what-is-information-warfare/

Cannon, S. (2024). The alliance's transition to multi-domain operations: An AIRCOM perspective. *The Journal of Joint Air Power Competence Centre*. https://www.japcc.org/articles/the-alliances-transition-to-multi-domain-operations/

Castellanos, J. J. (2022). ¿Un sistema antiacceso/denegación de área (A2/AD) español en el siglo XVI? *Global Strategy Report*, No. 19/2022.

Defense Education Enhancement Programme NATO. (2005). *DEEP NATO*. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf

Definiciones-de.com. (2024). *Significado de cognición*. https://www.definiciones-de.com/Definicion/de/cognicion.php

Du Cluzel, F. (2020). *Cognitive warfare*. Innovation Hub - Jan 2021. https://innovationhub-act.org/wp-content/uploads/2023/12/20210113_CW-Final-v2-.pdf

Fundación de Neurociencias. (2023). *¿Qué son las neurociencias?* https://fneurociencias.org/que-son-las-neurociencias/

García, R. (2022). Las nuevas operaciones multidominio de la OTAN. https://www.defensa.com/opinion/nuevas-operaciones-multidominio-otan

García, R., & Calvo, J. L. (2022). El dominio cognitivo en las operaciones multidominio: Concepto y problemática. *Academia de las Ciencias y las Artes Militares*. https://www.acami.es/publicacion/el-dominio-cognitivo-en-las-operaciones-multidominio/

Gradior. (2024). *Diferencia entre mente y cerebro: ¿Son realmente lo mismo?* https://www.gradior.es/diferencia-entre-mente-y-cerebro-son-realmente-lo-mismo/

Greene, R. (2020). *Las 33 estrategias de la guerra*. Editorial Océano.

Gniesko, C. (2019). Operaciones multidominio. *Revista de la Academia de Guerra del Ejército Ecuatoriano,* 12(1), 38-45.

Delgado, M., Rodríguez, H., & Solana, R. (2024). Information warfare and its main threats to today's society. *EasyChair Preprint*.

https://easychair.org/publications/preprint/Fk47/open

Kennan, G. (1948). The inauguration of organized political warfare. *Policy Planning Staff Memorandum.* https://archive.law.upenn.edu/live/files/9964-kennan-memo-political-warfarepdf

Martínez-Valera, G. (2022). El enfrentamiento avanzado, las operaciones multidominio. *Global Strategy Reports: Política de Defensa.* https://global-strategy.org/el-enfrentamiento-avanzado-las-operaciones-multidominio/

Morin, E. (2010). *La mente bien ordenada.* Editorial Seix Barral.

Méndez, L. A., Gaitán, S., & Fuquen, V. P. (2019). Los dominios de la guerra: Una aproximación al nuevo escenario de la COVID-19. *Estudios en Seguridad y Defensa*, 14(28), 237-257. https://doi.org/10.25062/19008325.282

NATO's Strategic Warfare Development Command. (2023). Multi-domain operations in NATO – Explained. https://www.act.nato.int/article/mdo-in-nato-explained/

Organización Internacional de Normalización (ISO). (2018). *ISO 31000: Gestión del riesgo.* Directrices. ISO.

Perkins, D. (2018). La batalla multidominio: Impulsando el cambio para ganar en el futuro. *Military Review,* primer trimestre 2018.

Pulido, G. (2018). La batalla multidominio y el campo de batalla futuro: La nueva doctrina que guía al US Army y al USMC. Ejércitos – *Revista Digital sobre Defensa, Armamento y Fuerzas Armadas.* https://www.revistaejercitos.com/articulos/batalla-multidominio/

Rüştü, S. (2024). NATO's Warfighting Capstone Concept: How able to anticipate the changing character of war? https://www.researchgate.net/publication/387209740_NATO's_Warfighting_Capstone_Concept_How_Able_to_Anticipate_the_Changing_Character_of_War

Sabater, V. (2023). *Siete diferencias entre el cerebro y la mente*. https://lamenteesmaravillosa.com/7-diferencias-entre-el-cerebro-y-la-mente/

Shah, M. (2024). The origins of victory: How disruptive military innovation determines the fates of great powers. *Journal of Aerospace & Security Studies*, 3, 162-165.

Sun Tzu. (1971). *The art of war* (p. 77). Oxford University Press. https://archive.org/details/suntzuartofwar0000samu/page/n5/mode/2up

Whiteaker, J., & Valkonen, S. (2022). Cognitive warfare: Complexity and simplicity. *NATO Collaboration Support Office*, 11, 1-5. https://hal.science/hal-03635948

Xi Jinping. (2022). Hold high the great banner of socialism with Chinese characteristics and strive in unity to build a modern socialist country in all respects. *Report to the 20th National Congress of the Communist Party of China. CGTN*. https://www.airuniversity.af.edu/CASI/Display/Article/3209912/itow-report-to-the-20th-national-congress-of-the-communist-party-of-china/

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Las tecnologías críticas y emergentes: Oportunidades y desafíos para la protección de los derechos humanos. Enfoque actual en República Dominicana

Critical and Emerging Technologies: Opportunities and Challenges for the Protection of Human Rights. Current focus on the Dominican Republic

Recibido: 29/ 05 / 2025 | Revisado: 21 / 08 / 2025 | Aprobado: 10 / 10 / 2025

DOI: https://doi.org/10.59794/rscd.2025.v11i11.152

Dra. Leany B. Araujo Rubio
Venezuela

Correo: leany.araujor@gmail.com

ORCID: https://orcid.org/0009-0005-3064-4661

Afiliación: Universidad del Zulia

La autora es abogada (1986). Doctora en Derecho (2005), egresada de la Ilustre Universidad del Zulia, especialista en Derecho Constitucional, Derechos Humanos, Derecho Internacional Humanitario. Jueza Profesional Titular en el sistema judicial venezolano (2000 – 2012) en áreas especializadas de Derecho Criminal, Penal Juvenil y Violencia de Genero. Facilitadora en DD. HH., protección de la niñez, violencia de género y Defensora de DD. HH., en alianza con las ONG's Agar Asesores, SC, Edulegal Consulting, S.C. para República Dominicana, Integras Group - USA. Integrante actualmente de proyectos de investigación de alcance nacional en Ecuador, Panamá, República Dominicana y Venezuela.

DOI: https://doi.org/10.59794/rscd.2025.v11i11.152

Resumen

El auge de las tecnologías críticas y emergentes (TCE's) transforma el mundo actual, desde la manera en cómo trabajamos hasta la forma en la que interactuamos en la Comunidad y en los núcleos familiares y sociales. Su impacto positivo en los Derechos Humanos DD. HH., incide sobre toda categoría de derechos fundamentales; su actividad genera alarmas de debilitamiento sobre principios básicos. El desarrollo de TCE's con doble uso plantea riesgos de seguridad y ética. Un desafío adicional, en países como la República Dominica requiere armonizar acciones de protección de los DD. HH. con el diseño de las nuevas tecnologías. Este estudio analiza cómo crear TCE's como herramientas de realización de los DD. HH., cómo garantizarlos en el diseño de aplicaciones y programas. Usar estrategias de protección de DD. HH., brinda la oportunidad de erradicar la pobreza, transformándola en bienestar global.

Palabras clave: Derechos Humanos DD. HH., Tecnologías críticas y emergentes (TCE's), riesgos, desafíos

Abstract

The rise of critical and emerging technologies (TCE's) is transforming today's world, from the way we work, the way we interact in the Community, family and social nuclei. Its positive impact on human rights affects all categories of fundamental rights; Their activity generates alarms of weakening of basic principles. The development of dual-use TCEs poses safety and ethical risks. An additional challenge in countries such as the Dominican Republic requires harmonizing actions to protect human rights with the design of new technologies. This study analyzes how to create TCE's as tools for the realization of human rights, and how to guarantee them in the design of applications and programs. Using human rights protection strategies provides the opportunity to eradicate poverty, transforming it into global well-being.

Keywords: Human Rights Human Rights, Critical and Emerging Technologies (TCE's), Risks, Challenges

Introducción

El presente estudio trata sobre la protección de los DD. HH. en el marco de las TCE hoy día, enfocando los desafíos que enfrenta la República Dominicana y proponiendo estrategias que preserven los principios fundamentales, cerrando las brechas existentes entre los riesgos actuales y las garantías que ameritan ser puestas en práctica para generar bienestar y prosperidad integral a los ciudadanos

Las TCE se han convertido en un factor fundamental para el desarrollo y progreso de las naciones en el siglo XXI. Ellas abarcan campos como la inteligencia artificial, la robótica, la biotecnología, la nanotecnología y la computación cuántica, tienen el potencial de transformar diversos aspectos de la sociedad, desde la forma en que trabajamos y vivimos hasta la manera como interactuamos local y globalmente. El acceso, uso, creación y publicación de contenidos digitales por parte de las personas es reconocido como derechos, cuidando que la tecnología no lesione su autoría. Los medios tecnológicos mantienen controles tales como aplicaciones especializadas, utilizadas a priori inclusive para garantizarlos.

Existe un creciente interés en el uso de las TCE para impulsar la competitividad económica, abordar problemas sociales, mejorando la calidad de vida, fortaleciendo la seguridad, defensa e inclusión social. Aumentan el crecimiento económico y la competitividad de un país, permitiendo desarrollar nuevos productos, servicios y procesos, promoviendo la innovación y la creación de nuevas formas de empleo.

En ese sentido, el Alto Comisionado de DD. HH. de la ONU ha expresado que:

> (...) Cuando la World Wide Web se puso a disposición del público en abril de 1993, su inventor, el científico británico Tim Berners-Lee, confiaba en que tendría un doble propósito: ser un instrumento con validez para siempre y que fuera accesible para todo el mundo, en todos los lugares, sin discriminación alguna. Treinta años más tarde, el mundo es testigo de una paradoja. Por un lado, las nuevas tecnologías han contribuido al progreso humano permitiendo a un número incontable de personas acceder a Internet, cerca de cinco mil millones de personas se conectaron en 2022, de acuerdo con la Unión Internacional de Telecomunicaciones (...) (a pesar de que muchos cientos de millones de estos usuarios continúan lidiando con un acceso que les es caro y a menudo de poca calidad). Las tecnologías digitales han ampliado de esta manera el modo en que las personas ejercen casi todos los derechos consagrados en la Declaración Universal de Derechos Humanos, desde la libertad de pensamiento, expresión, asociación, reunión, incluso el derecho a la vida privada, así como el derecho a una educación, atención sanitaria, a un trabajo y a protección social. (...)

Un tercio de la humanidad permanece desconectado

Por otro lado, casi 2,9 mil millones de personas, aproximadamente un tercio de la humanidad sigue sin acceso a la red y por tanto privados de las muchas ventajas que conlleva estar conectado. En cuanto al uso de las TCE's

para potenciar los DD. HH., existe creciente expectativa para que el avance de la protección de derechos fundamentales vaya a la par del adelanto tecnológico:

> (...) Podemos ver el enorme potencial que conlleva el uso de la IA y la tecnología: a la hora de mejorar los resultados de las cosechas agrícolas, a la hora de mejorar el acceso a la educación, de manera especial para las personas que viven con discapacidades, el acceso a información sobre salud o para lograr mejores resultados desde el punto de vista médico, para una mayor eficiencia en el empleo... Existe un enorme potencial a la vista. (...) Al mismo tiempo, hay mucho más que las empresas tecnológicas deben y pueden ya hacer en la actualidad aplicando los principios rectores sobre las empresas y los derechos humanos.

¿Cómo pueden los derechos humanos servir como brújula moral para las empresas tecnológicas? (...) Los Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas son principios no vinculantes, pero a pesar de esto son principios que se integran cada vez más en la legislación y normativas, y cada vez se espera con mayor ímpetu que las empresas pongan en práctica estos principios a la hora de llevar a cabo sus actividades empresariales.

En ese contexto, surge una interrogante fundamental: ¿Están preparadas las sociedades y gobiernos para respetar y proteger los DD. HH. en el creciente ámbito cibernético? Nos proponemos contrastar la situación real de los DD. HH. y las TCE, analizando los resultados de las estrategias implementadas y las iniciativas en curso.

Desarrollo

Metodología

El presente trabajo de investigación sigue la orientación metodológica documental y bibliográfica propuesto por Hernández-Sampieri, R. & Mendoza, C (2018), técnica referida a la investigación cualitativa, revisando datos de forma integral, abordando especialmente la realidad dominicana. Interpretación flexible que procura plantear un estudio cualitativo, reflexivo y propositivo con un análisis documental-digital para generar conceptos y categorías de acuerdo con elementos lógicos, históricos, sistemáticos que informan la hermenéutica jurídica como actividad para la comprensión normativa de los documentos legales y temas jurídicos a analizar.

Procedimiento de interpretación científico y privado, basado en obras de carácter dogmático, atendiendo el sentido de la norma en el ejercicio de sus respectivas funciones. Ello permitirá adentrarnos en el alcance del ordenamiento jurídico relacionado con los DD. HH. y las TCE, con carácter orientador, aportando recomendaciones con el propósito de efectivizar el respeto por los DD. HH. La combinación del método y la técnica escogidos, proporcionan un marco sólido para el estudio acerca de la importancia de preservar

a la persona humana como eje central en los avances de las TCE's en la actualidad.

Intervención del Hombre sobre bienes materiales y su transformación.

El Hombre es un ser tecnológico ya que no puede vivir en su hábitat natural sin modificarlo. Desde las primeras tecnologías creadas, como la transformación de la piedra convertida en ruedas, hachas, cabezas de martillos, o el fuego descubierto y dominado como fuente de calor, o los metales convertidos en utensilios para procesar la comida, la humanidad ha procurado mejorar las opciones de sobrevivencia.

Los objetos creados son en cierto modo una prolongación de su cuerpo. Por medio de la técnica, ha aprovechado las potencialidades del mundo, para su bienestar. Desde la intervención de la piedra o los minerales, el hombre fue cambiando el modo de vida, inclusive y a pesar de los efectos potencialmente negativos para su hábitat. El plástico, por ejemplo, tiene una enorme importancia en la expansión de todo tipo de industria; sin embargo, a pesar de su idoneidad para muchos usos, el material constituye una dificultad para mantener un medio ambiente sano por no ser un material fácilmente reciclable. Hoy son gran parte de la basura de todo el planeta, afectando la biodiversidad y el bienestar del Hombre.

En el intento de crear e innovar no todo es desfavorable. Vemos como el silicio, material natural más abundante de la corteza terrestre por detrás del oxígeno, si bien no es creado por el hombre, este tuvo el poder para transformarlo y beneficiar nuestro mundo actual. Cuando el hombre aprendió a usar las propiedades semiconductoras del silicio, halló un elemento atractivo para el mundo de la electrónica, como materia prima en la manufactura de componentes como micro o nano chips, láminas con las que operan desde teléfonos, ordenadores hasta máquinas para el hogar o la medicina.

En fin, bienes materiales de la naturaleza han sido intervenidos por el hombre para su utilidad y confort, siendo esencial como componentes físicos, tangibles y así las nuevas tecnologías críticas y emergentes, entre las que se inscriben los sistemas, programas, lenguajes diseñados por la mente humana que llegan para hacer de la vida un espacio de mayor confort, accesibilidad y bienestar.

Los bienes inmateriales y la creación del Hombre. Avances tecnológicos críticos y emergentes.

La naturaleza de las TCE como bienes inmateriales es un tema complejo. Son conocidos como activos intangibles y se caracterizan por no tener una forma física. Ejemplos de bienes inmateriales incluyen la propiedad intelectual —como los derechos de autor, las marcas comerciales y los secretos comerciales—, y el conocimiento —como la experiencia, el know-how, los datos y la información—.

Se cuentan, además, como bienes inmateriales la reputación —imagen, prestigio, reconocimiento—, las relaciones y el capital humano —clientes, proveedores, socios, habilidades, talento y creatividad—. En casi la totalidad de los casos, las TCE requieren de componentes materiales para su funcionamiento, los cuales hasta ahora se conocen como hardware, aunque el auge tecnológico cada día impulsa una mayor autonomía del software, que el autor clasifica (ver cuadro 1) en este trabajo de la siguiente manera:

DOI: https://doi.org/10.59794/rscd.2025.v11i11.152

Cuadro 1
Características y componentes materiales para el funcionamiento del software

Característica	Hardware	Software
Naturaleza	Componentes físicos, tangibles	Instrucciones intangibles, conjunto de programas
Función	Proporciona la estructura física	Proporciona funcionalidades y la interfaz de usuario
Ejemplos	CPU, memoria, monitor, teclado	Sistema operativo, navegador web, videojuego
Actualización	Se puede reemplazar o actualizar físicamente	Se puede actualizar o actualizar electrónicamente

Nota. Elaboración de la autora para este articulo (2025)

Las TCE tienen un impacto significativo en la sociedad, la economía y la seguridad nacional. Se caracterizan por ser innovadoras o en desarrollo, con un gran potencial para transformar diversos sectores. Su legado presenta beneficios, riesgos y dilemas; su evolución y futuro son inciertos.

Suponer a las TCE como bienes inmateriales infiere que están protegidas como propiedad intelectual, lo que las convierte en activos intangibles con un valor económico. En cuanto al conocimiento, su creación requiere de discernimiento especializado. Respecto a la reputación, las empresas y países que lideran el desarrollo de las TCE, pueden obtener una auge favorable y ventajas competitivas.

Es importante destacar que la clasificación de estas tecnologías como bienes inmateriales tiene implicaciones en diversos aspectos, como la gestión de activos, la valoración empresarial y la política pública. Y es allí donde puntualizaremos su valor frente a los DD. HH. como bien supremo de la Humanidad.

Naturaleza, características e importancia de los DD. HH.

Los DD. HH. son prerrogativas inherentes a todos los seres humanos, independientemente de su origen, etnia, género, religión, nacionalidad u otra condición. No poseen una forma física tangible, pero de acuerdo con su naturaleza, son inherentes a la persona humana. Describirlos como bienes inmateriales por su intangibilidad, resulta un tema complejo y con diversas perspectivas. En cuanto a los DD. HH., este trabajo clasifica sus características (ver cuadro 2), para mejor comprensión del lector, de la siguiente manera:

Cuadro 2
Clasificación y características de los principios de los DD. HH.

Características	Descripción - Ejemplo
Universalidad: Todos los derechos y libertades establecidos en la Declaración Universal de DD. HH. para todas las personas, sin rangos ni distinciones.	Las personas tienen derecho a la igualdad de oportunidades y a participar plenamente en la sociedad sin distinción de sus capacidades.
Indivisibilidad: Todos los DD. HH. son indivisibles, interdependientes e interrelacionados. Esto significa que no se pueden disfrutar de forma aislada, sino que están interconectados y se refuerzan mutuamente.	El derecho a la libertad de expresión está estrechamente vinculado al derecho a la educación, ya que ambos son esenciales para el desarrollo de una sociedad libre y democrática.
Inalienabilidad: Los DD. HH. son inalienables, lo que significa que no se pueden vender, transferir ni renunciar a ellos. Los Estados tienen la obligación de proteger y promover los DD. HH. de todas las personas dentro de su jurisdicción.	La prohibición de la tortura es absoluta y no admite excepciones, incluso en situaciones de emergencia o conflicto armado.
Progresividad: Los Estados tienen la obligación de adoptar medidas progresivas para la plena realización de los DD. HH.. Esto significa que deben tomar medidas concretas para mejorar el disfrute de los DD. HH. por parte de todas las personas, incluso si no pueden lograrlo de forma inmediata.	La adopción de leyes y políticas que protejan los derechos de las mujeres y las niñas es un ejemplo de medida progresiva para la plena realización del derecho a la igualdad.
Irreversibilidad: Los avances logrados en la realización de los DD. HH. son irreversibles. Los Estados no pueden retroceder en la protección y promoción de los DD. HH. que ya han sido reconocidos.	La abolición de la pena de muerte es un ejemplo de un avance irreversible en la realización del derecho a la vida.

Nota. Elaboración de la autora para este articulo (2025).

Conforme a esas características podemos establecer que los DD. HH. no se pueden tocar, ver ni sentir de manera física; pero su valor reside en su carácter universal, inherente, propio y perenne y en su papel fundamental para el respeto y bienestar humano. Los DD. HH. poseen una dimensión trascendental que se manifiesta en la capacidad de las personas para vivir con dignidad y libertad.

Los niveles de satisfacción se sublimizan cuando el status quo del ser humano preserva los valores de respeto y bienestar. Esas dimensiones refieren un estado de completo goce, tanto físico como mental, espiritual y social, que permite a los individuos vivir una vida plena y significativa.

La importancia de los DD. HH. como principios y libertades es que a partir de ellos se establecen reglas básicas de convivencia, pro-

mueven la dignidad humana, creando un marco para su respeto y protección, tutelan la propia vida, como el bien más preciado, junto con la libertad, la justicia y la igualdad y promueven la paz social como norte y el bienestar social, individual y colectivo.

Principios y libertades básicas vs. tecnologías emergentes

Los DD. HH. son valores fundamentales, esenciales para la dignidad humana y el desarrollo individual y social. Son la base de una sociedad justa y equitativa, donde todas las personas puedan vivir con respeto, libertad y seguridad. Es importante conocerlos, defenderlos y exigir su respeto para construir un mundo donde todas las personas puedan vivir con dignidad y plenitud. La rápida evolución de las tecnologías emergentes plantea desafíos inéditos a los principios y libertades básicas que han cimentado las sociedades democráticas. Conceptos como la privacidad, la libertad de expresión, la no discriminación y la autonomía individual se ven constantemente reexaminados ante el auge de la inteligencia artificial, el reconocimiento facial, la vigilancia masiva o la edición genética.

Es imperativo reconocer que, si bien estas innovaciones prometen eficiencia y progreso, su implementación sin un marco ético robusto que salvaguarde los derechos humanos puede erosionar progresivamente las libertades fundamentales, transformando herramientas de progreso en instrumentos de control o exclusión. En este escenario, los derechos humanos no son meras restricciones al avance tecnológico, sino que deben ser la brújula que oriente su desarrollo y aplicación. Priorizar el diseño de sistemas que incorporen desde su concepción principios como la transparencia, la explicabilidad, la equidad y la privacidad por defecto es crucial.

Las Tecnologías Críticas Emergentes (TCE) son innovaciones en desarrollo con potencial transformador en la sociedad y la economía. Son "críticas" por su capacidad de cambiar paradigmas y generar disrupciones a gran escala, presentando oportunidades y riesgos duales. Su desarrollo acelerado y naturaleza interconectada exigen una gobernanza ética que priorice los derechos humanos. Ejemplos incluyen IA y biotecnología. Su utilidad real se mide en cómo sirven al bienestar y los derechos fundamentales.

Las TCE son programas, soluciones funcionales, metodologías nuevas o en desarrollo que tienen el potencial de transformar significativamente la sociedad en un corto tiempo. Se caracterizan por su novedad, descubrimiento y potencial transformador de las formas cómo acceder a soluciones, bienes, servicios. La Inteligencia artificial (IA) que simula inteligencia humana, los hogares, cosas, ciudades inteligentes (IoT) que interconecta una red de objetos a través de Internet para reunir, procesar y compartir datos, la Big Data que procesa gran cantidad de datos de forma fácil, el Blockchain que crea registros contables inmutables y transparentes. Estas y otras TCE tienen como finalidad facilitar la vida en distintas áreas.

Sus beneficios incluyen el aprendizaje, automatización de áreas comerciales, industrias o comunidades, el diseño inteligente de servicios en áreas de salud, transporte, el razonamiento y la resolución de problemas, revelar patrones o tendencias, y un enorme potencial para crear aplicaciones en áreas como la cadena de suministro, la gestión de identidad y la votación. El entretenimiento, la educación y la formación también son áreas en las que las TCE como la inteligencia artificial (IA), la realidad virtual (VR) y la realidad aumentada (AR) pueden impactar positivamente para

generar bienestar. A diferencia de las tecnologías emergentes, que son nuevas y en constante evolución, los DD. HH. tienen una larga historia. (2024a).

Ello no significa que los DD. HH. sean estáticos, al contrario, así como el Hombre transforma su realidad, esa realidad debe ir interpretando los atributos de los DD. HH. de manera que las innovaciones respondan a su esencia. Solo si la tecnología se construye y se utiliza con una conciencia profunda de sus implicaciones para la dignidad humana y las libertades básicas, podrá cumplir su promesa de mejorar la vida sin comprometer los valores esenciales que nos definen como sociedad. La tecnología debe servir a la humanidad, no dominarla.

Realidades, desafíos y oportunidades que emergen de las TCE frente a los DD. HH.. Antecedentes en la República Dominicana

Las TCE pueden presentar tanto oportunidades como desafíos para la protección y realización de los DD. HH.. Por ejemplo, la inteligencia artificial puede utilizarse para mejorar el acceso a la justicia o para desarrollar nuevas formas de vigilancia. Sin embargo, pueden causar discriminación a las personas o invadir su privacidad. La relación entre las TCE y los DD. HH. es compleja y multifacética, pueden tener un impacto positivo como negativo en la realización de los principios básicos. Para conseguir ciertos beneficios, las TCE pueden afectar la privacidad de las personas.

La automatización impulsada por las TCE podría generar disminución de ocupaciones laborales en algunos sectores y con ello el desempleo y la pobreza. Las TCE son herramientas poderosas que pueden tener un impacto significativo en la vida de las personas. Las tecnologías de vigilancia, como el reconocimiento facial pueden plantear riesgos para la privacidad individual. Por ello es importante establecer salvaguardas para proteger la privacidad de las personas y garantizar el uso responsable de estas tecnologías.

En cuanto a la libertad de expresión, las plataformas de redes sociales pueden utilizarse para difundir información y opiniones, pero también pueden propagar discursos de odio o desinformación. Es primordial proteger la libertad de expresión y combatir el abuso de las plataformas en línea o que se usen para delinquir. Los algoritmos utilizados en las TCE pueden ser sesgados y discriminar a ciertos grupos de personas. Es elemental desarrollar algoritmos justos y transparentes que no permitan o acentúen la discriminación. Las TCE pueden desarrollar nuevos tratamientos médicos, mejorar la atención médica y promover estilos de vida saludables.

Desarrollar soluciones sostenibles para el cambio climático y la degradación ambiental, mejorando el planeta, haciéndolo más habitable para las generaciones futuras como parte de los beneficios de la protección al "medio ambiente limpio, saludable y sostenible" como derecho humano universal, de acuerdo al Programa de las Naciones Unidas para el medioambiente (PNUMA). La brecha entre el desarrollo de las tecnologías críticas emergentes y la realidad socioeconómica global, se ve exacerbada por factores de riesgo como la desigualdad y la pobreza extrema, amenazando gravemente el equilibrio con los derechos humanos. Si una porción significativa de la población carece de acceso básico a infraestructura digital, educación o incluso necesidades fundamentales, el avance de tecnologías sofisticadas en ese país, puede profundizar las disparidades existentes.

Esto crea un riesgo palpable de que las herramientas diseñadas para el progreso beneficien exclusivamente a una élite tecnológica y económica, mientras las poblaciones vulnerables son excluidas de sus beneficios, marginadas por sus requisitos o, peor aún, sujetas a nuevas formas de control o explotación digital, agudizando la ya precaria situación de sus derechos. Tomemos el caso de República Dominicana, que en 2021 registraba un Índice de Gini de 45.6, una cifra que subraya la persistente desigualdad económica en el país. En contextos así, la implementación irreflexiva de tecnologías críticas emergentes podría amplificar la exclusión.

Por ejemplo, el acceso limitado a Internet o a dispositivos inteligentes para amplios segmentos de la población pobre, podría impedirles beneficiarse de servicios esenciales digitalizados o de oportunidades laborales emergentes. Al mismo tiempo, la falta de marcos regulatorios sólidos y una gobernanza inclusiva podría exponer a estas poblaciones a riesgos desproporcionados, como la vigilancia sin control o la discriminación algorítmica.

Para salvaguardar los derechos humanos, es crucial que la adopción de estas tecnologías se haga con una visión de equidad, invirtiendo en infraestructura, alfabetización digital y políticas que garanticen que los beneficios del progreso tecnológico sean universales y no acentúen la exclusión social. Respecto al fortalecimiento de la democracia y la gobernanza, las TCE pueden utilizarse para aumentar la transparencia y la rendición de cuentas en los gobiernos, promover la participación ciudadana y defender el estado de derecho. El uso no reglado de las TCE puede resultar desigual, aumentando las brechas sociales y económicas existentes:

> La aplicación de las tecnologías de vanguardia puede acelerar considerablemente los esfuerzos por alcanzar los Objetivos de Desarrollo Sostenible y hacer frente al cambio climático; pero, por otro lado, también pueden incrementar las tensiones sociales y generar una dinámica de ganadores y perdedores, según advierte el nuevo Estudio Económico y Social Mundial 2018. (...)
>
> El secretario general de las Naciones Unidas, António Guterres, manifestó que aprovechar todo el potencial de estas innovaciones puede generar beneficios a la salud, al medioambiente y traer prosperidad para todo el mundo. Pero destacó que, para que funcionen, "necesitamos políticas que garanticen que las tecnologías de vanguardia -que trascienden cada vez más las fronteras sectoriales, geográficas y generacionales- no sólo sean viables desde el punto de vista comercial, sino también equitativas y éticas. Esto requerirá una evaluación rigurosa, objetiva y transparente, en la que participen todas las partes interesadas", dijo.

Durante el Examen Periódico Universal (EPU) del Consejo de DD. HH. de las Naciones Unidas en mayo de 2024, la situación de los DD. HH. en la República Dominicana ha sido objeto de revisión. Otras revisiones tuvieron lugar en mayo de 2009, enero de 2014 y enero de 2019. El EPU es un examen entre pares del historial de DD. HH. de los 193 Estados miembros de la ONU.

Los documentos en los que se basan los exámenes del país son: 1) los informes del Alto Comisionado en DD. HH., expertos y grupos independientes de DD. HH., órganos de tratados de DD. HH. y otras entidades de la

ONU; 2) la información proporcionada por otros interesados, incluidas las instituciones nacionales de DD. HH., organizaciones regionales y la sociedad civil y 3) el Informe del gobierno dominicano.

Al momento de acabar este estudio, los resultados finales del examen no habían sido publicados; sin embargo, los documentos en los que se basa la revisión contienen más de 90 recomendaciones a la República Dominicana, divididas en dos categorías: A. - Cumplimiento de las obligaciones internacionales en materia de DD. HH.; y, B. - Derechos de personas o grupos específicos.

A. – En cuanto al alcance de las obligaciones internacionales, cooperación con los mecanismos de DD. HH., el Informe del Alto Comisionado de DD. HH. ONU precisa:

> 2. El Comité para la Eliminación de la Discriminación contra la Mujer y el Comité de los Derechos del Niño recomendaron a la República Dominicana ratificar la Convención Internacional sobre la Protección de los Derechos de todos los Trabajadores Migratorios y de sus Familiares y la Convención Internacional para la Protección de todas las Personas contra las Desapariciones Forzadas.
> 3. El Comité de los Derechos del Niño recomendó a la República Dominicana que considerara ratificar la Convención sobre el Estatuto de los Apátridas y la Convención para Reducir los Casos de Apatridia. El equipo de las Naciones Unidas en el país recomendó a la República Dominicana adherirse a la Convención sobre el Estatuto de los Apátridas y a la Convención para Reducir los Casos de Apatridia, y ratificara el Convenio sobre la Violencia y el Acoso, 2019 (núm. 190) de la Organización Internacional del Trabajo (OIT).
> 4. La Experta Independiente sobre el disfrute de todos los DD. HH. por las personas de edad, recomendó que se ratificara la Convención Interamericana sobre la Protección de DD. HH. de las Personas Mayores.
> 5. Varios titulares de mandatos de los procedimientos especiales pidieron que se ratificara el Acuerdo Regional sobre el Acceso a la Información, la Participación Pública y el Acceso a la Justicia en Asuntos Ambientales en América Latina y el Caribe (Acuerdo de Escazú).
> 6. El equipo ONU en el país señaló que el Estado parte aún no había cursado invitación permanente a los procedimientos especiales. (ONU, 2024b).

B. - El Grupo de Trabajo ONU en su Informe recomendó proveer recursos suficientes para poner en funcionamiento el Plan Nacional de DD. HH. (periodo 2023-2024). El informe revela estos datos:

- En cuanto al derecho a la vida, la libertad y seguridad personales: El Comité contra la Tortura observó las alegaciones de tortura y malos tratos por parte de la policía con el fin de obtener confesiones. El Comité pidió información sobre las investigaciones relativas a la muerte de personas recluidas, el número de muertes atribuidas a agresiones cometidas o consentidas por agentes del Estado en las que se hizo un uso excesivo de la fuerza, así como sobre las medidas adoptadas para combatir la brutalidad policial y el uso excesivo de la fuerza por parte

de los agentes del orden, incluidas las ejecuciones extrajudiciales y las alegaciones de connivencia de agentes estatales en casos de violencia vinculada al sicariato y el narcotráfico. (ONU, 2024b).

- El mismo Comité recalcó la sentencia núm. 555/17 del Tribunal Supremo, en la que el Alto Juzgado calificó las condiciones de detención en las cárceles como una violación grosera y flagrante del orden constitucional. El equipo ONU en el país recomendó mejorar las condiciones de detención, especialmente en las provincias fronterizas. El Comité de los Derechos del Niño recomendó que las condiciones de internamiento se ajusten a las normas internacionales.
- Respecto al derecho a la salud: El acceso al agua potable salubre y al saneamiento de las personas y los grupos vulnerables debería ser una prioridad; aumentar la asignación presupuestaria al sector de la salud para garantizar el acceso a la atención sanitaria y su cobertura universal; y, establecer servicios de salud mental en el sistema público de salud.
- *El Comité para la Eliminación de la Discriminación contra la Mujer* expresó su preocupación por el acceso limitado a los servicios de aborto seguro y los cuidados posteriores, señalando que los abortos en condiciones de riesgo eran una de las principales causas de mortalidad y morbilidad materna en la República Dominicana.
- *El Comité de los Derechos del Niño expresó su honda preocupación por la persistencia de las altas tasas de embarazo de niñas y adolescentes.*

Otras notas agregadas para la revisión, de manera resumida se añaden las siguientes exhortaciones:

- Promoción y protección de los DD. HH., reforzando los mecanismos de lucha contra la corrupción, promoviendo la investigación y la rendición de cuentas de los funcionarios de la Dirección General de Migración u otros empleados públicos que hubieran sido hallados responsables de la comisión de delitos y violaciones de DD. HH. de los migrantes.
- Broken Chalk hizo un llamamiento a las autoridades de la República Dominicana para reforzar el acceso a una educación de calidad.
- El déficit de vivienda se veía agravado por el aumento de los desalojos forzosos masivos en comunidades empobrecidas, al tiempo que unas 2.000 familias permanecían en refugios tras el paso de tormentas y huracanes, sin una política o solución habitacional alternativa.
- La CCIA recomendó permitir a los dominicanos de ascendencia haitiana el acceso no discriminatorio a los programas públicos destinados a reducir la pobreza y la hambruna.

Por su parte, la República Dominicana en febrero 2024 informó los logros en la protección de los DDHH, en la implementación de las recomendaciones del examen o revisión de 2019: el gobierno dominicano reconoce el uso de la tecnología en casos de prohibición de la esclavitud y tráfico humano, en apego al

Plan Nacional de Acción Contra la Trata de Personas y Tráfico Ilícito de Migrantes 2022-2024.

Ello ha significado la implementación de agentes encubiertos y alta tecnología para el incremento de las interceptaciones y extracciones de datos10. Entre las acciones específicas respecto al derecho a la salud, refiriéndose a las personas con discapacidad, el gobierno dominicano destacó el desarrollo de mecanismos y servicios integrales para facilitar la inserción educativa y social de las personas con discapacidad, promoviendo el desarrollo de sus potencialidades humanas, incluyendo el uso de la tecnología y de la información y las nuevas comunicaciones dentro de un marco de equidad y justicia social.

Informó otros avances, respecto al derecho a la educación, como la entrega de equipos tecnológicos a docentes y estudiantes en colegios públicos, kits y laboratorios de robótica a estudiantes y centros educativos. *En cuanto a la buena gobernanza, la República Dominicana anuncia como novedoso en el Informe in comento, la aprobación de la Ley núm. 339-22, que habilita y regula el uso de medios digitales en los procesos judiciales y administrativos. Respecto a los derechos económicos, sociales y culturales y el derecho a un nivel de vida adecuado, señaló también la entrega de un bono navideño digital.*

Entre las acciones específicas respecto al derecho a la salud, refiriéndose a las personas con discapacidad, el gobierno dominicano destacó el desarrollo de mecanismos y servicios integrales para facilitar la inserción educativa y social de las personas con discapacidad, promoviendo el desarrollo de sus potencialidades humanas, incluyendo el uso de la tecnología y de la información y las nuevas comunicaciones dentro de un marco de equidad y justicia social. (ONU, 2024c).

Consideramos importantes los logros en materia de ratificación de tratados internacionales y el fortalecimiento del marco legal; sin embargo, el compromiso de la República Dominicana para la protección de los DD. HH. a nivel nacional e internacional no solo debe estar referido a la materia legislativa. Se requiere tomar acción ejecutiva para erradicar la pobreza y rescatar la calidad de vida.

Si bien los informes citados son muestra de los esfuerzos que realiza el gobierno dominicano para la protección de los DD. HH., también evidencian la grave situación de los derechos fundamentales que afectan a la Nación dominicana, ya que de acuerdo con las preliminares de esa revisión ONU, se registran condiciones de vida infrahumanas en el país. Además, según datos de la Oficina Nacional de Estadística (ONE) organismo gubernamental de la República Dominicana, en 2023 la tasa de pobreza extrema se ubicó en el 3.2%, lo que representa una leve disminución en comparación con el 3.8% del año 2022. Esta cifra significa que, alrededor de 360,000 personas en el país viven en condiciones de pobreza extrema, definidos como aquellos hogares con un ingreso *per cápita* mensual inferior a US$1.90.

En ese mismo orden, el Banco Mundial revela cifras alarmantes (2023) al considerar que:

> ...más del 40 por ciento de los dominicanos viven en condiciones vulnerables y están en riesgo de caer en la pobreza debido a los impactos relacionados con el clima y las crisis económicas. Asimismo, las brechas de género en los empleos y salarios, vidas laborales más cortas y mayor desempleo y roles no remunerados contribu-

> yen a una mayor incidencia de pobreza entre las mujeres.
>
> (...) según la reciente evaluación sobre pobreza del Banco Mundial, el crecimiento económico en la República Dominicana entre 2004 y 2019 fue casi tres veces superior al promedio de América Latina y el Caribe, pero la pobreza no disminuyó al mismo ritmo. Son las mujeres las más afectadas por la falta de oportunidades e ingresos estancados, los principales factores detrás de esta paradoja. En República Dominicana, la pobreza es cada vez más joven y más mujer."

En República Dominicana, como en el resto del mundo, el auge de las TCE presenta oportunidades sin precedentes para el desarrollo económico, social y cultural. Maximizar la protección de los DD. HH. frente a las TCE es una tarea fundamental. En Reunión del Grupo de Expertos, la Comisión de Ciencia y Tecnología para el Desarrollo (ONU) en su periodo de sesiones 2023 - 2024 ha publicado como prioridades el logro de objetivos con especial atención áreas de salud, bienestar, industria, innovación e infraestructura, paz, justicia e instituciones sólidas.

Las oportunidades y los desafíos de las TCE, para el desarrollo sostenible, han fijado como prioridades para 2024 redoblar los esfuerzos para construir una agenda mundial de TCE inclusiva, identificando y evaluando riesgos y beneficios potenciales; creando entornos digitales y de capacitación propicios y el acceso universal a Internet y las tecnologías digitales, entre otras. Sin duda, frente a las constantes transformaciones de las TCE, es necesario seguir interpretando y aplicando los DD. HH. de manera que las nuevas tecnologías respondan a la eficacia y eficiencia de estos, a su respeto y bienestar.

Armonización legal y tecnológica para la protección de los DD. HH. frente a las TCE's en República Dominicana.

La República Dominicana, al igual que otros países, enfrenta desafíos para proteger los DD. HH. en la era digital. Las TCE, como la inteligencia artificial, la biotecnología y la nanotecnología, tienen un enorme potencial para el desarrollo, pero también presentan riesgos para los DD. HH. si no se gestionan de manera responsable. El país ha implementado pasos importantes en los últimos años:

- Aprobación de leyes específicas, como la Ley 54-17 sobre Violencia Intrafamiliar, que incluye el uso de tecnologías digitales para acosar o controlar a las víctimas. La Ley 113-20 sobre Movilidad Humana y Comercio Ilícito de Personas, que busca proteger a las personas migrantes y combatir el tráfico de personas, incluyendo el uso de tecnologías digitales para reclutar, explotar y controlar a las víctimas.
- Creación de instituciones como la Unidad de Delitos Cibernéticos de la Policía Nacional, que se encarga de investigar y perseguir delitos cometidos en el entorno digital, como el fraude electrónico, el robo de identidad y el acoso cibernético.
- La Comisión Nacional para la Sociedad de la Información y el Conocimiento (CONASIC), creada con el objetivo de promover el desarrollo de la sociedad de la información en la República Dominicana, incluyendo el uso responsable de las tecnologías digitales.

- Desarrollo de estrategias y planes de acción, entre las que se cuentan la Estrategia Nacional de Ciberseguridad que tiene como objetivo proteger la infraestructura crítica del país y garantizar la seguridad de las comunicaciones digitales. El Plan Nacional de Protección de Datos Personales busca establecer un marco legal y regulatorio para la protección de datos personales en el entorno digital.

- La Estrategia Nacional de Inteligencia Artificial (ENIA) y el Memorando de Entendimiento (MOU), que busca como objetivos la automatización de los servicios estatales, predecir la corrupción y que el país se convierta en referencia regional en la innovación, lo cual impulsará el desarrollo de soluciones endógenas en áreas cruciales como seguridad, movilidad, salud, agricultura y medio ambiente.

El Memorando de Entendimiento, firmado con el Banco de Desarrollo de América Latina (CAF) sienta las bases para el proyecto "Computación de Alto Desempeño para la Inteligencia Artificial en América Latina y el Caribe" aborda necesidades apremiantes en el campo de la Inteligencia Artificial, tales como, la infraestructura de computación de alto rendimiento:

- Capacitación y sensibilización como objetivos de los programas de capacitación para funcionarios gubernamentales, jueces, abogados y otros profesionales y las campañas de educación pública sobre los riesgos y beneficios de las tecnologías emergentes y la importancia de proteger los DD. HH. en el entorno digital.

República Dominicana debe continuar trabajando para fortalecer su marco legal y regulatorio, las instituciones responsables de la protección de los DD. HH. en el entorno digital, aumentar la inversión en capacitación de sus funcionarios y profesionales, sensibilizar a la población y formar alianzas con otros países y organizaciones internacionales para abordar este desafío de manera efectiva. La protección de los DD. HH. en la era digital es un desafío complejo que requiere un enfoque multidisciplinario. La participación ciudadana es clave para efectivizar la protección de los DD. HH. frente al avance de las TCE.

Proteger los DD. HH. en la era digital es un desafío y una oportunidad. El rápido avance de las TCE presenta enormes oportunidades para el progreso humano. Sin embargo, también plantea nuevos desafíos para la protección de los DD. HH.. "En una sociedad cada vez más conectada, es de vital importancia entender qué son los derechos humanos y el impacto que tiene la tecnología en ellos".

Conclusiones

Navegando la Convergencia entre Tecnologías Críticas Emergentes y Derechos Humanos en la República Dominicana

El presente estudio ha discurrido a lo largo de la compleja intersección entre las Tecnologías Críticas Emergentes (TCE) y la salvaguarda de los Derechos Humanos (DD. HH.), aterrizando esta interacción en la realidad de la República Dominicana. La investigación subraya que las TCE no son meros avances tecnológicos, sino catalizadores de transformación social, económica y geopolítica que, a pesar de su innegable potencial para el progreso y el bienestar, conllevan desafíos sustanciales que exigen una gobernanza ética y una perspectiva anclada en los Derechos Humanos.

Desafíos y Estrategias para la Convergencia en la República Dominicana

La realidad de la República Dominicana ilustra de manera acuciante los factores de riesgo que amenazan el delicado equilibrio entre las TCE y los DD. HH.. La persistencia de la desigualdad, la pobreza extrema y la exclusión social son flagelos que, según se ha destacado, podrían ser exacerbados por una adopción irreflexiva de las tecnologías avanzadas.

El Índice de Gini de 43.1 en 202110 (aunque algunas fuentes sugieren 38.5, la conclusión de una desigualdad significativa se mantiene), subraya una distribución inequitativa de los beneficios del crecimiento económico, lo que genera una vulnerabilidad palpable a shocks externos y puede revertir los avances logrados en la reducción de la pobreza.

En este contexto, la falta de acceso a recursos básicos como educación e infraestructura, la marginación digital por escasez económica, y la prevalencia de incertidumbre y riesgo en la vida diaria de las poblaciones vulnerables, limitan su capacidad para innovar y participar plenamente de los beneficios de las TCE.

La Dualidad de las Tecnologías Críticas Emergentes: Promesa y Riesgo

Las TCE, concebidas como bienes inmateriales que operan con componentes materiales, encarnan la vanguardia de la innovación, prometiendo un confort y una eficiencia sin precedentes en diversos ámbitos de la vida. Desde la inteligencia artificial (IA) que simula el intelecto humano, hasta el Internet de las Cosas (IoT) que interconecta nuestro entorno, pasando por el Big Data y el Blockchain, estas tecnologías están redefiniendo las formas de interacción, trabajo y acceso a servicios.

Su naturaleza "crítica" radica en su capacidad para generar disrupciones a gran escala y reconfigurar paradigmas fundamentales, afectando la economía, la sociedad y el equilibrio de poder. Sin embargo, esta capacidad transformadora inherente a las TCE les confiere una naturaleza de doble uso.

Los Derechos Humanos como Brújula Moral Ineludible

En la vertiginosa era digital, los Derechos Humanos emergen no como un contrapeso, sino como la brújula moral indispensable que debe orientar el desarrollo y la aplicación de las TCE. Principios inherentes como la universalidad, indivisibilidad, inalienabilidad, progresividad e irreversibilidad, que definen la dignidad humana, se ven constantemente interpelados por las capacidades de las nuevas tecnologías.

La privacidad, la libertad de expresión, la no discriminación y la autonomía individual son pilares democráticos que deben ser salvaguardados activamente ante fenómenos como el reconocimiento facial o la edición genética. El estudio enfatiza que una implementación desprovista de un sólido marco ético puede no solo erosionar estas libertades, sino también transformar el progreso tecnológico en un instrumento de control o exclusión.

Un Futuro Digital Inclusivo y Digno

Las TCE ofrecen un potencial transformador para superar la escasez de agua potable en las poblaciones remotas de la República Dominicana, mediante la implementación de soluciones de desalinización portátiles y ener-

géticamente eficientes alimentadas por energías renovables emergentes (como pequeños sistemas solares o eólicos de bajo costo). Así se podría convertir el agua salobre o de mar en potable directamente en el punto de necesidad, sin depender de infraestructuras centralizadas.

El uso de sensores IoT y análisis de Big Data permitiría monitorear en tiempo real la calidad y cantidad del agua en fuentes subterráneas o superficiales, optimizando su extracción y distribución, y alertando sobre contaminación o escasez inminente. Complementariamente, el desarrollo de nuevas membranas de filtración basadas en nanotecnología podría purificar el agua de manera más efectiva y económica, incluso de contaminantes complejos, proveyendo así soluciones descentralizadas y sostenibles que empoderen a las comunidades más apartadas con acceso a un recurso vital, mejorando significativamente su salud y calidad de vida.

Combatir la trata de personas, el narcotráfico, el tráfico de personas, la República Dominicana puede apalancarse en Tecnologías Críticas y Emergentes (TCE). La Inteligencia Artificial y el Big Data son clave para analizar patrones y detectar redes de traficantes, complementado por ciberseguridad y análisis forense digital para rastrear operaciones en línea. Tecnologías móviles y el IoT pueden empoderar a víctimas con información y canales de denuncia seguros, incluso en áreas remotas.

Consideraciones finales

Es crucial la capacitación constante de las autoridades en el uso de estas herramientas para la investigación y el enjuiciamiento. La colaboración regional e internacional a través de plataformas tecnológicas seguras es indispensable para desarticular redes transnacionales, protegiendo así a las poblaciones vulnerables.

Para combatir el lavado de dinero en la República Dominicana, las TCE son clave. Las plataformas Blockchain pueden asegurar la transparencia y trazabilidad de transacciones. La IA y el Machine Learning son esenciales para analizar grandes volúmenes de datos financieros, detectando patrones atípicos y redes de blanqueo en tiempo real.

Las Tecnologías Críticas Emergentes son instrumentos poderosos que, cuando se alían con una visión de equidad y Derechos Humanos, pueden transformar realidades, generar soluciones de confort y bienestar simplificadas. La construcción de un entorno digital que respete los derechos fundamentales de cada individuo en la Nación Dominicana requiere un esfuerzo concertado y pluridisciplinario.

Las imágenes satelitales, análisis geoespacial servirían para monitorear deportaciones a gran escala, actividades fronterizas o las condiciones de los centros de detención en áreas remotas, proporcionando evidencia independiente de posibles violaciones.

La implementación de equipos y cámaras corporales que permitan el monitoreo con IA para las Fuerzas del Orden, son herramientas para dotar a los oficiales de inmigración y policía con dispositivos para el uso de IA y para analizar las grabaciones, lo que podría aumentar la transparencia y la rendición de cuentas durante redadas y detenciones, disuadiendo el uso excesivo de la fuerza, el robo y otros abusos. activando alertas ante comportamientos sospechosos o uso de la fuerza.

El gobierno debe asumir un papel protagónico en la formulación de políticas inclusivas, las empresas tecnológicas deben diseñar productos y servicios con una base ética inque-

brantable, la sociedad civil y las ONG's deben mantener su rol de vigilancia y defensa, y los ciudadanos deben participar activamente en la configuración de este futuro digital. Solo a través de una colaboración robusta y priorizando de forma genuina la dignidad humana sobre la mera eficiencia tecnológica, la República Dominicana podrá cerrar la brecha entre el progreso técnico y la plena realización de los Derechos Humanos, asegurando que las innovaciones generen un futuro justo, equitativo y próspero para todos.

Las TCE no son una panacea, pero en manos de una sociedad comprometida con sus principios más básicos, son herramientas para facilitar las transformaciones en la búsqueda del bien común, por lo que poseen el potencial para ser un aliado formidable en la necesidad urgente de vencer la pobreza extrema y construir una sociedad más justa.

Referencias

Álvarez, M. (1995). *Introducción al derecho.* McGraw-Hill.

Álvarez, G. (2002). *Metodología de la investigación jurídica: Hacia una nueva perspectiva*. Universidad Central de Chile, Facultad de Ciencias Jurídicas y Sociales.

Banco Mundial. (1986–2022). *Datos – Indicadores.* https://datos.bancomundial.org/indicator/SI.POV.GINI?locations=DO

Conferencia Mundial contra el Racismo, la Discriminación Racial, la Xenofobia y la Intolerancia. (2001, 31 de agosto–8 de septiembre). *Declaración y Programa de Acción 2001.* https://www.un.org/es/events/pastevents/cmcr/durban_sp.pdf

Hernández, R., & Mendoza, C. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta.* McGraw-Hill Education.

Ley núm. 137-03. (2003). Sobre Tráfico Ilícito de Migrantes y Trata de Personas. *Gaceta Oficial.* Santo Domingo, República Dominicana. 8 de octubre de 2003. Núm. 10.233,

Ley núm. 24-97. (1997). Sobre Violencia Intrafamiliar. (1997). *Gaceta Oficial.* Santo Domingo, República Dominicana. 31 de enero de 1997. Núm. 9.946.

Oficina Nacional de Estadística (ONE). (2023). *Boletín de estadísticas oficiales de pobreza monetaria en República Dominicana 2023.* https://www.one.gob.do/media/tm5paqul/pobreza-monetaria-en-la-república-dominicana-2023elfinal.pdf

Organización de las Naciones Unidas (ONU). (2023, mayo). Alto Comisionado de las Naciones Unidas para los Derechos Humanos. *Configurando tecnologías digitales que den capacidad a las personas para poder construir sus vidas.* https://www.ohchr.org/es/stories/2023/05/shaping-digital-technologies-empower-people-build-their-lives

Organización de las Naciones Unidas [ONU]. (2024a, febrero). Alto Comisionado de DD. HH.. *¿Es la IA un arma positiva?* https://www.ohchr.org/es/stories/2024/02/ai-force-good

Organización de las Naciones Unidas [ONU]. (2024b, 29 de abril a 10 de mayo). *Examen Periódico Universal 46° período de sesio-*

nes. Informe del Alto Comisionado de DD. HH. y del Grupo de Trabajo de las Naciones Unidas para los DD. HH. acreditado en el país del Consejo de DD. HH.. https://documents.un.org/doc/undoc/gen/g24/028/21/ pdf/g2402821.pdf?token=lX7mM0p1V1qu5tx-8qM&fe=true

Organización de las Naciones Unidas [ONU]. (2024c, 29 de abril a 10 de mayo). *Examen Periódico Universal 46° período de sesiones 29 de abril a 10 de mayo de 2024. Informe nacional presentado en virtud de las resoluciones 5/1 y 16/21 del Consejo de DD. HH.. Resumen del Informe Nacional presentado por la República Dominicana*. https://documents.un.org/doc/undoc/gen/g24/027/06/pdf/g2402706.pdf?token=0NAwhrsV8MDaJ6071a&fe=true y/o https://www.ohchr.org/es/hr-bodies/upr/do-index

Organización de las Naciones Unidas [ONU]. (2024d, 15 - 19 de abril). Consejo Económico y Social. Comisión de Ciencia y Tecnología para el Desarrollo 270 período de sesiones. Ginebra. Resumen p. 1. https://unctad.org/system/files/official-document/ecn162024d3_es.pdf

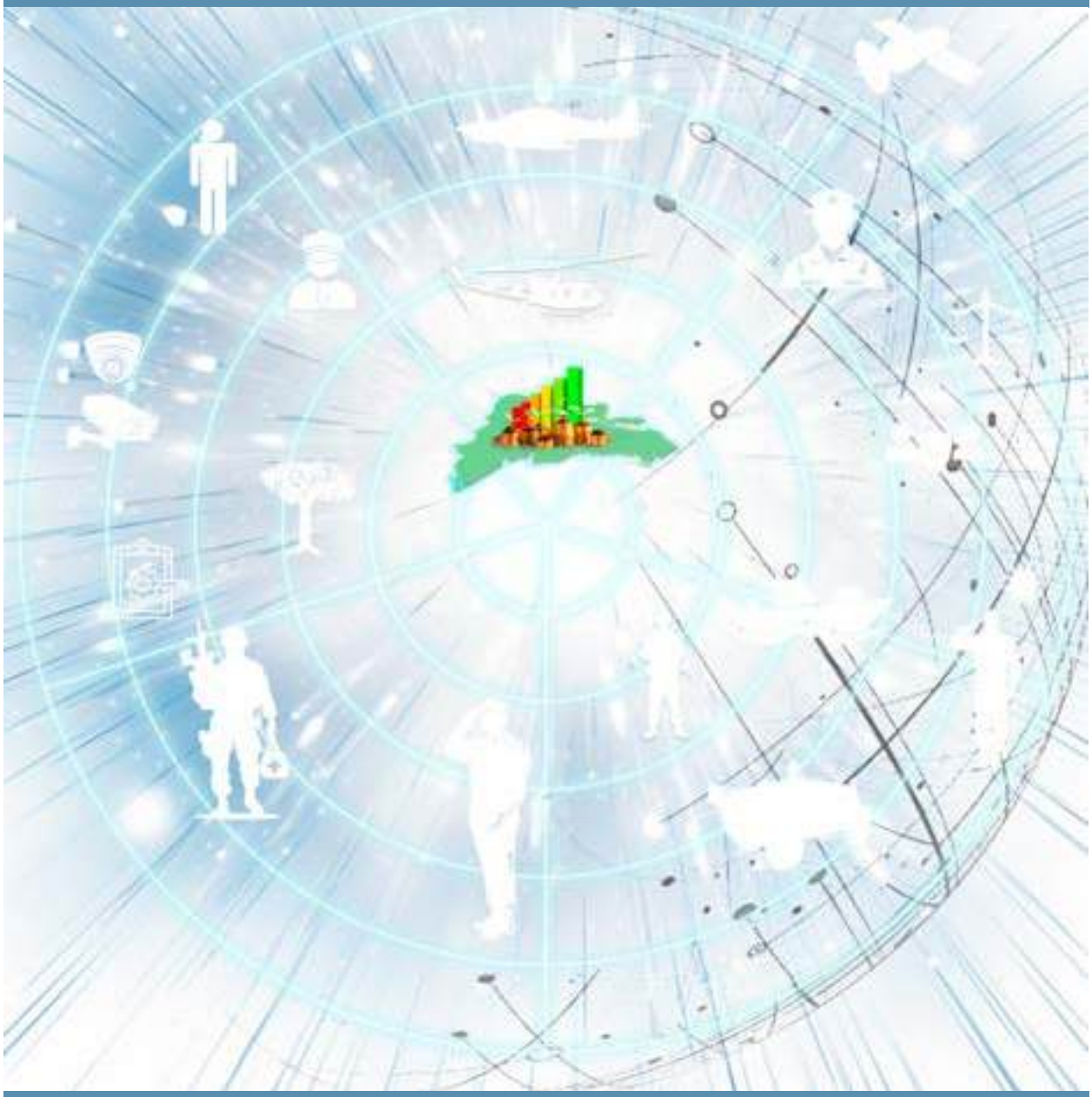
Organización de las Naciones Unidas (ONU), Departamento de Asuntos Económicos y Sociales. (s. f.). *World Economic Situation and Prospects (WESP) 2018*. https://www.un.org/es/desa/wess2018

Organización de las Naciones Unidas (ONU), Programa de las Naciones Unidas para el Medio Ambiente (PNUMA). (s. f.). *Decisión histórica: la ONU declara que el medio ambiente saludable es un derecho humano*. https://www.unep.org/es/noticias-y-reportajes/reportajes/decision-historica-la-onu-declara-que-el-medio-ambiente-saludable

Universidad Autónoma de Occidente. (s. f.). *Derechos humanos y tecnología: Desafíos en la era digital*. https://virtual.uao.edu.co/blog/derechos-humanos-y-tecnologia-desafios-en-la-era-digital

Valerio, A. (2024, marzo). *La importancia de invertir en mujeres dominicanas*. Banco Mundial. https://blogs.worldbank.org/es/latinamerica/importancia-invertir-en-mujeres-dominicanas

SECCIÓN NACIONAL



RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Seguridad y desarrollo en acción: Análisis de las capacidades híbridas en operaciones cívico-militares desarrolladas por la Comisión Militar y Policial (COMIPOL)

Security and development in action: analysis of hybrid capabilities in civil-military operations developed by the Military and Police Commission (COMIPOL)

Recibido: 01/ 05 / 2025 | Revisado: 26 / 06 / 2025 | Aprobado: 10 / 09 / 2025

DOI: https://doi.org/10.59794/rscd.2025.v11i11.144

Coronel Alfredo Rafael de la Cruz Concepción, ERD
República Dominicana

Correo:alfredo3015@gmail.com

ORCID: https://orcid.org/0009-0003-7179-440X

Afiliación: Universidad Nacional para la Defensa

El autor es coronel del Ejército de República Dominicana; Posee una Maestría en Estrategia y Relaciones Internacionales en la Universidad Nacional para la Defensa de la República de China; Licenciado en Ciencias Militares en la Academia Militar Batalla de las Carreras; Licenciado en Contaduría Pública Universidad Tecnológica de Santiago; Diplomando en Comando y Estado Mayor en la Escuela de Graduados en Comando y Estado Mayor Conjunto (EGCEM); Curso Avanzado de Armas Combinadas en la Dirección General de Entrenamiento Militar; Curso de Desarrollo de Políticas para la Defensa en el Centro de Estudios Hemisféricos de Defensa William J. Perry, entre otras capacitaciones militares. Diplomado en la Gestión de Calidad bajo la Norma ISO 9001:2015 en el INFOTEP. Ha ocupado numerosas funciones de gran relevancia tales como: Comandante del Batallón de Comandos; Comandante del Cuerpo de Cadetes; Subdirector Académico y de Investigaciones de la Academia Militar Batalla de la Carreras; Supervisor General del Programa de Protección y Asistencia Vial de la COMIPOL, Inspector General de la COMIPOL, Oficial de Planes y Operaciones de la COMIPOL, Encargado del Módulo de Estrategia y Oficial; Docente en la Escuela de Graduados de Estudios Militares del Ejército de República Dominica. Ha sido comandante de la 5ª y 6ª Compañía del ERD; ha prestado servicio en el Cuerpo Especializado para la Seguridad del Metro; se ha desempeñado como instructor del Bloque de Maniobra en el Curso Avanzado de Infantería de la Dirección General de Educación, Capacitación y Entrenamiento Militar del ERD; y actualmente ocupa el cargo de subdirector de Técnico Superior y Grado de la Universidad Nacional para la Defensa (UNADE).

Resumen

Este artículo analiza las capacidades híbridas de la Comisión Militar y Policial (COMIPOL) en el contexto de sus operaciones cívico-militares, enfocándose en su estructura organizacional, programas principales, eficiencia operativa y comparación con unidades similares en la región. El estudio se basó en un análisis cualitativo no experimental, realizado mediante revisión documental de leyes, manuales operativos, informes institucionales y literatura académica. Los resultados muestran que la doble adscripción ministerial de COMIPOL (MIDE-MOPC) potencia sinergias únicas que amplían su capacidad de respuesta multidisciplinaria. Sus logros incluyen más de 3 millones de asistencias viales, certificación bajo la norma ISO 9001:2015 y contribuciones significativas al desarrollo nacional y seguridad ciudadana. Este trabajo concluye que COMIPOL representa un modelo institucional único en América Latina, donde la interagencialidad y la integración de capacidades militares y civiles permiten abordar retos complejos con alta eficacia operativa.

Palabras clave: Operaciones cívico-militares, capacidades híbridas, seguridad-desarrollo, interagencialidad, comisión militar y policial (COMIPOL)

Abstract

This article analyzes the hybrid capabilities of the Military and Police Commission (COMIPOL) in the context of its civil-military operations, focusing on its organizational structure, main programs, operational efficiency and comparison with similar units in the region. The study was based on a non-experimental qualitative analysis, conducted through a documentary review of laws, operational manuals, institutional reports and academic literature. The results show that COMIPOL's dual ministerial affiliation (MIDE-MOPC) enhances unique synergies that broaden its multidisciplinary response capacity. Its achievements include more than 3 million road assistances, certification under ISO 9001:2015, and significant contributions to national development and citizen security. This paper concludes that COMIPOL represents a unique institutional model in Latin America, where interagencyism and the integration of military and civilian capabilities allow addressing complex challenges with high operational efficiency.

Keywords: Civil-military operations, hybrid capabilities, security-development, interagency, military and police commission (COMIPOL)

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Introducción

Las operaciones cívico-militares han ganado relevancia en América Latina como estrategias integradas para abordar desafíos complejos que combinan seguridad ciudadana, desarrollo local y gestión pública. En este contexto, la Comisión Militar y Policial (COMIPOL), adscrita al Ministerio de Obras Públicas y Comunicaciones (MOPC) y dependiente, a su vez, del Ministerio de Defensa (MIDE), emerge como una unidad con capacidades híbridas que integra funciones militares, policiales y civiles con el objetivo de fortalecer su contribución al desarrollo nacional.

Este artículo se basa en un análisis cualitativo no experimental, realizado mediante revisión documental de leyes, manuales operativos, informes institucionales y literatura académica, con el fin de examinar cómo COMIPOL articula capacidades de seguridad y desarrollo en sus operaciones, contrastándolas con modelos similares en la región.

El marco conceptual se sustenta en el Plan Estratégico Institucional 2021-2024 del Ministerio de Defensa (MIDE, 2021), particularmente en su Eje Estratégico N° 4: "Apoyo al Desarrollo Social y Económico del País a través de las Capacidades de las Fuerzas Armadas", así como en el Libro Blanco de la Defensa de República Dominicana (MIDE, 2022). Estos documentos refieren a las tareas misionales establecidas en el Artículo 252 de la Constitución Dominicana (2024), entre las cuales se incluyen el apoyo a la autoridad civil, la protección vial, la gestión de desastres y la contribución al desarrollo socioeconómico.

La doble adscripción ministerial de COMIPOL (MIDE-MOPC) permite una sinergia operativa poco común en otras unidades análogas, lo cual amplía su capacidad de respuesta multidisciplinaria. Este estudio analiza específicamente las operaciones desarrolladas a través del Programa de Protección y Asistencia Vial, el Programa de Asuntos Sociales y la Unidad en Control del Derecho Vial, con el propósito de identificar cómo su naturaleza interagencial e híbrida influye en la eficacia de sus intervenciones.

Los datos cuantitativos utilizados han sido validados mediante fuentes oficiales de los ministerios involucrados (Ministerio de Defensa (MIDE, Ministerio de Obras Públicas y Comunicaciones (MOPC), Instituto Nacional de Tránsito y Transporte Terrestre (INTRANT)), mientras que las conclusiones integran evidencia empírica y marco teórico. A partir de este análisis, se espera contribuir al entendimiento de las capacidades operativas de las unidades cívico-militares en contextos de desarrollo y seguridad.

Desarrollo

Marco teórico

Las operaciones cívico-militares han surgido como una estrategia clave a nivel internacional, integrando recursos militares con objetivos civiles para abordar necesidades sociales, de seguridad o desarrollo. En América Latina, este modelo se ha consolidado como un mecanismo eficaz ante desafíos complejos (González-Cuenca et al., 2019). En República Dominicana, la Comisión Militar y Policial (COMIPOL) ejemplifica este enfoque, com-

binando funciones de seguridad, asistencia ciudadana y apoyo al desarrollo nacional.

El concepto de "capacidad híbrida" (Del Vado, 2019) explica la articulación entre instituciones y roles tradicionalmente diferenciados, como militares y civiles, permitiendo respuestas ágiles y versátiles. Similar a la Guardia Nacional de México, COMIPOL opera con una doble adscripción ministerial (MIDE-MOPC), ampliando su alcance estratégico. Además, su interagencialidad —cooperación con entidades como el INTRANT, el Ministerio de Agricultura y otras— facilita abordar problemas multidimensionales, como seguridad vial o brotes zoonóticos (De la Cruz, 2024).

El Artículo 252 de la Constitución dominicana (2024) y el Libro Blanco para la Defensa (2022) sustentan jurídicamente a COMIPOL, al enmarcar las Fuerzas Armadas en roles no bélicos, como gestión de desastres y desarrollo socioeconómico. Este marco se complementa con el Plan Estratégico Institucional 2021-2024 del MIDE, que prioriza el apoyo al desarrollo social. Asimismo, COMIPOL ha innovado con herramientas como la app MOPC y su certificación ISO 9001:2015, reflejando adaptación a amenazas modernas mediante tecnología y calidad institucional (Muñoz Meoño, 2024; El Día, 2023).

COMIPOL fortalece la seguridad ciudadana mediante presencia visible en vías troncales, disuadiendo delitos y brindando tranquilidad a usuarios. (Dirección General de Planificación y Desarrollo, 2024), donde se destacan indicadores superiores al 95% en accesibilidad, fiabilidad y amabilidad, consolidando su imagen como institución cercana y eficiente. Esta percepción positiva refuerza su rol como modelo de operaciones cívico-militares centradas en el servicio público.

Metodología

Este estudio adoptó un enfoque cualitativo no experimental para analizar las capacidades híbridas de COMIPOL en operaciones cívico-militares, basándose en una revisión documental exhaustiva y la experiencia profesional del investigador durante seis años. La metodología incluyó el análisis crítico de documentos oficiales —manuales operativos, informes técnicos (COMIPOL, 2021;2024), planes estratégicos (MIDE, 2021; Ministerio de Defensa, 2022), y marcos legales como el Artículo 252 de la Constitución (2024) y la Ley 147-02 (2002)—, lo que permitió contextualizar histórica y jurídicamente a la institución.

Para enriquecer el análisis, se realizó una comparación regional con unidades análogas, como la Guardia Nacional de México (2019) y la Unidad Militar de Emergencias de España (2006), identificando buenas prácticas y diferencias estructurales. Además, se incorporaron datos cuantitativos de fuentes oficiales (Ministerio de Defensa (MIDE), Ministerio de Obras Públicas y Comunicaciones (MOPC), Instituto Nacional de Tránsito y Transporte Terrestre (INTRANT), Dirección General de Impuestos Internos (DGII) con indicadores clave: 3,376,254 asistencias viales, tiempos de respuesta (<20 minutos), operatividad vehicular (>90%) y satisfacción ciudadana (>95%), los cuales respaldaron la evaluación de eficiencia y cobertura territorial.

El estudio integró también percepciones públicas mediante testimonios en redes sociales, comunicados institucionales y cobertura mediática (El Día, 2023; COMIPOL, 2022), analizando el impacto subjetivo de la institución en la seguridad ciudadana. La triangulación metodológica combinó tres fuentes: 1) documentación institucional para procesos internos, 2) datos estadísticos para medición objetiva, y 3) experiencia directa del investi-

gador, contrastada con registros y testimonios externos para minimizar sesgos.

Si bien la experiencia en COMIPOL aportó profundidad al análisis, se mitigaron posibles sesgos mediante la priorización de documentos públicos y datos verificables. Este equilibrio aseguró una interpretación objetiva, manteniendo la rigurosidad académica sin perder la riqueza contextual que ofrece la participación directa en la unidad estudiada.

El servicio de asistencia vial tiene sus orígenes entre agosto de 2012 y febrero del año 2013. De forma más especifica el 13 de febrero de ese año, el Estado Mayor General de las Fuerzas Armadas aprobó el proyecto de ingreso de personal egresado del Servicio Militar Voluntario, también se aprobó el uso de uniformes y distintivos para la Comisión Militar y Policial del Ministerio de Obras Públicas. (Ministerio de Obras Públicas y Comunicaciones [MOPC] y Ministerio de Defensa [MIDE], 2021)

A partir de su implementación, este servicio fue ganando valoración entre los usuarios que transitan por las vías troncales, donde están desplegadas las unidades destinadas a ayudar a las personas cuando sus vehículos presentan un fallo que les impida continuar el viaje por sus propios medios.

Este tipo de unidad puede ser encontrada en diferentes países, desempeñando funciones parecidas en ciertos aspectos y muy diferencias en cuanto a las normativas legales y al contexto situacional de cada país. A continuación, se presenta una tabla con información de varias unidades militares y policiales que en sus operaciones contemplan la prestación de algún tipo de asistencia en las carreteras, en adición a otras operaciones propias de su naturaleza (Ver tabla 1).

Tabla 1
Información sobre unidades militares y policiales que contemplan en sus operaciones la prestación de asistencia en las carreteras
Comparación entre países con unidades militares o policiales que ejecutan misiones de apoyo a la población civil con asistencia en las carreteras

País	Unidad	Ejes de operaciones	Sustento legal	Observación
Brasil	Policía Rodoviaria Federal	Hacer cumplir las leyes federales en las carreteras, brindar apoyo en caso de accidentes.	Constitución de la República Federativa de Brasil, Ley 9.503/97 (Ley No. 9.503, 1997), Ley 9.654/98 (Ley No. 9.654, 1998), Decreto 1.655/95 y Decreto 9.662/2019.	Esta unidad tiene autonomía propia, no depende de ministerios civiles.
Colombia	Batallón de Apoyo de Acción Integral	Combina labores de asistencia vial con desarrollo social en zonas rurales.	Constitución Colombiana, leyes como la Ley 1861 de 2017 entre otras.	Opera en un contexto posconflicto

País	Unidad	Ejes de operaciones	Sustento legal	Observación
España	Unidad Militar de Emergencias (UME)	Interviene en desastres viales (ej.: accidentes masivos). Actúa solo en emergencias declaradas	Real Decreto 416 del 11 de abril de 2006. (Ministerio de Defensa, 2006)	• Actúa ante situaciones que desborden las capacidades de las autoridades locales.
México	Guardia Nacional (División Vial)	Integra personal militar y policial para seguridad vial en carreteras federales. Su enfoque se centre en la seguridad pública, no ofrece asistencia mecánica.	Ley de la Guardia Nacional de 27/5/2029 (Congreso General de los Estados Unidos Mexicanos, 2019).	• Está integrada por militares y policías. La seguridad pública es su prioridad.
República Dominicana	Comisión Militar y Policial (COMIPOL)	Asistencia vial, Seguridad ciudadana, Asuntos sociales, Seguridad patrimonial del MOPC	Constitución Dominicana (2024), Ley 163-13 orgánica de las FF.AA. (Ministerio de Defensa, 2013), Ley 1474 del 1938, entre otras.	• Está integrada por militares, policía y profesionales de la clase civil. • Opera de forma continua y atiende a múltiples situaciones. • Es dependiente de dos ministerios. • Opera bajo un amplio marco legal, pero carece de una legislación específica para esta unidad.

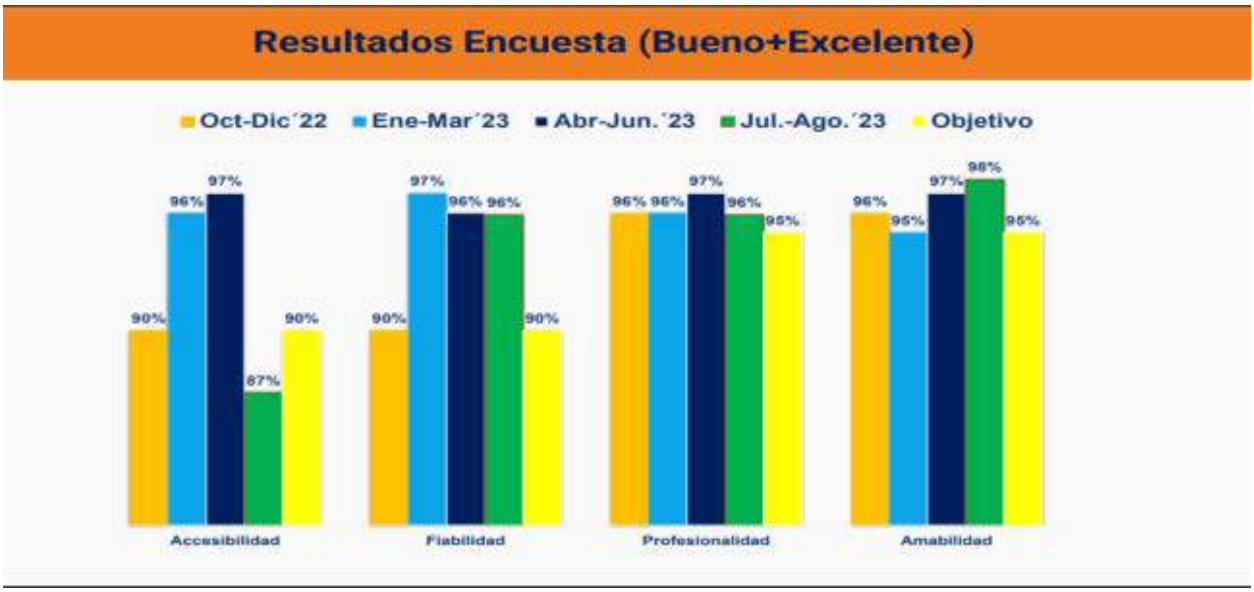
Nota: Tabla elaborada por el autor partiendo de las informaciones publicadas en sus respectivos sitios web oficiales donde presentan los documentos legales que dan origen a estas unidades.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Los datos institucionales revelan la experiencia acumulada, por el personal militar y civil, apoyados por una amplia flotilla vehicular equipada con herramientas especializadas para labores que van desde la prestación de asistencia vial hasta el rescate de personas atrapadas en vehículos accidentados.

La Dirección General de Planificación y Desarrollo, (2023) en la encuesta que muestra los niveles de satisfacción de las personas con los servicios que ofrece el MOPC expone que los logros alcanzados han consolidado a la COMIPOL como una de las instituciones mejor valoradas del Estado dominicano, por su capacidad de respuesta y la prestación de un servicio de calidad. Como se puede observar en la gráfica que muestra los resultados de la encuesta de satisfacción octubre 2022-agosto 2023 (Ver gráfico 1).

Gráfico 1
Resultados de la encuesta de satisfacción octubre 2022-agosto 2023



Nota: Encuesta de resultados de satisfacción elaborada por el autor, como Tiempo de Respuesta, Quejas/Sugerencias Servicios Comprometidos Carta Compromiso al Ciudadano octubre 2022-septiembre 2023 Dirección General de Planificación y Desarrollo (2023).

Esta unidad tiene presencia en un 90% de las provincias del país. Sus procedimientos establecen que el servicio de asistencia vial se ofrezca en las vías troncales, salvo excepciones como los tramos de Jamao en la provincia Espaillat, el corredor Jarabacoa en el municipio del mismo nombre de la provincia La Vega.

Esta capacidad territorial se potencia mediante su integración con el Sistema Nacional de Atención a Emergencia y Seguridad (Sistema 9-1-1, 2023). Siendo una de sus fortalezas la respuesta rápida y oportuna, menos a 20 minutos, en las carreteras antes las diferentes solicitudes que realizan las personas a través de ese sistema (Ver gráfico 2).

Gráfico 2
Resultados de la encuesta de satisfacción

Nota: Encuesta de resultados de satisfacción elaborada por el autor.

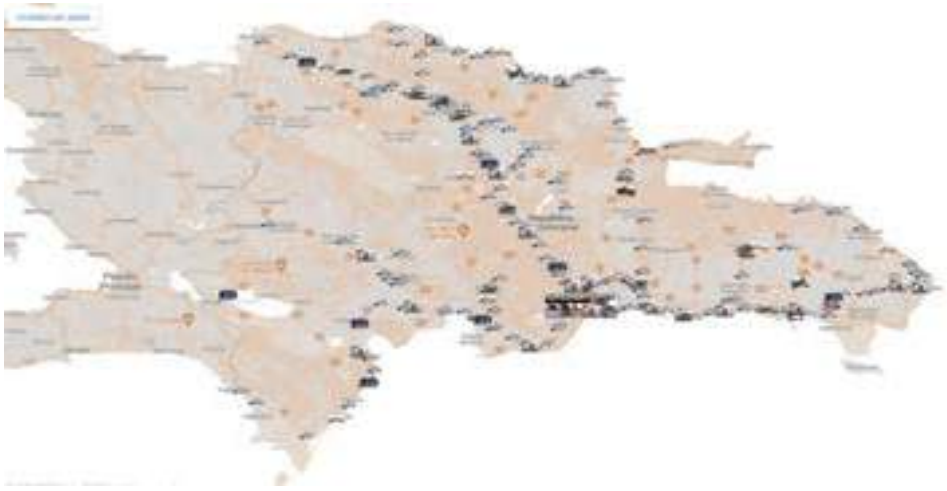
Los resultados presentados en los gráficos 1 y 2 evidencian la calidad del servicio brindado, manteniendo promedios por encima del 95% en los criterios de accesibilidad, fiabilidad, profesionalismo y amabilidad, establecido en la Carta Compromiso al Ciudadano (Dirección General de Planificación y Desarrollo, 2024). Obtener estos resultados implica mantener un nivel de operatividad superior al 90% del parque vehicular, disponer del 100% de los insumos necesarios para atender las situaciones que se les presenten a las personas y dar respuesta al 100% de las solicitudes recibidas.

Lo anterior se ha logrado gracias a la distribución estratégica de recursos en las diferentes vías troncales del país. Convirtiendo la COMIPOL en una unidad de repuesta tanto táctica como estratégica, bajo la óptica dual de los ministerios que rigen sus operaciones.

De un lado el Ministerio de Defensa quien aporta las capacidades militares (personal y armamento). La disciplina y el entrenamiento militar contribuyen de forma significativa a que cada tarea que se le asigne sea cumplida con un alto grado de profesionalismo con resultados muy positivos y con apego a los procedimientos establecidos.

Del otro lado el Ministerio de Obras Públicas y Comunicaciones, ministerio que aporta personal de la clase civil (profesionales y técnicos de diferentes áreas), equipos entre ellos el parque vehicular y la gestión administrativa. Elementos esénciales al momento de responder antes situaciones de emergencia (Ver figura 1).

Figura 1
Distribución estratégica de recursos en las diferentes vías troncales del país



Nota: Distribución de los recursos de la COMIPOL en vías troncales de RD.

Además de sus recursos esta unidad cuenta con una fortaleza institucional, representada en la documentación con que cuenta, desde manuales de organización y funciones, de procedimientos, manuales para la capacitación de su personal, plan de defensa, plan de emergencia, con los cuales se reducen la posibilidad de improvisación de sus integrantes en el desempeño de su misión.

Estos documentos fueron redactados y puesto a disposición de los ministros de Defensa y de Obras Públicas en su primera versión en la gestión del Mayor General Rafael Vásquez Espínola – ERD, (PhD) en el año 2021. El manual de Organización y Funciones de la Comisión Militar y Policial (Comisión Militar y Policial [COMIPOL], 2021), la define como una institución de servicios cuya misión principal es vigilar, proteger y brindar asistencia vial en las carreteras, autopistas y autovías del territorio dominicano. También es responsable de la seguridad patrimonial del Ministerio de Obras Públicas y Comunicaciones (MOPC) en instalaciones, peajes, vías de comunicación y campamentos de obras realizadas por éste, así como de fortalecer el Plan de Seguridad Ciudadana en su área de responsabilidad.

Esta documentación institucional se complementa con un programa de capacitación continua, diseñado para estandarizar protocolos y optimizar la ejecución operativa del personal. De forma programada el personal recibe nuevos conocimientos técnicos sobre sus áreas de competencia, que puede incluir desde la evaluación de casos atípicos hasta la especialización del personal mediante capacitaciones especiales.

Esta unidad tiene una naturaleza híbrida, donde coexiste personal militar con profesionales de diferentes áreas de la vida civil, quienes logran una sinergia operativa que benefician de forma directa a las personas. Además de contribuir con el desarrollo de la nación a través de su desempeño en materia de seguridad ciudadana, combate contra plagas tropicales, apoyo a comunidades vulnerables mediante la realización de operativos médicos y odontológicos, reparto de agua potable, preservación del derecho vial, apoyo al plan general de seguridad ciudadana y las acciones ejecutadas mediante el programa de protección y asistencia vial, cuyos resultados se presentan en la imagen siguiente (Ver imagen 1).

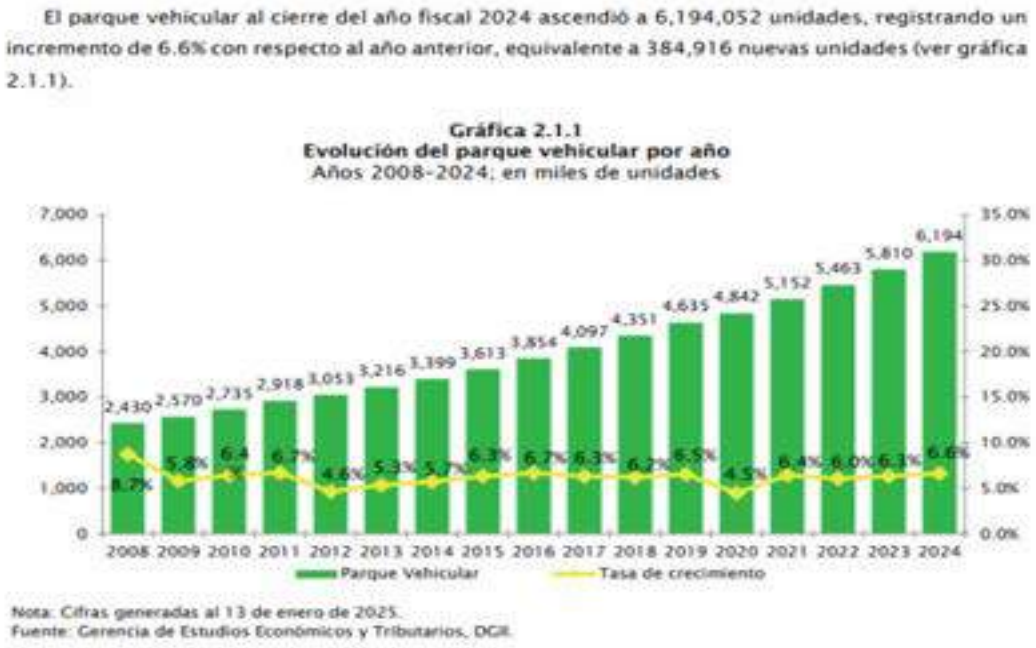
Imagen 1
Estadísticas de asistencias brindadas por la COMIPOL

TIPO DE ASISTENCIAS	CANTIDAD	%
ACCIDENTES	66,839	1.98%
SEGURIDAD	311,219	9.22%
NEUMÁTICO	1,026,860	30.41%
COMBUSTIBLE	399,931	11.84%
ELÉCTRICO	11,199	0.33%
CALENTAMIENTO	15,705	0.47%
MECÁNICA	1,405,636	41.62%
GRÚAS	32,409	0.96%
AMBULANCIA	27,797	0.82%
TALLERES MÓVILES	79,375	2.35%
CAMIÓN DE RESCATE	284	0.01%
CANTIDAD TOTAL	3,377,254	100%

Nota: Cuadro estadístico de las asistencias viales brindadas por la COMIPOL. Extraídas de las memorias correspondiente al primer semestre del año 2024.

Para contextualizar los datos del cuadro anterior es fundamental analizar la realidad del parque vehicular que circula en las vías troncales de República Dominicana. La Dirección General de Impuestos Internos [DGII] (2024, pp. 2-3), en su reporte sobre el parque vehicular plantea que, al 31 de diciembre de 2024, el stock de vehículos registrados ascendió a 6,194,052 unidades, registrándose un total de 384,916 vehículos de nuevo ingreso. Es decir que aproximadamente 5,809,136 vehículos circulan con en las carreteras con años que rondan entre el 2023 a años anteriores. (Ver gráfico 2).

Gráfico 2
Evolución del parque vehicular por año entre el 2008 al 2024



Nota: Evolución del parque vehicular por año entre el 2008 al 2024, elaborado por la DGII (2024).

De estos datos se infiere que circula una gran cantidad de vehículo con muchos años en servicio y por ende con un alto kilometraje. A esto se puede añadir que no todas las personas llevan sus vehículos a talleres mecánicos autorizados por los fabricantes de vehículos, dado que la mano de obra especializada y los repuestos originales aumentan los costos de reparación o de mantenimiento preventivo.

Un patrón similar se observa con la compra de neumáticos usados. Algunas personas prefieren adquirir neumáticos de segunda mano por que son menos costosos que los nuevos. Esta acción representa un riesgo para esos conductores, dado que desconocen el uso que recibió el neumático que compra, solo porque ven que las bandas de rodamiento lucen en buenas condiciones.

De acuerdo con los reportes oficiales de COMIPOL, durante el período evaluado se registraron un total de 3,376,254 asistencias viales, destacando que las atenciones por fallos mecánicos representaron la principal causa con 1,405,636 casos (41.6% del total), seguidas por las intervenciones relacionadas con neumáticos que alcanzaron 1,026,860 atenciones (30.4%), mientras que el 28% restante (943,758 casos) correspondió a otras tipologías de incidentes.

Las asistencias brindadas por las ambulancias y camiones de rescate (27,797 y 284 respectivamente), son asistencias con un valor no cuantificable dado que estas contribuyen a salvar las vidas de las personas que resultan lesionadas en eventos de tránsito.

Se resalta que la COMIPOL ha implementado capacidades médicas y de rescates de vanguardia para garantizar una respuesta efectiva en situaciones de emergencia vitales. Sus unidades médicas están equipadas para brindar soporte vital básico y avanzado, mientras que las unidades de rescate vehicular o de extricación cuentan con herramientas de última generación para liberar apersonas que queden atrapada en un vehículo accidentado.

Esta capacidad operativa se alinea con el concepto de "estrategia de huella ligera" propuesto por Del Vado (2019), que enfatiza la versatilidad que las Fuerzas Armadas del futuro deben poseer. De esa forma una entidad puede explotar las oportunidades de forma innovadora, abierta, evitando que estas lleguen a convertirse en amenazas. Los expresado por Del Vado en su artículo, toma forma concreta en la conducción de las operaciones que realizada la COMIPOL.

Tomando como ejemplo de esto; en el año 2022 por iniciativa del presidente constitucional de la República Dominicana Luis Abinader Corona, comandante supremo de las Fuerzas Armadas a través del Ministerio de Obras Públicas y Comunicaciones se comenzó a gestar el desarrollo de una aplicación tecnología que le permitiera a las personas acceder a los servicios de Asistencia Vial de la COMIPOL de forma ágil y oportuna.

Un equipo multidisciplinario desarrolló una aplicación móvil, apegada a las necesidades de las personas, que contribuyera a facilitar la prestación del servicio y a reducir el tiempo de respuesta de las unidades. Tras meses de arduo trabajo, inició el proceso de prueba de la Aplicación Asistencia Vial MOPC, herramienta que en el año 2023 ganó el primer lugar del Premio Nacional a la Innovación Pública (COMIPOL, 2023)

En su artículo publicado del 13 de diciembre de 2023, ese diario, reseña que esa herramienta le permite a las personas solicitar asistencia, reportar accidentes en las carreteras a la vez que le proporciona la ubicación exacta de las personas agilizando de esa for-

ma la llegada de las unidades y la prestación del servicio. Retomando el planteamiento de Del Vado, pero usando como contrapeso lo expresado por (Muñoz Meoño, 2024) en su trabajo monográfico, sobre las amenazas híbridas. Este autor sugiere la implementación de estrategias abarcadoras que sobrepasen las capacidades militares actuales, que incluyan la participación de la sociedad civil y tecnología de punta.

Ambos autores coinciden en la necesidad de ser innovadores para alcanzar objetivos estratégicos. Esa innovación debe ir de la mano con la realidad de las capacidades de las instituciones. No se lograrán los objetivos cuando los planes no puedan ser soportados por los recursos humanos y logísticos necesarios. En el contexto de la innovación, en el cumplimiento de la misión de la COMIPOL, fue necesario desarrollar una herramienta que apoyara la toma de decisiones en cuanto al posicionamiento en tiempo real de las unidades sobre el terreno.

Mediante el uso de teléfonos inteligentes con acceso a datos móviles y el análisis de las informaciones suministradas por las unidades fue desarrollado un mapa de calor a través del cual se disponía de la data necesaria para la reubicación de las unidades. De esa manera se contaba con unidades en los lugares donde el flujo del tráfico vehicular es más propenso a verse afectado por un accidente de tránsito, así fueron intervenidos los llamado puntos críticos. Esta herramienta contribuye a la eficiencia de esta unidad. Tanto así que (INTRANT, 2021, pp. 29, 43, 82-83), aborda en forma amplia la magnitud del problema que representan los puntos críticos para las personas que resultan involucradas en un accidente de tránsito.

En ese sentido, su Plan Estratégico para la Seguridad Vial, referencia el trabajo de la COMIPOL como un actor relevante en la respuesta a situaciones de emergencia, además de ser una fuente de información confiable, que es utilizada por el Observatorio Permanente de Seguridad Vial, en el análisis de las posibles causas de accidentes de tránsito (Instituto Nacional de Tránsito y Transporte Terrestre [INTRANT], 2023).

Acciones en las carreteras
Apoyo al desarrollo nacional

Parte de la misión de la COMIPOL es ser "responsable de la seguridad patrimonial del Ministerio de Obras Públicas y Comunicaciones (MOPC) en instalaciones, peajes, vías de comunicación" (Comisión Militar y Policial [COMIPOL], 2021). Esta unidad ha desplegado soldados en cada estación de peajes siendo estos responsables de la seguridad de esas estaciones. Esto representa un rol fundamental en el apoyo al desarrollo nacional a través de su labor de seguridad patrimonial en infraestructura crítica

En el año 2023 el Ministerio de Obras Públicas y Comunicaciones, a través del Fideicomiso RD Vial, reportó un recaudo en estaciones de peajes entre enero y diciembre de ese año ascendente a unos RD$ 1,311,285,450 (Un mil trescientos once millones doscientos ochenta y cinco mil cuatrocientos cincuenta pesos). Según datos del Ministerio de Obras Públicas y Comunicaciones (MOPC, 2023).

Tomando como referencia el monto recadado durante el año 2023, podemos inferir que la COMIPOL, al establecer un dispositivo de seguridad en las estaciones de peajes, contribuye al desarrollo nacional garantizando la integridad física de las personas que laboran en los peajes, así como también aseguran la

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

trasferencia física del dinero recaudado entre los peajes y la custodia de la Fiduciaria Banreservas SA (Pacific Credit Rating, 2021, p. 3).

De su parte la Dirección General de Aduana en su memoria del año 2023 reporta un recaudo de RD$224,937.87 millones (Doscientos veinticuatro mil novecientos treinta y siete con ochenta y siete millones de pesos dominicanos) (Dirección General de Aduanas [DGA], 2023, pp. 34, 36). Si se toma en consideración la cantidad de mercancías que salen de los puertos y aeropuertos por vía terrestres y que en caso de situaciones de emergencias esos transportes cuentan con el apoyo de la COMIPOL para resguardar tanto a las personas como a la carga. (Ver figura 2).

Figura 2
Recaudaciones realizadas por la Dirección General de Aduanas

Nota: Dirección general de aduanas, DGA. Datos preliminares sujetos a rectificación.

La producción agrícola del país depende críticamente del transporte por carretera desde las provincias donde se producen o son procesadas hasta los centros de expendio a nivel nacional y que en caso de necesitar asistencia los conductores solicitan el servicio de la COMIPOL para garantizar su integridad física y la de su carga. En otras palabras, el flujo logístico, vital para la seguridad alimentaria de República Dominicana enfrenta riesgos como fallos mecánicos, accidentes o sustracción de su carga. Con el apoyo de la COMIPOL se minimizan o eliminan esos riesgos.

La COMIPOL desempeña un rol estratégico en eventos que trascienden sus funciones centrales, aportando valor institucional en tres dimensiones clave: seguridad operativa, logística especializada y promoción de la imagen país. Múltiples instituciones giran comunicaciones tanto al Ministerio de Defensa como al de Obras Públicas solicitando apoyo con personal y equipos de la esa unidad. Esto es así por esas entidades reconocen el grado de profesionalismos con que se desempeña el personal, su alta experiencia en situaciones de emergencia en eventos masivo, que disponen de los medios y de muy buena voluntad para el servicio. Como se detalla en la Memoria institucional del 2023 (p. 28).

Coordinaciones con otras instituciones

En el desarrollo de su misión de la COMIPOL mantiene estrecha coordinación con diferentes agencias del Estado Dominicano, con las cuales ejecuta acciones que persiguen detener un determinado ilícito, prevenir su ocurrencia o contribuir el desarrollo de una tarea en común. Un ejemplo emblemático ocurrió a mediado del año 2021 con la reaparición en el país de la Fiebre Porcina Africana, el Ministerio de Agricultura a través del Ministerio de Defensa se apoyó en la COMIPOL para implementar operativos conjuntos para el control de cerdos vivos. Para ello se estableció un procedimiento que permitiese identificar cuales animales podrían movilizarse de una provincia a otra y así prevenir la propagación de la enfermedad.

Es de esa forma que la COMIPOL, con el personal desplegado en las diferentes estaciones de peajes del país y unidades patrulleras en las carreteras en combinación con inspectores del Ministerio de Agricultura realizaban la verificación de las guías de movilización de cerdos, (documento otorgado por agricultura para validar que los cerdos transportados no estaban enfermos) que autorizaban la movilización contaba con las firmas autorizadas y que no estuviesen alteradas. En las memorias del año 2024 la COMIPOL reporta que fueron verificados de ciento noventa y dos mil doscientos ochenta y siete (192,287) cerdos vivos en los diferentes peajes del país, los cuales fueron transportados por unos 4,131 vehículos. De ese total 52 vehículos fueron multados por no contar con la guía que les autoriza a mover cerdos de una provincia a otra. (COMIPOL, 2024).

Esas acciones contribuyeron de forma significativa a controlar la propagación de la enfermedad. Como lo documenta De la Cruz (2024), en el Diario Libre, quien explica que la comisión integrada por Departamento de Agricultura de los Estados Unidos (USDA) y el Servicio de Inspección Sanitaria de Animales y Plantas (Aphis), se retiraron del país en noviembre del 2024 tras considerar que esa enfermedad estaba controlada en República Dominicana.

Centro de Operaciones de Emergencia

El artículo 12 de la Ley Núm. 147-02 sobre Gestión de Riesgos, plantea que tanto el Ministerio de Defensa como el Ministerio de Obras Públicas y Comunicaciones son parte de las instituciones que integran el Centro de Operaciones de Emergencia. Siendo la COMIPOL parte de ambos ministerios, esta unidad juega un rol fundamental en la gestión de situaciones de emergencia dentro de su área de responsabilidad.

Un ejemplo paradigmático fue su intervención durante el huracán Fiona en septiembre de 2022. Según las memorias institucionales (COMIPOL, 2022), tras activar su Plan de Emergencia, se coordinó el despliegue de personal y equipos hacia las zonas más afectadas del este del país. El lunes 19 de septiembre a las 13:30 horas, el mayor general Rafael Vásquez Espínola, ERD, lideró un contingente de 100 efectivos y 55 vehículos hacia las provincias de La Altagracia, Hato Mayor y El Seibo. A la llegada de las unidades de la COMIPOL a la provincia la Altagracia prácticamente todos los servicios estaban colapsados. Luego de las reuniones de coordinación de emergencia en

la gobernación provincial, donde se trazó el plan de trabajo con mira al rescate de personas, habilitación de los servicios básicos, garantizar la seguridad ciudadana para que el proceso de reconstrucción se realizara de forma eficiente.

Por disposición del Ministerio de Defensa, la COMIPOL se integró a la estrategia de acción multidisciplinaria durante la emergencia, focalizando sus esfuerzos en tres ejes prioritarios: (1) Seguridad Ciudadana, coordinando operativos conjuntos con la Policía Nacional y el Ministerio de Defensa para proteger a la población y bienes afectados; (2) Restablecimiento de Vías, realizando labores de despeje de escombros en colaboración con equipos del MOPC para garantizar la movilidad en zonas críticas; y (3) Asistencia Humanitaria, distribuyendo agua potable mediante un sistema logístico establecido con la Gobernación Provincial y la Defensa Civil. Este esquema operativo permitió optimizar recursos y maximizar el impacto de las intervenciones en las comunidades afectadas.

En las memorias institucionales de la COMIPOL (2020–2024) se detallan los logros obtenidos durante las operaciones de apoyo tras el paso del huracán Fiona: unas 296,303 personas en la zona este del país fueron beneficiadas mediante los repartos de agua potable, limpieza de escombros, fumigación y desinfección de viviendas, además de ejecutar mil cincuentaisiete (1,057) misiones de seguridad, realizadas en coordinación con el Ministerio de Defensa (MIDE) y la Policía Nacional (PN).

Durante esos operativos fueron recogidos mil novecientos sesenta y ocho (1,968) toneladas de escombros en diferentes sectores de las provincias La Altagracia, Hato Mayor y El Seíbo; se distribuyeron trescientos veinticuatro mil (324,000) galones de agua potable; por último, dieciocho mil sesentaiuna (18,061) viviendas fueron fumigadas contra plagas tropicales. (COMIPOL, 2022). Estos esfuerzos permitieron restaurar condiciones básicas de habitabilidad en las provincias más afectadas

Durante la pandemia de COVID-19, la institución demostró nuevamente su capacidad adaptativa al implementar operativos masivos de vacunación Con la ejecución de operativos en provincias como El Seíbo, La Altagracia y Santiago de los Caballeros, María Trinidad Sánchez y el municipio Santo Domingo Norte la COMIPOL en coordinación con el Gabinete de Salud, esta unidad llegó a vacunar a doscientos cincuenta y ocho mil setecientos cuarenta y cinco (258,745) personas. (COMIPOL, 2024).

Complementariamente, fueron desplegados vehículos con turbinas pulverizadoras, que fueron adquiridas por el MOPC, tecnología que aceleró la recuperación sanitaria nacional en apoyo a las acciones implementadas por el Estado dominicano ante esta pandemia. Esta experiencia fue extendida al combate contra El Dengue, apoyando al Ministerio de Salud Pública y Asistencia Social, la COMIPOL se constituyó en un aliado eficiente en las labores de fumigación y eliminación de cacharros como forma de prevenir esa enfermedad. Esta sinergia interinstitucional evidenció cómo sus capacidades logísticas y operativas pueden reorientarse eficazmente hacia diferentes desafíos de salud pública (Ver tabla 2).

Tabla 2
Estadísticas de las capacidades logísticas y operativas de la COMIPOL

Estadísticas de los operativos de fumigación, eliminación de criaderos y reparto de agua potable realizados por el Departamento de Asuntos Sociales, desde agosto 2020 hasta julio 2024								
	VIVIENDAS FUMIGADAS	CRIADEROS ELIMINADOS	DELTAMETRINA (LITROS)	GALONES DE AGUA POTABLE	PERSONAS BENEFICIADAS DE FUMIGACIÓN	PERSONAS BENEFICIADAS DE AGUA POTABLE	PERSONAS BENEFICIADAS DE DESINFECCIÓN	PERSONAS BENEFICIADAS EN TOTAL
2020	89,066	5,718	148	3,704,000	445,330	926,000	0	1,371,330
2021	171,335	22,638	534	3,436,000	856,675	859,000	0	1,715,675
2022	192,899	24,848	571	3,352,000	964,495	838,000	53,735	1,856,230
2023	210,452	39,070	611	2,216,000	1,042,840	495,350	54,000	1,592,190
2024	52,675	7,259	160	1,192,000	248,045	256,430	0	504,475
TOTAL	716,427	99,533	2,024	13,900,000	3,557,385	3,374,780	107,735	7,039,900

Mota: Departamento de Estadística de la COMIPOL, 2024.

Como preámbulo a las conclusiones, destacamos dos hitos significativos para la COMIPOL que a nuestro juicio consolidan el tema del presente artículo. El primero, fue la creación en marzo del 2022 de la Unidad en Control del Derecho Vial (CODEVIAL). Esta unidad fue aprobada por el Estado Mayor General de las Fuerzas Armadas y cuenta con un uniforme diferente para identificarla de las demás que integran la COMIPOL. Esa unidad especializada, tiene la responsabilidad de velar por la preservación del Derecho de vía, que está definido en la Ley 1474 del año 1938, como el espacio que el estado reserva a ambos lados de la carretera para realizar futuras ampliaciones (Ver imágenes 1 y 2).

Imágenes 1 y 2
Unidad en Control del Derecho Vial (CODEVIAL)

Nota: Imágenes de archivo COMIPOL (Comisión Militar y Policial, Departamento de Relaciones Públicas, 2025). De izquierda a derecha: uniforme de CODEVIAL, y el desalojo en el km 9 de la autopista Duarte.

Los resultados operativos de CODEVIAL han sido contundentes: según las memorias institucionales (COMIPOL, 2024), fueron intervenidas mil doscientas noventa obras (1,290), que violentaban el derecho vía. Estas acciones preventivas han generado ahorros millonarios al erario nacional al evitar procesos de expropiación que hubieran sido necesarios para corregir estas ocupaciones ilegales. La efectividad de esta unidad ha convertido a la COMIPOL en garante técnico de la planificación vial (Ver tabla 3).

Tabla 3
Estadísticas de los resultados operativos de CODEVIAL

ZONAS	REGIÓN NORTE	REGIÓN SUR	REGIÓN ESTE	CIRCUNVALACIÓN STO. DGO.	AVENIDA ECOLÓGICA	REGIÓN NORDESTE	TOTAL GENERAL
OBRAS PARALIZADAS:	103	72	58	26	13	31	303
OBRAS NOTIFICADAS:	41	31	26	12	5	27	142
ACCESOS Y CIERRES ILEGALES:	26	22	11	25	3	18	105
OBRAS CON PERMISOS:	4	8	10	4	4	3	33
DESMANTELAMIENTOS:	283	22	26	95	66	16	508
DEMOLICIONES:	26	1	16	17	40	9	109
EN ESPERA DE RESPUESTA:	3	14	4	4	2	10	37
CONSTRUCCIÓN ABANDONADA:	0	3	1	0	0	1	5
CORREGIDA:	6	6	16	8	0	0	36
DESISTIERON DE LA OBRA:	6	0	3	0	2	1	12
TOTAL GENERAL	**498**	**179**	**171**	**191**	**135**	**116**	**1290**

Nota: Departamento de Estadística de la COMIPOL, 2024.

El segundo hito institucional le corresponde al compromiso con la calidad asumido por la COMIPOL. Alcanzando un sitial privilegiado cuando 21 de agosto del 2024, fue entregado el certificado que avala esta unidad bajo la Norma ISO 9001: 2015 en la gestión de la calidad de los procesos de Protección y Asistencia Vial y Emergencias Médicas y Rescate Vehicular.

Antes de obtener esta certificación, y como se ha señalado anteriormente, esta unidad es distinguida por las personas que reciben su servicio como un referente de trabajo profesional, excelente desempeño de su personal, compromiso con el usuario, alto nivel ético. El haber sido certificada bajo una norma internacional en la gestión de la calidad, ratifica el grado de eficiencia que se les proporciona a los usuarios.

Conclusiones

Este estudio analizó las capacidades híbridas de la Comisión Militar y Policial (COMIPOL), adscrita al Ministerio de Obras Públicas y Comunicaciones (MOPC), en el contexto de sus operaciones cívico-militares. A partir de un análisis cualitativo no experimental, se evaluaron su estructura organizacional, programas principales, eficiencia operativa y comparación con unidades similares en la región.

Los hallazgos indican que COMIPOL ha evolucionado más allá de las funciones tradicionales de las Fuerzas Armadas, integrando disciplina militar con expertise civil para responder a múltiples demandas sociales, logísticas y de seguridad. Durante el período evaluado, la unidad brindó más de 3.3 millones de asistencias viales, apoyó la aplicación de 258,745 vacunas durante la pandemia de COVID-19, e intervino en 1,290 casos de violación al derecho de vía, evitando costosas expropiaciones futuras.

Estos resultados respaldan la hipótesis de que las unidades con doble adscripción ministerial (seguridad-desarrollo) pueden generar impactos transversales en el desarrollo nacional, cumpliendo roles definidos en el Libro Blanco de la Defensa de República Dominicana (MIDE, 2022). Además, la certi-

ficación bajo la norma ISO 9001:2015 refuerza la percepción ciudadana de calidad y profesionalismo, validando institucionalmente su enfoque orientado al usuario.

La creación de la Unidad en Control del Derecho Vial (CODEVIAL) y el desarrollo de herramientas tecnológicas —como la aplicación móvil de asistencia vial MOPC— demuestran la capacidad de innovación de la unidad. Asimismo, su desempeño en emergencias como el huracán Fiona (2022) confirma su versatilidad y coordinación interinstitucional.

No obstante, el análisis también revela algunas limitaciones metodológicas, entre ellas el uso predominante de fuentes internas y la posible subjetividad derivada de la experiencia directa del autor/a en la unidad. Futuros estudios podrían complementar este análisis con evaluaciones externas e independientes, así como con estudios comparativos ampliados en otros países de la región.

Los aportes de la COMIPOL al desarrollo de la República Dominicana pueden ser evaluados desde varios puntos de vistas. Entre ellos, defensa nacional, apoyo a la autoridad civil, gestión de desastre y calamidad pública, contribución al desarrollo socio económico y protección de áreas estratégicas vitales.

Los integrantes de COMIPOL son reconocidos por los usuarios como "los ángeles de la carretera", gracias a la calidad, respeto y seguridad que caracterizan su servicio. Además, los ciudadanos destacan que no solicitan ni aceptan dinero a cambio de su labor, lo que refuerza su imagen de integridad y compromiso.

En conclusión, COMIPOL representa un modelo institucional único en América Latina, donde la interagencialidad y la integración de capacidades militares y civiles permiten abordar retos complejos con alta eficacia operativa. Su caso ofrece lecciones valiosas sobre cómo las fuerzas armadas pueden contribuir al desarrollo nacional sin perder su rol estratégico de defensa.

Referencias

Comisión Militar y Policial (COMIPOL). (2021). *Manual de organización y funciones COMIPOL 2021 (MOPC-COMIPOL/ DGAV-MOF)* [Documento institucional interno]. Ministerio de Obras Públicas y Comunicaciones.

Comisión Militar y Policial (COMIPOL). (2023). *Memoria institucional 2023* [Documento institucional]. Ministerio de Obras Públicas y Comunicaciones.

Comisión Militar y Policial (COMIPOL). (2024). *Memoria institucional 2020-2024* [Documento institucional]. Ministerio de Obras Públicas y Comunicaciones.

Comisión Militar y Policial (COMIPOL). Departamento de Relaciones Públicas. (2022). *Lanzamiento de la unidad CODEVIAL en Santo Domingo* [Comunicado institucional]. Comisión Militar y Policial.

Comisión Militar y Policial (COMIPOL). Departamento de Relaciones Públicas. (2025). *Desalojo de buhoneros en el km. 9 de la autopista Duarte* [Reporte operativo]. Comisión Militar y Policial.

COMIPOL gana primer lugar nacional Innovación 2023. (2023, 13 de diciembre). *El Día*. https://eldia.com.do/comipol-gana-primer-lugar-nacional-innovacion-2023/

Constitución de la República Dominicana [Const.]. (2024). *Gaceta Oficial No. 11170*, 27 de octubre de 2024. https://www.consultoria.gov.do/Documents/GetDocument? reference=88cd6dd0-268b-4fda-a12a-0f3ae7fcfa7e

De la Cruz, I. (2024, noviembre 14). La peste porcina ya no es una emergencia en RD. *Diario Libre*. https://www.diariolibre.com/economia/agro/2024/11/14/peste-porcina-deja-de-ser-emergencia-en-el-pais/2911965

Del Vado, S. F. (2019, septiembre). Las Fuerzas Armadas del futuro. *Revista Española de Defensa,* 364, 48–49. https://www.defensa.gob.es/Galerias/gabinete/red/2019/09/p-48-49-red-364-fas-futuro.pdf

Dirección General de Aduanas. (2023). *Memoria institucional 2023*. https://www.aduanas.gob.do/media/dkflg42m/memoria-institucional-direccion-general-de-aduanas-2023.pdf

Dirección General de Impuestos Internos. (2024). *Parque vehicular 2024*. https://dgii.gov.do/estadisticas/parqueVehicular/1Informes%20Parque%20Vehicular/ParqueVehicular2024.pdf

Dirección General de Planificación y Desarrollo. (2023). *Resultados de satisfacción, tiempo de respuesta, quejas/sugerencias: Servicios comprometidos carta compromiso al ciudadano (octubre 2022–septiembre 2023)*. Ministerio de Obras Públicas y Comunicaciones. https://www.mopc.gob.do/media/26015/informe-de-resultados-de-satisfaccion-octubre-2022-septiembre-2023.pdf

Dirección General de Planificación y Desarrollo. (2024). *Resultados indicadores carta compromiso al ciudadano: enero–diciembre 2024*. Ministerio de Obras Públicas y Comunicaciones. https://www.mopc.gob.do/media/29049/informe-resultados-enero-diciembre-2024.pdf

González-Cuenca, D., Montes Ramírez, A. M., & Idrobo Velasco, J. A. (2019). *La política de defensa y seguridad nacional en Colombia: Análisis de condiciones sostenibles para el desarrollo social*. ESDE. https://esdeglibros.edu.co/index.php/editorial/catalog/download/79/105/1211?inline=1

Instituto Nacional de Tránsito y Transporte Terrestre (INTRNT). (2021). *Plan estratégico nacional para la seguridad vial 2021–2030*. https://intrant.gob.do/transparencia/phocadownload/PlanEstrategico/PENSV-2021-2030.pdf

Ley No. 147-02. Santo Domingo, República Dominicana. (22 septiembre del 2002). Ley sobre gestión de riesgos y su reglamento de aplicación. *Gaceta Oficial. núm. 10172*. https://www.coe.gob.do/phocadownload/SobreNosotros/MarcoLegal/Ley_147-02_Sobre_Gestion_de_Riesgos.pdf

Ley No. 9.503. (1997, septiembre 23). Instituye el Código de Tránsito Brasileiro. *Diario Oficial de la Unión, sección 1,* 3-10–15. https://www.gov.br/prf/pt-br/acesso-a-informacao/institucional/base-juridica

Ley de la Guardia Nacional (2019). Congreso General de los Estados Unidos Mexicanos. (2019, mayo 27). Ley de la Guardia Nacional. Capítulo III - Atribuciones y obligaciones de la Guardia Nacional. *Diario Oficial de la Federación*. https://www.dof.gob.mx/nota_detalle.php?codigo=5561285&fecha=27/05/2019

Ministerio de Defensa de la República Dominicana. (2022). *Libro Blanco de la Defensa de República Dominicana*. https://unade.edu.do/wp-content/uploads/2023/10/Libro-Blando-comprimido.pdf

Ministerio de Defensa. (2006, abril 22). Real Decreto 416/2006, por el que se establece la organización y el despliegue de la Fuerza del Ejército de Tierra, de la Armada y del Ejército del Aire, así como de la Unidad Militar de Emergencias. *Boletín Oficial del Estado, núm. 96.* https://www.boe.es/buscar/pdf/2006/BOE-A-2006-7168-consolidado.pdf

Ministerio de Defensa (MIDE). (2021). *Plan estratégico institucional 2021–2024*. http://new.insude.mil.do/transparencia/index.php/plan-estrategico/planeacion-estrategica

Ministerio de Defensa (MIDE). (2022). *Libro Blanco para la Defensa de República Dominicana.* https://mide.gob.do/wp-content/uploads/2023/02/Libro-Blando-comprimido.pdf

Ministerio de Obras Públicas y Comunicaciones. (2023). *Recaudación anual por concepto de peajes*. https://www.mopc.gob.do/transparencia/estadisticas-institucionales/ recaudacion-anual-por-concepto-de-peajes/

Ministerio de Obras Públicas y Comunicaciones & Ministerio de Defensa. (2021). *Manual para la formación especializada de la Comisión Militar y Policial.*

Muñoz Meoño, R. E. (2024). *Desafíos y soluciones en la defensa nacional.* Escuela Superior de Guerra "General Rafael Reyes Prieto". https://www.esdegrepositorio.edu.co/ bitstream/handle/20.500.14205/11266/TG-MY%20MU%C3%91OZ%20RONALD MAESD%20AULA%20I.pdf?sequence=1&isAllowed=y

Pacific Credit Rating. (2021, octubre). *Informe de calificación: Fideicomiso para la Operación, Mantenimiento y Expansión de la Red Vial Principal de la República Dominicana (RD VIAL).* https://rdvial.gob.do/wp-content/uploads/2023/10/pacific-credit-rating-octubre-2021.pdf

Sistema 9-1-1. (2023, 22 de diciembre). *9-1-1 entrega 18 nuevas motocicletas a COMIPOL para fortalecer la asistencia via*l. https://911.gob.do/9-1-1-entrega-18-nuevas-motocicletas-a-comipol-para-fortalecer-la-asistencia-vial/

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Aportes de la COOPINFA a través de la educación y la responsabilidad social al desarrollo económico y social de los miembros de las fuerzas armadas y de la sociedad dominicana

Contributions of COOPINFA through Education and Social Responsibility to the Economic and Social Development of Members of the Armed Forces and Dominican Society

Recibido: 01/ 05 / 2025 | Revisado: 15 / 07 / 2025 | Aprobado: 15 / 09 / 2025
DOI: https://doi.org/10.59794/rscd.2025.v11i11.145

Mayor general Juan José Otaño Jiménez, ERD
República Dominicana

Correo:jjoj20@hotmail.com

ORCID: https://orcid.org/0009-0002-1690-172X

Afiliación: Universidad Nacional para la Defensa

El autor es mayor general del Ejército de la República Dominicana. Es Magister Scientiarum en Ciencias y Artes Militares por la Universidad de Venezuela, posee una Licenciatura en Derecho; es especialista en Cooperativismo y Gestión de Empresas Cooperativas y posee un Diplomado en Seguridad Física e Industrial. Fue Director General de las Escuelas Vocacionales de las FF. AA. y la P.N, director general de la Radioemisora Cultural La Voz de las FF. AA., director administrativo de la Comandancia General, ERD, director Asuntos Civiles, ERD, subdirector general del Instituto de Seguridad Social de las FF. AA., subcomandante Cuartel General, ERD, y actualmente es presidente del Consejo de Administración de la Cooperativa de Ahorros, Créditos y Servicios Múltiples de los Integrantes de las Fuerzas Armadas (COOPINFA).

DOI: https://doi.org/10.59794/rscd.2025.v11i11.145

Teniente coronel Jorge Alejandro De La Paz Beltré, ERD
República Dominicana

Correo:delapaz_ja@hotmail.com

ORCID: https://orcid.org/0009-0009-2013-1896

Afiliación: Universidad Nacional para la Defensa

El coautor es teniente coronel piloto del Ejército de la República Dominicana. Es Magister en Seguridad, Defensa y Geoestrategia. Posee una Licenciatura en Relaciones Internacionales y una Licenciatura en Administración de Empresas, posee una Especialidad en Geopolítica, una en Cooperativismo y Gestión de Empresas Cooperativas, además de varios Diplomados en diferentes áreas del saber, y es piloto de alas rotatorias. Fue subdirector Técnico de las Escuelas Vocacionales de las FF. AA. y la PN, S-1, Oficial de Personal del 1er. Escuadrón de Caballería Aérea, ERD, y actualmente es gerente de Educación, Bienestar y Responsabilidad Social de la Cooperativa de Ahorros, Créditos y Servicios Múltiples de los Integrantes de las Fuerzas Armadas (COOPINFA).

DOI: https://doi.org/10.59794/rscd.2025.v11i11.145

Resumen

En el contexto mundial, el cooperativismo se ha promovido como una vía de inclusión de las personas al sistema económico y como una alternativa eficaz para combatir las desigualdades sociales. Representa la articulación de lo social y lo empresarial en una sola institución orientada a alcanzar metas integrales en diferentes ámbitos. En una época marcada por la desintegración de los fundamentos solidarios y colectivos de la sociedad y sobre todo de la cooperación como fuente inagotable de bienestar, el cooperativismo emerge como una sabia decisión para contrarrestar los procesos de deterioro económico existentes. Es por eso que la Cooperativa de Ahorros, Créditos y Servicios Múltiples de los Integrantes de los Fuerzas Armadas (COOPINFA) a través de los principios cooperativos, sus valores, así como su filosofía colectiva y de inclusión social constituye un pilar fundamental en el desarrollo socioeconómico equitativo de sus asociados, promoviendo bienestar entre estos por medio de la educación y una responsabilidad social solidaria y democrática disminuyendo las brechas y la exclusión de los miembros de las Fuerzas Armadas, sus familiares y la sociedad en general, fomentando mecanismos de transformación en áreas como la salud, el apoyo a las comunidades y el desarrollo ambiental convirtiéndose en un productor de desarrollo y distribuidor de riqueza y prosperidad.

Palabras clave: Cooperativismo, COOPINFA, principios cooperativos, responsabilidad social, valores cooperativos

Abstract

Throughout the global context, cooperativism has been promoted as a form of inclusion for people in the economic system and as a solution to combat social, social and business inequalities mixed in a single institution that seeks to achieve comprehensive goals in different spaces. In times where the foundations of the solidarity and collective bases of society are disintegrating and, above all, cooperation as an endless source of well-being, cooperativism emerges as a wise decision to reverse the prevailing processes of existing economic deterioration. That is why the Cooperative of Savings, Credits and Multiple Services of the Members of the Armed Forces (COOPINFA) through the cooperative principles, its values, as well as its collective philosophy and social inclusion constitutes a fundamental pillar in the equitable socioeconomic development of its members, promoting well-being among them through education and a solidary and democratic social responsibility, reducing the gaps and exclusion of the members of the the Armed Forces, their families and society in general, promoting mechanisms of transformation in areas such as health, support for communities and environmental development, becoming a producer of development and distributor of wealth and prosperity.

Keywords: Cooperativism, COOPINFA, cooperative principles, social responsibility, and cooperative values

DOI: https://doi.org/10.59794/rscd.2025.v11i11.145

Introducción

Las Fuerzas Armadas son una institución que tiene a cargo la defensa de la nación, su misión es defender la independencia y soberanía de la nación, la integridad de sus espacios geográficos, la Constitución y las instituciones de la República (Ministerio de Defensa, 2022).

Pero además de su propósito y tareas esenciales dadas en la carta magna, este estamento militar también es generador de bienestar económico y social para sus miembros, familiares y el entorno comunitario que lo rodea al estimular la economía creando demanda de bienes y servicios, impulsando la innovación tecnológica y creando empleos por medio del gasto militar, convirtiéndose en un pilar de apoyo al desarrollo social y económico de un País a través de sus capacidades, (González, Mora & López, 2024).

Las cooperativas son entidades financieras situadas en una posición única para erradicar la pobreza y dignificar la calidad de vida de las personas, puesto que son instituciones que tienen como eje central el ser humano y por tanto buscan satisfacer las necesidades de sus miembros. Es así como la Cooperativa de Ahorros, Créditos y Servicios Múltiples de los Integrantes de las Fuerzas Armadas (COOPINFA), aunque es una entidad sujeta a los cánones militares se suscribe a los siete principios cooperativos que garantizan la adhesión abierta y voluntaria, el control democrático, la autonomía e independencia y el interés por su comunidad, al situar la equidad, la igualdad y la justicia social en el centro de su modelo empresarial (COOPINFA, 2025).

En ese tenor, al comprender la importancia de COOPINFA como un actor clave en el desarrollo socioeconómico de la República Dominicana, especialmente por su singular integración de la filosofía cooperativista con las capacidades de las Fuerzas Armadas y de manera particular en un contexto global, donde el cooperativismo emerge como un modelo inclusivo y una respuesta a las desigualdades, COOPINFA se erige como un faro de bienestar para sus asociados y la sociedad en general (ver gráficos 1 y 2) al conceder soluciones crediticias para la creación y capitalización de MiPymes otorgando la cantidad de 2,554 préstamos solidarios por un monto total de RD$495 millones, impactando directamente a igual cantidad de personas y 13,026 personas indirectamente, así mismo contrató 144 colaboradores entre personal civil y militares retirados (Gerencia General, COOPINFA, 2024).

Gráfico 1
Relación de préstamos concedidos a socios para capitalizar y crear MiPymes

PRESTAMOS DESEMBOLSADOS PARA MIPYMES EN 2024				
Cantidad	**Monto total en RD$**	**Tipo de empresa**	**No. Personas impactadas directamente**	**No. Personas impactadas indirectamente**
2,554	RD$495,000.000.00	Micro y pequeñas empresas	2,554	13,026

Nota: Gerencia Financiera de COOPINFA.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Gráfico 2
Relación de personal contratado en COOPINFA

CONTRATACIÓN DE PERSONAL CIVIL Y MILITARES RETIRADOS	
Personas contratadas	**Cantidad**
Colaboradores civiles	134
Militares retirados	12
TOTAL	**144**

Nota: Gerencia de Gestión Humana, COOPINFA.

Su estructura, fundamentada en los principios y valores cooperativos, le permite trascender la mera actividad financiera, convirtiéndose en un agente de transformación social y económica. Es por esto que COOPINFA a través de la Presidencia de la Comisión de Educación, Bienestar y Responsabilidad Social, así como de la Gerencia de Educación, Bienestar y Responsabilidad Social promueven la participación democrática, (ver gráfico 3) la educación y la responsabilidad social, por lo que no solo reduce las brechas de exclusión dentro de la comunidad militar y sus familias, sino que también irradia beneficios hacia el desarrollo del país en áreas cruciales como la salud, el apoyo institucional y comunitario y la sostenibilidad ambiental (ver gráfico 4). Esta labor, intrínsecamente ligada a las capacidades de las Fuerzas Armadas, posiciona a COOPINFA como un distribuidor de riqueza y prosperidad, fortaleciendo el tejido social y económico de la nación.

Gráfico 3
Relación jerárquica de delegados de la Asamblea General de COOPINFA

DELEGADOS	NIVEL	MIDE	ERD	ARD	FARD	TOTAL
Oficiales generales y/o almirantes	1		5	5	5	15
Oficiales superiores	2		15	15	15	45
Oficiales subalternos	3		20	20	20	60
Alistados	4		23	23	23	69
Asimilados	5	5	6	6	6	23
Retirados	6		5	5	5	15
TOTALES		**5**	**74**	**74**	**74**	**227**

Nota: Gerencia de Educación, Bienestar y Responsabilidad Social, COOPINFA.

Gráfico 4
Relación de inversión en educación, salud y apoyo institucional y comunitario en COOPINFA

PROGRAMAS SOCIALES DE COOPINFA			
PROGRAMA SOCIAL	MONTO RD$	IMPACTADOS DIRECTOS	IMPACTADOS DIRECTOS
Programa Social Educativo	34,892,006.92	182	4,468
Programa Social Salud	92,239,472.09	307	1,289
Programa Social Vivienda	1,051,746,970.00	2,992	11,968

PROGRAMAS SOCIALES DE COOPINFA			
Programa Social Recreaciones, Deportes y Cultura	5,560,826.79	30	4,327
Programa Social a la Comunidad e Instituciones	1,343,613.26	17	1,018
Programa Social de Alimentación, Hogar y Autos	156,680,658.70	1,734	6,936
Programa Social de Medio Ambiente	1,000,000.00	6	50
Programa Social Funerario	609,584,00	19	72
Programa Social de Equidad de Género	394,100.00	1	214
TOTAL			

Nota: Gerencia de Educación, Bienestar y Responsabilidad Social, COOPINFA.

Desarrollo

El hombre como ser social por naturaleza ha necesitado de sus congéneres para sobrevivir, es así como históricamente la cooperación es un hecho que se ha manifestado en todas las funciones sociales y en todos los procesos de la cultura universal. El espíritu de cooperación se ha manifestado a lo largo de la historia de las sociedades humanas. Los historiadores del cooperativismo están de acuerdo en señalar como antecedentes del sistema cooperativo a diferentes manifestaciones organizativas de tipo grupal en las que los individuos, utilizando como medio de acción la ayuda mutua, buscaron fortalecer sus intereses comunes.

El Cooperativismo surgió como una de las alternativas de lucha utilizadas por los trabajadores para defenderse de las condiciones económicas y sociales que surgieron como consecuencia de la revolución industrial. Se rige por valores y principios basados en el desarrollo integral del ser humano, que resaltan la importancia de la visión del cooperativismo. En este tenor se procede a definir los conceptos de cooperativismo, cooperativa y cooperativa financiera, (Concepción, 2015).

Por lo que el cooperativismo puede ser definido como un "movimiento socioeconómico fundamentado en la cooperación el cual promueve la libre asociación de individuos y familias con intereses comunes y sustentado en valores de solidaridad, equidad y ayuda mutua" (Guilarte y Chávez, 2023).

En ese mismo orden una "cooperativa es una asociación autónoma de personas unidas voluntariamente para satisfacer necesidades y aspiraciones económicas, sociales y culturales comunes a través de una empresa de propiedad conjunta y gestión democrática. En esencia, son empresas centradas en las personas, donde los miembros son dueños, controlan y dirigen la cooperativa" (Alianza Cooperativa Internacional, 1995).

Las cooperativas son instituciones voluntarias, abiertas a todo aquel que pueda ser capaz de usar sus servicios, pero que también esté dispuesto a asumir las responsabilidades

DOI: https://doi.org/10.59794/rscd.2025.v11i11.145

de asociarse, sin prejuicios políticas, sociales o de género, raciales o religiosas. Dentro de estas se encuentran las cooperativas financieras que son asociaciones sin fines de lucro que brindan servicios financieros a sus miembros, los cuales a su vez también ejercen como propietarios de la cooperativa. A diferencia de la banca tradicional, las cooperativas financieras persiguen el beneficio equitativo de sus socios y priorizan el desarrollo comunitario y la inclusión financiera (Buendía, Redjah & Tremblay, 2012).

Existen otros tipos de cooperativas y dentro de esa clasificación están las siguientes cooperativas, (Ressel, 2013).

- **Cooperativa de consumo**: La forman consumidores que buscan abaratar los precios de los bienes y servicios obteniendo productos al por mayor y distribuyéndolos entre sus socios con un margen mínimo para cubrir gastos.
- **Cooperativas agrarias**: Su naturaleza radica en ofrecer ayuda a los agricultores en la compra de materias primas, venta de las cosechas y la optimización de las técnicas agrícolas, para luego finalmente asistir en la producción y comercialización de dichos productos.
- **Cooperativas de provisión de servicios**: Agrupan a profesionales de una misma ocupación para adquirir insumos o servicios a costos más bajos.
- **Cooperativas de seguros**: Ofertan seguros a sus miembros a precios más asequibles que las aseguradoras tradicionales.
- **Cooperativas de servicios públicos**: Tramitan servicios básicos buscando eficiencia y precios justos para sus miembros.
- **Cooperativas de vivienda**: Proveen el acceso a viviendas asequibles para sus miembros, a través de la edificación, adquisición o alquiler a precios de costo.
- **Cooperativas de crédito**: Son organizaciones financieras que brindan servicios de ahorros y préstamos a sus socios, fomentando la inclusión financiera.
- **Bancos cooperativos**: Son cooperativas que funcionan como bancos, brindando una vasta gama de servicios financieros a sus socios.

Una vez aclarados los conceptos anteriormente citados podemos expresar que la Cooperativa de Ahorros, Créditos y Servicios Múltiples de los Integrantes de las Fuerzas Armadas (COOPINFA), se enmarca dentro de las cooperativas de créditos, pero además de eso aunque es una entidad sujeta a los cánones militares se suscribe a los siete principios cooperativos que garantizan la adhesión abierta y voluntaria, el control democrático, la autonomía e independencia y el interés por su comunidad, al situar la equidad, la igualdad y la justicia social en el centro de su modelo empresarial como lo hacen todas las cooperativas sin importar sus naturaleza.

La Cooperativa de Ahorros, Créditos y Servicios Múltiples de los Integrantes de las Fuerzas Armadas (COOPINFA) es una entidad financiera solidaria constituida por militares y civiles que ha adoptado las bondades cooperativistas, bajo la modalidad de la filosofía cooperativista, siendo regulada por la Ley 127-64 (1964), sobre Asociaciones Cooperativas y su Reglamento; pero sin olvidarse de su esencia militar (ver gráfico 5).

DOI: https://doi.org/10.59794/rscd.2025.v11i11.145

Gráfico 5

Relación de socios inscritos en COOPINFA

CANTIDAD DE SOCIOS ACTIVOS Y RETIRADOS	
Socios	**Cantidad**
Militares activos	66,306
Militares retirados	8,224
Total	74,580

Nota: Gerencia General, COOPINFA.

COOPINFA en una institución que ha podido convertirse y sincronizarse con las políticas de bienestar para ir acorde a los lineamientos de la Constitución de la República (2015), en el Artículo 222, valida el rol de las cooperativas como motores de desarrollo, fomentando la integración del sector informal en la economía formal; las estrategias y objetivos de la Ley 1-12, Estrategia Nacional de Desarrollo 2030; la Ley 139-13 Orgánica de las FF. AA. Dominicana; el Plan Nacional Plurianual del Sector Público (PNPSP) y el Plan Estratégico Institucional (PEI) del Ministerio de Defensa, en cuanto a este último documento, COOPINFA se alinea con cuatro ejes estratégicos, (Ministerio de Defensa, 2017):

1. "Unas Fuerzas Armadas que promuevan el bienestar de sus miembros con igualdad de derechos y oportunidades, a través de una buena salud, con instalaciones adecuadas y que les facilite el acceso para la adquisición de viviendas dignas".

2. "Unas Fuerzas Armadas que contribuyan con su accionar al desarrollo nacional".

3. "Unas Fuerzas Armadas que velan por una sociedad de producción y consumo sostenible, que garantizan la protección de la población, del medio ambiente, los recursos naturales y promueven con eficiencia la gestión de riesgo y la adaptación al cambio climático".

4. "Unas Fuerzas Armadas que promuevan el bienestar de sus miembros a través del mejoramiento de la educación, capacitación, entrenamiento, el desarrollo integral, profesional, deporte y cultura".

Las Fuerzas Armadas cumplen un rol esencial de acompañamiento debido al interés del Estado de que se promuevan y ejecuten estrategias que impulsen el desarrollo del país, tales como el acompañamiento en el cumplimiento de la Estrategia Nacional de Desarrollo 2030 (END), alineada a los Objetivos de Desarrollo Sostenible (ODS), el cual su cumplimiento colocar en un nivel más alto al país, y posiciona a este en el marco de los países de la región (Guerrero, 2023).

Para cumplir con su misión dentro de las Fuerzas Armadas, COOPINFA genera bienes y servicios que sustenten la visión de futuro de dicha institución, entre las cuales se pueden mencionar préstamos personales, para vehículos, comerciales, médicos y de educación, así como ayudas solidarias en mobiliarios, equipos, alimentos, útiles escolares, utilería deportiva y electrodomésticos, contribuyendo a lograr una República Dominicana más desarrollada en cuanto al nivel económico, social y educativo de sus miembros y familiares, así como de la sociedad en general (Gerencia de Educación, Bienestar y Responsabilidad Social, 2024).

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

El impulso que presenta COOPINFA le permite cumplir en el apoyo al desarrollo social y económico del país a través de las capacidades de las Fuerzas Armadas, ya que ello se manifiesta en diversas dimensiones. En primer lugar, su naturaleza de cooperativa fomenta la inclusión financiera de un sector importante de la población, facilitando el acceso a créditos, ahorros y otros servicios que de otra manera podrían ser inaccesibles (International Cooperative Alliance, 2021).

Esta inclusión no solo mejora la calidad de vida de los miembros y sus familias, sino que también dinamiza la economía local al impulsar el consumo y la inversión. Además, al estar integrada por miembros de las Fuerzas Armadas, COOPINFA aprovecha la disciplina, la organización y la capacidad logística de esta institución para llevar a cabo proyectos de desarrollo comunitario. Esto se traduce en iniciativas de apoyo en áreas vulnerables, construcción de infraestructuras básicas, y asistencia en situaciones de emergencia, demostrando un compromiso con el bienestar social que va más allá de sus asociados directos al aprovechar su organización y capacidad logística para llegar a todo el territorio nacional en coordinación con el Ministerio de Defensa y las Comandancias Generales de las instituciones castrenses (MIDE, 2023).

Una de las principales ventajas que ofrece COOPINFA es que provee soluciones crediticias a sus miembros, tanto activos como retirados los cuales la mayoría de las veces forman parte de un segmento de la población que normalmente no tendría acceso a los grandes bancos comerciales. Esto reviste una gran importancia en los mercados en los que los proveedores de servicios financieros tradicionales no existen o no están interesados debido a los altos riesgos, los elevados costos de transacción o las bajas perspectivas de ingresos (ver gráficos 6 y 7).

Gráfico 6

Tabla de préstamos por rango, sueldo y tiempo para miembros activos en COOPINFA

TABLA DE PRÉSTAMOS POR SUELDO, RANGO Y TIEMPO			
RANGO	**SUELDO EN RD$**	**MONTO DEL PRÉSTAMO**	**CANT. DE CUOTAS**
Mayor General	60,049.00	850,000.00	60
General	50,275.72	750,000.00	60
Coronel	42.907.52	600,000.00	60
Tte. Coronel	39,234.81	550,000.00	60
Mayor	36,615.53	520,000.00	60
Capitán	34,575.75	480,000.00	60
1er. Teniente	32,541.78	440,000.00	60
2do. Teniente	31,510.28	400,000.00	60
Sgto. Mayor	30,394.94	370,000.00	60
Sargento	28,765.02	350,000.00	60
Cabo	26,233.36	300,000.00	60
Raso	24,555.90	250,000.00	60

Nota: Presidencia del Consejo de Administración, COOPINFA

DOI: https://doi.org/10.59794/rscd.2025.v11i11.145

Gráfico 7

Tabla de préstamos por rango, sueldo y tiempo para miembros retirados en COOPINFA

TABLA DE PRÉSTAMOS POR SUELDO, RANGO Y TIEMPO				
RANGO	**SUELDO EN RD$**	**MONTO DEL PRÉSTAMO**	**CUOTA**	**CANT. DE CUOTAS**
Ministro	300,000.00	4,000.000.00	74,585.66	7 años
Comandante Gral.	250,000.00	3,500,000.00	65,262.45	7 años
Subcomandante Gral.	200,000.00	3,000,000.00	55,939.24	7 años
Director General	150,000.00	2,500,000.00	46,616.04	7 años
Director	120,000.00	2,000,000.00	37,292.83	7 años
Subdirector General	100,000.00	1,500,000.00	27,969.63	7 años
Subdirector	80,000.00	1,200,000.00	22,375.70	7 años
División 1	75,000.00	1,100,000.00	25,739.19	5 años
División 2	70,000.00	1,000,000.00	23,399.27	5 años
División 3	65,000.00	940,000.00	21,995.32	5 años
Sección 1	60,000.00	870,000.00	20,357.36	5 años
Sección 2	55,000.00	790,000.00	18,485.43	5 años
Sección 3	50,000.00	725,000.00	16,964.47	5 años
Sección 4	45,000.00	650,000.00	15,209.52	5 años
Sección 5	40,000.00	580,000.00	13,571.58	5 años
Sección 6	35,000.00	500,000.00	11,699.63	5 años
Sección 7	30,000.00	450,000.00	10,737.23	5 años

Nota: Presidencia del Consejo de Administración, COOPINFA

A causa de su baja estructura de costos y sus reducidas metas en materia de beneficios, COOPINFA puede ofrecer servicios de crédito a tasas atractivas, (ver gráfico 8) representando así alternativas a los préstamos de carácter usurero y disminuyendo la vulnerabilidad de sus miembros menos pudientes a la explotación; de igual manera, le dedica mucha importancia en el otorgamiento de créditos a la pequeña y mediana empresa, que es un destacado sector generador de empleo en las economías locales; sin embargo, todo este aporte que proporciona esta dependencia, a nivel de las provincias y comunidades donde existen unidades militares, es limitado, ya que su sede principal está en la capital de la república y los diez puntos de negocios que posee aun no son suficientes para cubrir las necesidades de todos sus socios.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Gráfico 8
Relación de tipos de soluciones crediticias en COOPINFA

TIPOS DE SOLUCIONES CREDITICIAS QUE OFRECE COOPINFA			
SERVICIO	**TASA O PORCENTAJE (%)**	**TIEMPO**	**VARIACIÓN O REVISIÓN**
Préstamos personales	13	5-7 años	Fija
Préstamos vehículos	14	7	Fija
Préstamos MiPymes	12	5	Fija
Préstamos emprendedores	13	5	Fija
Préstamos comerciales	13	6 meses a 24 meses	Fija

Nota: Gerencia de Negocios y Canales Digitales, COOPINFA

Obviamente es una necesidad que la institución deba tener presencia en estas o en sus cercanías, ya que, la cooperativa es la principal organización a la que acuden quienes desean obtener liquidez y facilidades de financiamiento para emprender o fortalecer sus negocios, especialmente porque la Cooperativa de Ahorros, Créditos y Servicios Múltiples de los Integrantes de las Fuerzas Armadas constituye una vía de entrada, donde muchos socios y sus familiares encuentran el camino más accesible para desarrollarse en diversos órdenes. La institución más que un agente financiero se ha transformado en una pieza esencial para llevar soluciones sociales y educación en general a sectores que antes no habían sido tomados en cuenta para tales fines.

Otro de los aportes que desarrolla la COOPINFA está representado por el rol fundamental en la creación de empleos y en el desarrollo económico y social de los lugares en los que no se encuentra por medio de la presencia de sus puntos de negocios, una forma de expresarlo es que el empleo en o dentro del ámbito de COOPINFA concierne a más de 200 personas entre las diferentes jerarquías militares y del ámbito civil, (ver gráfico 9) contribuyendo así a la erradicación de la pobreza y creando oportunidades de empleo al brindar empleos asalariados directos a sus miembros militares activos o retirados y civiles, empleo por cuenta propia para los emprendedores y empleo indirecto por medio de la propagación de sus actividades generadoras de ingresos en y el entorno de las comunidades cercanas, (Gerencia de Gestión Humana, 2025).

Gráfico 9
Relación de colaboradores civiles y militares en COOPINFA

CANTIDAD DE COLABORADORES CIVILES Y MILITARES	
CONTRATADOS	**CANTIDAD**
MILITARES ACTIVOS	58
MILITARES RETIRADOS	12
COLABORADORES	134
TOTAL	204

Nota: Gerencia de Gestión Humana, COOPINFA

Esta cooperativa juega un papel clave en el apoyo al bienestar económico de los militares, ya que cuenta con una estructura organizativa y modelo de gobernanza funcional, que abarca entre otros aspectos:

1. **Gobernanza democrática**: Las cooperativas se rigen de manera democrática, con los miembros participando activamente en la toma de decisiones.
2. **Estructura descentralizada**: Cuentan con sucursales a nivel local para brindar servicios cercanos a los miembros.
3. **Liderazgo militar**: Los puestos de liderazgo son ocupados por personal activo o retirado de las Fuerzas Armadas.

La cooperativa de las Fuerzas Armadas apoya el desarrollo económico y social de todos sus socios y colaboradores como un componente de las relaciones cívico-militares, afirmándose como un poderoso mecanismo de construcción social creado por actores sociales como soluciones específicas para mitigar las vulnerabilidades y riesgos asociados a los sistemas financieros tradicionales a través de la cooperación interinstitucional con los organismos del Estado y privados, aprovechando su presencia en todo el territorio nacional.

Entre los beneficios que se destacan y que son recibidos por los miembros de las Fuerzas Armadas se pueden observar los siguientes:

a. **Tasas preferenciales**: Los miembros obtienen tasas de interés más bajas en préstamos y cuentas de ahorro.
b. **Asesoramiento financiero**: Reciben orientación experta sobre planificación financiera y gestión del dinero.
c. **Apoyo a la comunidad**: La cooperativa organiza actividades y programas de apoyo para las familias militares.
d. **Seguridad y confianza**: Los miembros se sienten seguros y respaldados por una institución comprometida con su bienestar.

La educación regla de oro para la Cooperativa

COOPINFA ha adoptado la educación como "Regla de Oro" por excelencia, incorporando dicho principio rector como la base fundamental para el desarrollo y fortalecimientos del sector a través de la capacitación continua, alcanzando así mantener el enfoque en el fortalecimiento de su eje misional, la organización y ejecución de actividades de formación de sus miembros y la destinación de recursos para eventos que promuevan la cultura solidaria-cooperativa y afines.

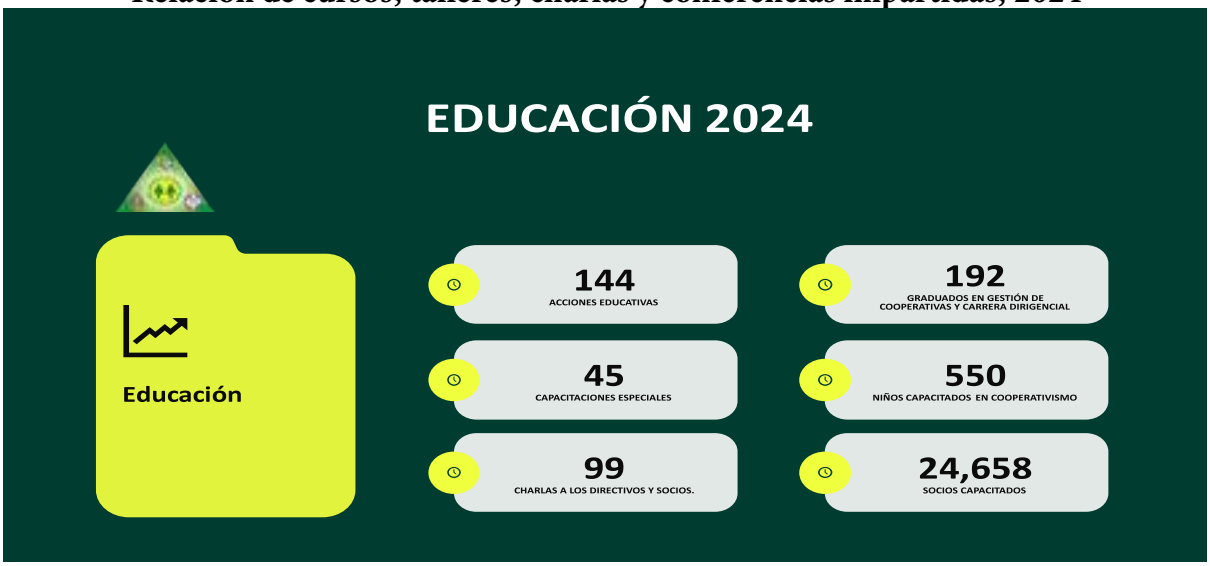
Durante más de una década el propósito fundamental de COOPINFA ha sido ampliar las contribuciones que como cooperativa son dirigidas al desarrollo de nuestros integrantes; es decir, la forma en que colaboramos para transformar la realidad y las condiciones de vida de nuestros socios y sus familias, alcanzando a través de la educación, formación e información crear mejores condiciones de vida y prosperidad colectiva, convirtiéndose en un factor fundamental en su operación, desarrollo, crecimiento y sostenibilidad, tanto de las fuerzas armadas como de la sociedad.

Para lograr estas metas COOPINFA ha recorrido toda la geografía nacional haciendo un acercamiento con los socios y llevándoles a sus guarniciones de origen diplomados, pasantías, congresos, talleres, simposios, seminarios y conferencias (ver gráficos 10 y 11) con el objetivo de que conozcan de primera mano el modelo cooperativo, así como también aquellas acciones formativas transversales orientadas a fortalecer sus conocimientos

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

en el correcto manejo de la economía, finanzas y liderazgo, así como también aquellas que contribuyan a su desarrollo y superación personal, entre estas se pueden citar: Gestión de Riesgos, Ciberseguridad, Inteligencia Emocional, Trabajo en Equipo, Inteligencia Artificial, entre otros. Abarcando así, un enfoque multidimensional cooperativista en lo educacional, cultural, social, deportivo, ambiental y económico y así poder completar la visión del Consejo de Administración (Gerencia de Educación, Bienestar y Responsabilidad Social, 2025).

Gráfico 10
Relación de cursos, talleres, charlas y conferencias impartidas, 2024



Nota: Gerencia de Educación, Bienestar y Responsabilidad Social, COOPINFA.

Gráfico 11
Relación de cursos, talleres, charlas y conferencias impartidas, 2025

CAPACITACIÓN	CANTIDAD	LUGAR	CAPACITADOS
Diplomados	3	EGAEE Salón Restauración, MIDE	83
Congresos	1	Colombia	11
Pasantía	1	Panamá	2
Talleres	64	1ra. Brig. -7ma. Brig. ERD Brigada de Apoyo de servicio Brigada de Apoyo de Combate ESCAFRONT Colegio Ntra. Sra. Perpetuo Socorro, FARD Colegio San Miguel Arcángel, ERD Bases Navales Las Calderas y Boca Chica Base Aérea Puerto Plata CUSEP CESMET	3,164
Simposios	1	Salón Prof. Paulino Pérez, COOPNAMA	6

CAPACITACIÓN	CANTIDAD	LUGAR	CAPACITADOS
Seminario	2	The Inter-American Center of Business Administration, Accounting and Public Management, LLC., Madrid España Salón Multiusos, Club Banreservas	12
Conferencia	1	Cine Auditorio Juan Isidro Pérez (ISSFFAA)	214
TOTAL	**73**		**3,492**

Nota: Gerencia de Educación, Bienestar y Responsabilidad Social, COOPINFA.

Adicionalmente, la promoción de la educación y la formación dentro de COOPINFA fortalece el capital humano de sus miembros y, por extensión, del país. A través de programas de capacitación y talleres, se empodera a los asociados con nuevas habilidades y conocimientos que les permiten mejorar sus oportunidades económicas y su participación en la sociedad. Esta inversión en el desarrollo personal y profesional se alinea con los objetivos de desarrollo sostenible, contribuyendo a la reducción de la pobreza y la promoción del crecimiento económico inclusivo (Programa de las Naciones Unidas para el Desarrollo, 2022).

Figura 1
Programa de ejecución de capacitación y talleres para miembros activos de las Fuerzas Armadas

Nota: Gerencia de Educación, Bienestar y Responsabilidad Social, COOPINFA.

La educación cooperativa ha tocado casi todos los estamentos de las Fuerzas Armadas, desde el Ministerio de Defensa y sus dependencias, las Unidades Mayores Terrestres, Navales y Aéreas con sus unidades subordinadas o que las componen de las tres ramas castrenses hasta las Escuelas de Comando y Estado Mayor, las Academias Militares y las Direcciones de Educación, Capacitación y Entrenamiento de estas, como a la parte civil siendo esta las cooperativas hermanas. Pero también COOPINFA ha incluido capacitaciones transversales afines a los perfiles profesionales de nuestros socios acorde a los desafíos presentes para brindarles a sus socios herramientas para su superación personal.

Próximamente la cooperativa estará llegando a todos los programas de la Universidad Nacional para la Defensa (UNADE), tocando todos los niveles de mando educativos abarcando todas las fuerzas armadas, así como los programas de las universidades e institutos técnicos con las que poseerá acuerdos edu-

DOI: https://doi.org/10.59794/rscd.2025.v11i11.145

cativos, para esto ya COOPINFA ha sometido a través del Ministerio de Defensa dos programas educativos sobre cooperativismo (uno de nivel de diplomado para la Maestría en Seguridad y Defensa y uno tipo taller para las especialidades en Geopolítica y Derechos Humanos, lo mismo para las universidades e institutos técnicos), (COOPINFA, 2025).

Un renglón nuevo que la cooperativa ha iniciado es la capacitación de la matrícula de los niños de 8° y 3° del Colegio Militar Nuestra Señora del Perpetuo Socorro, Fuerza Aérea de República Dominicana (FARD) y del Centro Educativo Militar San Miguel Arcángel del Ejército de República Dominicana (ERD), cumpliendo con la Ley 28-63 (1963), que obliga a impartir cooperativismo infantil en estos niveles, ensenándoles las bondades del modelo cooperativista y fomentando en ellos la cultura del ahorro.

COOPINFA y la responsabilidad social

En un entorno donde los valores suelen inclinarse hacia lo individual por sobre lo colectivo, prefiriendo la competencia sobre la cooperación y las jerarquías sobre las relaciones democráticas, el modelo cooperativo surge como una opción para atender las desigualdades sociales transformándolas en oportunidades de desarrollo integral de su entorno y en producción y distribución colectiva de riqueza, (Zalazar, 2021) y en la institución la responsabilidad social ha sido adoptada como una respuesta consciente y obligatoria, teniendo como propósito el bienestar de los socios, colaboradores y sus familiares, pero también haciéndolo extensivo al entorno que la rodea y a la comunidad.

En ese tenor, la COOPINFA ha decidido desarrollar su responsabilidad social por medio de la implementación de una metodología que se sustente en la elaboración del Balance Social y el cumplimiento de los principios cooperativos, esta planificación funciona a partir de las necesidades detectadas y los recursos disponibles de COOPINFA para poder resolverlas, se han diseñado y aprobado 10 programas de desarrollo social los cuales son:

- Programa Social de Educación,
- Programa Social de Salud,
- Programa Social de Vivienda (reparaciones),
- Programa Social de Actividades Recreativas, Deportivas y Culturales,
- Programa Social de Alimentación, Hogar y Vehículos,
- Programa Social de Apoyo a la Comunidad e Instituciones,
- Programa Social de Protección al Medio Ambiente,
- Programa Social de Equidad de Género,
- Programa Social Fúnebre y
- Programa Social de Emprendimiento, (Gerencia de Educación, Bienestar y Responsabilidad Social, 2024).

Partiendo de estas acciones, COOPINFA ha efectuado un ejercicio de gestión social responsable consistente en donaciones igualitarias a las tres instituciones castrenses y las unidades que las conforman, como a sus miembros y familiares, como también prestamos solidarios para atender distintas necesidades entre las que podemos citar para vivienda, salud, educación y hogar, atendiendo sus necesidades y mejorando así la calidad de vida de los mismos, sus familiares, colaboradores y la comunidad, (López, 2020).

De la misma manera, que la educación permite afianzar la responsabilidad que tiene

DOI: https://doi.org/10.59794/rscd.2025.v11i11.145

COOPINFA en cuanto a la intervención social que debe realizar para reivindicar socialmente las necesidades y requerimientos de sus socios y familiares, esta siempre extenderá una mano amiga especialmente a las necesidades que el orden social establecido muchas veces ignora o desprecia (ver gráfico 12).

Gráfico 12
Relación de programas, donaciones y ayudas de desarrollo social

Nota: Gerencia de Educación, Bienestar y Responsabilidad Social, COOPINFA.

La Cooperativa de Ahorros, Créditos y Servicios Múltiples de los Integrantes de las Fuerzas Armadas dentro de su programa de actividades recreativas, deportivas y culturales promueve el desarrollo y fomento a la cultura, específicamente en el apoyo de obras literarias de nuestros autores militares, (ver gráfico 13) haciéndose COOPINFA cargo de la impresión de los ejemplares, auspicio de la presentación de la obra, además de la adquisición de dichos ejemplares para luego ser diseminados en todas las direcciones, academias y escuelas militares, impulsando así la difusión de sus obras para fortalecer la ciencia del saber dentro de los miembros de las Fuerzas Armadas.

Gráfico 13
Relación de libros adquiridos de autores militares

ADQUISICIÓN Y PATROCINIO DE LIBROS.		
TITULO	AUTOR	ADQUIRIDOS
Trujillismo	Eurípides Antonio Uribe Peguero	200
Héroes Militares que nadie conoció		200
El deporte como instrumento de desarrollo	Gilberto Soriano Román	200
Academia Militar y Ejército de República Dominicana	José Guadalupe Almonte Sánchez	200

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

ADQUISICIÓN Y PATROCINIO DE LIBROS.		
TITULO	AUTOR	ADQUIRIDOS
La Fuñenda	José Miguel Soto Jiménez	200
El Doctor		200
¡Machete, Carajo!		200
Los que mataron el miedo		200
Fundamentos de Oratoria Castrenses	Justo Fernando Méndez Romero	200
100 amores, 100 Poemas y Tú	Nicolás Rodríguez Ramírez	50
Desenfreno Patria y Lodo		200
1000 curiosidades		200
Cuentos de Guardia	Patricia Blanco	100
El Estado Mayor	Vicente Mota Medina	200
TOTAL		2,550

Nota: Gerencia de Educación, Bienestar y Responsabilidad Social, COOPINFA.

También COOPINFA desarrolla grandes esfuerzos para lo que considera uno de sus grandes compromisos siendo este el cuidado y preservación del medio ambiente, a través de una labor de reforestación con el objetivo de demostrar su compromiso al contribuir con el medio ambiente y al desarrollo sostenible del país, dando muestras de compromiso con los principios cooperativos de Educación, responsabilidad social y cuidado del medio ambiente (ver figura 2).

Figura 2
Impacto de la responsabilidad social

Nota: Gerencia de Educación, Bienestar y Responsabilidad Social, COOPINFA.

Finalmente, la filosofía de responsabilidad social de COOPINFA se extiende a la protección del medio ambiente, promoviendo prácticas sostenibles y apoyando iniciativas que buscan la preservación de los recursos naturales. Esta visión integral del desarrollo, que abarca lo económico, lo social y lo ambiental, consolida a COOPINFA como un actor fundamental en la construcción de un futuro más equitativo y próspero para la República Dominicana (ver gráfico 14).

DOI: https://doi.org/10.59794/rscd.2025.v11i11.145

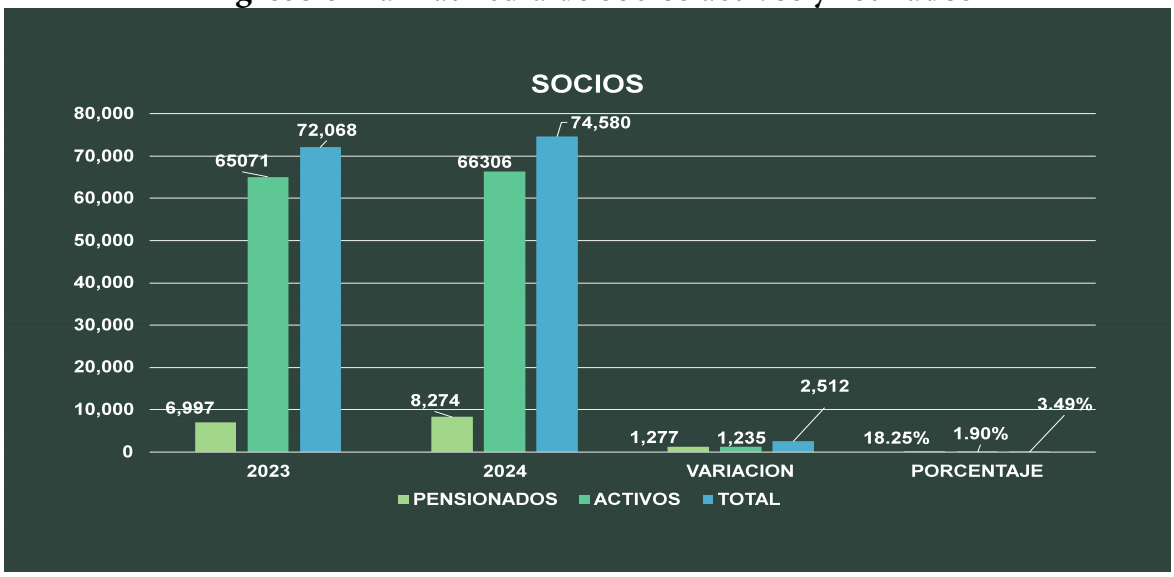
Gráfico 14
Relación de árboles sembrados y proyectados

REFORESTACIÓN		
AÑO	SEMBRADOS	LUGAR
2023	200	Humedales del Ozama
2024	200	Humedales del Ozama
2025	300 proyectados	Humedales del Ozama
TOTAL	700	

Nota: Gerencia de Educación, Bienestar y Responsabilidad Social, COOPINFA.

El año 2024 fue el período de tiempo de mayor ingreso de socios a nuestra matricula, sobre todo en el segmento de los socios retirados, ya que por las acciones que la cooperativa lleva a cabo pudieron comprobar que es una institución aliada y con deseos de que estos continúen una vida productiva al preocuparse por ellos después de haber dedicado la mayor parte de su vida a las fuerzas armadas, convirtiendo a la COOPINFA en una institución a la cual pueden acudir en caso de necesidad de cualquier índole y mostrarles el respeto que merecen por haber servido de manera honorable en las fuerzas armadas, dicho aumento se produjo casi en aproximadamente 2,512 socios, entre activos y retirados (ver gráfico 15).

Gráfico 15
Ingreso en la matrícula de socios activos y retirados



Nota: Gerencia Financiera, COOPINFA.

COOPINFA, SUS PRODUCTOS Y SERVICIOS

Una particularidad que COOPINFA posee es que estimula y apoya a sus socios para que incursionen en actividades generadoras de ingresos para mejorar sus medios de vida, otorgando prestamos solidarios de emprendimiento a socios con pequeñas y medianas empresas, ayudándolos a crear riquezas para

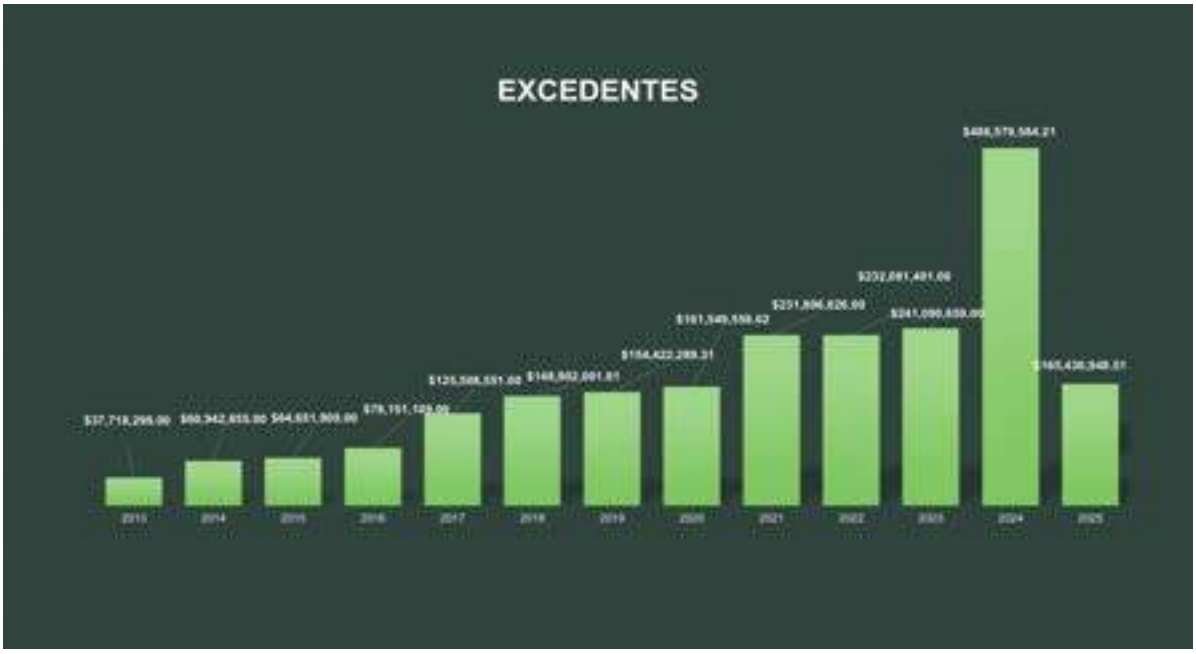
RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

ellos, sus familias y sus comunidades (ver gráficos anexos).

Dentro de estos productos de ahorros, préstamos y servicios múltiples COOPINFA a diseñado una gama de soluciones crediticias consistentes en Ahorros Retirables, Certificados Financieros, Préstamos Personales, Préstamos Comerciales, Préstamos para vehículos, Préstamos para Pólizas de Seguros, Servicios de Previsión Funeraria, Servicios con Agencias de Viajes y Préstamos para Pequeñas y Microempresas (MYPES) con el propósito de que sus socios puedan contar con acceso a productos y servicios que complementen sus necesidades financieras, así como fomentar el desarrollo social y económico en todo el país por medio de la cooperación y la solidaridad.

Uno de los factores que motiva a los socios de la Cooperativa de Ahorros, Créditos y Servicios Múltiples de los Integrantes de las Fuerzas Armadas (COOPINFA) y que a su vez fortalece la confianza de sus socios, se denota en que durante el ejercicio financiero 2024 se acreditaron RD$241,090,659.00 entre los afiliados de la entidad, que fueron depositados el pasado 30 de enero en las cuentas de los beneficiarios, evento este que se cumple mediante un proceso completamente transparente en la distribución de sus excedentes a través de los años (ver gráfico 16).

Gráfico 16
Relación de distribución de excedentes



Nota: Gerencia Financiera, COOPINFA.

EN COOPINFA la transparencia el manejo de los recursos es fundamental para que los socios militares y sus familias puedan entender con claridad y precisión el destino de los excedentes, fomentando en estos un sentido de pertenencia y compromiso con la cooperativa. Esta política de apertura y rendición de cuentas no solo refuerza la estabilidad financiera de la entidad, sino que también tiene un impacto directo en la calidad de vida de sus socios. Al disponer de recursos destinados a fortalecer el desarrollo económico y social, se mejora el acceso a servicios financieros de calidad y se impulsa el desarrollo de iniciativas

DOI: https://doi.org/10.59794/rscd.2025.v11i11.145

que contribuyen al bienestar integral de los socios integrantes de las Fuerzas Armadas y de sus familiares.

Asimismo, la transparencia en la distribución de excedentes promueve una participación activa en la toma de decisiones de los procesos, lo que incrementa la confianza de los socios en la gestión de la cooperativa. Con cada distribución que se realiza, COOPINFA reafirma que el crecimiento sostenible es posible cuando se trabaja con integridad, responsabilidad y un compromiso firme hacia el bienestar de su comunidad.

Conclusiones

Este artículo constituye un interesante aporte del cooperativismo en el contexto mundial y el auge de la disminución de la brecha y desigualdad en el ámbito militar. La metodología usada para desarrollar este artículo involucró la revisión exhaustiva de fuentes secundarías sobre cooperativismo y cooperativas, luego se procedió a compilar datos cualitativos y cuantitativos en las áreas pertinentes del escrito y luego analizarlos y convertirlos en información de interés sobre la labor que realiza COOPINFA al servicio de sus socios y la comunidad, dando como resultado un artículo que expone de manera clara y concisa la naturaleza solidaria de la cooperativa.

La Cooperativa de Ahorros, Créditos y Servicios Múltiples de los Integrantes de las Fuerzas Armadas (COOPINFA) es el producto de la visión de un grupo de oficiales y alistados preocupados por el bienestar de los miembros de las fuerzas armadas, entendiendo que el modelo cooperativo es una opción más beneficiosa para disminuir las vulnerabilidades a las que están expuestos nuestros socios, ya que muchos de estos por sus perfiles de profesión no son atractivos financieramente para el sistema financiero tradicional, por lo que deben acudir a la solidaridad que representa COOPINFA.

Las cooperativas son el espacio de inclusión social para la gente que ha sido olvidada por la sociedad de mercado capitalista, para las cooperativas, el éxito y progreso están más allá de datos y gráficas. Lo saben las familias que han podido mejorar su condición de vida a través de la adquisición de un sin número de facilidades entre las que podemos considerar tres áreas principales: educación y capacitación, salud y bienestar, y gestión financiera y emprendimiento. Al combinar estas estrategias con las mejoras materiales que ya están realizando, las familias pueden construir una base sólida para una calidad de vida sostenible y en constante mejora.

En pocas palabras, COOPINFA desde el punto de vista sociológico se está convirtiendo en un constructor social, el cual fue creado por actores sociales como una solución específica para resolver los problemas que surgen ante las diferentes eventualidades que se les presentan a nuestros socios, marcando la diferencia para nuestros socios, colaboradores y sus familiares al lograr impactarlos de manera positiva para sean entes productivos dentro de nuestra sociedad, demostrando con estas acciones que COOPINFA siempre estará "Al Servicio del Soldado" pudiendo lograr "Esparcir la semilla de la educación y ayudar a los más necesitados".

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Referencias

Alianza Cooperativa Internacional. (1995). *Declaración sobre identidad cooperativa.* https://ica.coop/es/cooperativas/que-es-una-cooperativa.

Buendía, I., Redjah, Y., & Tremblay, B. (2012). *Las cooperativas de servicios financieros en el continente americano.* [Informe]. https://www.google.com/search?q=cooperativas+financieras.

Concepción, Y. (2015). *Guía educativa Vega Real. Capítulo I: Historia del Cooperativismo.* https://www.cvr.com.do/wp-content/uploads/2017/01/guia-educativa-cooperativismo-modulo1.pdf.

Constitución de la República Dominicana [Const.]. (2015, 10 de julio). *Gaceta Oficial No. 10805.* Santo Domingo, República Dominicana.

COOPINFA. (2025). *Oficio No. 132-2025.* Gerencia de Educación, Bienestar y Responsabilidad Social de la Cooperativa de Ahorros, Créditos y Servicios Múltiples de los Integrantes de las Fuerzas Armadas (COOPINFA).

Gerencia Financiera. (2025). *Balance de Gestión Financiera.* Cooperativa de Ahorros, Créditos y Servicios Múltiples de los Integrantes de las Fuerzas Armadas (COOPINFA).

Gerencia General. (2024). *Balance de Gestión General Financiera.* Cooperativa de Ahorros, Créditos y Servicios Múltiples de los Integrantes de las Fuerzas Armadas (COOPINFA).

Gerencia General. (2025). *Sistema de Registro de socios activos y retirados.* Cooperativa de Ahorros, Créditos y Servicios Múltiples de los Integrantes de las Fuerzas Armadas (COOPINFA).

Gerencia de Educación, Bienestar y Responsabilidad Social. (2024). *Informe de Educación y Responsabilidad Social: Memoria VII Asamblea General Ordinaria de Delegados 2025*. https://consulta.coopinfa.coop.

Gerencia de Educación, Bienestar y Responsabilidad Social. (2025). *Informe de Gestión Educativa y de Responsabilidad Social.* Cooperativa de Ahorros, Créditos y Servicios Múltiples de los Integrantes de las Fuerzas Armadas (COOPINFA).

Gerencia de Educación, Bienestar y Responsabilidad Social. (2024). *Metodología de balance social.* Cooperativa de Ahorros, Créditos y Servicios Múltiples de los Integrantes de las Fuerzas Armadas (COOPINFA).

Gerencia de Gestión Humana. (2025). *Listado de nómina de militares y civiles contratados.* Cooperativa de Ahorros, Créditos y Servicios Múltiples de los Integrantes de las Fuerzas Armadas (COOPINFA).

Gerencia de Gestión Humana. (2025). *Listado General del Personal de COOPINFA*. Cooperativa de Ahorros, Créditos y Servicios Múltiples de los Integrantes de las Fuerzas Armadas (COOPINFA).

Gerencia de Negocios y Canales Digitales. (2017). *Resolución 35/2017, Tabla de Préstamos Comerciales.* Cooperativa de Ahorros, Créditos y Servicios Múltiples de los Integrantes de las Fuerzas Armadas (COOPINFA).

González, Y., Mora, R., & López, S. (2024). Capacidades militares en el ámbito europeo de la defensa (Vol. 1, cap. 8, pp. 173–182). En *El reto industrial*. Editorial Ingeniería de Sistemas para la Defensa de España.

Guilarte, E., & Chávez, L. (2023). Actualidad de la cooperativa y su identidad: Análisis teórico y práctico. *Revista Cooperativismo y Desarrollo (COODES)*. https://coodes.upr.edu.cu/index.php/coodes/article/view/560

Guerrero, S. (2023, julio 21). Relaciones civiles y militares y los nuevos roles de la defensa en la época actual. *El Nuevo Diario*. https://elnuevodiario.com.do/relaciones-civiles-y-militares-y-los-nuevos-roles-de-la-defensa-en-la-epoca-actual.

International Cooperative Alliance (ICA). (2021). *¿Qué es una cooperativa?* https://ica.coop/es/cooperativas/que-es-una-cooperativa

Ley 28-63. (1963, enero 1). Que declara obligatoria la enseñanza del cooperativismo en las escuelas. *Gaceta Oficial (No. 8799)*. Santo Domingo, República Dominicana.

Ley 127-64. (1964, enero 27). Sobre asociaciones cooperativas y su reglamento. *Gaceta Oficial No. 8828*. Santo Domingo, República Dominicana.

Ley 1-12. (2012, enero 26). Estrategia Nacional de Desarrollo 2030. *Gaceta Oficial No. 10656*. Santo Domingo, República Dominicana.

Ley 139-13. (2013, septiembre 19). Orgánica de las Fuerzas Armadas Dominicana. *Gaceta Oficial No. 10728*. Santo Domingo, República Dominicana.

López, V. (2020). Cooperativismo como un modelo de desarrollo socioeconómico más humano. *Revista FAECO Sapiens,* 3(2), 40–42. https://revistas.up.ac.pa/index.php/faeco_sapiens/article/view/1363/1120

Ministerio de Defensa (MIDE). (2017). *Plan estratégico institucional (PEI) 2017–2020*. https://mide.gob.do/wp-content/uploads/2021/06/Plan-Estrategico-2017-2020-MIDE.pdf

Ministerio de Defensa (MIDE). (2022). *Rol de las Fuerzas Armadas en el desarrollo nacional*. https://unade.edu.do/wp-content/uploads/2023/10/Libro-Blando-comprimido.pdf.

Presidencia del Consejo de Administración. (2023). *Resolución 35/2023, del Comité Ejecutivo, Tabla de Préstamos*. Cooperativa de Ahorros, Créditos y Servicios Múltiples de los Integrantes de las Fuerzas Armadas (COOPINFA).

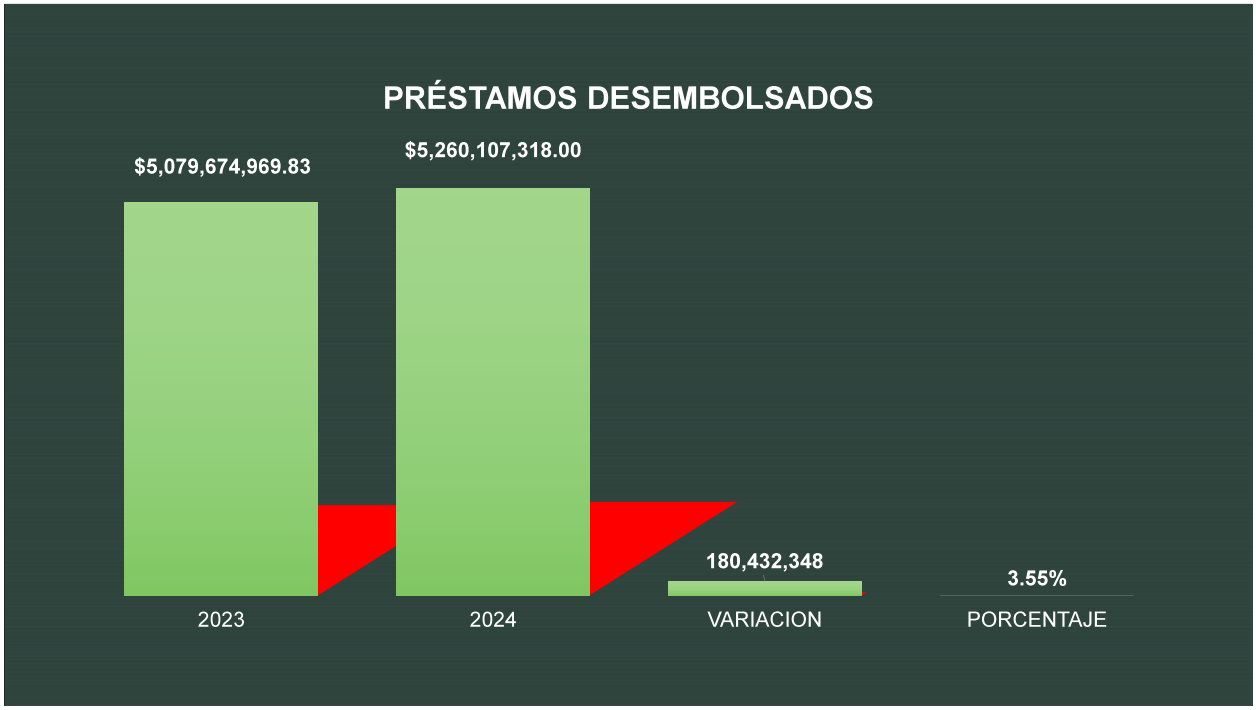
Programa de las Naciones Unidas para el Desarrollo (PNUD). (2022). *Informe sobre desarrollo humano 2021/2022*. https://www.undp.org/sites/g/files/zskgke326/files/2022-09/hdr2021-22overview.pdf

Ressel, A. (2013). *Manual teórico-práctico de introducción al cooperativismo*. Universidad Nacional de La Plata. https://www.econo.unlp.edu.ar/frontend/media/77/10177/e1ff-4382da72b51e0ea7011e0f436299.pdf

Zalazar, S. (2021). Las cooperativas como organizaciones inteligentes para disminuir la desigualdad social. ICAP: *Revista Centroamericana de Administración Pública, 80*, 86–98. https://www.infocoop.go.cr/sites/default/files/2021-06/ICAP-Revista-80-Doc-2-Salazar.pdf.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

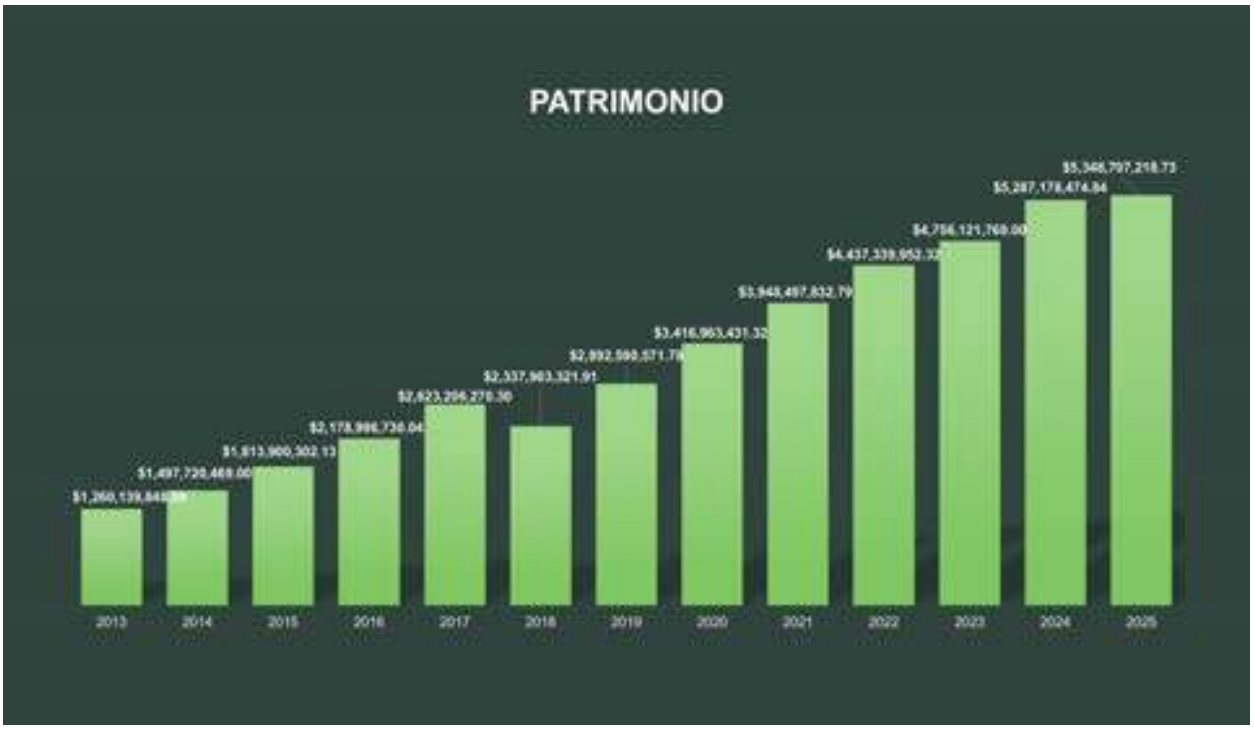
ANEXOS



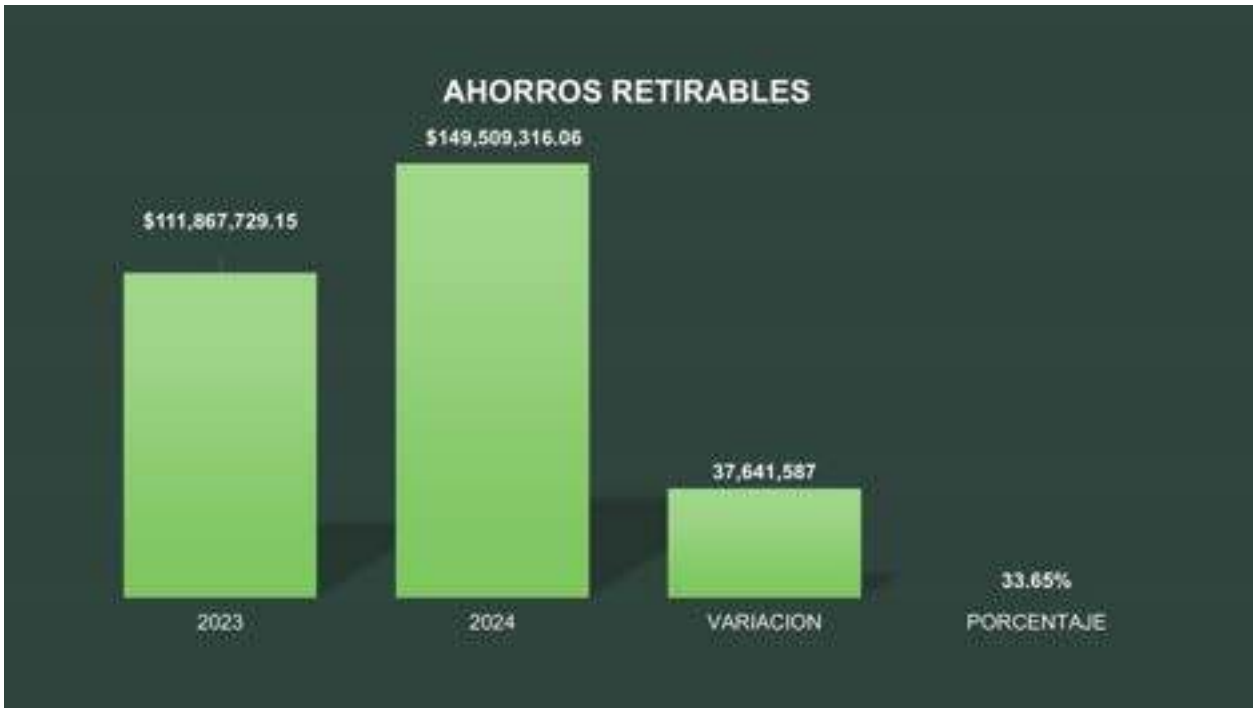
Nota: Gerencia Financiera, COOPINFA.

Nota: Gerencia Financiera, COOPINFA.

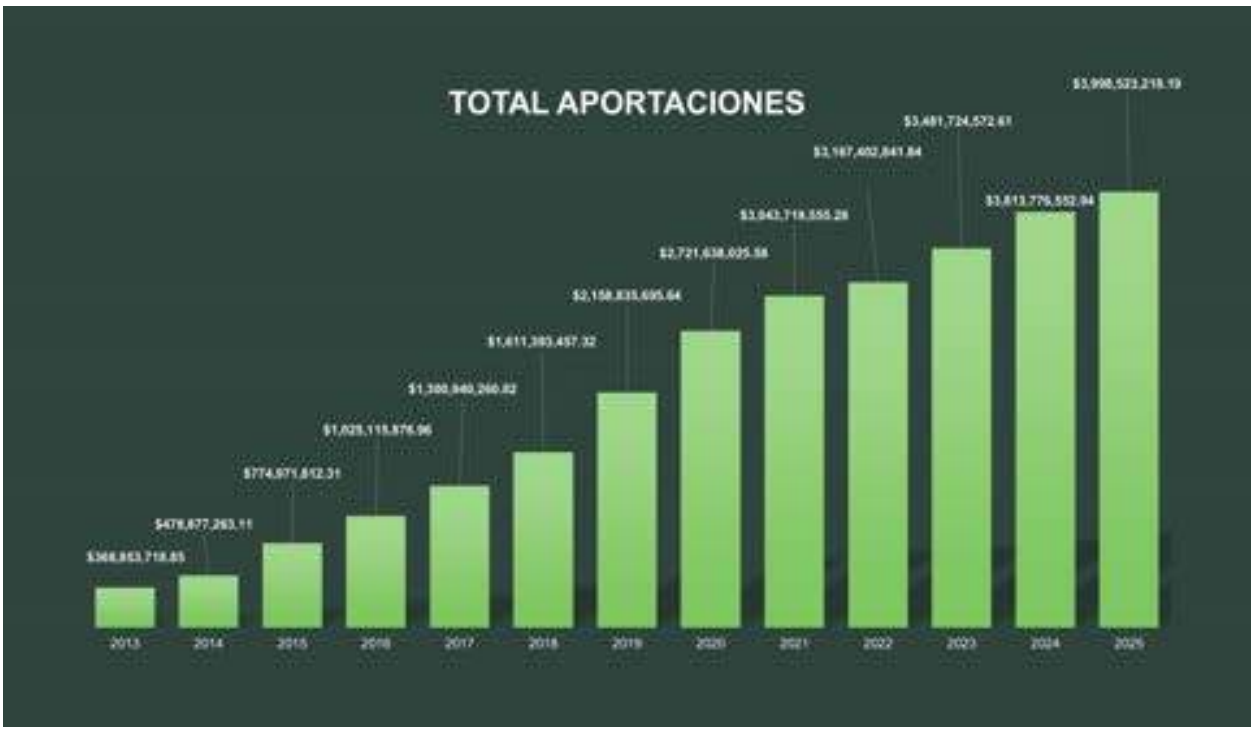
DOI: https://doi.org/10.59794/rscd.2025.v11i11.145



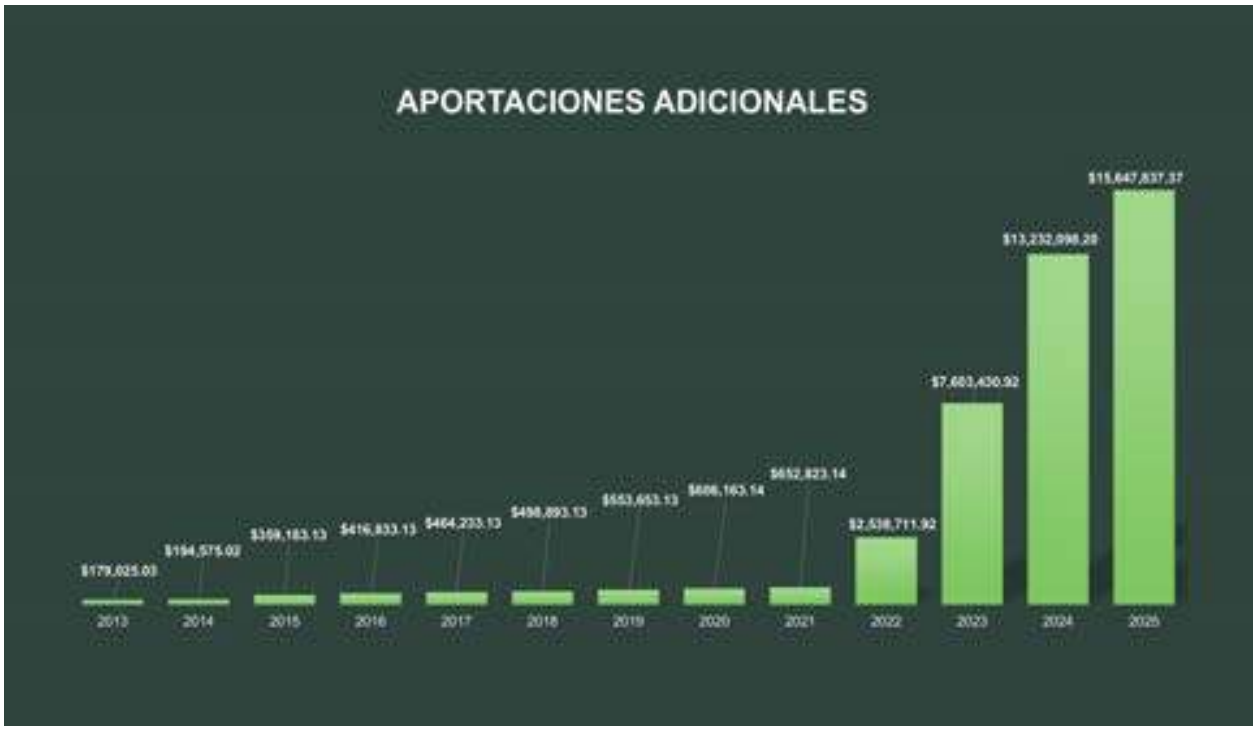
Nota: Gerencia Financiera, COOPINFA.



Nota: Gerencia Financiera, COOPINFA.



Nota: Gerencia Financiera, COOPINFA.



Nota: Gerencia Financiera, COOPINFA.

DOI: https://doi.org/10.59794/rscd.2025.v11i11.145

Nota: Gerencia Financiera, COOPINFA.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

La defensa nacional como imperativo constitucional en República Dominicana tras la reforma del 2010[1]

National Defense as a constitutional imperative in the Dominican Republic after the reform of 2010

Recibido: 07/ 05 / 2025 | Revisado: 12 / 08 / 2025 | Aprobado: 30 / 09 / 2025
DOI: https://doi.org/10.59794/rscd.2025.v11i11.146

General de brigada Vicente Mota Medina, ERD
República Dominicana

Correo: vmotamedina@gmail.com

ORCID: https://orcid.org/0009-0004-2633-7266

Afiliación: Universidad Nacional para la Defensa

El autor es general de brigada del Ejército de República Dominicana. Es Doctorando por la Universidad Internacional Iberoamericana de México; Magíster en Seguridad y Defensa Nacional, Escuela de Graduados de Altos Estudios Estratégicos de la UNADE; Magíster en Derecho Empresarial y Legislación Económica por la PUCMM; Magíster en Derecho Procesal Civil por la PUCMM; Licenciado en Ciencias Militares, Academia Militar del Ejército de República Dominicana, UNADE; Licenciado en Derecho, Universidad Eugenio María de Hostos; Diplomado en Comando y Estado Mayor, IMES. Docente e investigador, Universidad Nacional para la Defensa, "General Juan Pablo Duarte y Díez" (UNADE).

1 Oportuno es destacar que, este escrito es un artículo asociado a la tesis doctoral del General de Brigada Mota Medina para obtener el título de Doctor en Derecho, en fase de culminación por la Universidad Internacional Iberoamericana de México, agradeciendo la labor del Dr. Alejandro José Gutiérrez Dávila, quien es el director de tesis asignado por la universidad.

DOI: https://doi.org/10.59794/rscd.2025.v11i11.146

Dr. Alejandro José Gutiérrez Dávila
Guatemala

Correo: alejandrojgd@gmail.com

ORCID: https://orcid.org/0009-0008-2421-4915

Afiliación: Universidad San Carlos de Guatemala

El autor es Postdoctorado en Filosofía del Derecho egresado de la Universidad de Hawái, Estados Unidos de América. Doctor en Filosofía egresado de la Universidad de Hawái, Estados Unidos de América. Doctor en Derecho egresado de la Universidad de San Carlos de Guatemala, con distinción Cum Laude. Maestro Scientiae en Derecho Penal egresado de la Universidad de San Carlos de Guatemala. Licenciado en Ciencias Jurídicas y Sociales Egresado de la Universidad de San Carlos de Guatemala. Abogado, Notario. Ex Letrado de la Corte Suprema de Justicia de Guatemala. Catedrático de Maestrías y Doctorados en la Universidad de San Carlos de Guatemala y otras universidades de Guatemala. Conferencista nacional en internacional en temas de Derecho Constitucional, Derecho Penal, Filosofía del Derecho y otros. Director de Tesis Doctorales en la Universidad Internacional Iberoamericana de México -UNINI. Director de Tesis de maestría en la Universidad Internacional de la Rioja de España -UNIR. Catedrático del curso Teoría General del Derecho en la Universidad Internacional de la Rioja de España -UNIR. Director de la Academia de Alto Rendimiento en Ciencias Jurídicas FRONESIS, desde el año 2006. Autor de varios Libros: "Fundamentos Filosóficos de la Constitución Política de la República de Guatemala", Primera Edición, Ciudad de Guatemala. Marzo 2020. "Fundamentos Filosóficos del Amparo y Demás Garantías Constitucionales en Guatemala", Primera Edición, Ciudad de Guatemala, septiembre 2020. "Homo Spiritus: El Ser Humano Ético", Primera Edición, Ciudad de Guatemala. Abril 2021. "Teoría del Delito aplicada al Proceso Penal guatemalteco", 1ra Edición, Ciudad de Guatemala. Noviembre 2022. "Interpretación y argumentación constitucional". 1ra Edición. Ciudad de Guatemala: septiembre 2024. "Teoría del derecho y del Estado en Guatemala". 1ra Edición. Ciudad de Guatemala: marzo 2025. "Tratado de Lógica Jurídica I y II". Primera Edición. Ciudad de Guatemala: septiembre 2025. Autor de la Novela literaria "Existencia". Primera Edición. Ciudad de Guatemala: mayo 2024.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Resumen

El presente ensayo analiza la configuración del imperativo constitucional de la Defensa Nacional en el ordenamiento jurídico dominicano tras la reforma constitucional del año 2010, evaluando su articulación normativa, como se materializa este mandato, así como la percepción de la ciudadanía respecto al cambio de modelo constitucional. La defensa nacional como imperativo constitucional se refiere a la obligación establecida en la Constitución de la República Dominicana para que el Estado garantice la protección de su soberanía, integridad territorial, independencia política y estabilidad institucional. Implica que la defensa nacional no es solo una política de gobierno, sino una política de Estado, con visión de largo plazo y que involucra a todos los sectores de la sociedad. Este estudio, de diseño no experimental, con alcance exploratorio-documental, de enfoque cualitativo y que utiliza la hermenéutica como método de interpretación jurídica, aborda cómo se concreta el imperativo constitucional de la defensa nacional en el ordenamiento jurídico dominicano tras la reforma constitucional del 2010, a través de los principales servicios que las Fuerzas Armadas brindan a la nación. Dentro de los hallazgos se destaca la ausencia de una ley sobre Seguridad y Defensa Nacional como falencia del sistema. Como recomendaciones para seguir fortaleciendo este mandato constitucional, se plantea redactar la Ley de Seguridad y Defensa Nacional bajo el paradigma de la seguridad humana, donde la protección estatal priorice derechos fundamentales sobre enfoques tradicionales de seguridad nacional sin desmedro de esta última.

Palabras clave: Defensa nacional, fuerzas armadas, imperativo constitucional, seguridad nacional

Abstract

This essay focuses on analyzing the configuration of the constitutional imperative of National Defense in the Dominican legal system after the constitutional reform of 2010, evaluating its normative articulation, how this mandate materializes, as well as the perception of citizens regarding the change of constitutional model. National defense as a constitutional imperative refers to the obligation established in the Dominican Constitution for the State to guarantee the protection of its sovereignty, territorial integrity, political independence, and institutional stability. It implies that national defense is not only a government policy, but a state policy, with a long-term vision and that involves all sectors of society. This study, of non- experimental design, with exploratory-documentary scope, with a qualitative approach, whose social science research is a discipline that is responsible for studying social phenomena and their relationship with society and that uses hermeneutics as a method of legal interpretation that addresses how the constitutional imperative of national defense is concretized in the Dominican legal system after the constitutional reform of 2010, through the main services that the Armed Forces provide to the nation. Among the findings, the absence of a law on National Security and Defense stands out as a failure of the system. As recommendations to continue strengthening this constitutional mandate, it is proposed to draft the National Security and Defense Law under the paradigm of human security, where state protection prioritizes fundamental rights over traditional approaches to national security without detriment to the latter.

Keywords: National defense, armed forces, constitutional imperative, national security

DOI: https://doi.org/10.59794/rscd.2025.v11i11.146

Introducción

La defensa nacional como imperativo constitucional se refiere a la obligación establecida en la Constitución de la República Dominicana para que el Estado garantice la protección de su soberanía, integridad territorial, independencia política y estabilidad institucional. Es una función esencial e indelegable del Estado dominicano, que se expresa en la existencia y misión de las Fuerzas Armadas, las cuales están constituidas para defender el país ante amenazas externas o internas, mantener la paz y el orden constitucional, y cooperar con otras instituciones del Estado cuando sea necesario.

Este imperativo constitucional implica que la defensa nacional no es solo una política de gobierno, sino una política de Estado, con visión de largo plazo y que involucra a todos los sectores de la sociedad. La defensa nacional se basa en principios como el respeto al Derecho Internacional, la subordinación de las Fuerzas Armadas a la autoridad civil democrática, y la necesidad de mantener una capacidad militar adecuada para salvaguardar los intereses nacionales en los espacios terrestres, marítimos y aéreos, así como cumplir con compromisos internacionales de paz y seguridad.

El objetivo del presente ensayo es analizar cómo la reforma constitucional de 2010 redefinió y fortaleció la defensa nacional como una obligación jurídica prioritaria para el Estado dentro de un contexto multidimensional. En concreto, el presente trabajo investigativo aborda la siguiente pregunta: ¿Cómo se configura el imperativo constitucional de la defensa nacional en el ordenamiento jurídico dominicano tras la reforma constitucional del 2010? De dónde surgen las siguientes interrogantes: ¿Cuál es el marco constitucional y legal actual de la defensa nacional dominicana? ¿Cuáles son los principales servicios con que las Fuerzas Armadas Dominicanas concretan el imperativo constitucional de la defensa nacional?

Esta investigación se desarrolla bajo un diseño no experimental, de alcance exploratorio- descriptivo con enfoque cualitativo, utilizando la hermenéutica como método de interpretación jurídica. Se fundamenta en una revisión documental exhaustiva de la Constitución de la República Dominicana, leyes complementarias, reglamentos, jurisprudencia relevante, así como libros de doctrina para comprender el marco normativo surgido tras la reforma de 2010. Se aplica la observación en campo para registrar de forma directa el funcionamiento, prácticas y dinámicas institucionales vinculadas a la defensa nacional, lo que permite contrastar la normativa con su aplicación real y detectar posibles brechas. La combinación de análisis documental y observación empírica facilita una comprensión integral del fenómeno, enriquecida por la interpretación jurídica y la evaluación contextual de su implementación en el marco del Estado constitucional de derecho.

Marco conceptual

Un imperativo constitucional constituye un mandato normativo que emana directa e inmediatamente de la Constitución —de sus reglas, principios, valores y fines— y que impone obligaciones de acción u omisión a los poderes públicos, y en determinados supuestos a particulares, para asegurar la realización efectiva del orden constitucional. Estos mandatos pueden adoptar la forma de prohibiciones, deberes de protección y de promoción,

así como de "mandatos de optimización" que exigen ser satisfechos en la mayor medida posible según las posibilidades fácticas y jurídicas del caso (Alexy, 1997; Hesse, 1992). En tal sentido, el imperativo constitucional no es una mera directriz política, sino una exigencia jurídicamente vinculante que condiciona la legislación, la administración y la jurisdicción, y sirve de parámetro de control constitucional (Ferrajoli, 2011; Zagrebelsky, 1995).

Así se tiene que, los principales rasgos característicos de este concepto expresan la fuerza vinculante de la Constitución frente a todos los poderes, garantizando su primacía en la producción y aplicación del derecho (Hesse, 1992; Ferrajoli, 2011). Aquí se incluyen deberes de abstención (prohibiciones de lesión de derechos) y deberes de acción (protección, promoción y organización institucional) que condicionan el margen de configuración del legislador (Bernal Pulido, 2007; Ferrajoli, 2011), como se evidencia en el título XII. De las Fuerzas Armadas, de la Policía Nacional y de la Seguridad y Defensa, consagrado en la vigente Constitución dominicana. El incumplimiento de estos imperativos puede dar lugar a control de constitucionalidad tanto por acción como por omisión, así como a exigencias de ponderación y proporcionalidad en la actuación estatal.

La reforma constitucional dominicana de 2010 consolidó un Estado Constitucional de Derecho que pone en el centro la supremacía de la Constitución, la soberanía popular y la protección de los derechos fundamentales. En el contexto filosófico y ético, la nueva constitución se fundamenta en aspectos axiológicos cuyos valores centrales son la dignidad humana, justicia, libertad, igualdad. Este marco jurídico redefine la organización del Estado y establece la subordinación de las Fuerzas Armadas al poder civil, asegurando el respeto a los derechos humanos y la legalidad.

Según Ray-Guevara (2014), tradicionalmente los textos constitucionales latinoamericanos solamente abordaban el tema de las Fuerzas Armadas, sin embargo, a partir de la reforma del 2010, por vez primera en nuestra historia constitucional, se introducen dos elementos importantes: a) se dota de acta de nacimiento constitucional a la Policía Nacional, y b) se introduce un capítulo sobre seguridad y defensa que crea un órgano consultivo que asesorará al presidente de la República, en la formulación de las políticas y estrategias en la materia. Para el pasado presidente del Tribunal Constitucional dominicano, la defensa es la primera función del Estado y ella es inconcebible sin unas Fuerzas Armadas, más o menos organizadas. Ser es defenderse; por tanto, las Fuerzas Armadas forman parte de la cultura de la paz, ya que son un instrumento para alcanzarla, restaurarla o garantizarla.

Las Fuerzas Armadas dominicana, de conformidad con el marco legal nacional al amparo de la constitución vigente, son las instituciones castrenses del Estado, cuya misión fundamental, según el artículo 252 de la Constitución (2024), es defender la soberanía y la integridad territorial del país. Están conformadas, según el artículo 7 de la Ley Orgánica 139- 13, por diferentes ramas o servicios armados, divididos en Ejército de Tierra, Armada (Fuerza Naval) y Fuerza Aérea, cada uno con funciones específicas relacionadas con la defensa terrestre, marítima y aérea, respectivamente.

En República Dominicana, la Seguridad Nacional, es definida como la situación en la cual el Estado tiene garantizada su existencia, la integridad de su patrimonio, sus intereses nacionales, así como su estabilidad, permanencia, soberanía e independencia; con facul-

tad de actuar con plena autonomía en el campo interno y libre de toda subordinación en el campo externo; implementando estrategias y políticas para el permanente desarrollo social, económico y político del pueblo dominicano, a partir de la plena vigencia del Estado social y democrático de derecho (Decreto No. 86-21).

Esta definición de Seguridad Nacional, conforme al referido decreto, adquiere un carácter integral y moderno al destacar no solo la protección de la existencia y soberanía del Estado, sino también su capacidad de actuar de manera autónoma en el ámbito interno y externo, en línea con los principios del Estado Social y Democrático de Derecho; esto implica que la seguridad del país no puede limitarse a la defensa clásica frente a amenazas externas tradicionales sino que debe incorporar una visión multidimensional que abarque la protección de los derechos ciudadanos, asegurando así una estabilidad política, social y económica que garantice no solo la supervivencia, sino también el avance y la calidad de vida del pueblo dominicano en un marco de respeto a los derechos humanos, participación ciudadana y cooperación internacional.

En la evolución conceptual de la seguridad nacional, emerge el concepto de seguridad humana, que se centra en la protección de las personas y sus libertades fundamentales frente a diversas amenazas que afectan su vida cotidiana. Según la Comisión de Seguridad Humana de las Naciones Unidas, la seguridad humana se define como la protección del núcleo vital de todas las vidas humanas, de forma que se mejoren las libertades humanas y la realización de las personas.

La seguridad humana significa proteger las libertades fundamentales, aquellas libertades que son la esencia de la vida. Significa proteger a las personas de situaciones y amenazas críticas y extendidas. Significa utilizar procesos que se basen en las fortalezas y aspiraciones de las personas. Significa crear sistemas políticos, sociales, medioambientales, económicos, militares y culturales que, de forma conjunta, aporten a las personas los fundamentos para la supervivencia, el sustento y la dignidad (Comisión de Seguridad Humana, 2003).

Este enfoque se diferencia de la seguridad tradicional, que se centraba en la protección del Estado frente a amenazas militares, al poner en el centro a la persona y sus derechos, integrando aspectos de desarrollo, derechos humanos y seguridad, en este sentido la Corte Constitucional colombiana al declarar la ley como inexequible la Ley de Seguridad y Defensa Nacional número 684 de 2001, ha señalado al respecto que:

> ...en un Estado democrático, que se encuentra al servicio de la comunidad, las autoridades estatales se reservan el monopolio de la coacción, pero con el deber de ser ellas las garantes de la convivencia pacífica. Y por ello corresponde al Estado proteger y ser garantes de la seguridad de las personas, y no a las personas proteger y ser garantes de la seguridad del Estado. Por el contrario, la presente ley, al incorporar a los particulares al poder nacional, termina convirtiéndolos en garantes de la seguridad institucional, lo cual es inaceptable, pues desnaturaliza la estructura constitucional del Estado colombiano y desconoce el principio de exclusividad de la Fuerza Pública. Y es que una cosa es que las personas tengan ciertos deberes específicos en materia de orden público, y otra muy distinta es que ellas queden integradas en un poder nacional, y se conviertan

> entonces en los garantes de la seguridad institucional y en servidores de los objetivos nacionales que el Ejecutivo indique (Corte Constitucional de Colombia, C- 251/02, 2002).

La lección aprendida fundamental de esta jurisprudencia colombiana para República Dominicana es clara: el Estado Constitucional de Derecho que se asumió como paradigma constitucional en el artículo 7 en la Constitución de la República Dominicana a partir de la reforma del 2010, debe proteger a los ciudadanos, no convertirlos en instrumentos de su propia seguridad institucional, se evidencia aquí esa transición de la seguridad con enfoque estadocentrista a un enfoque antropocentrista, mantener esta distinción es esencial para preservar tanto la legitimidad democrática como la efectiva protección de los derechos fundamentales en el ordenamiento constitucional dominicano, puesto que la seguridad humana abarca múltiples dimensiones como la seguridad económica, alimentaria, de salud, ambiental, personal, comunitaria y política.

En lo que respecta a la Defensa Nacional, según Martínez (2020), la Defensa Nacional es el conjunto de recursos materiales y humanos destinados al cumplimiento de las actividades políticas civiles y militares desarrolladas por el Estado para la protección de la sociedad, de su Constitución, de los valores superiores, principios e instituciones que en esta se consagran, del Estado social y democrático de derecho, del pleno ejercicio de los derechos y libertades, y de la garantía, independencia e integridad territorial.

En 1963 la República Dominicana inicia el denominado Estado social, en el que se reconocen, a través de la Constitución del 63, derechos sociales, así como elementos de la ciudadanía (Ramírez et al, 2011). En lo relativo a la Defensa Nacional, en su artículo 161, se establece, por primera vez, que las Fuerzas Armadas podrán ser llamadas por el Poder Ejecutivo a cooperar en los planes de desarrollo socioeconómico del país. Estos avances muy novedosos para la época fueron revertidos tras el golpe de Estado ocurrido en la madrugada del 25 de septiembre de 1963.

En este sentido, la Defensa Nacional se articula en un ámbito interdisciplinario y multisectorial, integrando recursos materiales y humanos provenientes tanto de las Fuerzas Armadas como de la sociedad civil, lo que evidencia su carácter integral y participativo. Esta integración es necesaria para responder eficazmente a las diversas amenazas, ya sean convencionales o no convencionales, que puedan poner en riesgo la estabilidad política, social y económica del Estado.

Según apuntan Moliner González, J.A. y Caracuel Raya, M.A. citados por Martínez (2020), la Defensa se ejerce con todos los recursos de la nación, pero los medios militares constituyen la punta de lanza para mantener la integridad territorial, para asegurar la vida de la población ante agresiones externas y para protegerla ante riesgos y amenazas de naturaleza y origen cada vez más diverso y difuso.

Las Fuerzas Armadas, a través de su estructura, capacidades y procedimientos, son el principal actor que contribuye a la Defensa Nacional, pero no el único, pues esta compete a las instituciones del Estado y a la sociedad en su conjunto para afrontar conjuntamente los retos y desafíos a la Seguridad Nacional. La Defensa Nacional ya no es un elemento aislado, sino parte indisoluble del más extenso y global concepto de Seguridad Nacional, a cuyo sustento contribuyen conjuntamente,

desde medios militares y de la diplomacia, hasta la cooperación y los recursos civiles de que dispone la sociedad.

Marco constitucional y legal de la defensa nacional dominicana

La Constitución del 1963 luego de un turbulento periodo histórico nacional, fue sustituida por la reforma de 1966, la cual estuvo vigente, con ligeros cambios, hasta el 26 de enero del 2010. Durante esos 43 años de vigencia, la Constitución dominicana fue objeto de revisión en dos ocasiones: una para resolver la situación de tranque post electoral en el 1994 y otra, en el 2002, para reinsertar la reelección presidencial y eliminar los colegios electorales cerrados, estrategia incorporada en la anterior reforma para evitar los denunciados fraudes electorales (Ramírez et al. 2011).

La reforma constitucional desarrollada por la Asamblea Nacional durante el año 2009 y proclamada el 26 de enero del 2010, marcó para la República Dominicana un cambio significativo en el ordenamiento jurídico nacional, al pasar de un Estado liberal a uno social y democrático de derecho. Esto implicó transformaciones en múltiples áreas, incluida la defensa nacional, en la que el paradigma filosófico jurídico adoptado por la nueva Constitución Política de la nación, respecto de la garantía y protección de los derechos fundamentales, es el Estado Constitucional de Derecho, propio de la escuela filosófica jurídica del neoconstitucionalismo.

En este orden de ideas, en el Derecho Constitucional, cuando se habla del marco constitucional de la defensa y seguridad nacional, se hace referencia al conjunto de normas, principios y disposiciones contenidas en la Constitución Política que regulan la organización, competencias, funciones y límites de las instituciones encargadas de la defensa nacional, los derechos y deberes de los ciudadanos en esta materia y la garantía de la protección de la soberanía, la independencia y la integridad territorial del Estado, dentro del respeto al orden democrático y los derechos fundamentales.

Antes de la reforma del año 2010, la Constitución del año 2002, establecía únicamente, en el Título XI, de las Fuerzas Armadas, dos artículos, el 93 y el 94:

> Art. 93. Las Fuerzas Armadas son esencialmente obedientes y apolíticas y no tienen, en ningún caso, facultad para deliberar. El objeto de su creación es defender la independencia e integridad de la República, mantener el orden público y sostener la Constitución y las leyes. Podrán intervenir, cuando así lo solicite el Poder Ejecutivo, en programas de acción cívica y en planes destinados a promover el desarrollo social y económico del país.
> Art. 94. Las condiciones para que un ciudadano pueda ser miembro de las Fuerzas Armadas están contenidas en la ley de su creación.

Bajo este marco constitucional, la concepción de la Seguridad Nacional y las Fuerzas Armadas se caracterizaba por un enfoque tradicional y un marco jurídico fundamentado en principios clásicos de la defensa del Estado centrado en la protección de este contra amenazas externas e internas y que se desarrollaba en la Ley Orgánica de las Fuerzas Armadas de 1978.

Este sistema pre-2010, cuyo antecedente inmediato fue la Constitución del 1966, presentaba varias características restrictivas, tales

como la ausencia de un enfoque multidimensional, toda vez que no contemplaba amenazas no tradicionales como narcotráfico, terrorismo o desastres naturales, así como falta de integración al no existir los organismos especializados en seguridad integral, desarrollado sobre un marco legal inflexible ante los nuevos desafíos a la seguridad.

Amenazas contemporáneas como el cibercrimen y el terrorismo transnacional, en un país cuya Ley contra el Terrorismo No. 267-08 data del 29 de mayo de 2008, requieren respuestas flexibles y adaptativas (Adams, 2023). Una ley integral de seguridad y defensa proporcionaría el marco legal necesario para desarrollar capacidades y estrategias que evolucionen en conjunto con el entorno dinámico y permita la respuesta ante estos desafíos.

Ante esta realidad, fue impulsada bajo el patrocinio de las Fuerzas Armadas y dentro de ese contexto de reforma constitucional, la necesidad de un replanteamiento en la Carta Magna que ampliara y modernizara la concepción de la seguridad nacional y el rol de las fuerzas militares, culminando en la Constitución del 2010 que introdujo conceptos más amplios como el carácter defensivo de los cuerpos castrenses, objetivos de alta prioridad nacional y la creación del Consejo de Seguridad y Defensa Nacional.

Marco constitucional a partir de la reforma del año 2010

La reforma constitucional dominicana de 2010 transformó radicalmente la concepción de seguridad nacional, defensa y fuerzas armadas, estableciendo un marco moderno y multidimensional que amplió significativamente el alcance y enfoque respecto al sistema anterior. A partir de esta reforma, la Constitución establece en su Artículo 252 que la defensa de la Nación está a cargo de las Fuerzas Armadas, definiendo su misión de manera integral:

> Defender la independencia y soberanía nacional, la integridad de sus espacios geográficos, así como la Constitución y las instituciones de la República.
> Podrán intervenir, cuando así lo disponga el presidente de la República, en programas destinados a promover el desarrollo social y económico del país; también en labores de mitigación en situaciones de desastres y calamidad pública;
> Concurrir en auxilio de la Policía Nacional para mantener o restablecer el orden público en casos excepcionales, manteniéndose el principio de que son obedientes al poder civil, apartidistas y no tienen facultad, en ningún caso, para deliberar.

Ha sido la Constitución del año 2010 la que ha consagrado con rango constitucional, en su artículo 254, la competencia de la jurisdicción militar, así como la existencia de un régimen disciplinario, como dos aspectos paralelos y totalmente diferenciados. Al respecto, la referida Constitución establece que: La jurisdicción militar solo tiene competencia para conocer las infracciones militares previstas en las leyes sobre la materia. Las Fuerzas Armadas tendrán un régimen disciplinario militar aplicable a aquellas faltas que no constituyan infracciones del régimen penal militar.

Se observó en este análisis que el legislador ordinario ha continuado la obra de seguir fortaleciendo la Jurisdicción Militar en la Ley 139-13, Orgánica de las Fuerzas Armadas, desarrollando este tema en los artículos 183,

184 y 185, los cuales permanecen vigentes, no obstante la sentencia TC/0350/19, del Tribunal Constitucional, que sorprendentemente expresa: "las Fuerzas Armadas tienen un régimen disciplinario militar aplicable a aquellas faltas que no constituyan infracciones del régimen penal militar, de ahí que deba considerarse que los tribunales penales militares son inexistentes en nuestro ordenamiento jurídico".

Sin embargo, la sentencia de marras TC/0350/19 no examinó en detalle el artículo 183 de esta misma ley orgánica, que trata sobre los tribunales militares. Mucho menos se atrevió a expurgarlo del ordenamiento jurídico nacional porque, en puridad de derecho, el Tribunal, integrado por expertos en la materia, entendía muy bien lo que significa el primer párrafo del artículo 254 de la Constitución y optó por una salida salomónica al declarar que los tribunales militares son inexistentes en lugar de inconstitucionales.

En el Capítulo III, sobre Seguridad y Defensa propiamente dichas, se crea en el artículo 258 el Consejo de Seguridad y Defensa Nacional, como un órgano consultivo que asesora al presidente de la República en la formulación de las políticas y estrategias en esta materia, así como en cualquier otro asunto que el Poder Ejecutivo someta a su consideración.

Cabe destacar que el artículo 75 establece como deber fundamental de todo dominicano, prestar los servicios civiles y militares que la patria requiera para su defensa y conservación, de conformidad con lo establecido por la ley. Es decir, que la defensa de la nación no es exclusiva de los militares, sino un deber de todos, lo que refuerza la correspondencia entre el Estado y la ciudadanía en materia de seguridad.

El artículo 259 establece que las Fuerzas Armadas tienen un carácter esencialmente defensivo en el cumplimiento de su misión, lo cual significa que las fuerzas militares de la nación se enfocan principalmente en proteger la soberanía y la integridad territorial de la nación, en lugar de participar en operaciones ofensivas o intervenciones militares en el extranjero, que no sean misiones de paz autorizadas por organismos internacionales, como se establece en el artículo 80 y sin perjuicio de lo dispuesto en el artículo 260, ambos de esta misma constitución.

En este mismo orden, el artículo 260 establece como objetivos de alta prioridad nacional: combatir actividades criminales transnacionales que pongan en peligro los intereses de la República y de sus habitantes; así como organizar y sostener sistemas eficaces que prevengan o mitiguen daños ocasionados por desastres naturales y tecnológicos. Del análisis hermeneútico de este canon constitucional se revela una innovación en la Carta Magna de la nación que institucionaliza la seguridad multidimensional como paradigma constitucional, toda vez que los dos objetivos de alta prioridad nacional redefinen la relación Estado- ciudadanía en materia de seguridad, estableciendo obligaciones estatales específicas frente a amenazas contemporáneas que trascienden la seguridad tradicional.

La interpretación sistemática demuestra que estos objetivos deben armonizarse con el Estado Social y Democrático de Derecho, respetando derechos fundamentales mientras protegen efectivamente los intereses nacionales y ciudadanos.

En el artículo 261, la Constitución señala que, cuando así lo requiera el interés nacional, el Congreso Nacional, a solicitud del presidente de la República, podrá disponer la formación

de cuerpos de seguridad pública o de defensa con integrantes de los cuerpos armados adscritos al ministerio o institución correspondiente, según el ámbito de sus respectivas competencias y conforme a lo dispuesto en la ley. A partir de esta disposición constitucional, los cuerpos especializados no podrán crearse mediante decretos, como los creados antes de esta nueva Constitución, y que han sido recogidos en el artículo 58 de la nueva Ley Orgánica 139-13 sobre los Cuerpos de Defensa. Como ejemplo más reciente, citamos la creación del Cuerpo Especializado de Mitigación a Emergencias y Desastres (CEMED), creado mediante la Ley número 28-24.

Finalmente, en el Título XIII, "De los Estados de Excepción", la Constitución define, en el artículo 262, a estos estados como aquellas situaciones extraordinarias que afecten gravemente la seguridad de la Nación, de las instituciones y de las personas, frente a las cuales resultan insuficientes las facultades ordinarias. En este sentido, se establecen y detallan tres modalidades: el Estado de Defensa (artículo 263), el Estado de Conmoción Interior (artículo 264) y el Estado de Emergencia (artículo 265). Estas disposiciones constitucionales constituyen la base de sustentación del imperativo constitucional de la defensa y, a su vez, son desarrolladas por varias leyes dentro del ordenamiento jurídico nacional. Entre ellas citamos las de mayor relevancia.

Ley Orgánica de las Fuerzas Armadas de la República Dominicana, No. 139-13, del 13 de septiembre de 2013. Tiene por objeto, tal como se denota en su artículo 1, "establecer la estructura, organización y funcionamiento de los órganos e instituciones que conforman las Fuerzas Armadas, así como el accionar de sus miembros y las bases de la carrera militar". Según el artículo 6, de esta ley orgánica, son funciones esenciales de las Fuerzas Armadas para el cumplimiento de las misiones constitucionales que tienen encomendadas la elaboración, ejecución y ejercitación de planes para la seguridad y defensa nacional, que sirvan de base para dar respuestas a las diversas contingencias que puedan presentarse, contribuyendo con su accionar a la consecución de los objetivos nacionales.

Se resalta en esta Ley Orgánica, el impacto del nuevo paradigma constitucional en los artículos 244, por medio del cual el personal de las Fuerzas Armadas deberá conocer y cumplir estrictamente todas las normas, reglas y principios instituidos por el Derecho Internacional Humanitario y Convenios Internacionales, que hayan sido ratificados por República Dominicana, así como también en el artículo 245, que dispone la capacitación necesaria sobre manejo de conflictos, reglas de enfrentamiento, operaciones-humanitarias, normas de Derechos Humanos y de Derecho Internacional Humanitario, y en general, todo lo concerniente a las disposiciones de la Organización de las Naciones Unidas (ONU), relacionadas con las operaciones de mantenimiento de paz.

Ley Orgánica No. 21-18 sobre regulación de los Estados de Excepción contemplados por la Constitución de la República Dominicana. Desarrolla el texto del artículo 262 la carta magna, tiene por objeto establecer los mecanismos legales para declarar estados de excepción relacionados con la defensa nacional, reglamentarlos durante su vigencia en sus distintas modalidades, conforme a lo previsto en la Constitución, para garantizar que su uso sea legítimo y proporcional, evitando la vulneración de derechos fundamentales y preservando el Estado Social y Democrático de Derecho.

Decreto 86-21. Tiene por finalidad dar cumplimiento a la parte in fine del artículo 258 de la Constitución de la República, al estructurar y reglamentar el Consejo de Seguridad y Defensa Nacional, así como establecer su composición y las directrices generales para garantizar su funcionamiento.

Ausencia de una ley sobre seguridad y defensa nacional, una falencia del sistema.

En fecha 13 de marzo del 2019, el entonces senador por la provincia Elías Piña (2006-2020) Adriano Sánchez Roa presentó el proyecto de Ley Orgánica de Seguridad y Defensa Nacional, el cual fue aprobado por el Senado de la República el 10 de abril del mismo año y remitido a la Cámara de Diputados para los fines constitucionales correspondientes en fecha 13 de mayo del 2019; sin embargo, dicho proyecto no ha sido aprobado a la fecha, por lo que la República Dominicana aún carece de este tipo de legislación, y solo cuenta con la Ley Orgánica de las Fuerzas Armadas que incluye también al Ministerio de Defensa.

Para la República Dominicana, la seguridad y defensa nacional constituyen pilares fundamentales para la estabilidad y soberanía del país. Aunque las Fuerzas Armadas desempeñan un rol crucial en la defensa nacional, es esencial contar con un marco legal que aborde de manera integral, aspectos más amplios de la seguridad y defensa, articulando políticas civiles y estrategias de seguridad interna. La seguridad nacional contemporánea trasciende las amenazas militares tradicionales, para Buzan et al. (1998), el concepto de "seguridad multidimensional" incluye dimensiones políticas, económicas, ambientales y sociales. En ese sentido, situaciones como los ciberataques, las pandemias o las crisis climáticas exigen respuestas interinstitucionales que las fuerzas militares, por sí solas, no pueden gestionar (Nye, 2011).

En este sentido, si bien la Constitución de la República Dominicana representa una aplicación exitosa y avanzada de este concepto de seguridad multidimensional, toda vez que operacionaliza las cinco dimensiones de la seguridad, institucionaliza procesos de securitización a través de marcos normativos específicos como la Ley Orgánica 139-13, e integra seguridad y desarrollo de manera más avanzada que la teoría original, como se evidencia en la Ley Orgánica 1-12 sobre la Estrategia Nacional de Desarrollo, en la actualidad se carece de una legislación que supere las limitaciones del enfoque tradicional estatocéntrico para incorporar una visión integral que abarque las múltiples amenazas, actores y dimensiones que caracterizan la seguridad en el siglo XXI.

Por tanto, se necesita una nueva legislación que proporcione el marco idóneo para articular a los distintos actores civiles y militares, evitando la fragmentación de competencias. En esta línea, Berkowitz y Goodman (2000) sostienen que la teoría de la coordinación institucional y la gestión integrada de la seguridad nacional ofrecen una vía para enfrentar dichos desafíos. Si bien la República Dominicana presenta experiencias que reflejan esta perspectiva, como las Fuerzas de Tareas Conjuntas e Interagenciales (FTC-I) desplegadas en la región fronteriza, persiste un vacío legal crítico en materia de seguridad nacional que refuerza la pertinencia de esta tesis.

Como señala Huntington (1957), las leyes castrenses, como es la Ley Orgánica 139-13 sobre las Fuerzas Armadas dominicanas, suelen limitarse a regular la estructura, la disciplina interna, las jerarquías, y las operaciones

militares, lo que las hace insuficientes para abordar desafíos híbridos. En este sentido, la experiencia dominicana demuestra que las leyes castrenses mantienen validez para su ámbito específico (estructura, disciplina, jerarquías, operaciones militares) pero requieren el complemento de una ley de seguridad nacional para articular la coordinación interinstitucional sin eliminar la especialización militar, regular participación militar en funciones multidimensionales sin militarizar, así como optimizar respuestas integrales sin fragmentar competencias.

La existencia de un marco legal que integre diferentes sectores y niveles de gobierno facilita la coordinación entre instituciones como la Policía Nacional, las agencias de inteligencia y los ministerios de Relaciones Exteriores y de Interior (García, 2021). Esta coordinación es vital para garantizar que, ante las amenazas, las respuestas sean eficaces y oportunas.

Por tanto, la República Dominicana constituye un caso paradigmático de cómo la ausencia de una ley de seguridad nacional confirma las limitaciones identificadas por Huntington en 1957, validando la necesidad de marcos legales integrales que complementen (no sustituyan) las leyes castrenses tradicionales para enfrentar efectivamente las amenazas multidimensionales del siglo XXI. Una ley integral de seguridad y defensa proporcionaría el marco legal necesario para desarrollar capacidades y estrategias que evolucionen en conjunto con el entorno dinámico y permitiría una mejor respuesta ante estos desafíos.

En consecuencia, la promulgación de una ley de seguridad y defensa nacional que complemente, sin limitar las funciones de las Fuerzas Armadas, resulta esencial para garantizar una seguridad integral, como parte del imperativo constitucional. Este marco legal no solo permitiría una respuesta coordinada y eficaz ante las amenazas, sino que también contribuiría a la protección de los derechos humanos y el fomento de la resiliencia nacional.

Servicios de las Fuerzas Armadas que concretan el imperativo constitucional de la defensa nacional

Desde una perspectiva institucional, la defensa militar se enmarca en el concepto más amplio de Defensa Nacional, siendo definida por el Comando General de las Fuerzas Militares colombianas como el conjunto de medidas y actividades tendientes a alcanzar y mantener esa situación [Seguridad Nacional]. De manera que la defensa nacional no es otra cosa que el medio de que se vale el Estado para lograr uno de sus más importantes fines: la seguridad (Comando General de las Fuerzas Militares, 1996, p. 45).

El principal instrumento de la defensa militar de la nación son las Fuerzas Armadas, que, en términos organizacionales, están conformadas por el Ejército de República Dominicana (ERD), la Armada de República Dominicana (ARD) y la Fuerza Aérea de República Dominicana (FARD). Estas se dedican esencialmente a la elaboración, ejecución y ejercitación de planes para la seguridad y defensa nacional, que, a su vez, sirven de base para dar respuestas a las diversas contingencias que puedan presentarse, contribuyendo con su accionar a la consecución de los objetivos nacionales.

Dichas instituciones militares se relacionan con el Poder Ejecutivo por conducto del Ministerio de Defensa, cuyo titular es la más alta autoridad del sistema de defensa, designado por el presidente de la República para la administración de los cuerpos armados.

En tiempos de paz, los recursos humanos y materiales de las Fuerzas Armadas también se utilizan para apoyar el desarrollo nacional y prestar cooperación a las instituciones del Estado que lo requieran (artículo 252 de la Constitución), todo ello dentro del marco jurídico que caracteriza al Estado Constitucional, en el cual se inserta el quehacer fundamental de las Fuerzas Armadas.

El imperativo constitucional de la defensa nacional se concreta entonces a través de los principales servicios públicos que las Fuerzas Armadas ofrecen a la nación dominicana, organizados en siete ejes medulares, conforme a la descripción de las misiones establecidas en el artículo 252 y a los objetivos de alta prioridad consignados en el artículo 260 de la Constitución dominicana. Estos ejes comprenden:

1) En el contexto de la defensa de la independencia y soberanía de la Nación, la integridad de los espacios geográficos, la Constitución y las instituciones de la República, esta labor se materializa mediante los servicios de:

- Salvaguarda del espacio aéreo.
- Salvaguarda de los espacios marítimos.
- Salvaguarda de la frontera y territorio nacional.
- Protección de los recursos naturales.
- Protección de los aeropuertos.
- Protección de los muelles.
- Protección del metro y teleféricos.
- Salvaguarda de las demás instituciones del Estado.
- Protección de infraestructuras vitales.
- Salvaguarda del sistema de combustibles del país.
- Servicio penitenciario.
- Proveer y garantizar la legítima defensa de la Nación, en caso de ataque armado actual o inminente por parte de la nación extranjera o poderes externos.

2)En lo que respecta a la promoción del desarrollo social y económico del país, esta función se materializa a través de los siguientes servicios:

- El Servicio Militar Voluntario
- Las Escuelas Vocacionales.
- Escuelas públicas.
- Capacitación de personal civil en defensa, seguridad, geopolítica, derechos humanos y derecho internacional humanitario.
- Servicio de alfabetizaciones para adultos.
- Atenciones médicas (Acciones Cívicas).
- Servicio de cartografía.
- Salvaguarda de los derechos de la ciudadanía frente a las empresas de vigilancia y seguridad privada.

3) En lo que corresponde a la mitigación de situaciones de desastres y calamidad pública, esta función se desarrolla mediante los siguientes servicios:

- Servicio de búsqueda y rescate.
- Evacuaciones.
- Limpieza de escombros.
- Transporte estratégico, terrestre, naval y aéreo.
- Protección de orden público, seguridad de la propiedad privada y los ciudadanos.

4) Cuando concurre en auxilio de la Policía Nacional para mantener o restablecer el orden público en casos excepcionales, se encarga de:

- Servicio de protección a la propiedad privada.
- Servicio de protección ciudadana.
- Restablecimiento del orden público.

5) En lo que respecta al combate de las actividades criminales transnacionales que pongan en peligro los intereses de la

República y de sus habitantes se ejecutan los siguientes:

- Patrullaje en apoyo a la DNCD contra el narcotráfico, tanto a gran escala (macrotráfico) como a menor escala (microtráfico).
- Interceptación de aeronaves y embarcaciones en actividades criminales.
- Intercepción de vehículos que penetren por la frontera en tráfico de armas o ilegales.

6) En lo que concierne a la custodia, supervisión y control de todas las armas, municiones y demás pertrechos militares, se realiza:

- Control del material y de los equipos de guerra que ingresen al país o que sean producidos por la industria nacional.

7) En el marco de la cooperación internacional se lleva a cabo lo siguiente:

- Servicio de ayuda humanitaria y de paz en el exterior.

Estos siete ejes medulares, producto de un análisis al título XII de la Constitución de la República Dominicana así como de la observación a procesos, funciones y tareas que realizan a diario las unidades militares desarrollado por el autor de este ensayo mientras prestaba servicios en la Dirección General de Programas, Planes y Proyectos del MIDE, representan la concreción práctica del imperativo constitucional de la defensa nacional post-2010, transformando conceptos abstractos en servicios públicos específicos con sus respectivas medidas políticas y que las Fuerzas Armadas dominicanas ofrecen a la nación dentro de un modelo de cadena de valor público.

Esta arquitectura misional demuestra cómo la reforma constitucional no solo modernizó la defensa nacional, sino que la redefinió como un servicio público puro e integral orientado al desarrollo sostenible, la seguridad multidimensional, así como al fortalecimiento democrático de República Dominicana en el siglo XXI.

Conclusiones

La reforma constitucional del 26 de enero de 2010, la número 38 desde la independencia en 1844, representó una transformación paradigmática en la concepción, estructura y alcance de la defensa nacional, elevándola desde una función estatal tradicional hacia una obligación jurídica constitucional prioritaria que redefine integralmente el rol del Estado en la protección y desarrollo de la nación. Esta reforma estableció, redefinió y fortaleció la defensa nacional a través de múltiples dimensiones constitucionales innovadoras.

El marco constitucional y legal actual de la defensa nacional en la República Dominicana se fundamenta principalmente en la Constitución de la República y en leyes específicas que regulan la seguridad y defensa nacional, así como la organización y funciones de las Fuerzas Armadas. Cabe destacar que la Constitución, en su Título XII, Capítulo I, Artículo 252, establece que la defensa de la nación está a cargo de las Fuerzas Armadas, además de sus misiones, y que son obedientes al poder civil, apartidistas y no tienen facultad para deliberar políticamente.

Dentro del marco legal aprobado al amparo de esta constitución se encuentra la Ley Orgánica de las Fuerzas Armadas (Ley No. 139-13), que regula la organización, funciones y misión de las Fuerzas Armadas, alineadas con la Directiva de Seguridad y Defensa Nacional. Esta ley erige al Ministerio de Defensa como el órgano responsable de la di-

rección y conducción de las Fuerzas Armadas. Sin embargo, el país carece a la fecha de una Ley de Seguridad y Defensa, lo que constituye una falencia importante dentro del sistema.

Se ha podido determinar que el marco constitucional de la Defensa Nacional se materializa como imperativo constitucional a través de unos 32 servicios públicos que las Fuerzas Armadas, por intermedio del Ejército (ERD), la Armada (ARD), la Fuerza Aérea (FARD), así como los distintos cuerpos especializados, ofrecen a la nación dominicana. Estos servicios han sido estructurados en siete ejes medulares, estructurados en base a la descripción de las misiones establecidas en el artículo 252 y los objetivos de alta prioridad en el artículo 260 de la Constitución dominicana.

La defensa nacional, tras la reforma de 2010, se ha constituido así en un imperativo constitucional integral que vincula indisolublemente seguridad, desarrollo, democracia, y soberanía como pilares fundamentales de la República Dominicana del siglo XXI; una transformación que posiciona al país como modelo regional de modernización institucional democrática y adaptación estratégica ante los desafíos multidimensionales contemporáneos.

Sin embargo, esta consolidación constitucional requiere aún de instrumentos legales específicos que operacionalicen plenamente el mandato transformador de la reforma de 2010. Como recomendaciones o perspectivas futuras para continuar fortaleciendo este mandato constitucional, se considera necesaria la aprobación y promulgación de una Ley de Seguridad y Defensa Nacional bajo el paradigma de la seguridad humana, donde la protección estatal priorice los derechos fundamentales sobre enfoques tradicionales de seguridad nacional sin desmedro de esta última, así como un moderno Código de Justicia Militar.

Esta legislación complementaria permitiría articular definitivamente la arquitectura institucional prevista constitucionalmente, coordinar sistemáticamente las respuestas multidimensionales, regular específicamente la participación militar en funciones subsidiarias, y garantizar permanentemente que la evolución de la defensa nacional mantenga su orientación antropocéntrica y su compromiso democrático completando así la transformación constitucional iniciada en 2010 y consolidando a República Dominicana como referente hemisférico de modernización exitosa de la defensa nacional en el marco del Estado Social y Democrático de Derecho del siglo XXI.

Referencias

Alexy, R. (1997). *Teoría de los derechos fundamentales.* Centro de Estudios Políticos y Constitucionales.

Berkowitz, B., & Goodman, A. (2000). *Best truth: Intelligence in the information age.* Yale University Press.

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis.* Lynne Rienner Publishers.

Comisión sobre la Seguridad Humana. (2003). *Human security now: Final report. Nueva York: CSH.* https://digitallibrary.un.org/record/503749?ln=en&v=pdf

Constitución de la República Dominicana. [Const]. (1963). *Gaceta Oficial.* Santo Domingo, República Dominicana. 30 de abril 1963, No. 8758.

Constitución de la República Dominicana. [Const]. (1966). *Gaceta Oficial,* Santo Domingo, República Dominicana. 28 de noviembre de 1966. No. 9014.

Constitución de la República Dominicana. [Const]. (2002). *Gaceta Oficial.* Santo Domingo, República Dominicana. 25 de julio 2002, No. 10240.

Constitución de la República Dominicana. [Const]. (2010). *Gaceta Oficial.* Santo Domingo, República Dominicana. 26 de enero de 2010, No. 10561.

Constitución de la República Dominicana. [Const]. (2024). *Gaceta Oficial.* Santo Domingo, República Dominicana. 31 de octubre de 2024, No. 11170.

Corte Constitucional de Colombia (2002). Sentencia C-251 de 2002. https://www.corteconstitucional.gov.co/relatoria/2002/C-251-02.htm

Decreto 86-21. (2021). Establece el reglamento que establece la composición y funcionamiento del Consejo de Seguridad y Defensa Nacional. *Gaceta Oficial.* Santo Domingo, República Dominicana. 12 de febrero de 2021. Núm. 11010.

Decreto No. 323-06. (2006, 1 de enero). Crea e integra la Comisión encargada de preparar las consultas que fueren necesarias tendentes a modificar la Constitución de la República. *Gaceta Oficial.* Santo Domingo, República Dominicana. *Núm. 10383.*

Ferrajoli, L. (2011). *Principia iuris: Teoría del derecho y de la democracia* (Vols. 1–2). Trotta.

García, M. (2021). *Coordinación interinstitucional en defensa nacional: Principios y prácticas.* Routledge.

Hesse, K. (1992). *La fuerza normativa de la Constitución*. Centro de Estudios Constitucionales.

Huntington, S. P. (1957). *The soldier and the state: The theory and politics of civil-military relations.* Harvard University Press.

Ley No. 139-13. (2013). Orgánica de las Fuerzas Armadas. *Gaceta Oficial.* Santo Domingo, República Dominicana. 13 de septiembre 2013. No. 10728.

Ley No. 21-18. (2018). Orgánica sobre regulación de los Estados de Excepción contemplados por la Constitución de la República Dominicana. *Gaceta Oficial.* Santo Domingo, República Dominicana. 25 de mayo de 2018. Núm. 10911.

Ley No. 28-24. (2024). Que crea el Cuerpo Especializado de Mitigación a Emergencias y Desastres (CEMED). *Gaceta Oficial*, Santo Domingo, República Dominicana. 30 de julio de 2014. Núm. 11157.

Ley No. 873. (1978). Orgánica de las Fuerzas Armadas. *Gaceta Oficial.* Santo Domingo, República Dominicana. 31 de julio de 1978. Núm. 6487.

Ley No. 267-08. (2008). Sobre terrorismo, y crea el Comité Nacional Antiterrorista y la Dirección Nacional Antiterrorista. *Gaceta Oficial.* Santo Domingo, República Dominicana. 29 de mayo de 2008. Núm. 10477.

Miller, S. (2022). *Resiliencia en la seguridad nacional: Participación comunitaria y civil.* Harvard University Press.

Nye, J. S. (2011). *The future of power.* PublicAffairs.

Ramírez, A., Del Rosario, D., Pola Zapico, M., & Cepeda, Z. (2011). *Impacto socio-jurídico de la nueva Constitución en los derechos de las mujeres en República Dominicana.*

Tribunal Constitucional de la República Dominicana. (2019, 16 de septiembre). *Sentencia TC-05-2019-0108.*

Valadés, D. (2022). *La Constitución dominicana de 2010 "enriquece con nuevos enfoques al constitucionalismo de nuestro hemisferio".* https://colnal.mx/wp-content/uploads/2022/08/La-Constitucio%CC%81n-dominicana-de-2010.docx_compressed.pdf

Williams, P. (2012). *Entendiendo la seguridad: Teoría y práctica.* Palgrave Macmillan.
Zagrebelsky, G. (1995). *El derecho dúctil: Ley, derechos, justicia.* Trotta.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Integración de dominios y ejércitos multimisión: De operaciones conjuntas al multidominio

Integration of Domains and Multi-Mission Armies: from joint to multi-domain operations

Recibido: 01/ 05 / 2025 | Revisado: 15 / 07 / 2025 | Aprobado: 30 / 09 / 2025
DOI: https://doi.org/10.59794/rscd.2025.v11i11.123

Teniente coronel Kelvin Leandro Encarnación González, ERD
República Dominicana

Correo: kelvinencarnacióng@gmail.com

ORCID: https://orcid.org/0009-0004-2488-5090

Afiliación: Universidad Nacional para la Defensa

El autor es teniente coronel del Ejército de la República Dominicana. Es máster en Seguridad, Defensa y Geoestrategia, así como en Derecho y Relaciones Internacionales; posee la Especialidad en Comando y Estado Mayor para Fuerzas Terrestres (graduado de honor, 2021); la Especialidad en Derechos Humanos y Derecho Internacional Humanitario; es licenciado en Derecho (Magna Cum Laude); y licenciado en Ciencias Militares de la Academia Militar de las Fuerzas Armadas "Batalla de las Carreras". Ha realizado, además, un Diplomado Internacional en Operaciones Psicológicas y Psicosociales; un Diplomado en Comunicación Estratégica para la Seguridad y Defensa Nacional; un Diplomado en Ciberdefensa y Ciberseguridad; un Diplomado en Metodología de la Investigación Científica; un Diplomado en el Modelo Educativo UNADE; un Diplomado en Gobernabilidad y Administración de Cooperativas (2023); un Diplomado en Seguridad Fronteriza; un Diplomado en Hacienda e Inversión Pública; un Diplomado en Derecho Procesal Civil; un Diplomado en Derecho de Familia; un Diplomado en Derecho Inmobiliario; un Diplomado en Derecho Laboral y Seguridad Social; y un Diplomado en Derecho de Familia (2009), entre otros cursos y talleres especializados. Durante su carrera ha ocupado numerosas funciones de relevancia, tales como: director de Pensiones de la Junta de Retiro y Fondo de Pensiones de las Fuerzas Armadas; subdirector de Planificación y Desarrollo del Instituto de Seguridad Social de las Fuerzas Armadas; subdirector de Recursos Humanos del mismo instituto; y docente titular de la Escuela de Graduados del Ejército de la República Dominicana (EGEMERD), en asignaturas como Defensa Nacional, Planificación para la Defensa, Fundamentos de Seguridad y Defensa Nacional, entre otras materias militares del bloque de Doctrina del Ejército y Operaciones Conjuntas. A lo largo de casi 26 años de servicio ininterrumpido, ha adquirido capacidades, experiencias y cualidades de liderazgo que le han permitido cumplir de manera efectiva con las misiones asignadas.

DOI: https://doi.org/10.59794/rscd.2025.v11i11.123

Resumen

En el presente artículo se analiza que en las últimas décadas, tanto la guerra como las operaciones militares han experimentado una mutación considerable. De la coordinación de fuerzas terrestres, aéreas y navales, se ha pasado a un concepto más amplio: las operaciones multidominio. El concepto de operaciones conjuntas se afianzó posterior a la Segunda Guerra Mundial y a lo largo de la Guerra Fría. Para entonces, cualquier fuerza militar que pretendiera alzarse con el éxito debía contar con el apoyo de las demás fuerzas. En 2018, el Comando de Entrenamiento y doctrina del Ejército de los Estados Unidos (TRADOC) publica un concepto doctrinal formal para las Operaciones Multidominio, en donde las define como operaciones en múltiples dominios y espacios disputados para superar las fortalezas de un adversario presentándole múltiples dilemas operativos y tácticos. Las Operaciones Multidominio desvanecen la frontera entre el conflicto, la crisis y la paz, igualmente entre lo convencional y lo no convencional, constituyéndose esto, junto a la disuasión y la escalada, en aspectos estratégicos característicos de este tipo de operaciones. República Dominicana, en cuanto a los medios materiales, enfrenta el reto tecnológico de adoptar las capacidades propias de las operaciones multidominio con recursos un tanto limitados. Las guerras del futuro tienen mucha probabilidad de continuar por el camino de la integración multidominio y añadiéndose más tecnología que revolucionará la forma de combatir; y las fronteras que separan lo humano y la máquina, lo civil y lo militar, será cada vez más difusa.

Palabras clave: Operaciones multidominio, ciberespacio, multimisión, operaciones conjuntas, guerra híbrida

Abstract

In this article, we will examine how, in recent decades, both warfare and military operations have undergone considerable transformation. From the coordination of land, air, and naval forces, we have moved toward a broader concept: multi-domain operations. The concept of joint operations became entrenched after World War II and throughout the Cold War. By then, any military force seeking success had to rely on the support of other forces. In 2018, the United States Army Training and Doctrine Command (TRADOC) published a formal doctrinal concept for Multi-Domain Operations, defining them as operations in multiple domains and contested spaces to overcome an adversary's strengths by presenting them with multiple operational and tactical dilemmas. The Multi-Domain Operations blur the lines between conflict, crisis, and peace, as well as between conventional and unconventional operations. This, along with deterrence and escalation, constitutes characteristic strategic aspects of this type of operation. In terms of material resources, the Dominican Republic faces the technological challenge of adopting the capabilities of multi-domain operations with somewhat limited resources. Wars of the future are likely to continue along the path of multi-domain integration, adding more technology that will revolutionize the way we fight; and the lines separating human and machine, civilian and military will become increasingly blurred.

Keywords: Multi-domain operations, cyberspace, multi-mission, joint operations, hybrid warfare

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Introducción

La guerra históricamente ha significado el uso de las fuerzas convencionales o no, que, por medio de una organización estructurada de éstas, de forma estratégica y coordinada, tienen como estado final deseado hacerse con un objetivo previamente planteado, a través, de las tradicionalmente conocidas operaciones conjuntas.[1] En décadas recientes, tanto la guerra como las operaciones militares han experimentado una mutación considerable, pues, de la coordinación de las fuerzas terrestres, aéreas y navales, se ha pasado a un concepto más amplio: las operaciones multidominio (MDO, por sus siglas en inglés).

El enfoque e/o integración multidominio reconoce una extensión del campo de batalla moderno, más amplia y extensa de los límites conocidos de los dominios físicos ya conocidos, que ahora incluyen nuevas áreas como el ciberespacio, el espacio ultraterrestre y el ámbito cognitivo o informativo inclusive. La transición de una cooperación entre fuerzas armadas tradicionales hacia las MDO no solo representa un cambio conceptual, sino que conlleva una transformación doctrinal exhaustiva y profunda; por las implicaciones que tiene pasar de la acostumbrada coordinación entre fuerzas (ejércitos, armadas y fuerzas aéreas) a la integración de manera sincronizada de las herramientas militares y no militares disponibles, que van desde misiones en tierra hasta operaciones espaciales, cibernéticas e informativas y/o psicológicas.

Los hechos de las últimas décadas han demostrado que no es suficiente dominar un ámbito de la guerra, sino dominarlos todos a la vez o por lo menos negar al enemigo esa ventaja, creando múltiples dilemas al mismo, con tanta rapidez que este se vea limitado al responder. Atendiendo a lo anterior, pretendemos en este artículo describir cómo ha sido la evolución de las operaciones conjuntas hacia las operaciones multidominio y la integración de éstas. Procuramos analizar el concepto desde el punto de vista histórico y conocer las implicaciones tecnológicas de este tipo de guerra para el nivel estratégico. Además, describiremos casos recientes de cómo y dónde han sido aplicadas estas operaciones.

Finalmente, pretendemos enfocarlo hacia los retos para las Fuerzas Armadas de República Dominicana al momento de adoptar dicho tipo de operación y brevemente exponer las tendencias que a futuro presenta la guerra en múltiples dominios y sus implicaciones a partir de la dirección que proyecta.

1 La manera básica en la que el Departamento de Defensa (DOD) emplea dos o más Servicios (de al menos dos Departamentos Militares) en una única operación es mediante operaciones conjuntas. Las operaciones conjuntas son acciones militares realizadas por las fuerzas conjuntas y las fuerzas del Servicio empleadas en relaciones de mando específicas, pero que no conforman fuerzas conjuntas. Una fuerza conjunta está compuesta por elementos importantes, asignados o agregados, de dos o más Departamentos Militares que operan bajo un único comandante de Fuerza Conjunta o JFC (Publicación Conjunta [JP], 3-0, 2018).

DOI: https://doi.org/10.59794/rscd.2025.v11i11.123

Desarrollo

De Operaciones Conjuntas a Multidomio: Evolución.

A la participación coordinada de más de una rama de las Fuerzas Armadas en una operación se le conoce como operaciones conjuntas. De acuerdo con la publicación conjunta JP 3-0 (2018), la manera básica en la que el Departamento de Defensa (DOD,[2] emplea dos o más Servicios (de al menos dos Departamentos Militares) en una única operación es mediante operaciones conjuntas. Una fuerza de este tipo está compuesta por elementos importantes, asignados o agregados, de dos o más Departamentos Militares que operan bajo un único comandante de la Fuerza Conjunta (JFC).

El concepto de operaciones conjuntas se afianzó a partir de la finalización de la Segunda Guerra Mundial y a lo largo de la Guerra Fría. Para entonces estaba claro que cualquier fuerza militar que pretendiera alzarse con el éxito en combate debía contar con el apoyo de las demás fuerzas. Es por esto por lo que vimos cómo occidente y su doctrina desarrollaron el concepto de armas combinadas[3] con el fin de aprovechar y explotar sus fortalezas complementarias (Manual de campo [FM], 100-5, 1982). Entrada la década de 1980 irrumpe en escena el concepto de Batalla Aeroterrestre introducido por el Ejército de Estados Unidos, que consistía y hacia énfasis en una sincronización armoniosa y total de las fuerzas terrestres y las fuerzas del aire a los fines de alcanzar profundidad en las operaciones y que permitiera la derrota del enemigo de manera eficiente (Manual de campo [FM], 100-5, 1982).

La doctrina descrita anteriormente sienta las bases de "lo conjunto", indicando básicamente, que las unidades y armas serán siempre más efectivas siempre y cuando operen en conjunto, no así si lo hacen de manera individual o por separado ((Manual de campo [FM], 100-5, 1982, pp. 7-3); significando esto la importancia de la integración de fuerzas en las operaciones, obviando por completo la individualización de las acciones. La experiencia de la Guerra del Golfo en 1991 lleva a gran parte de las potencias militares a acoger de manera absoluta las operaciones conjuntas como parte de su doctrina. Los triunfos conseguidos en la operación Tormenta del Desierto demostraron la eficacia de una campaña conjunta (tierra, mar y aire), con el apoyo simultaneo de información satelital y de geolocalización y una robusta y eficaz logística.

Posteriormente, el Departamento de Defensa de los Estados Unidos en su visión conjunta a 2020, aspiraba a obtener la superioridad en todos los ámbitos de la guerra con la implementación del concepto de operaciones del espectro total. No obstante, a inicios del siglo XXI, la aparición de nuevas tecnologías y con esto, de nuevas amenazas, tales como las estrategias anti-acceso/denegación de área (A2/AD), el apogeo del ciberespacio como escenario de conflictos y el espacio ultraterrestre y su militarización, empezaron a exponer las limitaciones de la doctrina conjunta tradicional.

La aparición de estos entornos y la necesidad de enfrentarlos al nivel adecuado hace que las potencias militares empiecen a ser conscientes de enfocar las operaciones militares hacia

2 Equivalente al Ministerio de Defensa para el caso de República Dominicana.
3 Consiste en integrar infantería, blindados, artillería, fuerzas aéreas tácticas, etc., en un esfuerzo unificado.

los dominios múltiples. Por medio del impulso dado por el Ejército de Estados Unidos, el concepto de multidominio resalta en la década del 2010, específicamente como operaciones multidominio (MDO por sus siglas en inglés), buscando operar frente a adversarios (El Rusia y China) que claramente podían desafiarlos en varios dominios a la vez. El Comando de Entrenamiento y Doctrina del Ejército de los Estados Unidos (TRADOC) (2018). Pública un concepto doctrinal formal para las Operaciones Multidominio en donde las define como, cito: "operaciones en múltiples dominios y espacios disputados para superar las fortalezas de un adversario presentándole múltiples dilemas operativos y/o tácticos" (p. 6).

Según Borne (2019), lo que procuran las MDO es aprovechar el dominio terrestre, aéreo, marítimo, espacial, ciberespacial y otros como el espectro electromagnético y la información de manera simultánea, para alcanzar efectos complementarios que detengan o anulen la respuesta de un enemigo. Las MDO representan un salto cualitativo, aunque en sus inicios algunos consideraban que era una modificación o extensión de las batallas aeroterrestres de la década de los 80, pues, procura no solo coordinar a fuerzas convencionales, sino que busca integrar de manera efectiva nuevas capacidades, como drones, inteligencia artificial, guerra electrónica (EW), operaciones psicológicas (PSYOPS) y ciberataques.

Como también señalan King y Boykin (2019), las MDO no son unas "Airland Battle 2.0", sino que incluye nuevas herramientas y escenarios que anteriormente se consideraban ajenos a una operación militar tradicional o convencional. Es por esto por lo que el nuevo enfoque que requiere el multidominio procura descentralizar la planificación y la ejecución a los niveles bajos, permitiendo a los comandantes sincronizar efectos en diversos ámbitos en tiempo real,[4] consiguiendo que haya una afinidad en las acciones que sean concebidas desde la planificación, difuminando las fronteras antes estrictas, entre lo terrestre, naval, aéreo, etc., y creando un único espacio interconectado de batalla.

Actualmente, gran parte de las potencias militares del mundo están en el proceso de incorporación del concepto de multidominio en sus doctrinas; siendo los Estados Unidos, según Brading (2021), quienes han procurado acelerar el paso con la implementación de iniciativas que crean Fuerzas de Tarea Multidominio (MDTF por sus siglas en inglés) en su Ejército, y el desarrollo de la estrategia conjunta de Mando y Control Conjunto en todos los Dominios (JADC-Joint All Domain Command and Control) que procura conectar los diferentes nodos y sensores de las distintas ramas en una red única y unificada de mando y control (C2).

Alianzas militares internacionales, como la Organización del Tratado del Atlántico Norte (OTAN, 2013), han sido coherentes en importantizar la operación simultanea y coordinada en los cinco dominios actualmente reconocidos[5] y desarrolla una "noción de guerra multidominio" para dirigir a una transformación total de sus fuerzas; consiguiendo que países de la Unión Europea (UE) ya traten y hablen de la integración al multidominio en sus actualizaciones de defensa y que inicien los aprestos para ajustar sus adquisiciones, capacidades y organización a este novedoso concepto.

4 Por ejemplo, en combate, una unidad terrestre podría recibir apoyo no solo de artillería y fuerza aérea aliada, sino también de operaciones de guerra electrónica que cieguen los sensores enemigos y ataques cibernéticos contra los sistemas de mando y control enemigos.

5 Tierra, mar, aire, espacio y ciberespacio.

De esta manera, potencias como China inician reformas que se proponen mejorar sus capacidades en una guerra conjunta y multidominio de manera integral, y desde 2015 reorganiza sus regiones militares en comandos conjuntos, creando la Fuerza de Apoyo Estratégico que aglutina capacidades ciber, de espacio e información, adoptando una doctrina de "operaciones conjuntas integradas" con un enfoque primordial en guerra informática (Tosi, 2023). Asimismo, Rusia, independientemente de que no hace uso del término multidominio como tal en su doctrina, en la práctica demuestra una integración del enfoque al combinar la ciberguerra con ataques convencionale,[6] guerra electrónica, uso de fuerzas especiales y campañas de desinformación.[7]

Podemos ver como claramente existe un consenso en que el panorama doctrinal global indica que la superioridad militar de cualquier potencia va a depender necesaria y exclusivamente de su capacidad de llevar a cabo operaciones integrales en todos los dominios. La evolución desde "lo conjunto" a la integración multidominio ya se encuentra en marcha, sostenida por lecciones aprendidas y en curso por conflictos pasados y recientes, apoyado además por el veloz desarrollo tecnológico que indefectiblemente ha redefinido el campo de batalla que tradicionalmente conocíamos.

Lo estratégico y tecnológico: Implicaciones.

Las Fuerzas Armadas, en términos estratégicos, no solo deben planificar de forma integral, sino, que deben pensar en esos términos, teniendo en cuenta y considerando que las operaciones ejecutadas en un dominio deben y puede influir y afectar los demás dominios. Por esto podemos considerar y deducir que al adoptar un enfoque multidominio necesariamente se traduce en cambios profundos en la estrategia militar.

Como consecuencia directamente proporcional a esta, la necesidad de que los mandos conjuntos sean y estén más integrados, debiendo el mando y control (C2) estar en la capacidad de dirigir distintas unidades en todo ámbito de manera simultánea, cambiando con esto los tradicionales obstáculos entre Fuerzas. Aquellos que logren sincronizar con rapidez sus fuerzas en los múltiples dominios conseguirán tomar, mantener y explotar la iniciativa y abrumar al enemigo con la presentación de múltiples amenazas al mismo tiempo (TRADOC, 2018).

Las MDO, por sus implicaciones, desvanecen la frontera entre el conflicto, la crisis y la paz, igualmente entre lo convencional y lo no convencional, constituyéndose esto, junto a la disuasión y la escalada, en otros aspectos estratégicos característicos de este tipo de operaciones. Un ejemplo puntual puede ser el hecho de que un país emplee sus capacidades cibernéticas y/o acciones en el espacio (interferencia de satélites) en fases iniciales de un conflicto sin traspasar el umbral o la frontera de un ataque cinético tradicional.[8] Esta última forma se considera guerra híbrida o estrategias de zona gris, al combinar múltiples instrumentos, sean militares o no, con el fin de lograr objetivos políticos sin que sea desencadenada una guerra abierta (Morris et al., 2019).

6 Por ejemplo, los ataques en 2015-2017 a las redes eléctricas ucranianas.
7 En occidente se conoce como guerra híbrida al uso simultaneo de estas capacidades.
8 El término "ataque cinético" se aplica a cualquier acción destructiva que utiliza la energía cinética de un objeto en movimiento para causar daño.

Desde el punto de vista de una gran estrategia, las MDO y su integración, hacen necesario e imperativo una adecuada coordinación interagencial, entrelazando la dimensión militar con la dimensión económica, diplomática e informativa. Un ejemplo es cómo la Organización del Tratado del Atlántico Norte (OTAN, 2023), destaca el hecho de que, al aprovechar todos estos instrumentos del poder nacional en su conjunto, es vital para imponerse y lograr los objetivos en los conflictos modernos. Resumidamente, a nivel estratégico una guerra multidominio exige una orquestación y estructuración holística de las capacidades y una toma de decisiones compleja y más rápida que la de una guerra convencional y/o tradicional.

Es obvio pensar en este punto, de que el componente tecnológico, más allá de solo ser un área de competencia, es una parte fundamental y central para la ejecución de las MDO. Hay consenso en el hecho de que para poder integrar de manera efectiva múltiples dominios se hace necesario y obligatorio contar con sistemas de comunicaciones e información avanzados, así como con plataformas innovadoras y armamento con tecnología de punta.

Dentro de las implicaciones tecnológicas principales podemos mencionar cuatro vitales. La primera es la necesidad de que las redes de mando y control estén integradas y que puedan resistir los entornos hostiles.[9] La segunda es la necesidad de aplicación o uso de inteligencia artificial (IA) a los fines de que se pueda manejar con rapidez y precisión el gran volumen de datos generados en los múltiples dominios (imágenes satelitales, información e inteligencia humana, señales de radar, flujo de redes sociales, etc.).

Una tercera implicación es la adquisición y aplicación de plataformas no tripuladas y armamento de precisión, permitiendo estos sistemas[10] atacar y golpear objetivos con precisión y eficacia, reduciendo de manera considerable la exposición de las tropas propias y limitando a prácticamente al mínimo los daños colaterales y la pérdida de no combatientes y personas de la clase civil no involucradas en los conflictos. Por último, una cuarta implicación sería tanto el espacio y el ciberespacio como dominios de combate, debiendo una fuerza militar garantizar su acceso al espacio[11] y garantizar además la protección de éstos. Igualmente debe tener la capacidad y libertad de poder operar en el ciberespacio, tanto ofensiva como defensivamente, desarrollando para esto recursos humanos especializados en ciberdefensa.

A resumidas cuentas, las implicaciones tecnológicas en las MDO están determinadas tanto por la precisión como por la conectividad, esto en la ofensiva, defensiva y el mando control. Entonces podemos inferir, que la fuerza o potencia militar que haga un mejor aprovechamiento de la tecnología para atacar y defenderse contará con una ventaja considerable y se traducirá en la consecución de los objetivos planteados inicialmente.

Casos de conflictos recientes

Azerbaiyán y Armenia 2020

La segunda guerra de Nagorno-Karabaj en 2020 entre Azerbaiyán y Armenia es un conflicto que puso en evidencia las nuevas dinámicas multidominio. Con una duración de 44 días, Azerbaiyán combinó el uso intenso y constante

9 Referido a interferencias del espectro electromagnético, ciberataques, guerra electrónica, etc.
10 Misiles guiados, proyectiles inteligentes, drones aéreos, drones terrestres y vehículos aéreos no tripulados (UAVs).
11 Navegación GPS, comunicaciones satelitales, inteligencia geoespacial, etc.

de drones armados y municiones merodeadoras (kamikaze) con ciberataques propagandísticos y con ataques terrestres convencionales, logrando con esto una rápida superioridad. Los análisis sobre este enfrentamiento coincidieron en que los daños en combate fueron infligidos por plataformas no tripuladas, y que a opinión de Hertlein (2023), ha sido algo sin precedentes históricos. Por su parte Armenia, que basa sus defensas en tanques, blindados y sistemas antiaéreos tradicionales, fue abrumada prácticamente de inmediato.

Con apenas una semana de combate los drones azeríes destruyeron cientos de vehículos y sistemas antiaéreos enemigos, incluyendo modernizadas baterías de misiles s-300 (Hertlein, 2023). Al negarle a Armenia la capacidad de operar con libertad en el dominio aéreo, sus aviones casi no pudieron levantar el vuelo, y al ser empleado con destreza el dominio informativo (con publicación de videos de ataques masivos de drones para minar la moral de los armenios), Azerbaiyán estableció y creó el efecto de control multidominio local. Demostrando este caso que incluso si países pequeños integran en su doctrina tecnologías como drones se puede derrotar de manera rápida a fuerzas más tradicionales.

Rusia y Ucrania 2022-actualidad

La invasión rusa a gran escala en Ucrania en febrero de 2022 ha sido descrita como el primer conflicto en décadas entre potencias que ocurre en todos los dominios de manera intensa. Una fuerza convencional masiva rusa (tanques, artillería, aviación e infantería), se complementaron con ataques en el ciberespacio y campañas de desinformación; sin embargo, sus resultados iniciales quedaron muy por debajo de lo esperado. La falta de integración efectiva de dominios fue uno de los factores que incidieron en dicho relativo fracaso. A pesar de su potencia de fuego, Rusia no logró anular las comunicaciones ucranianas ni consiguió la supremacía aérea. Por otro lado, Ucrania aprovechó de manera creativa la guerra multidominio a su favor a pesar de tener menos medios convencionales. En el dominio cibernético Ucrania recibió gran apoyo de países y empresas aliadas para contrarrestar y resistir los ciberataques rusos. Además, utilizó con éxito la información y las redes sociales para ganar la batalla de la opinión pública mundial contrarrestando la narrativa rusa.

En el dominio espacial, Ucrania fue beneficiada de servicios como la constelación satelital Starlink para mantener las comunicaciones seguras de sus tropas en el campo de batalla, aun cuando la infraestructura tradicional fue destruida. Pudo rastrear además los movimientos enemigos a través de la obtención de inteligencia que fue proporcionada por los satélites occidentales. En el dominio aéreo, conscientes de una fuerza aérea potente, Ucrania desplegó enjambres de drones tanto de ataque como de reconocimiento (modelos militares y comerciales adaptados) para guiar la artillería con una letal precisión. En el dominio terrestre las fuerzas ucranianas demostraron una coordinación superior a nivel de unidades pequeñas, explotando su conocimiento del terreno y la inteligencia recibida para llevar a cabo contraataques efectivos.

Rusia por su lado, empleó operaciones multidominio, pero con importantes deficiencias; por ejemplo, lanzó poderosos ciberataques en paralelo con la invasión contra las redes gubernamentales ucranianas y cortes de energía eléctrica, pero la rápida respuesta ucraniana y su previa preparación limitaron su impacto. Como señala Martínez (2024), la invasión rusa ha expuesto las carencias de una estrategia híbrida mal ejecutada, mientras que la defensa

ucraniana demostró la eficacia de saber combinar recursos de múltiples fuentes en todos los ámbitos y dominios.

Israel: lecciones recientes

Israel ha sido pionero en la aplicación de principios multidominio a pequeña escala. Ya es conocido que este se encuentra rodeado de amenazas irregulares, por lo que es lógico pensar la necesidad imperante de adaptar sus operaciones a la realidad particular que enfrentan. En la guerra del Líbano de 2006 las milicias de Hezbolá sorprendieron a las fuerzas israelíes al operar en dominios inesperados: consiguieron alcanzar con un misil antibuque a una corbeta de la marina israelí (INS Hanit) durante los combates causándole daños severos. Israel admitió que subestimó la amenaza en el dominio marítimo por parte de un actor no estatal, lo que a todas luces reveló una brecha en su conciencia situacional multidominio (Harel & Issacharoff, 2008). Producto de esto Israel posteriormente reforzó su inteligencia y la integración de esta para vigilar todos los ámbitos, incluso los que anteriormente eran considerados de bajo riesgo.

En conflictos recientes como las operaciones contra Hamás en Gaza, las Fuerzas de Defensa de Israel (FDI) han combinado operaciones cinéticas de precisión (bombardeos aéreos guiados) con acciones cibernéticas y campañas informativas. Por ejemplo, durante la operación Guardián de los Muros en mayo de 2021, Israel afirmó haber frustrado intentos de hacking de Hamás contra su sistema de defensa aérea Domo de Hierro (Iron Dome), y como respuesta fue ejecutado un ataque aéreo para neutralizar los hackers adversarios, combinando así los dominios cibernéticos y aéreos. Israel utiliza una amplia y sofisticada red inteligencia humana, drones de vigilancia y análisis de señales para detectar a los lanzadores de cohetes enemigos que se encuentran ocultos entre la población civil, integrando así, el dominio informativo con el militar.

Las lecciones israelíes hacen énfasis en la relevancia de que no se debe dejar ningún dominio sin la debida atención, incluso contra enemigos asimétricos, siendo la falta de control en uno solo una brecha que conlleve a consecuencias catastróficas. Esto evidencia también la utilidad de responder en todos los dominios a las amenazas para lograr los resultados más contundentes posibles y reducir la libertad de acción del adversario.

Fuerzas Armadas de República Dominicana: retos frente a las MDO

Para el caso de la República Dominicana, país que en la actualidad no enfrenta de manera directa amenazas militares convencionales, se hace lógico preguntarse cómo se podría asumir y aplicar el concepto de MDO atendiendo a esa realidad y contexto. Primero, es de rigor mencionar que de acuerdo con la Constitución de la República Dominicana las Fuerzas Armadas dominicanas se componen por tres ramas, fuerzas y/o servicios (Ejército, Armada y Fuerza Aérea) teniendo a su cargo la defensa de la Nación, su independencia y soberanía. (Constitución de la República Dominicana, 2015). El propio texto legal además les indica participar y/o apoyar en lo referido a la seguridad interna y el apoyo a situaciones de emergencia nacional.

Sus misiones en las últimas décadas se orientan en la lucha contra el crimen organizado, el narcotráfico y la respuesta a desastres naturales y antropogénicos. Si bien es cierto que estas tareas difieren de lo que doctrinalmente se conoce como guerra convencional entre naciones,

no menos cierto es el hecho de que para llevarse a cabo requieren una coordinación e integración en múltiples dominios. Por ejemplo, la seguridad de la frontera y espacio terrestre (tierra), la vigilancia de las costas y las operaciones navales contra el contrabando (mar), patrullaje y transporte aéreo (aire), la inteligencia y la seguridad de las comunicaciones (ciberespacio) y las campañas de información pública y cooperación civil y militar (informativo).

Las Fuerzas Armadas dominicanas se han enfocado en fortalecer una estructura de mando y control conjunto, y por esto vemos como en 2020 fue inaugurado el Centro de Comando, Control, Comunicaciones, Ciberseguridad e Inteligencia (C5I) como instalación que tiene el fin de lograr la integración de los flujos de información y mejorar la toma de decisiones de las tres ramas militares y múltiples agencias gubernamentales en tiempo real.

Con esta implementación se ha conseguido gestionar de manera óptima la seguridad fronteriza y el apoyo a la Policía Nacional en lo referido a la seguridad ciudadana. Esto refleja la priorización que se le ha dado al dominio ciberespacial e informativo, y desde el Ministerio de Defensa se ha reiterado que "el ciberespacio es el quinto dominio de las operaciones militares", indicando la prioridad que tiene el proteger la información y las redes ante cualquier amenaza digital (Díaz Morfa, 2023).

En ese tenor el Ministerio de Defensa (2024), a través de la Universidad Nacional para la Defensa (UNADE) han iniciado programas de capacitación en diversos niveles sobre ciberdefensa para el personal militar y civil, incluyéndolo además como parte de los distintos programas de grado y posgrado que allí se imparten, reconociendo, evidentemente, que la Seguridad Nacional comprende también el ámbito digital. Asimismo, la cooperación internacional ha jugado un papel importante en el entrenamiento y donación de equipos que fortalezcan las FF. AA.

República Dominicana, en cuanto a los medios materiales, enfrenta el reto tecnológico de adoptar las capacidades propias de las operaciones multidominio con recursos un tanto limitados. Comparado con países mayores nuestras Fuerzas Armadas disponen con un modesto equipamiento, por ejemplo, pocos aviones de transporte y helicópteros, así como una cantidad discreta de drones, lanchas para patrullas y vigilancia costera y sistemas de radar básicos para el control aéreo. La integración de nuevas tecnologías[12] requiere de inversiones significativas y un personal altamente capacitado, no debiendo obviar el reto que conlleva además la parte doctrinal y organizacional para dicha adecuación.

No obstante, es innegable que se han dado pasos firmes y positivos encaminados a avanzar, incorporando tecnologías para el monitoreo fronterizo y modernización de las redes de radio comunicación. Pudiendo decir, en síntesis, que República Dominicana se ha ido adaptando de manera gradual a los principios de la guerra multidominio acorde a sus necesidades y capacidades.

Operaciones Multidominio: proyección.

Proyectando las MDO, evidentemente, van a seguir evolucionando a la par con los avances tecnológicos y los cambios en la manera de hacer la guerra. Para Pulido (2022), algunas

12 Drones de vigilancia, sistemas de mando y control interconectados o herramientas de ciberseguridad de última generación.

de las tendencias que se vislumbran son las siguientes:

- Sistemas autónomos y automatización, en el sentido de que la próxima generación de fuerzas va a incluir un número considerable de plataformas no tripuladas en todos los ámbitos, como enjambres de drones aéreos y terrestres, submarinos autónomos, robots de combate, etc.
- Integración total de la inteligencia artificial, no solamente en lo relativo al manejo de datos, sino en que podrá asumir funciones relevantes en la conducción de las operaciones, capaces de proponer cursos de acción en tiempo real con la simulación de escenarios para procurar adelantarse al enemigo.
- Dominio informacional y cognitivo, referente a la batalla por influir en la voluntad, percepción y toma de decisiones del contrario, con una integración mayor de operaciones psicológicas en redes sociales y campañas agresivas de desinformación.
- Militarización del espacio ultraterrestre, por la dependencia en constante crecimiento de los satélites, la navegación y la observación por medio de este tipo de tecnología, con una proliferación de satélites militares y surgimiento de armas avanzadas antisatélite.
- Operaciones hipersónicas y multidominio en tiempo real, promovido por la aparición de misiles hipersónicos[13] y plataformas de ataque de muy largo alcance, difuminando la distinción entre el frente y la retaguardia.

Las guerras del futuro tienen mucha probabilidad de que continúen por el camino de la integración multidominio, sumándose los dominios cognitivos, espacial profundo y electromagnético, añadiéndose más tecnología que va a revolucionar constantemente la forma de combatir, y que las fronteras que separan lo humano y la máquina, lo civil y lo militar, será cada vez más difusa.

Conclusiones

Hemos podido constatar cómo han evolucionado las operaciones conjuntas hacia la integración multidominio, convirtiéndose este hecho en una realidad palpable, tanto en la doctrina como en la práctica militar contemporánea. A lo largo de este escrito hemos mostrado que el concepto de guerra y operaciones multidominio ha surgido para dar respuesta a un entorno estratégico en donde ningún dominio puede operar de forma aislada y conseguir una superioridad militar frente a su enemigo, y que, por el contrario, dicha superioridad se construye a partir de la combinación de las fuerzas terrestres, navales, aéreas, espaciales, cibernéticas y cognitivas o de información de manera integral y sincronizada.

A lo largo de la historia las fuerzas armadas han transitado por medio de modelos de cooperación conjuntas relativamente simples, o sea, el apoyo aéreo al Ejército, etc., hacia modelos altamente integrados y más complejos que permiten a un comandante accionar todas las palancas que tiene a su disposición en varios dominios a la vez. Presentando un análisis doctrinal se puso en evidencia cómo conceptos anteriores y experiencias previas allanaron el camino al punto que nos encontramos hoy, representando las operaciones multidominio un salto cualitativo importante con la integración de dominios emergentes y enfoque flexibles

13 Con capacidad para maniobrar hasta cinco veces la velocidad del sonido.

DOI: https://doi.org/10.59794/rscd.2025.v11i11.123

ante las amenazas complejas que se han ido presentando.

La necesidad de mandos conjuntos más efectivos y con capacidad de respuesta más rápida son de las implicaciones estratégicas que se requieren, aunado a nuevos modos de disuasión y acciones en la zona gris previo a llegar a un conflicto abiertamente. En lo referido a la tecnología, queda claro que las operaciones multidominio tienen una dependencia considerablemente importante de estos sistemas avanzados de información y manejo de datos, redes de mando seguras, una rápida adopción de innovaciones (ciberdefensa, drones, IA) y de armamento de precisión.

A su nivel, la República Dominicana ha reconocido esta necesidad y ha actuado en consecuencia, dando los pasos que fortalezcan sus operaciones conjuntas y tendentes a ir reforzando su estructura para operar en múltiples dominios de manera simultánea, desarrollando la ciberdefensa, mejorando la coordinación interinstitucional y asegurando una respuesta eficaz a los retos y desafíos en su entorno. Estos cambios exigirán Fuerzas Armadas flexibles y tecnológicamente avanzadas, pero también marcos normativos éticos y doctrinales actualizados.

Finalmente, se ha de reconocer que la integración multidominio no es una "moda" y como tal pasajera, sino una evolución lógica de la forma de hacer la guerra en el siglo XXI. Las fuerzas militares que la acojan de manera integral estarán en una posición ventajosa para disuadir, y de ser necesario, prevalecer en los conflictos que han de venir.

Referencias

Borne, K. (2019). Targeting in Multi-Domain Operations. *Military Review* (ed. en español). https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2019/

Brading, T. (2021). First Multi-Domain Task Force plans to be centerpiece of army modernization. U.S. *Army News Service*. https://www.army.mil/article/242849/first_multi_domain_task_force_plans_to_be_centerpiece_of_army_modernization

Comando de Entrenamiento y Doctrina del Ejército de los Estados Unidos (TRADOC). (2018). El Ejército de los Estados Unidos en Operaciones de Múltiples Dominios 2028. *Panfleto 525-3-1 del TRADOC.*

Constitución de la República Dominicana. [Const.]. (2015). *Gaceta oficial. Núm. 10805.* Santo Domingo, República Dominicana. 10 de julio 2015. https://presidencia.gob.do/sites/default/files/statics/transparencia/baselegal/Constitucion-de-la-Republica-Dominicana-2015-actualizada.pdf

Díaz Morfa, C. (2023, 21 de octubre). Alto mando de Fuerzas Armadas se reúne en C5i para evaluar estrategia de ciberseguridad. *Listín Diario*. https://listindiario.com/la-republica/ gobierno/20231021/alto-mando-fuerzas-armadas-reune-c5i-evaluar-estrategia-ciberseguridad_778300.html

Harel, A., & Issacharoff, A. (2008). *How the navy missed its boat. Haaretz*. https://www.haaretz.com/1.4980917

Hertlein, R. M. (2023, 23 de febrero). *Commentary: Army logistics survivability against multidomain threats. Army.mil.* https://www.army.mil/article/264190/commentary_ army_logistics_survivability_against_multidomain_threats

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

King, S., & Boykin, D. B. IV. (2019, 20 de febrero). *Distinctly different doctrine: why multi-domain operations isn't airland battle 2.0. Association of the United States Army.* https://www.ausa.org/articles/distinctly-different-doctrine-why-multi-domain-operations-isnt-airland-battle-20

Manual de campo, FM 100-5: *Operaciones.* (1982). Departamento del Ejército de EE. UU. U.S. Government Printing Office.

Ministerio de Defensa. (2024). *Fuerzas Armadas capacitan civiles y militares en temas de ciberseguridad y ciberdefensa.* https://www.youtube.com/watch?v=-Dw7TzD4W8I

Morris, L., Mazarr, M., Hornung, J., Pezard, S., Binnendijk, A., & Kepe, M. (2019). *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War.* RAND Corporation. https://www.rand.org/pubs/research_reports/RR2942.html

Organización del Tratado del Atlántico Norte (OTAN). (2023, 5 de octubre). *Multi-Domain Operations in NATO – Explained.* Mando Aliado de Transformación (NATO ACT). https://www.act.nato.int/article/mdo-in-nato-explained/

Pulido, G. (2022, 28 de agosto). La guerra de Ucrania y la guerra mosaico. *Revista Ejércitos.* https://www.revistaejercitos.com/artículos/la-guerra-de-ucrania-y-la-guerra-mosaico/

Publicación *Conjunta. (2018).* Operaciones conjuntas (Manual JP 3-0). Departamento de Defensa de los Estados Unidos.

Tosi, S. J. (2023). Xi Jinping's PLA reforms and redefining "active defense." *Military Review, 103*(5), 46-57.

Normas para autor (es) sobre redacción de artículo científico a ser publicado en la revista científica: "Seguridad, Ciencia & Defensa"

LISTA PRELIMINAR PARA LA PREPARACIÓN DE ENVÍOS

Como parte del proceso de envíos, los autores/as están obligados a comprobar que su envío cumpla todos los elementos que se muestran a continuación.

- Se devolverán a los autores/as aquellos envíos que no cumplan estas directrices.
- Constatar que el envío no ha sido publicado previamente ni se ha sometido a consideración por ninguna otra revista (o se ha proporcionado una explicación al respecto en los comentarios al editor/a).
- El texto reúne las condiciones estilísticas y bibliográficas incluidas en pautas para el autor/a, en acerca de la revista.
- En el caso de enviar el texto al Comité de Evaluación por pares ocultos, se siguen las instrucciones incluidas a fin de asegurar una evaluación anónima.

DATOS ACERCA DE LA REVISTA

Objetivo

La revista **Seguridad, Ciencia & Defensa**, es el órgano de divulgación científica de la Universidad Nacional para la Defensa "General Juan Pablo Duarte y Díez" (UNADE), referente indiscutible en el ámbito de la investigación científica aplicada a la seguridad y defensa nacional de alto impacto y arbitrada por pares ciegos, se posiciona como una plataforma clave para compartir los hallazgos más recientes en áreas estratégicas como las Ciencias Militares, Navales y Aeronáuticas, así como en temas de Geopolítica, Derechos Humanos y Derecho Internacional Humanitario, Derecho Castrense y las Ingenierías. Su alcance radica en fortalecer el conocimiento con rigor científico y académico en diversas áreas de las ciencias, promoviendo la innovación y el desarrollo de soluciones efectivas para los desafíos actuales y futuros, a fin de garantizar el fortalecimiento de las capacidades militares y civiles de la defensa nacional, con apertura a la comunidad científica en general y, en particular, para cualquier profesional interesado en la investigación.

Descripción

La revista **Seguridad, Ciencia & Defensa** es una publicación anual de divulgación científica de la Universidad Nacional para la Defensa "General Juan Pablo Duarte y Díez" (UNADE). Está abierta igualmente a colaboraciones nacionales e internacionales. Se da prioridad a aquellos trabajos afines a las áreas académicas de la UNADE; a saber: ciencias militares, ciencias navales y ciencias aeronáuticas; además de la seguridad y defensa nacional, geopolítica y derechos humanos y derecho internacional humanitario, ciencias de la salud, derecho castrense y las ingenierías.

Características de la publicación

Seguridad, Ciencia & Defensa abarca los temas que se corresponde a los programas de naturaleza estrictamente militar y civil–militar, en lo concernientes a los programas de naturaleza estrictamente militar, es donde los estudiantes o cursantes son militares y son impartidos en el **Nivel de grado en las Academias Militares** (Ejército República Dominicana, Armada República Dominicana y Fuerza Aérea República Dominicana) y en el **Nivel de postgrado en el Comando y Estado Mayor** (Conjunto, Terrestre, Naval y Aéreo). En el caso de los programas de naturaleza cívico-militar, son aquellos donde participan personal de la clase civil y militar como estudiantes. Estos programas incluyen: a) Doctorado en Seguridad Nacional y Humana, b) Especialidad en Derechos Humanos y Derecho Internacional Humanitario, c) Especialidad en Geopolítica y d) Maestría en Defensa y Seguridad Nacional, Especialidades en las Ciencias de la Salud, Derecho Castrense y de las Ingenierías; así como, otros cursos de postgrado y de educación continua que tengan la misma naturaleza.

Esta herramienta divulgativa constituye una de las vías para propiciar la formación permanente de los docentes en el área de la investigación científica, convocándoles a participar con textos científicos, ensayos, entrevistas, testimonios y reseñas bibliográficas. La publicación, además, acoge artículos de autores invitados, tanto nacionales como internacionales.

En consideración a los aspectos antes citados, describiremos las normas a seguir por parte de los autores, elementos requeridos para ser publicados en la revista

y las cuales tienen que ver con información sobre los autores, con el artículo y con los procedimientos:

1. INFORMACIÓN SOBRE EL AUTOR O AUTORES

1. Nombre completo
2. Institución donde se desempeña laboralmente, con la dirección y teléfono.
3. Correo electrónico.
4. Un breve currículum de un máximo de 20 líneas.
5. Cada autor debe anexar una foto de frente, a color, en fondo blanco, en formato jpg. con un tamaño no menor de 100.0 píxeles.
6. Código ORCID (REQUISITO OBLIGATORIO REQUERIDO).

2. LOS ARTÍCULOS

A. La primera página del artículo debe contener:

1. **Título en español**: Conciso, e ilustrativo que resuma el espíritu de la investigación, en mayúscula sostenida, negrillas y centrada. No más de 15 palabras, sin acrónimos, símbolos, siglas y abreviaturas.
2. **Título en inglés**: Con las mismas características antes mencionadas
3. **Autor(es)**: Identificación con el nombre científico del (los) Investigador (es), incluyendo una breve descripción de su hoja de vida, recomendando a los investigadores escribir su nombre científico con un formato constante en sus publicaciones.
4. **Resumen**: **No debe exceder de 250 palabras**, escrito en un solo bloque y estar compuesto por el propósito de la investigación, la metodología utilizada y los principales hallazgos y conclusiones. No debe tener referencias, ni siglas.
5. **Palabras clave**: Se deben incluir de 5 a 7 palabras clave que tengan relación con la investigación y que ayuden a su clasificación e indización. Para ello se recomienda utilizar el Tesauro de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (Unesco), en la página web http://databases.unesco.org/thessp/.
6. **Abstract**: El contenido debe estar ajustado a lo indicado en el ítem anteriormente indicado (Resumen, pero en idioma inglés).
7. **Email**: Agregar el o los Email de los investigadores, este facilitará la comunicación con los investigadores, así como el **registro ORCID del investigador**.

B. Se estipula que los artículos no deben ser menos de 12 páginas y no exceder de 15 páginas. Sin embargo, queda a disposición del Comité de publicaciones la posibilidad de variar dichos límites.

C. .Se dará preferencia a los trabajos de investigación que no hayan sido publicados con anterioridad. Los artículos serán recibidos en formato de Microsoft Word, en páginas tamaño 8 ½ X 11, a 1 espacio y en tipografía debe ser tipo **Time New Roman 12 puntos**, en papel tamaño carta y escrito en Word (no debe estar bloqueado o protegido); márgenes: izquierdo 2,54 cm. derecho 2,54 cm. Superior e inferior 2,54 cm. Todas las páginas deben estar numeradas al pie en el lado derecho de la hoja, así como cada figura, imagen, gráfica o tabla.

D. Los Artículos deben ser originales y resultados de alguna investigación o estudio.

E. No se aceptan artículos que no cumplan con el contenido anteriormente indicado.

F. Todos los trabajos deben estar en español.

G. Identificación del título del trabajo y se aceptan subtítulos aclaratorios.

H. A pie de página solo deberán ser colocadas las notas aclaratorias.

I. Los párrafos de cada sección no deberán ser menor de 5 y mayor de 10 líneas e irán separados por un interlineado de 1 espacio, dejando una sangría de un (0,5) centímetro al comienzo de cada párrafo.

J. La composición del artículo deberá cubrir los siguientes aspectos: Resumen en español e inglés, las palabras clave en español e inglés, introducción, desarrollo del artículo, conclusiones y referencias:

   1) **Introducción**: Expresando el contexto o antecedentes de la investigación, naturaleza del problema, propósito y alcance de la investigación, importancia y enunciando los objetivos de la investigación.
   2) **Desarrollo**: Exposición clara y coherente de los hallazgos
   3) **Figuras Tablas y Gráficas**: Deben ser identificadas con números arábigos, con sus respectivas leyendas, título que explique su contenido, las fotografías deben ser originales y de calidad, así mismo debe citarse explícitamente en el texto del artículo e insertarse a continuación del fin de párrafo de donde fue citado, su numeración es única y secuencial, sin importar la sección donde se encuentre (separando la secuencia entre tablas y gráficas). No deben repetirse en el texto los datos expuestos en tablas o gráficos, fuente de

origen, en las notas de pie de las tablas y gráficas explique las abreviaturas y observaciones relevantes.

Las tablas y gráficas editables dentro de word, y las imágenes en formato JPG en el archivo y anexadas en una carpeta.

4) **Citas en el texto**: Deben ser relevantes para el artículo científico evitando la excesiva redundancia en las citas, las citas con menos de cuarenta palabras se incluirán como parte del párrafo, entre comillas y dentro del contexto-Las citas de longitud mayor se colocará en un párrafo separado, cumpliendo una sangría de 5 espacios en ambos márgenes, a espacio sencillo. Utilizando para ello el sistema apellido, fecha, pagina (Suarez H., 2016, pp. 50-52), o Suarez H. (2016) (pp.50-52).
5) **Niveles en los encabezados**: las secciones y subsecciones del artículo científico deben estar ajustados a las siguientes características:
   5.1. Nivel 1: Encabezado centrado en negrillas con mayúsculas y minúsculas, letra Time New Roman, Tamaño del texto 14 puntos
   5.2. Nivel 2: Encabezado alineado a la izquierda en negrillas con mayúsculas y minúsculas, letra Time New Roman, Tamaño del texto 12 puntos.
6) **Conclusiones**: Síntesis de la comprobación de los objetivos de investigación con sus argumentos y discusiones, se permite la incorporación de recomendaciones, propuestas y futura líneas de investigación
7) **Referencias**: Todas y solamente las citas realizadas dentro del articulo deberán ser incluidas en las referencias bibliográficas y viceversa, las cuales deben apoyar a los planteamientos realizados en el artículo científico, ordenadas alfabéticamente, utilizando la sangría francesa, para ello deberá seguir las especificaciones al Manual de Estilo de Publicaciones de la American Psychological Association (APA) última versión en español. Su veracidad es de exclusiva responsabilidad de sus autores.
8) **Fuente**: American Psychological Association. (2021). Datos del Manual de publicaciones de la American Psychological Association, última versión en español.

K. Las **Referencias** se colocarán al final del documento, empleando el **formato APA (ÚLTIMA VERSIÓN DEL ESPAÑOL)** y deben ser colocadas en orden alfabético.

Para el uso de citas se indican a continuación muestras de algunos casos:

i. Cuando la cita directa o textual es corta (menos de 40 palabras), se coloca integrada al texto del informe, entre comillas, siguiendo la redacción del párrafo donde se hace la cita. Por ejemplo:
ii. En el proceso de la investigación, "no se debe empezar a escribir hasta que uno no haya completado el estudio." (Acosta Hoyos, 1979, p. 107).
iii. Cuando la cita directa o textual es de 40 o más palabras, se cita en un bloque, sin comillas, a espacios sencillos y con un tamaño de letra 12 en cursiva, con una sangría de 5 espacios ó 0,5 cm en el margen izquierdo del texto del informe. Por ejemplo:
   a) Aunque sólo las investigaciones o inventos realizados puedan alcanzar los derechos de autor que concede la ley, entre investigadores siempre se respeta la prioridad que alguien ha tenido para elegir un tema; ya que existen infinidad de problemas para investigar y de nada vale una competencia que no lleve a un mejor perfeccionamiento. (Acosta Hoyos, 1979, pp.16-17)
      i. Apellido, A. A., Apellido, B. B. & Apellido, C. C. (Año de publicación). *Título del documento: subtítulo* (Edición). Editora.
      ii. Artículo de publicaciones periódicas: Autor, A., Autor, B. & Autor, C. (Año de publicación, mes). Título del artículo. *Título de la publicación periódica*, Vol., (núm.), página inicial - final.
      iii. Revista en formato electrónico: Autor, A., Autor, B. & Autor, C. (Año de publicación día / mes). Título del artículo. *Título de la publicación periódica,* Vol., (núm.), página inicial - final. Recuperado día mes, año, de [URL].
      iv. Referencias jurídicas: Constitución, leyes y decretos.
      Nombre oficial de la Constitución [abreviación]. Artículo específico citado. Fecha de promulgación (País).
      - Constitución de la República Dominicana [Const]. (2015). Art. 6. *Gaceta Oficial* de 10 de julio de

2015. (República Dominicana). Núm. 10805.
Número y año de la ley. Asunto. Fecha de promulgación. Número en la Gaceta Oficial.

- Ley No. 139-13. Orgánica de las Fuerzas Armadas de República Dominicana. *Gaceta oficial.* 19 de septiembre de 2013. (República Dominicana). Núm. 10561.
Número y año del decreto. Asunto. Fecha de promulgación del decreto. Número en la Gaceta Oficial.
- Decreto núm. 2811 de 1974. Por medio del cual se expide el Código de Recursos Naturales Renovables y de Protección al Medio Ambiente. *Gaceta Oficial.* 27 de enero de 1974. República Dominicana. Núm. 34243.

3. LOS PROCEDIMIENTOS

A. El envío de los artículos en versión digital (formato Word) dirigidos a la Vicerrectoría de Investigaciones e Innovación, será a través de las direcciones electrónicas: jfabriziot@unade.edu.do y/o revistacientifica@unade.edu.do.

B. El Consejo Editorial someterá los trabajos recibidos a un sistema de arbitraje a través de tres (03) miembros del Comité Científico (revisión por pares ciegos), quienes examinarán cada artículo según criterios de pertinencia, coherencia, aporte, calidad y estilo para decidir sobre la conveniencia de su publicación. En el proceso de evaluación se mantiene el anonimato de los evaluadores puesto que su selección es secreta y se mantiene el anonimato del autor enviando el material ciego, a saber, borrando toda información que pueda identificarlo.

C. El proceso de evaluación comienza con la selección de los expertos sobre el tema en cuestión, luego se les envía el artículo con un formato de dictamen corto y preciso, pero a la vez flexible.

D. El Comité Editorial remite a los autores de forma anónima las opiniones y recomendaciones sobre el artículo, realizadas por los pares ciegos y el resultado de la revisión puede ser: ***a. Se acepta el artículo para publicación. b. Aceptar el artículo con las mejoras de los autores. c. Aceptar el artículo con algunas sugerencias. d. Se podría aceptar el artículo, pero con una corrección amplia y e. No aceptar***

E. Los autores dan permiso para que sus trabajos sean publicados en la versión electrónica de la revista que aparece en la página de la Web de la UNADE.

F. El Comité Editorial de publicaciones se reserva el derecho de no publicar un artículo que no haya sido entregado a tiempo y valorar las posibilidades de publicarlo en un próximo número.

G. Los artículos que no se ajusten a lo establecido serán devueltos, hasta tanto cumplan con los requisitos señalados.

H. El envío de una colaboración para su publicación implica por parte del autor, la autorización a la UNADE para su reproducción en otras ocasiones, por cualquier medio, en cualquier soporte y en el momento que lo considere conveniente, siempre que el autor sea informado y esté de acuerdo con los fines de la reproducción y se haga expresa la referencia a la autoría del documento.

I. Copyright. Es condición para la publicación que el autor o autores ceda(n) a la Revista, en exclusiva, los derechos de reproducción. Si se producen peticiones de terceros para reproducir o traducir artículos o partes de estos, la decisión corresponderá al Consejo de Redacción.

J. Advertencia. Cualquier incumplimiento de las presentes Normas constituirá motivo para el rechazo del original remitido.

K. Es responsabilidad de los autores atenerse a las normas editoriales, revisando estructura, redacción, y ortografía. Asumirán, por medio de la carta de originalidad y cesión de derechos, subida con el resto de los archivos exigidos al momento de realizar el envío, el compromiso de evaluar manuscritos durante el tiempo que dure el proceso editorial de su artículo.

L. Los autores son responsables del contenido del manuscrito, de la veracidad y exactitud de los datos, cumpliendo con presentar trabajos originales e inéditos, que no estén siendo sometidos simultáneamente a evaluación en otra revista o medio, así como de contar con todos los derechos de publicación.

Arbitraje

Todos los trabajos originales enviados para publicación son sometidos a arbitraje o evaluación por pares expertos, quienes realizaran una evaluación sobre la calidad y pertinencia técnica y científica del trabajo propuesto. La Universidad Nacional para la Defensa "General Juan Pablo Duarte y Díez" (UNADE), a través de la Vicerrectoría de Investigación e Innovación, entrega a los evaluadores una serie de aspectos para uniformar las revisiones. Los elementos de revisión y el formulario de evaluación en el que se indican los aspectos a considerar en la evaluación les serán entregados a los expertos encargados de valorar los trabajos.

Todos los evaluadores son externos, tanto nacionales como internacionales. Por ello, la Revista "Seguridad, Ciencia & Defensa", tiene una base de datos de potenciales evaluadores. En el proceso de análisis y valoración, se les solicita a los evaluadores que traten el artículo con la misma rigurosidad científica con que se tratan en otras revistas internacionales arbitradas. El nombre de los evaluadores no le es revelado a los autores de los artículos; más, sin embargo, los evaluadores tampoco conocen la identidad de los autores del artículo sometido a revisión.

Excelente Evaluación del Año.

La Revista "Seguridad, Ciencia & Defensa", otorgará un premio anual denominado: "Excelente Evaluación del Año", reconocimiento otorgado al evaluador que realice la mejor evaluación de los trabajos que les han sido confiados para evaluar.

La elección del mejor evaluador será realizada por el Rector, la Vicerrectoría de Investigación e Innovación y el Editor de la Revista, quienes son las únicas personas que, en forma confidencial, conocen de las opiniones de los evaluadores sobre un determinado artículo. Se considerará las evaluaciones recibidas en la Universidad Nacional para la Defensa "General Juan Pablo Duarte y Díez" (UNADE), durante el año calendario por el cual se otorga el premio.

El ganador o ganadora se hace acreedor a un Certificado de reconocimiento otorgado por la Universidad Nacional para la Defensa "General Juan Pablo Duarte y Díez" (UNADE).

COLOFÓN

La presente edición de la Revista Científica
"Seguridad, Ciencia & Defensa",
Volumen XI, N° 11, año 2025
de la Universidad Nacional para la Defensa
"General Juan Pablo Duarte y Díez" (UNADE),
fue impresa en el mes de diciembre de 2025
.
La edición consta de 500 ejemplares.
Santo Domingo, República Dominicana.

MINISTERIO DE DEFENSA

UNIVERSIDAD NACIONAL PARA LA DEFENSA
"GENERAL JUAN PABLO DUARTE Y DÍEZ"
(UNADE)

Dirección postal y electrónica de la Revista Científica Seguridad, Ciencia & Defensa: Universidad Nacional para la Defensa
"General Juan Pablo Duarte y Díez" (UNADE)
Avenida 27 de Febrero, Esquina avenida Luperón (Plaza de la Bandera)
Santo Domingo, Distrito Nacional, República Dominicana
Apartado postal: 11112. Tel: 809-531-2971, Ext. 3879
https://unade.edu.do/
Email: revistacientifica@unade.edu.do | jfabriziot@unade.edu.do

Versión electrónica de la Revista Científica "Seguridad, Ciencia & Defensa": https://revista.unade.edu.do/index.php/rscd

Indexaciones en las siguientes bases de datos:

Latindex 2.0
Scielo Dominicana
Google Scholar
ErihPlus
Base Search
Copernicus Index?
MIAR
DOAJ
Eurasian Indexing
LatinRev
Rootindexing
Directory Research Indexing
ISSN Portal
AURA Amelica
Clasificación CIRC